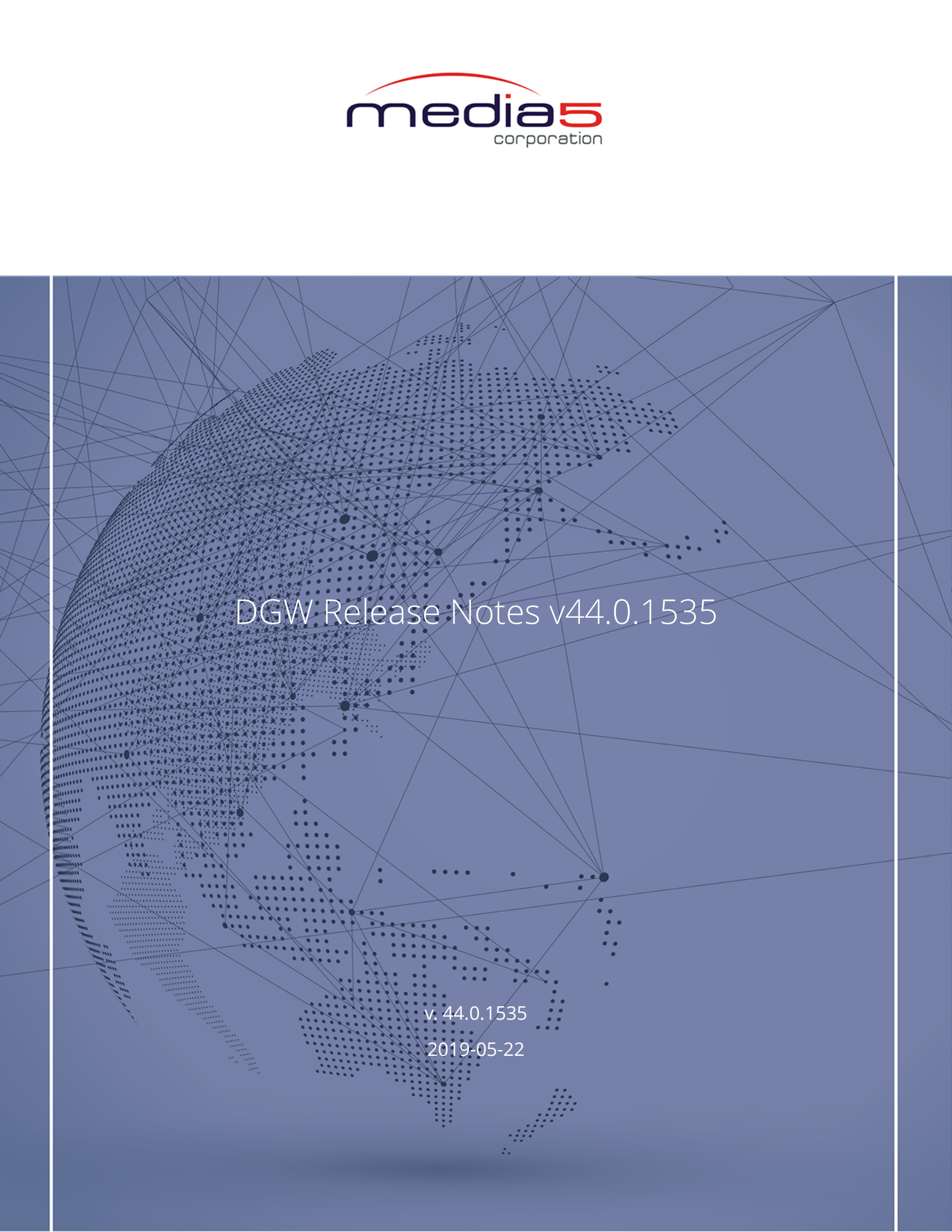


The background of the page is a dark blue field filled with a complex network of thin, light blue lines connecting numerous small black dots. These dots are arranged in a way that suggests a global map, with higher concentrations of dots and connections in the North Atlantic and Europe. The overall effect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

DGW Release Notes v44.0.1535

v. 44.0.1535

2019-05-22

Table of Contents

Firmware Pack	3
New Functionalities	4
Modified Features, Functionalities and Interface Modifications	5
Issues Fixed	7
Copyright Notice	10

Firmware Pack

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

When unzipping the firmware pack, the content is extracted according to a pre-defined tree architecture. This creates a directory that contains the files required for the Mediatrix unit to properly upgrade its firmware.

