2024

voipfuture

RELEASE NEWS

Qrystal 9

Monitoring Encrypted Traffic:

Analysis of encrypted traffic in LTE and fixed networks

Major Security Updates:

New operating system hardened according to CIS

Adaptive User Interface:

Dynamic GUI layout, new portlets and more

MONITORING ENCRYPTED TRAFFIC

SIP over TLS Decryption

- Integrated key management
- VSupport for common TLS 1.2 cipher suites

Decryption of SIP in LTE IPSec tunnels

- Automatic key detection at the SGi
- Support for AES-CBC ciphers

Encrypted RTP Monitoring

- New indicator for SRTP
- Analysis of encrypted media streams

MAJOR SECURITY UPDATES

- Future-proof OS: Rocky Linux 9 with planned support until 2032
- Cyber security hardening according to the CIS recommendations
- Improved inter-service communication security

NEW ADAPTIVE USER INTERFACE

Dynamic GUI rendering

- GUI now adapts to the width of the browser, flexibly re-arranging the page contents and re-sizing the charts
- Font-size can be changed in browser settings

Dashboard improvements

- All available Dashboards now directly accessible from main menu
- Many new and improved Dashboard portlets

EXTENDED CODEC SUPPORT

Opus Codec Monitoring

- Full support for Opus (IETF RFC 6716), the main WebRTC codec
- Detection and full analysis of all 24 codec modes

Full-Band MOS

- New support for full-band MOS according to ITU-T G.107.2
- Users can now choose between narrowband, wideband and full-band MOS scales, depending on user expectations and used codecs

OTHER NEW FEATURES

Network-wide licenses

- More effective use of available licenses
- Simplified license management via the GUI

Other Features

- Significant performance improvements for systems with many users
- Greater resilience to defects of Manager hardware
- Alternative callhash algorithms for improved call correlation

MONITORING ENCRYPTED TRAFFIC

Monitoring Encrypted Traffic

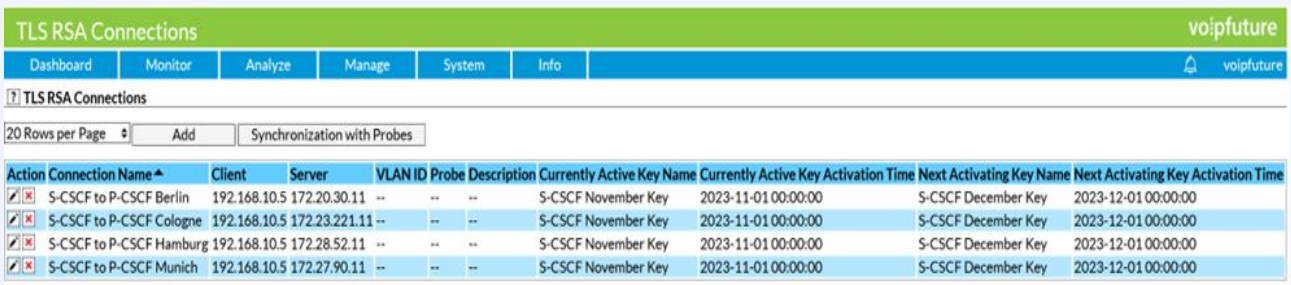
Security is becoming increasingly important to customers and thus more and more VoIP traffic is being encrypted. While Qrystal could always provide essential data on the transport quality of media streams, encryption did lead to visibility gaps on call signaling and partially on user experience data. Qrystal 9 is now able to decrypt encrypted signaling in many common scenarios and highlights media encryption.

SIP over TLS Decryption

SIP over TLS, also known as SIPS, is used in fixed networks to encrypt the call signaling between endpoints, e.g. between end user devices and a CSP's access SBC. Qrystal 9 can decrypt SIP over TLS for ciphers with a non-ephemeral key exchange algorithm. Currently decryptable TLS ciphers are:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

When a TLS server's private key has been configured in the Qrystal Manager, the Qrystal Probe automatically learns the symmetric key during the TLS negotiation and registration as well as signaling data records are created even for encrypted signaling.



The keys can be added on the new TLS RSA Keys and Add/Edit TLS RSA Key pages. On the new TLS RSA Connections and TLS RSA Connection pages the different private keys can then be assigned to different SBC connections. and It is also possible to set an automatic activation time, to ensure keys are changed at the same time as by the monitored SBCs will activate them can be scheduled.

