REDCOM Sigma V4.0

Software Release Information

The following REDCOM® Sigma® software release information is listed by version number and release date.

> **NOTE:** It is expected that Sigma V4.0 will have patch releases at least through June 2024. This schedule is subject to change.

V4.0.3

07DEC2023

Improved:

- A Sigma status report can now be downloaded as a text file from the **System Monitor** app. Previously, this report was only available by executing a script and collecting logs from the command line.

  > **NOTE:** This report is intended for use with REDCOM Customer Support when diagnosing system issues.
- A read-only permission was added for the **Trunks** app. Users with this permission turned on can view trunks but cannot add, modify, or delete them.
- The **Microphone Input Boost** setting was added for analog radio lines to be used when a microphone that requires higher audio levels than the adjustable input gain range is connected directly to the associated radio port.
- The **Announce Security Level** setting was added for secure vIPer analog trunks. If this setting is on, an announcement stating the security level of the call involving the trunk is played immediately after the call is answered and before a two-way talk path is established.
- The Secure Client provisioning template was updated with new REST API address and port override settings.

Fixed:

- The following issues were fixed in the **Command and Control Console** app:
  - Items on the dashboard did not always resize properly when the viewport size or overall window size was changed.
  - The **Talk volume/mute for operator PTT audio** setting for monitors did not update properly in real time if changed while push-to-talk (PTT) was asserted.
  - Audio was duplicated if a connection was included in the operator Select both directly and indirectly through a patch.
- A connected Sectéra® vIPer™ phone sometimes got stuck in a state of powering up.
- Port status LED indicators on SVG-1200 and XRI modules sometimes were blue incorrectly after a call on a radio port went idle or when editing a radio line.
- When there was an error joining a conference, the conference would drop instead of issuing an error log message.
- Initiating a conference with lines using a Session Description Protocol (SDP) set with Alternative Network Address Types (ANAT) semantics resulted in several issues including no announcements, no talk path, and members remaining in the conference even after hanging up.
- Some REST API endpoints allowed the POST operation without the correct permissions.

- When a Session Initiation Protocol (SIP) INVITE was received with an unresolvable hostname in the From, P-Asserted-Identity, or P-Preferred-Identity headers, the trunk matching timed out before proper handling was reached.
- Due to timing issues, multiple unnecessary system reboots sometimes occurred during standby system configuration.
- The **Software Update** app sometimes incorrectly indicated no difference between the current software version and the available software version.

Security:

- A privilege escalation vulnerability was found in the REST API regarding the use of JSON web tokens (JWT).
- An out-of-bounds write vulnerability was detected in WebP, as addressed in CVE-2023-4863. This vulnerability is considered to be high severity and can potentially be exploited in Sigma to corrupt memory. As a result, WebP was upgraded to version 1.3.2.
- An insufficient information vulnerability was detected in Python®, as addressed in CVE-2023-40217. This vulnerability is considered to be medium severity and has little to no effect on Sigma because Python is not used in a way that exposes it. However, Python was still upgraded to version 3.8.18.
- Multiple vulnerabilities were detected in Apache®. As a result, Apache was upgraded to version 2.4.58.
  - CVE-2023-31122
    This out-of-bounds read vulnerability is considered to be high severity but has little to no effect on Sigma because mod_macro is not used.
  - CVE-2023-43622
    This uncontrolled resource consumption vulnerability is considered to be high severity and can potentially be exploited in Sigma to cause a remote denial of service (DoS) in the web user interface.
  - CVE-2023-45802
    This uncontrolled resource consumption vulnerability is considered to be medium severity and can potentially be exploited in Sigma to cause a remote DoS in the web user interface.
- Multiple vulnerabilities were detected in cURL. As a result, cURL was upgraded to version 8.4.0.
  - CVE-2023-38039
    This allocation of resources with limits vulnerability is considered to be high severity but has little to no effect on Sigma because cURL is not likely used in a way to expose it. However, it may cause process DoS if exploited.
  - CVE-2023-38545
    This out-of-bounds write vulnerability is considered to be critical severity but has little to no effect on Sigma because cURL is not used with a SOCKS5 proxy.
- Multiple vulnerabilities were detected by FreeBSD® as security advisories. As a result, FreeBSD was upgraded to version 13.2p5.
  - FreeBSD-SA-23:11.wifi [CVE-2022-47522]
    This authentication bypass vulnerability is considered to be high severity but has little to no effect on Sigma because wireless (Wi-Fi) communications are not used.
  - FreeBSD-SA-23:10.pf [CVE-2023-4809]
    This improper handling of additional special element vulnerability is considered to be high severity but has little to no effect on Sigma because the vulnerable rule is not used by default. A web user would need access to the **System Configuration** app to edit configuration files to add this rule and, by default, this access is restricted to system administrators.
  - FreeBSD-SA-23:12.msdosfs [CVE-2023-5368]
    This insecure default initialization of resource vulnerability is considered to be medium severity and has little to no effect on Sigma because MS-DOS file systems are not used.

