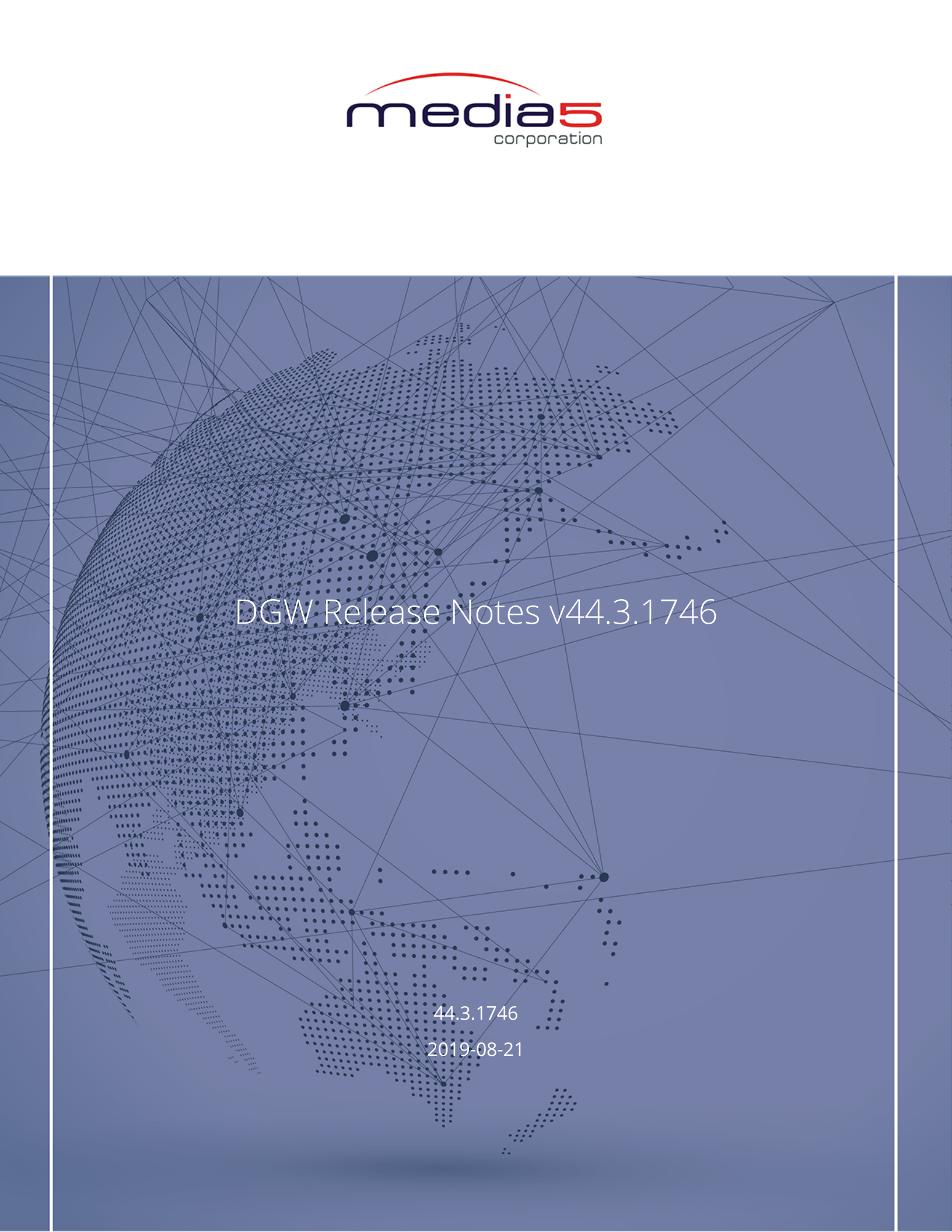


The background of the page is a dark blue field filled with a complex network of thin, light grey lines connecting numerous small black dots. These dots are arranged in a way that suggests a global map, with higher concentrations of dots and lines in the North Atlantic and Europe. The overall effect is a sense of interconnectedness and global reach.