Decryption of SIP in LTE Networks

Qrystal 9 Probes can now decrypt EPS tunnels in the LTE packet core, which carry the SIP traffic. Qrystal Probes monitoring VoLTE traffic are typically deployed close to the SGWs to monitor the S1-U and S11 interfaces. If the same probe also monitors the SGi interface (P-CSCF to PGW), then it can automatically learn the ESP encryption type/key during the initial registration. Subsequently, RDRs and xDRs are created for encrypted SIP bearers with a supported encryption type, namely No Encryption and AES-CBC.

SRTP Monitoring

Qrystal 9 Probes detect payload encryption using The Secure Real-time Transport Protocol (SRTP) defined in IETF RFC 3711. Encrypted payloads of the fixed size payloads G.711, G.722 and G.729 are flagged with a dedicated SRTP indicator. Quality data for these SRTP streams is available to the same extent as for unencrypted RTP.

The SRTP indicator is shown on the Stream data record and the Stream Summary page Indicators tab. It is also accounted for in the Media Plane statistics and can be seen on the Indicator Monitor page.

MAJOR SECURITY UPDATES

Major Security Updates

Future-proof New OS

Qrystal 9 introduces Rocky Linux 9 [MW1] as new operating system. Previous Qrystal versions were based on the stable CentOS 7, which is end-of-life after June 30th 2024. This means that there will be no security updates following this date. Voipfuture strongly recommends upgrading to Qrystal 9 with Rocky Linux 9 as soon as possible, because running software without security support in a critical infrastructure system is not a good idea. The Rocky Enterprise Software Foundation plans to provide Rocky 9 security support until May 2032.

The migration to Qrystal 9 requires a fresh installation of Rocky Linux 9. The fresh OS installation from an USB image, which can be either plugged in locally or mounted remotely via the iLOM of the HP Proliant server, overwrites the complete content of the old OS disk. It creates a new LVM partition scheme with many separated partitions. The Qrystal 9 application software RPMs are installed on top of Rocky 9. All data and configuration is migrated during the installation process

CIS Hardening

The new Qrystal 9 operating system is hardened following the Rocky Linux 9 benchmarks of the Center for Internet Security (CIS). The CIS Benchmarks are configuration baselines and best practices for securely configuring a system. This ensures maximum Qrystal security in critical infrastructure environments.

Improved Inter-Service Communication Security

All Qrystal Manager and Probe services, daemons, jobs and scripts are executed by specific technical user accounts. Qrystal 9 now uses SSL client certificates to secure inter-service communication. This means that no configuration file or script needs a password, thus further enhancing security especially in public cloud environments, such as AWS and Google Cloud.