- FreeBSD-SA-23:13.capsicum [CVE-2023-5369]
  This improper check for dropped privileges vulnerability is considered to be high severity but has little to no effect on Sigma because capsicum is not used.
- FreeBSD-SA-23:14.smccc [CVE-2023-5370]
  This improper initialization vulnerability is considered to be medium severity and has little to no effect on Sigma because ARM processors are not supported.

V4.0.2

27SEP2023

New:

- Added support for the Curtiss-Wright® PacStar® 421 Small Form Factor Extended Radio Interoperability (XRI), which can be managed as an extension module in the **Device Management** app. This tactical computing module includes radio gateway services for both modern and legacy radios.

  NOTE: Use of this module requires a valid XRI Extension Modules feature license.

V4.0.1

05SEP2023

Improved:

- The option to listen to deleted messages was removed from the voice mail menu if there are no deleted messages.
- The maximum length of time to dial a conference PIN was increased to prevent unnecessary time-outs when attempting to enter a conference with a long PIN.
- The **Secure Downgrade Allowed** setting was added for secure vIPer analog trunks.

Fixed:

- The following issues were fixed regarding the SVG-1200:
  - Conference calls with a connected Sectéra vIPer phone sometimes did not end as expected.
  - A call to a preset conference member via a secure vIPer analog trunk appeared in the **Conferences** app as joined while it was still pending.
  - In scenarios involving a secure vIPer analog trunk, dialing a conference PIN sometimes did not result in joining the conference as expected.
  - Transferring a secure vIPer analog trunk into a conference was not successful.
  - Some displayed call security level mappings from a device using a secure vIPer analog trunk were incorrect.
  - The caller ID and security level sometimes did not display or update properly in the **Conferences** app for a call using a secure vIPer analog trunk.
  - A secure vIPer analog trunk in Public Switched Telephone Network (PSTN) mode or using auto attendant did not send caller ID information to the destination.
  - PTT digits did not send over a secure vIPer analog trunk.
  - A call over a secure vIPer analog trunk to a SIP phone continued to ring the phone even after the secure call failed.
  - Incoming calls over a secure vIPer analog trunk were not always successful with certain settings on the vIPer phone such as ASEC turned off or soft modem set to 4800.

  - The ring and call volume settings did not always work as expected and sometimes caused attempts to unlock the device to fail after a reboot.
  - The **ACC Downgrade Allowed** setting for secure vIPer analog trunks was not working properly.
- Icons did not display throughout the User Guide, and some table formatting was incorrect in the API reference documentation.
- Attempting to run the Sigma status report using the command line resulted in an error message.
- Adding a quick build analog trunk incorrectly required a routing address.
- Deleting and recreating lines and trunks associated with radio ports sometimes resulted in loss of talk path.
- Rebooting a Sigma XRI-400 system with the **Radio Port Status** app open in a separate browser tab resulted in database initialization issues.
- Changing the system date in the **System Monitor** app or **Fill** app did not always work.
- After an initial database fill, the default Interactive Connectivity Establishment (ICE) SDP set was not populated with any media streams, which is necessary for the operator to use “This device” for the audio connection in the **Command and Control Console** app.
- The operator sometimes incorrectly appeared to be connected in the **Command and Control Console** app.
- The **Mute Select members** setting for monitors in the **Command and Control Console** app was not working properly.
- There was low quality audio when using a 16 kHz codec.
- Making changes to a Unified Contact Management (UCM) group tag in Sigma sometimes resulted in all contacts within that group incorrectly receiving an Extensible Messaging and Presence Protocol (XMPP) authorization request from Secure Client.

Security:

- A valid REST JSON web token (JWT) could potentially have been used on a different Sigma instance.
- An out-of-bounds write vulnerability was detected in libX11, as addressed in CVE-2023-3138. This vulnerability is considered to be high severity but has little to no effect on Sigma because libX11 is not used for providing or accessing display services. However, libX11 was still upgraded to version 1.8.6.
- Multiple vulnerabilities were detected by FreeBSD as security advisories. As a result, FreeBSD was upgraded to version 13.2p2.
  - FreeBSD-SA-23:04.pam_krb5 [CVE-2023-3326]
    This improper authentication vulnerability is considered to be critical severity but has little to no effect on Sigma because Kerberos is not explicitly used by default. A web user would need shell access or access to the **System Configuration** app to exploit it and, by default, this access is restricted to system administrators.
  - FreeBSD-SA-23:06.ipv6 [CVE-2023-3107]
    This integer overflow vulnerability is considered to be high severity and can potentially be exploited in Sigma instances with IPv6 turned on and a security level less than high to cause denial of service (DoS).
  - FreeBSD-SA-23:07.bhyve [CVE-2023-3494]
    This buffer overflow vulnerability is considered to be high severity but has little to no effect on Sigma because bhyve is not used.
  - FreeBSD-SA-23:08.ssh [CVE-2023-38408]
    This unquoted search path vulnerability is considered to be critical severity but has little to no effect on Sigma because ssh-agent is not used by default. A web user would need shell access or access to the **System Configuration** app to exploit it and, by default, this access is restricted to system administrators.

