



DGW Firmware

v49.1.2884

Release Notes

Release Notes

DGW Application 49.1.2884

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

Summary

Incident Number	ID	Synopsis
IN-15745	DGW-15841	New parameters SipEp.InteropLockDnsSrvRecordForRegister and SipEp.InteropLockDnsSrvRecordWithInviteBoundToRegisterEnable
	DGW-15914	New File.InstallFile command
	DGW-15971	The Sentinel CS now supports ARM CPUs
	DGW-15991	Sentinel CS does not wait for network to be ready on bootup
IN-15411	DGW-15998	The redundant port is now monitoring both the primary port (ETH4) and the secondary port (ETH5)
IN-15475	DGW-16000	SIP requests always used the same DNS SRV record when the parameter SipEp.InteropLockDnsSrvRecordPerCallEnable was set to enable.
	DGW-16051	SNMPv3 password for certain profiles

Incident Number	ID	Synopsis
IN-15519	DGW-16070	The device responds with a 415 Unsupported Media Type if the peer has comfort noise payload as first payload and the parameter SipEp.AnswerCodecNegotiation is set to FirstCommonPeerPriority
IN-15602	DGW-16087	The notification Sbc.810 should display the reason near the beginning of the notification.
IN-15492	DGW-16096	New feature allowing a gateway to change its source port after consecutive connection failures.
	DGW-16129	SIP check-sync can now refresh the EMS service
IN-15067	DGW-16182	New parameter Eth.Links.IgnoreLinkDown allows an ethernet port to appear Up when cable is disconnected.
IN15612	DGW-16183	The support of a call blind transfer (SIP REFER) without second call has been added.
	DGW-16201	Upgrade to OpenSSL 1.1.1t
IN-15394	DGW-16205	The description of the UseImplicitInbandInfoEnable parameters is inaccurate in some cases
	DGW-16206	New High Availability ("Ha") service / VRRP

New Features

DGW-16206 - New High Availability ("Ha") service / VRRP

DGW 49.1 introduces the first iteration of the High Availability (Ha) service.

Using the Virtual Redundancy Routing Protocol (VRRP), the service enables a shared/floating IP address between two devices (Master and Backup).

It currently supports VRRP in IPv4 multicast mode and is available for the Sentinel series.

The HA service requires a license key. Contact your account manager or Technical Assistance Center specialist.

DGW-16201 - Upgrade to OpenSSL 1.1.1t

The application is rebuilt using OpenSSL 1.1.1t.

This security upgrade fixes several vulnerabilities:

- Fixed X.400 address type confusion in X.509 GeneralName ([CVE-2023-0286](#))
- Fixed Use-after-free following BIO_new_NDEF ([CVE-2023-0215](#))
- Fixed Double free after calling PEM_read_bio_ex ([CVE-2022-4450](#))

Fixed Timing Oracle in RSA Decryption ([CVE-2022-4304](#))

DGW-16183 - The support of a call blind transfer (SIP REFER) without second call has been added.

Incident Number: IN-15612

The Dgw application can now make a blind transfer (SIP REFER) without initiating a second call to the transfer target. The behavior will be changed to a single-line extension.

A new parameter **EpServ.DefaultTransferBlindType** has been added to the EpServ service to control the blind transfer behavior.

To enable, the feature, configure:

```
EpServ.DefaultSecondCallEnable=Disable  
EpServ.DefaultTransferBlindType=TargetDial
```

Note: the feature uses the "confirmation" tone, which may be different in some countries, or silent (Australia). It is suggested to override the default tone with North American values with this configuration:

```
Telif.CountryCustomizationTone[Tone=Confirmation].Pattern="f1=350:-17,f2=440:-  
17,l=3,s1=on:f1:f2:100:s2,s2=off:100:l:s1,s3=off"  
Telif.CountryCustomizationTone[Tone=Confirmation].Override=Enable  
Telif.Restart
```

DGW-16182 - New parameter Eth.Links.IgnoreLinkDown allows an ethernet port to appear Up when cable is disconnected.**Incident Number:** IN-15607

New parameter Eth.Links.IgnoreLinkDown.

When enabled, it allows an ethernet port to appear Up when cable is disconnected.

The overall behavior is similar to having the unit connected to an ethernet switch that gets disconnected from the network: the ethernet interface stays Up while network connection is lost.

This feature solves a problem in configurations where two parts of Dgw communicate together through a "real" ethernet interface instead of the loopback. For instance in a survivability use case where the calls flow between a gateway and the SBC. Normally, when the link is down, communication is lost between them. Using this feature, communication still works.

Notes:

- Static IP addresses must be used on the links configured with this feature.
- If using the loopback interface is possible instead of using this feature, it is likely a better choice.
- This feature is not supported on the Sentinel CS.

DGW-16129 - SIP check-sync can now refresh the EMS service

The SIP check-sync mechanism can now refresh the EMS service if EMS provisioning is enabled and SipEp/GwEventHandling/CheckSync is set to "TransferScript".

DGW-16096 - New feature allowing a gateway to change its source port after consecutive connection failures.**Incident Number:** IN-15492

The new parameter SipEp.TransportCriticalConnectionFailureMaxCount can be used to configure a gateway to change its source port after a certain number of consecutive connection errors.