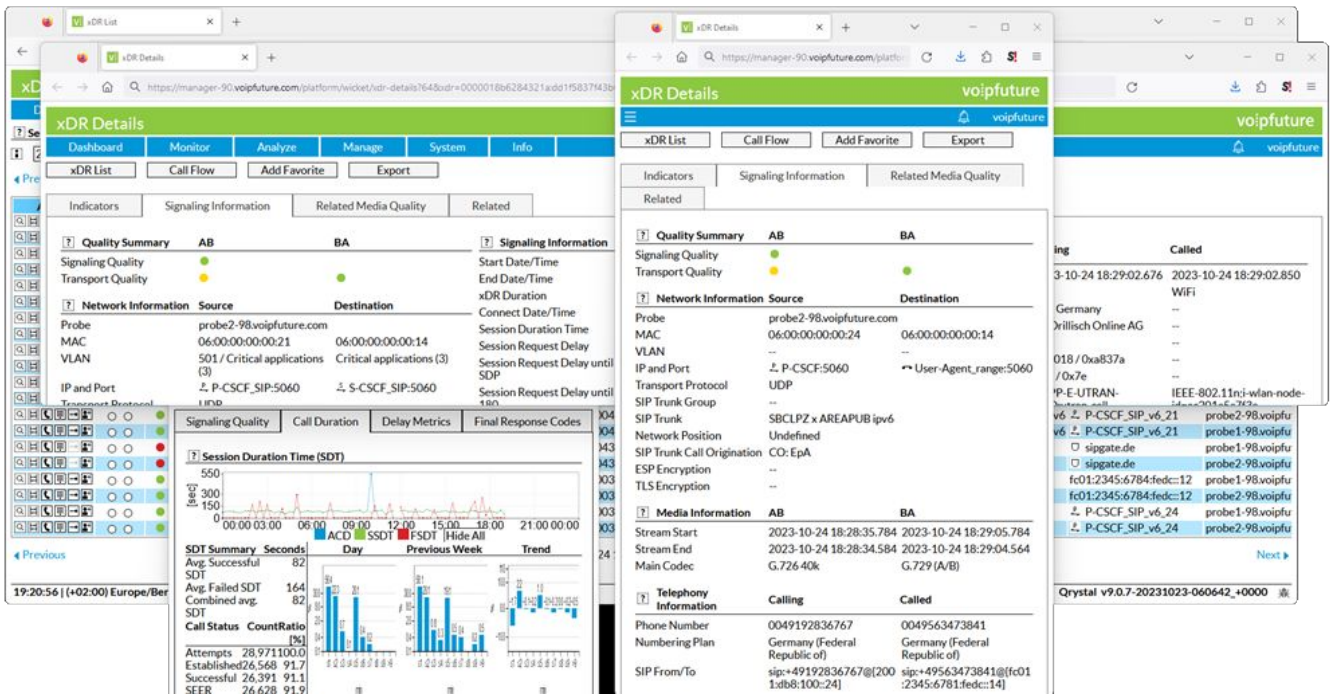
NEW ADAPTIVE USER INTERFACE

New Adaptive User Interface

Qrystal 9 implements numerous enhancements to the system's usability, including dynamic rendering for better use of screen real estate and a greatly improved Dashboard

Dynamic GUI Rendering

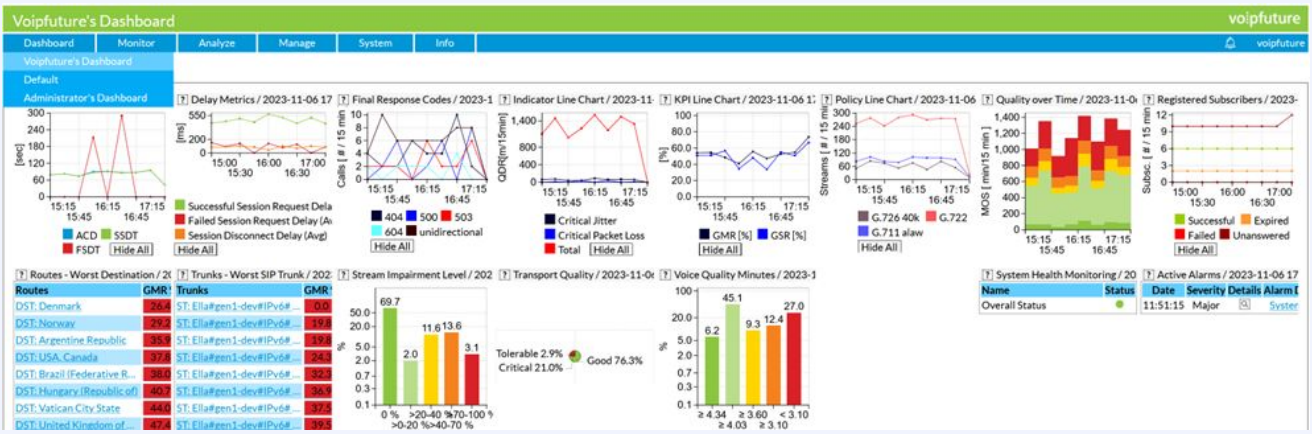
The Qrystal Manager 9 User Interface utilizes any available Web-browser window width, wherein the Web-browser's HTML engine is flexibly re-arranging the page contents and re-sizing the charts. Previously the UI enforced a fixed width landscape grid layout.



Finally, you can binge-watch Qrystal 9 data on a 60" 4K display as well as on a 10" tablet or 5" smart-phone in both portrait or landscape orientation. The new dynamic rendering adapts to any screen size and orientation.

Dashboard Improvements

Qrystal 9 offers many additional user interface improvements, particularly in regards to the dashboard.



First of all, Qrystal 9 now provides access to all available Dashboards directly from the homepage. The previous Home main menu entry is now labelled Dashboard - click it to chose from all dashboards available to you.

Dashboard tabs now support grids of up to 8 by 8 portlets.

Portlets are no longer restricted to appear only on specific grid size. Smaller graph portlets shrink graphs and smaller list portlets show only the top rows and left column that fit.

Portlets showing lists now have scrollbars to view potentially invisible content. To fine-tune the dashboard for the big screen in NOCs, list portlets also allow to configure the maximum number of rows.

Adding to this, a new caching algorithm significantly boosts the Dashboard performance on systems with many dozens and hundreds of users.

Qrystal 9 also introduces the following new dashboard portlets and enhancements:

- The new **Final Response Codes** line chart portlet shows the 5 worst or up to 5 selected SIP Final Response Codes over time.