V4.0.0

28JUN2023

New:

- Support for configuring a system with the SVG-1200 multi-party secure voice conferencing solution developed in partnership with General Dynamics Mission Systems® for call control and conferencing capabilities with attached Sectéra vIPer phones. Some new features include:
  - A feature license to determine the access to on-board interface ports for secure trunking.
  - Configuration of “Secure vIPer” analog trunks in the **Trunks** app.
- Support for configuring Foreign Exchange Office (FXO) analog trunks in the **Trunks** app and associating them with available port addresses to connect with another phone system using a standard analog line circuit.

  NOTE: To have functional FXO trunks, you must use the REDCOM FXO adapter to connect a PSTN line circuit to an analog port on your Sigma XRI-400, XRI-M4K, or SVG-1200.
- Added a **View Trunk Status** option in the **Trunks** app to view operational status and details of analog trunks and send commands to associated devices for monitoring and debugging purposes.
- Added a **Test Translation** option in the **Lines** and **Trunks** apps to select a line or trunk and test translations configured in the system without needing the equipment to make any actual test calls.
- Added the REDCOM Automatic Conference Code Generator (RACCG) tool to generate conference code files in Sigma with an option to automatically send the codes to a specified email address.
- Added echo cancellation settings for analog trunks and radio lines.
- Added REST API endpoints for language files, analog trunks, and general hunt translator rule.

Improved:

- The following improvements were made in the **Command and Control Console** app:
  - An operator can now select “This device” for the **Operator audio connection** to use a selected microphone and speaker from their local device.

    NOTE: This feature is supported if used with Microsoft Edge®, Google Chrome™, or Opera™. This feature may work with other browsers, but support is not guaranteed.
  - Connections and patches can now be added as members when creating a monitor instead of just when editing an existing one.
  - Indication of the operator push-to-signal (PTS) state was added to patches on the dashboard.
  - The overall layout of the toolbar and panel on the right side of the screen was improved for more intuitive navigation.
- The **Language Support** app was redesigned with improved functionality including copying existing languages as templates to create new languages from, downloading and uploading CSV files with edited language strings to be used throughout the software, and filtering the table to view language strings that were added or modified as a result of a software update.
- A sequence of digits can now be configured to request and cancel conference operator attention instead of just a single digit.

  NOTE: The new default digit sequences are 1# for requesting attention and 2# for canceling attention.
- Dial codes are now displayed in the **Conferences** app for inactive conferences.
- When a line being deleted causes a device to no longer have any lines associated with it, there is now an option to delete the device also.
- Changes to line or trunk settings are not applied to active calls and will only take effect on future calls, so there is now an option to terminate active calls after editing a line or trunk.
- If voice mail is turned on for a line in the **Lines** app, the linked basic phone rule is now automatically set to go to voice mail if it was previously set to ring only.

- When creating resources using quick build, settings that were not necessary for basic functionality were moved to be advanced settings.
- With the proper feature license, more than one TSM gateway radio can now be added in the **Device Management** app.
- Fan speed was added as a chart option in the **System Monitor** app for the XRI-400 and SVG-1200.
- All wizards, windows, and confirmation dialog boxes can now be dragged to a different location on the screen.
- FreeBSD was updated to version 13.2.
- PostgREST was updated to version 10.0.0.

Fixed:

- The following issues were fixed regarding the REST API:
  - Using several endpoints, the PATCH or POST operation allowed incorrect values for some fields.
  - Using the /lines_sip endpoint, the PATCH operation for the vm_enable field resulted in an error.
  - Using the /translators_macro_rule_advanced endpoint, the GET operation for a preset conference rule resulted in an error.
  - Using several endpoints, the POST operation sometimes resulted in an error regarding permissions.
  - Using the /translator_macro_rule_auto_attendant endpoint, the POST operation resulted in an error if the pattern-ref field was previously empty.
  - Several endpoints were missing the Location header from the POST response.
  - The connection_max_retry_timer field was missing.
  - Trunks could be deleted by a user with insufficient permissions.
- The following issues were fixed in the **Command and Control Console** app:
  - Switching between the light and dark color scheme did not work.
  - Operator audio connection volume and mute settings were not always preserved correctly if there were multiple operators.
  - The **PTT All** button sometimes stayed active even when **Latched PTT** was turned off.
  - If a PTT button was released while a connection was disconnected, PTT incorrectly remained active for that connection.
  - If the operator device disconnected while using PTT to a patch, PTT incorrectly remained active to the patch and no other patch members could use PTT.
  - Turning **Monitor audio to and from members** on and off did not always work.
  - A connection failed to establish if the selected line had more than one associated device.
  - Due to configured SIP timers, there was a delay in re-establishing connections with SIP devices.
- The caller ID of a line with **Block Caller ID** turned on was still displayed in the **Conferences** app.
- A radio could not enter a conference password because the password prompt announcement held the radio in a receiving state.
- In a conference, a SIP phone was unable to assert PTS immediately after a radio asserted and deasserted PTS.
- Pegged connections with radios were not always re-established after rebooting the system and sometimes caused error messages.
- Port status LED indicators on the XRI-400 sometimes remained blue after a failed call or green during radio-to-radio calls.
- The **Radio Port Status** app did not load properly if it was the only assigned app.
- The **Ringing Tone** setting for radio lines did not work.
- From the **Tags** app, a line could incorrectly be tagged with the TEMPLATE system tag.

- Tags and SDP sets could have duplicate names, which resulted in errors.
- The feature expiration warning did not display properly on the **Capabilities and Capacity** widget.
- Editing settings in the **Fill** app sometimes created duplicate widgets on the dashboard.
- There were duplicate to do task entries regarding checking media files.
- There were several errors with permissions in the **Media Manager** app.
- In a military system, there were incorrect warnings that valid files did not exist in the system.
- In a military system, the database activation icon in the upper-right corner was shown even after activation was complete.
- Changing the value of the LIMITED_CLI_ENABLE system configuration key to YES caused error messages in the debug log.
- TSM radio lines caused error messages in the system core log after being registered or deleted.
- Settings could not be configured for the NIIM log in the **System Monitor** app.
- Entering valid system hostnames values sometimes resulted in error messages instead of being allowed.
- In the **Reports** app user permissions, the **Allowed Reports** field did not populate with any selectable options.
- Archived reports could not be viewed in the **Reports** app.
- Deleting a routing address that was being used by a translator rule resulted in error messages. Now, a routing address cannot be deleted if it is currently in use.
- Moving translator rules to different folders in the **Routing and Translations** app was sometimes unsuccessful and resulted in the rules no longer working.
- Changing the **Digit Manipulation** value when editing trunk members did not always save properly.
- If there was more than one translator folder on the **Trunk** tab in the **Routing and Translations** app, creating a quick build trunk resulted in error messages.
- The **Destination URI Address** in the **Trunks** app incorrectly accepted a value with whitespace at the end, which resulted in the trunk not working.
- When a trunk had **Reverse Caller ID** turned on, the terminating name field was not populated in the call detail record (CDR).
- On the **Local PKI** tab in the **Certificate Management** app, downloading certificates and keys resulted in error messages and downloaded invalid certificate files.
- If **Use Common CAs** was turned on in the **Certificate Management** app, XMPP incorrectly did not allow connections with certificates signed by an uploaded Certificate Authority (CA).
- Table sorting was not working properly in the **XMPP Administration** app.
- Checkboxes in the **TLS Profiles** app would automatically clear themselves.
- Viewing settings in the **Registrations** app sometimes caused auto-refresh to no longer work.
- A transcoded call would sometimes lose talk path after being placed on hold.
- A large number of transcoded calls caused a memory leak in the system after a long period.

Security:

- Multiple vulnerabilities were detected in OpenSSL®. As a result, CryptoComply was updated to use OpenSSL version 1.0.2zh.
  - CVE-2022-4304
    This vulnerability is considered to be medium severity but has little to no effect on Sigma because it is not practically exploitable.
  - CVE-2023-0464
    This improper certificate validation vulnerability is considered to be high severity and can potentially be exploited in Sigma with a crafted certificate to cause DoS.
  - CVE-2023-0465

This improper certificate validation vulnerability is considered to be medium severity and can potentially be exploited in Sigma with a malicious CA resulting in certificate policies not being enforced.

- CVE-2023-0466
  This improper certificate validation vulnerability is considered to be medium severity but has little to no effect on Sigma because it is not practically exploitable.
- CVE-2023-2650
  This allocation of resources without limits or throttling vulnerability is considered to be high severity and can potentially be exploited in Sigma with a crafted certificate to cause DoS.

Contact REDCOM Customer Service at **+1.585.924.6500** or **service@redcom.com**.