DGW Release Notes v44.3.1746

44.3.1746
2019-08-21

Table of Contents

Firmware Pack	3
New Functionalities	4
Modified Features, Functionalities and Interface Modifications	5
Issues Fixed	6
Copyright Notice	10

Firmware Pack

The firmware pack is a binary file that contains the modules and the features to install on your Mediatrix unit when a new release is available.

New Functionalities

Incident #	CR #	Synopsis	Applies To
Description			
---	DGW-9485	Collect call information must be sent to outgoing R2 and ISDN calls based on a proprietary "P-Asserted-Service-Info: service-code=Collect Call" SIP INVITE header if the InteropCollectCallProprietaryHeader parameter is set to relay.	SIP, ISDN and R2
The proprietary P-Asserted-Service-Info is now parsed in SIP to extract the service-code number. In the case the service-code indicates an incoming collect call, the information is relayed to the R2 and ISDN interfaces. • if the InteropCollectCallProprietaryHeader parameter is set to relay, the ISDN interface will add a new IE (Information Element) reverse charging to indicate to the called user that charges apply. In R2, the collect call tone is sent to the called user to indicate the calling party call type. • If the InteropCollectCallProprietaryHeader parameter is set to decline or ignore, the INVITE is respectively declined with a 603 or the call collect is simply ignored and the INVITE is treated as a normal call.			

Modified Features, Functionalities and Interface Modifications

Incident #	CR #	Synopsis	Applies To
Description			
IN-14243	DGW-11224	TCP and TLS communications are vulnerable to a Denial of Service (DoS) known as the TCP SACK Panic (CVE-2019-11477 and CVE-2019-11478).	all
TCP SACK processing is now permanently disabled.			
	DGW-10955	DGW Web pages cannot be accessed.	all
When the NTC feature is enabled or disabled on an interface, DGW automatically optimises the network performance for that interface.			
IN-14085	DGW-10589	When the priority of the SipEp.AllCommonLocal parameter is set to FirstCommonPeer and the first media in the offer is an Fmtp and not audio, the unit rejects the call with a 415 Unsupported media error message.	SipEp
The order of media in an offer is no longer important, the unit can at all times select the first common media from the offer.			

Issues Fixed

Incident #	CR #	Synopsis	Applies To
Description			
IN-14253	DGW-11253	The value of 189 in the SipEp.InteropTcpConnectTimeout parameter included in the Gateway_Configuration.cfg file is out of range (1..127).	all
The value of the SipEp.InteropTcpConnectTimeout parameter was changed to 127 in the Gateway_Configuration.cfg file.			
IN-14243	DGW-11224	TCP and TLS communications are vulnerable to a Denial of Service (DoS) known as the TCP SACK Panic (CVE-2019-11477 and CVE-2019-11478).	all
An important security flaw was found in the handling of TCP Selective Acknowledgement (SACK) packets. A remote attacker could exploit this to cause an unexpected restart of the unit. The vulnerability has been resolved by permanently disabling TCP SACK. This will not affect the quality of VoIP calls.			
	DGW-11216	The ISDN, R2, and Eam DGW Web pages are not available with the custom profile.	PRI
The ISDN, R2, and Eam DGW Web pages are now available with the custom profile.			
IN-13833	DGW-11201	Unable to import a 100 GB VM image file in the Sentinel 400.	VM
It is now possible to import a 100 GB VM image file in the Sentinel 400.			
	DGW-11052	Unable to upload configuration scripts if the login password is saved in the Web browser.	all
When a user logs to the Mediatrix via the DGW Web page and chooses to have the Web browser to save and remember their password, this may cause Password or Privacy Key fields to be mistakenly filled by the Web browser, using the login credentials. This may cause the upload of configuration scripts through the Web browser to fail because DGW tries to decrypt the file with the Privacy Key automatically filled with the login password. This may also cause the download of configuration scripts from the Web browser to be automatically encrypted with the login password, unknowingly to the user.			
IN-13430	DGW-11047	When a SIP gateway is set to the Endpoint mode, force locking one port causes all ports to become idled-unusable.	SipEp