New Functionalities

Incident #	CR #	Synopsis	Applies To
Description			
IN-12607	DGW-10093	The IPV4 header TTL must be configurable.	all
The IPV4 header TTL was hardcoded to 64. The new Bni.IpGroup.IpTtlValue parameter was created to be able to the change the IPV4 header TTL in the range of 64..255. This new parameter is only available using the CLI, a MIB browser, or in a configuration script.			
---	DGW-9371	Allow the VNC to be disabled on the virtual machine.	VM
The VNC can be now be disabled on the virtual machine of the Vm service by setting the value of the Vm.Vm.VncDisplayId parameter to -1.			
---	DGW-6559	Support of new BRI telephony ports on existing Mediatrix platforms.	BRI, C7, G7, Sentinel 100, Sentinel 400
The BRI telephony port is now supported by the DGW application for the Mediatrix C7, Mediatrix G7, and Mediatrix Sentinel 100/400.			

Modified Features, Functionalities and Interface Modifications

Incident #	CR #	Synopsis	Applies To																																								
Description																																											
IN-13430	DGW-9954	The local crypto parameter key, timestamp, and CSeq number are regenerated on each session update.	SDES, SDP																																								
The Mipt.SessionUpdateCryptoMode parameter enables regenerating or keeping the local crypto values was added.																																											
---	DGW-9371	Allow the VNC to be disabled on the virtual machine.	VM																																								
The range of the accepted value for Vm.Vm.VncDisplayId parameter have changed from 0 - 99 to -1 - 99 and the type from unsigned integer to signed integer.																																											
IN-13562	DGW-9270	Allow multiple user login attempts without locking the account.	AAA																																								
The new Lock protection parameter was added to the DGW Web interface, in the Users/Management/Access Control table.																																											
<table><tr><th colspan="5">Users</th></tr><tr><th>User Name</th><th>Password</th><th>Access Rights</th><th>Lock Protection</th><th></th></tr><tr><td>NewUser</td><td>*****</td><td>User</td><td>Enable</td><td>-</td></tr><tr><td>admin</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td></tr><tr><td>observer</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td></tr><tr><td>public</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td></tr><tr><td>user</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td></tr><tr><td></td><td></td><td></td><td></td><td>+</td></tr></table>				Users					User Name	Password	Access Rights	Lock Protection		NewUser	*****	User	Enable	-	admin	*****	Admin	Enable	-	observer	*****	Admin	Enable	-	public	*****	Admin	Enable	-	user	*****	Admin	Enable	-					+
Users																																											
User Name	Password	Access Rights	Lock Protection																																								
NewUser	*****	User	Enable	-																																							
admin	*****	Admin	Enable	-																																							
observer	*****	Admin	Enable	-																																							
public	*****	Admin	Enable	-																																							
user	*****	Admin	Enable	-																																							
				+																																							
When the parameter is enable, the user's account may be temporary locked after repetitive login failures. When the parameter is not enabled, the user's account is not locked after repetitive login failures.																																											
IN-13548	DGW-9122	The diagnostic trace for the CConfScriptsModifiers::ApplyScriptModifiers function is reported as an error.	Conf																																								
The diagnostic trace for CConfScriptsModifiers::ApplyScriptModifiers function will be a Debug trace and not an error.																																											
---	DGW-6559	Support of new BRI telephony ports on existing Mediatrix platforms.	BRI, C7, G7, Sentinel 100, Sentinel 400																																								

Incident #	CR #	Synopsis	Applies To
Description			
The BRI telephony port is now supported by the DGW application for the Mediatrix C7, Mediatrix G7, and Mediatrix Sentinel 100/400.			