- The **Indicator Line Chart** can be switched from **QDR View** to the **xDR/Stream View** chart type to also show Control Plane indicators

- The new **Policy Line Chart** portlet shows worst **Audio Codecs, DSCP Codes, Media Plane Indicators** or **Control Plane Indicators** over the time.

- The Control Plane indicators are also selectable on the **Policy Monitor** portlet

- The **Trunks/Routes** portlet has a new show **Trunks** (regex)/**Routes** (regex) mode and an additional **Routes** view filter for the **Trunks** portlet and Trunks view filter for Routes portlet.

EXTENDED CODEC SUPPORT

Extended Codec Support

Qrystal 9 adds support for the Opus codec and the fullband MOS scale.

Opus for WebRTC

The **Opus** codec defined in RFC 6716 provides a wide range of modes from narrowband speech encoding up to full-band music. The WebRTC framework (RFC 7478) mandates that endpoints support the G.711 and Opus codecs.

Qrystal 9 Probes detect all 24 Opus codec RTP payload variants and use their specific E-Model parameters to calculate the R-factor for every QDR- and stream measurement. The Qrystal Manager fully supports the Opus codec on all pages, portlets, reports and alarms with codec specific information.

Fullband MOS

The Opus and EVS codec suites both offer a number of high-quality modes that extend the encoded frequency range to up to 24,000 Hz. These fullband codecs cover the entire frequency spectrum of human hearing and beyond. In simple terms, human hearing cannot distinguish between an original signal and its fullband encoded version; this is referred to as transparency.

To account for the constant improvement of codecs and the rising user expectations the ITU has revised G.107 and the E-Model numerous times. To this end, the range of R-Factor values was extended and different MOS scales were introduced.

Solution MOS Class Scaling	Frequency Band	Max. R-factor	R defined by
Narrow-Band (NB)	300 – 3,400 Hz	100	G.107 (12/1998)
Wide-Band (WB)	50 – 7,000 Hz	129	G.107.1 (12/2011)
Super-Wide-Band (SWB)	50 – 14,000 Hz	129	G.107.1 (12/2011)
Full-Band (FB)	20 – 24,000 Hz	148	G.107.2 (06/2019)

Qrystal 9 extends the R-factor scale to 148, i.e. the maximum achievable value for fullband codecs as defined in G.107.2, and provides a mapping to fullband MOS. Users can now choose between displaying MOS on the narrowband, wideband and fullband scales.