Incident #	CR #	Synopsis	Applies To
Description			
As for the Trunk mode behavior, when a SIP gateway is set to the Endpoint mode, force locking a port now only affects the port.			
	DGW-11043	Call ends 32 seconds after the TLS and TCP assert.	SipProxy
Missing transport parameter in Record-Route headers issued by the SipProxy causes SIP phones to use incorrect transport. Also, the Record-Route and Route headers issued by the SipProxy may contain the wrong port in TLS. The SipProxy does not add the UDP/TCP transport parameter in the record-route headers as it is done in TLS. The absence of a transport parameter means that the transport is UDP. This caused some devices to use UDP instead of TCP when replying to the SipProxy. The SipProxy now adds the transport parameter in the Record-Route headers when only one transport is enabled. The transport parameter is not added if UDP and TCP transports are enabled. The SipProxy only applied the port translation between the listening port and the persistent port on the first Record-Route inserted by the SipProxy and the translation is not applied on Route header. This means that if a call is done between two endpoints behind the SipProxy, the same call may be forwarded twice by the SipProxy and two Record-route headers are added by the SipProxy and only the first header is correctly translated. This also means that in the same scenario, a Route header generated from the Record-Route header is not translated. The SipProxy now translate the port of all Record-Route header inserted by the SipProxy and the Route header generated from the Record-route header inserted by the SipProxy.			
	DGW-10955	DGW Web pages cannot be accessed.	all
The DGW Web pages could not be accessed because of a low QoS bandwidth (Egress Speed) limitation on the WAN. When the NTC feature is enabled or disabled on an interface, DGW now automatically optimises the network performance for that interface.			
IN-14131	DGW-10901	The Web service should not return the "Server" HTTP headers.	Web
The Web service no longer returns the "Server" HTTP headers to prevent false positives in security scanning.			
IN-14157	DGW-10830	The VM must be restarted if the VNC is disabled.	VM
Disabling the VNC no longer requires to restart the VM.			
IN-14116	DGW-10662	When receiving an ISDN STATUS message the call is not always cancelled even if the Isdn.SignalingChannel.StrictHandlingErrorConditions parameter is set to "Enable".	ISDN

Incident #	CR #	Synopsis	Applies To
Description			
When receiving an ISDN STATUS message, the call is now always cancelled when the Isdn.SignalingChannel.StrictHandlingErrorConditions parameter is set to "Enable".			
IN-14085	DGW-10589	When the priority of the SipEp.AllCommonLocal parameter is set to FirstCommonPeer and the first media in the offer is an Fmtp and not audio, the unit rejects the call with a 415 Unsupported media error message.	SipEp
The unit can now always manage the call when the priority of the SipEp.AllCommonLocal parameter is set to FirstCommonPeer and the first media in the offer is not audio.			
---	DGW-10122	Deprecated parameters must be removed or changed to the "Obsolete" status, and some "Obsolete" parameters must also be removed.	Crout, Hoc, Conf, SipEp, EpServ
Old "Deprecated" parameters were removed or changed to the "Obsolete" status and some "Obsolete" parameters were also removed. The following commands were removed: • CRout.DeleteAllRoutes • CRout.DeleteAllMappingTypes • CRout.DeleteAllMappingExpressions • CRout.DeleteAllHunts • CRout.DeleteAllSignallingProperties • CRout.DeleteAllSipHeadersTranslations • CRout.DeleteAllCallPropertiesTranslations The following parameters were removed: • EpServ.DefaultEmergencyCallOverride • MbAgw24.ResetButtonManagement • MbAgw24.Eth.PortsConfiguration • MbLdp.ResetButtonManagement • MbLdp.RingManagement • MbLdp.Eth.PortsConfiguration • MbSbc.ResetButtonManagement The following parameters were changed from Deprecated to Obsolete: • SipEp.InteropWaitConfirmedDialogForBlindTransfer			

Incident #	CR #	Synopsis	Applies To
Description			
• Conf.ScriptsTransferTimeOfDay • Hoc.SntpTimeZone • Hoc.SntpServerHostInfo • Hoc.StaticSntpServerHost			

Copyright Notice

Copyright © 2019 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.





4229, rue de la Garlock
Sherbrooke (Quebec)
J1L 2C8 Canada
media5corp.com