Typical usage is when the gateway source port can be blocked by a firewall.

This feature supports trunk gateways using TLS.

DGW-16051 - SNMPv3 password for certain profiles

Some customer profiles were updated for easy migration from 48.4 to later versions. When upgrading, custom existing SNMP passwords will be migrated to the new Snmp.SnmpV3Password parameter.

DGW-15998 - The redundant port is now monitoring both the primary port (ETH4) and the secondary port (ETH5)**Incident Number:** IN-15411

When the redundant ports feature is enabled, both the primary (ETH4) and the secondary (ETH5) ports are now monitored for their link state and notifications are sent on state changes and there are no more switchovers to the secondary port when the link is down on that port.

Additionally, a gratuitous ARP is now also sent when the active port becomes up even without port switching.

Finally, the gratuitous ARP target IP address is changed from 0.0.0.0 to the host IP address.

The new notifications are:

- 2400.80 %1\$s link down detected.
This message is issued when the Eth.RedundantPorts parameter is enabled, and a link failure is detected on one of the redundant ports.
- 2400.90 %1\$s link up detected.
This message is issued when the Eth.RedundantPorts parameter is enabled, and the link is back up on one of the redundant ports.
- 2400.100 Switching over from %1\$s to redundant port %2\$s.
This message is issued when the Eth.RedundantPorts parameter is enabled, and a link failure is detected on the primary port.
- 2400.110 Switching back from %2\$s to primary port %1\$s.
This message is issued when the Eth.RedundantPorts parameter is enabled, and the primary port is back up and running.

DGW-15971 - The Sentinel CS now supports ARM CPUs

The Sentinel CS now supports ARM CPUs

There are now two Sentinel CS firmware files:

- SentinelCS_x86-64 : For the x86_86 64bits CPUs, originally SentinelCS
- SentinelCS_arm32: Supports gnuabi architecture, compiled for ARM32, but will also run on ARM 64bit CPUs provided the kernel is compiled with ARM32 support.

The Sentinel CS for ARM has been tested on the Raspberry Pi 3, various Pi clones and embedded boards (Allwinner, Marvell, and RockChip processors), and the AWS Graviton2.

DGW-15928 - SBC rulesets can now be exported in configuration scripts

SBC rulesets are exported alongside certificates if the option All Config & Files is selected when exporting the unit's configuration.

The rulesets files are encoded in Base64.

DGW-15914 - New File.InstallFile command

A new file installation command is now available, File.InstallFile. Primarily designed to simplify the SBC Rulesets installation when using a management server such as Virtuo.

The command installs the Base64 text-encoded file in the Mediatrix unit, no external server repository is required.

It is recommended to use this command within a configuration script, or through the CLI.

Fixed Issues

DGW-16205 - The description of the UseImplicitInbandInfoEnable parameters is inaccurate in some cases

Incident Number: IN-15394

The description of the Isdn.PrimaryRateInterfaceInterop.UseImplicitInbandInfoEnable and Isdn.BasicRateInterfaceInterop.UseImplicitInbandInfoEnable parameters have been amended to note that they can also have some side effects on incoming calls under certain circumstances.

DGW-16087 - The notification Sbc.810 should display the reason near the beginning of the notification.

Incident Number: IN-15602

The notification Sbc.810 was showing the "reason" field at the end of the syslog message, which was often truncated because of its large size.

The notification now shows "reason" near the beginning of the notification. The other fields (ruri, from, to, call-id) are still kept even if empty, to account for future use.

DGW-16070 - The device responds with a 415 Unsupported Media Type if the peer has comfort noise payload as first payload and the parameter SipEp.AnswerCodecNegotiation is set to FirstCommonPeerPriority

Incident Number: IN-15519

The device will no longer respond with 415 Unsupported Media Type if the peer has comfort noise payload as first payload and the parameter SipEp.AnswerCodecNegotiation is set to FirstCommonPeerPriority.

DGW-16000 - SIP requests always used the same DNS SRV record when the parameter SipEp.InteropLockDnsSrvRecordPerCallEnable was set to enable.

Incident Number: IN-15475

SIP requests will now correctly choose a target according to the weight in the DNS SRV record. They will continue to be locked for requests sent by the same SIP context (same Call-ID).

The problem was only present when the parameter SipEp.InteropLockDnsSrvRecordPerCallEnable was enabled.

DGW-15991 - Sentinel CS does not wait for network to be ready on bootup

On some Sentinel CS systems, the SBC service started too soon before the network was completely initialized resulting in no network links detected and using the default MAC address instead of the real one.

The start-up mechanism has been improved to better handle network interface initialization.

DGW-15841 - New parameters SipEp.InteropLockDnsSrvRecordForRegister and SipEp.InteropLockDnsSrvRecordWithInviteBoundToRegisterEnable

Incident Number: IN-15475

New parameters were added to provide finer control of the behavior of SipEp.InteropLockDnsSrvRecordForRegister.

- New parameter SipEp.InteropLockDnsSrvRecordForRegister controls whether REGISTER refreshes start from the DNS target of the last successful REGISTER or from the highest priority target of the DNS response.
- New parameter SipEp.InteropLockDnsSrvRecordWithInviteBoundToRegisterEnable to control whether INVITEs start from the DNS target of the last successful REGISTER or from the highest priority target of the DNS response.

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