



DGW Firmware

v49.2.2941

Release Notes

Release Notes

DGW Application 49.2.2941

- [Summary](#)
- [New Features](#)
- [Known Issues](#)

Summary

Incident Number	ID	Synopsis
	DGW-10063	The command Cert.MakeCertificateFactory was added to convert a host certificate to a factory host certificate.
	DGW-16146	SBC: improvements in the Limit CAPS ruleset action
	DGW-16228	SBC: The port is not present in notification 810
	DGW-16289	Sentinel CS: implemented support for network link state changes notifications.
IN-15627	DGW-16290	SIP Proxy: Monitoring state remains to unknown until a persistent connection is established when using TLS.
	DGW-16291	Sentinel 400/RS: added diagnostics for slot 1 card
IN-15391	DGW-16320	Add support of SIP authentication password encryption in SipEp service.

Incident Number	ID	Synopsis
IN-15631	DGW-16359	SBC: The symmetric RTP is activated by default if a call agent doesn't define RTP anchoring in Sbc service.
	DGW-16364	The maximum number of authentication rows in SipEp.Authentication table is now synchronized with the maximum number of registration allowed on the device.
	DGW-16365	New DCM notifications 60200 and 60210.
IN-15997	DGW-16376	Added support for HTTP redirects.
	DGW-16407	HA: New parameter StartupStatus
	DGW-16411	HA: New parameter Ha.VrrpInstances.Preemption

New Features

DGW-16411 - HA: New parameter **Ha.VrrpInstances.Preemption**

The High Availability service supports a new configuration parameter **Ha.VrrpInstances.Preemption**

By default, preemption is enabled (as was the default behavior in the previous version), meaning the primary will take control of the HA service as soon as possible.

However, in circumstances where there is high network intermittence or "server flapping", disabling preemption will reduce the transitions from one instance to the other.

DGW-16407 - HA: New parameter **StartupStatus**

Parameter **Ha.StartupStatus** was added to the High Availability service to provide better information about the service state.

DGW-16376 - Added support for HTTP redirects

Incident Number: IN-15997

The Cert, Conf, File and Fpu service now follow HTTP redirection when downloading a file.

DGW-16365 - New DCM notifications 60200 and 60210

Added two new general notifications to all service and hardware components:

- Notification 60200: Sent when the service/component fails to load the persistent configuration file because the file is too big.
- Notification 60210: Sent after saving the configuration file if the file is too big and would be lost at the next service/component startup.

DGW-16364 - The maximum number of authentication rows in **SipEp.Authentication** table is now synchronized with the maximum number of registration allowed on the device

The maximum number of authentication rows in **SipEp.Authentication** table is now synchronized with the maximum number of registrations allowed on the device.

- The 4102S, C7 and S7 are now limited to 64.
- The S400, S100, and G7 keep the limit of 500.

DGW-16320 - Add support of SIP authentication password encryption in SipEp service**Incident Number:** IN-15391

The SipEp service SIP authentication password **SipEp.Authentication.Password** parameters can now be encrypted.

The encryption can be activated on the web interface via **Management/Misc/Password Encryption** table, or by CLI/SNMP using the **Dcm.PasswordEncryption** parameters.

The encryption methods are:

- None (default): The password will not be encrypted.
- Enc1: The password will be encrypted by hashing with a private key unique to the device (generated randomly at manufacture time).

Activating the encryption will trigger an encryption of unencrypted passwords. Deactivating the encryption will not decrypt encrypted passwords.

The password encryption will be executed at the next service start if the service of the parameter is not already started.

DGW-16291 - Sentinel 400/RS: added diagnostics for slot 1 card

On the Sentinel 400 and Sentinel RS platforms, the first slot contains additional diagnostic information that can be useful to diagnose backplane issues.

When performing a diagnostic dump, a new file, `dmesg_u1.txt`, which contains the kernel messages for slot1, will be included in the `logs*.tar.gz` diagnostic files.

DGW-16289 - Sentinel CS: implemented support for network link state changes notifications

The Sentinel CS now properly handles network link state change notification with the High Availability service.

DGW-10063 - The command `Cert.MakeCertificateFactory` was added to convert a host certificate to a factory host certificate

This command converts a specific host certificate from the **Cert.HostCertificatesInfo** table into a factory certificate. The certificate will be automatically inserted into the **Cert.HostCertificatesInfo** table when performing a factory reset.

Example: `Cert.MakeCertificateFactory FileName=0090f8xxxxxx.pem`

Fixed Issues

DGW-16359 - SBC: The symmetric RTP is activated by default if a call agent doesn't define RTP anchoring in Sbc service

Incident Number: IN-15631

The RTP symmetric feature was activated by default when a call passed through the SBC via an entry call agent with RTP anchoring defined and an exit call agent without RTP anchoring. This could cause one-way audio issue in certain configurations.

The RTP symmetric is now disabled by default on the exit side in that scenario.

DGW-16290 - SIP Proxy: Monitoring state remains to unknown until a persistent connection is established when using TLS

Incident Number: IN-15627

The monitoring state was set to unknown until the OPTIONS keepalive mechanism was started, which occurred after the establishment of the persistent connection.

The monitoring state now detects DNS and TLS problems and will set the trigger to survivability mode if the persistent connection cannot be established.

DGW-16228 - SBC: The port is not present in notification 810

Fixed missing port number issue in notification 810 in the Sbc service.

DGW-16146 - SBC: improvements in the Limit CAPS ruleset action

Fixed two bugs in the Limit CAPS ruleset action:

- Bug #1: The "Time unit" parameter was ignored. A value of 30 seconds was used instead.
- Bug #2: The Limit CAPS action was blocking SIP messages for the first 30 seconds, which was incorrect.

Known Issues

There are no known issues.

Copyright Notice

Copyright © 2023 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.



130, rue Sauvé
Sherbrooke (Québec)
J1L 0A7 Canada
media5corp.com