Issues Fixed

Incident #	CR #	Synopsis	Applies To
Description			
---	DGW-10048	The Local Firewall (LFW) service of DGW cannot rate limit Web page login failures.	Web
The maximum number of Web page login failures can now be restricted by the rate limit of the Local Firewall (LFW) service of DGW.			
---	DGW-9981	When T.38 is enabled in the Mipt service, the DSP ressource allocation for T.38 is missing.	T.38
When T.38 is enabled in the Mipt service, the DSP ressource allocation is now done correctly.			
IN-13430	DGW-9954	The local crypto parameter key, timestamp, and CSeq number are regenerated on each session update.	SDES, SDP
The local crypto parameter key is present in the SDP packet sent by the user to the peer. The value of the key is regenerated by default on each re-offer (hold-resume). The timestamp and CSeq number are present in the RTP packets. These values are re-randomized after each re-offer breaking the continuity of the numbering. The new Mipt.SessionUpdateCryptoMode parameter now enables regenerating or keeping the local crypto values			
---	DGW-9938	Some AOC information may be wrongly present in the 200 OK SIP response message.	Isdn, Aoc
When a remote peer returns some AOC information in the SIP BYE, the 200 OK message may return some AOC information although it should not. AoC information is no longer wrongly included in the 200 OK SIP response message.			
---	DGW-9928	Failback to primary server for Endpoint Gateways does not work correctly in TLS.	all
Failback to primary server for Endpoint Gateways are now properly managed and now work correctly in TLS.			
---	DGW-9586	The CWMP Inform message is sent even if the parameter list is empty.	CWMP
As described in the TR-069 standard, the CWMP Inform message must always contain all parameters with active notification. This behavior is now fixed. If one of these parameters cannot be read, the CWMP Inform message is not sent.			
---	DGW-9518	The Media Security Agreement headers can appear in multiple instances.	SipEp

Incident #	CR #	Synopsis	Applies To																																																
Description																																																			
The Media Security Agreement headers were appearing in multiple instances when the same packet was sent to more than one destination. Media Security Agreement headers are no longer appearing in multiple instances.																																																			
---	DGW-9511	Web pages are potentially vulnerable to clickjacking (User Interface redress attacks).	Web																																																
Protection to avoid clickjacking attacks were added in the DGW Web interface.																																																			
IN-13765	DGW-9356	Reading parameters via the Web page temporary locks the configuration for 30 seconds.	Web																																																
Reading parameters via the Web page no longer locks the configuration.																																																			
IN-13562	DGW-9270	Allow multiple user login attempts without locking the account.	AAA																																																
It is now possible to allow multiple user login attempts without locking the account. 3 new parameters were added:																																																			
Aaa.UsersTable.UsersLockProtectionEnable available in the DGW Web Interface, in the Users/Management/Access Control table.																																																			
<table><tr><th colspan="5">Users</th><th></th></tr><tr><th>User Name</th><th>Password</th><th>Access Rights</th><th>Lock Protection</th><th></th><th></th></tr><tr><td>NewUser</td><td>*****</td><td>User</td><td>Enable</td><td>-</td><td></td></tr><tr><td>admin</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td><td></td></tr><tr><td>observer</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td><td></td></tr><tr><td>public</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td><td></td></tr><tr><td>user</td><td>*****</td><td>Admin</td><td>Enable</td><td>-</td><td></td></tr><tr><td></td><td></td><td></td><td></td><td>+</td><td></td></tr></table>				Users						User Name	Password	Access Rights	Lock Protection			NewUser	*****	User	Enable	-		admin	*****	Admin	Enable	-		observer	*****	Admin	Enable	-		public	*****	Admin	Enable	-		user	*****	Admin	Enable	-						+	
Users																																																			
User Name	Password	Access Rights	Lock Protection																																																
NewUser	*****	User	Enable	-																																															
admin	*****	Admin	Enable	-																																															
observer	*****	Admin	Enable	-																																															
public	*****	Admin	Enable	-																																															
user	*****	Admin	Enable	-																																															
				+																																															
When the parameter is enable, the user's account may be temporary locked after repetitive login failures. When the parameter is not enabled, the user's account is not locked after repetitive login failures.																																																			
- LoginLockedMaxRetry (integer – default 5 attempts) (available only via CLI, SNMP, or script) - LoginLockedTimeoutS (integer – default 300 seconds)(available only via CLI, SNMP, or script)																																																			
IN-13548	DGW-9122	The diagnostic trace for the CConfScriptsModifiers::ApplyScriptModifiers function is reported as an error.	Conf																																																
The diagnostic trace for the CConfScriptsModifiers::ApplyScriptModifiers function will be a Debug trace and not an error.																																																			

Incident #	CR #	Synopsis	Applies To
Description			
---	DGW-8477	The partially converted image is displayed under the Management/Files DGW Web page when the VM conversion is interrupted.	VM
During VM conversion, the partially converted image will no longer be displayed in the DGW Web under Management/Files. Once the conversion is completed, the VM converted image will be displayed in the DGW Web page under Management/Files.			

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