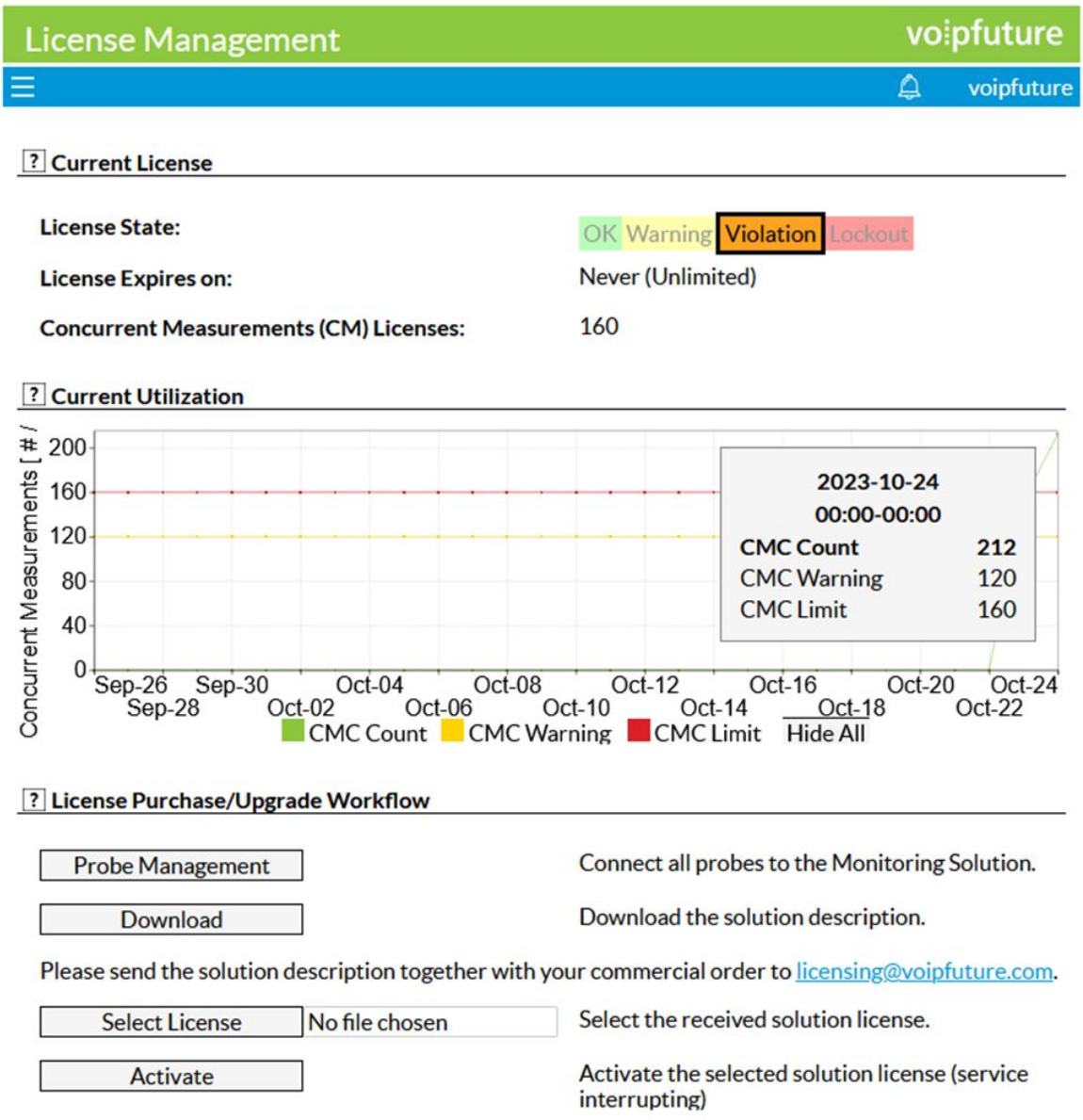
OTHER NEW FEATURES

Other new features

Qrystal 9 introduces many additional improvements, such as simplified network-wide licenses and greater resilience against defects of Manager hardware.

Network-wide licenses

Qrystal licenses are based on the measurement of concurrent calls. So far the Qrystal Probes had to be licensed individually for the peak amount of concurrent calls that was expected to be monitored by the probe. Starting with Qrystal 9, the concurrent call measurement (CCM) license limit is supervised and enforced system-wide by the Qrystal Manager. This means that the available licenses can be used much more effectively, especially if individual probes do not experience peak load at the same time.



Another benefit is that license management is now more transparent and greatly simplified through the GUI. You can easily check for the amount of used licenses and receive early warnings, when your system is about to exceed its license limit. The GUI also allows the preparation of license purchase requests to the Voipfuture Sales Team and the activation of the purchased licenses.

More improvements

Greater Resilience

Qrystal is an extremely reliable tool, thanks to its loosely coupled architecture. However, as with airplane crashes, sometime the Swiss cheese holes align, and incidents happen. With very large clustered Manager installations it could happen that the user interface would show exceptions when one Manager node failed.

Qrystal 9 now allows to re-configure the Manager database nodes on the fly. A defect node can be removed and the cluster connections will be re-build. After disabling a defect node, the Qrystal Manager user interface will operate normally again, lacking just the data from the disabled node.

More Correlation Options

Qrystal 9 introduces a configuration option for the Callhash to configure algorithms to use as backup if the preceding algorithm is not applicable. Also, the number of phone number digits that are used to generate the callhash can be limited.

Configurable Callhash algorithms:

- Default (backwards compatible) – hash using the normalized calling and called phone numbers with a specified number of digits
- Calling – hash using only the normalized calling phone number limited by specified number of digits
- Callid – hash based on the SIP Call-ID header
- Sessionid – hash based on the optional SIP Session-ID

The Callhash calculation algorithm must be configured by the Voipfuture Support team.

ABOUT VOIPFUTURE

Voipfuture is a premium voice service monitoring and analytics company, which provides a unique technology for assessing, aggregating, analyzing, and visualizing voice quality information, for better data-based insights,

Voipfuture products offer a precise view on both the media and control planes to communication service providers, wholesalers, enterprises, call centers and cloud-based voice services. Since its launch, Voipfuture has been at the forefront of voice quality monitoring and continues to redefine Voice over IP by connecting customers' view on service quality with high resolution user experience, as well as with insights that enable next gen voice services.

Follow us to stay in the know

voipfuture

Watch a Demo

Contact Us