



Ribbon Application Management Platform

Release Notes

Software Release: 24.12.00R001
Document Revision: 02.02
Published: 13 February 2025

Copyright

© 2020-2025 Ribbon Communications Operating Company, Inc. © 2020-2025 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

Disclaimer and Restrictions

The publication is for information purposes only and is subject to change without notice. This publication does not constitute a commitment on the part of Ribbon. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Ribbon assumes no liability resulting from technical or editorial errors or omissions, or for any damages whatsoever resulting from the furnishing, performance, or use of the information contained herein. Ribbon reserves the right to make changes to this publication and to Ribbon products without notice in its sole discretion. This publication is not meant to define any interfaces between Ribbon products and any third-party hardware or software products.

Warranties

THIS INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT SHALL RIBBON BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR PERFORMANCE OF THIS INFORMATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Compliance with Applicable Laws and Export Control Laws

The information in this publication is subject to all applicable U.S. federal, state, and local laws. The customer use, distribution, and transfer of any technical information shall be in compliance with all applicable export and import laws and regulations. All Ribbon products and publications are commercial in nature; and the use, duplication, or disclosure by the United States Government is subject to the restrictions set forth in DFARS 252.227-7013 and FAR 52.227-19.

Trademarks

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

UNCONTROLLED COPY:

The original content is stored in an electronic database and is "write protected"; it may be altered only by authorized persons. While copies may be printed, it is not recommended. Viewing of the original content electronically ensures access to the current content. Any hardcopies taken must be regarded as uncontrolled copies.

Ribbon Application Management Platform 24.12R1 Release Notes

Contents

- [About Ribbon Application Management Platform Release Notes](#)
 - [Release Notes Use and Distribution](#)
 - [Associated Ribbon Announcements](#)
- [Ribbon Application Management Platform](#)
 - [Compatibility with Ribbon Products](#)
- [New Features and Functionalities](#)
 - [New Features in Release 24.12.00R001](#)
 - [New Features in Previous Releases](#)
- [SOAP API Deprecation Notice](#)
- [Security Vulnerabilities](#)
- [Hardware and Software Requirements](#)
 - [Software Bundles](#)
 - [Ribbon OEM Host Operating System \(ROHOS\)](#)
 - [App Service](#)
- [Upgrade Notes](#)
- [Migration Notes](#)
- [Checksums and ID Details](#)
- [Resolved Issues](#)
 - [RAMP 24.12.00R001](#)
 - [RAMP 24.12.00R000](#)
 - [RAMP 24.09.00R001](#)
- [Known Issues](#)
- [Known Limitations](#)

About Ribbon Application Management Platform Release Notes

This document describes new features, latest hardware and software requirements, known limitations and other pertinent release information for the latest release of the Ribbon Application Management Platform.

Note

All Ribbon bugs reported by the customers on a given software release are fixed in the latest release of that software release branch.

To view and download the latest End of Product Sale (EoPS) and other End Of Life (EOL) notices, open a web browser and navigate to the Resource Library on the corporate website (<https://ribboncommunications.com/company/get-help/resource-library>)

Release Notes Use and Distribution

Ribbon product release notes are protected under the copyright laws of the United States of America. This work contains proprietary information of [Ribbon Communications](#). Use, disclosure or reproduction in any form is strictly prohibited without prior authorization from [Ribbon Communications](#).

Associated Ribbon Announcements

The following Ribbon announcements (formerly known as WBAs) are referenced in this release note:

Warning-24-000008211: FM process restart issue post switchover in the RAMP GR.

Note: If you use RAMP GR on a pre-23.12 release, apply this WBA and upgrade to 24.12R1.

To view/subscribe to announcements (Warnings, Bulletins, Alerts, or PCNs):

1. [Click here](#) to go to the "Announcements" page in the Ribbon Support Portal.
2. Enter the announcement number (last eight numbers) in the search field and click the magnifying glass icon (or press **Return**). You can alternatively use the filter tools located on the left side of the screen to narrow your search.

Problems or Questions

For problems or questions, contact the Global Support Assistance Center:

Ribbon Support Portal: <https://ribboncommunications.com/services/ribbon-support-portal>

Voice: +1-833-RIBBON1 (1-833-742-2661)

Ribbon Application Management Platform

The Ribbon Application Management Platform (RAMP) provides a centralized, cloud-optimized solution for the efficient management of every Ribbon element in a customer's network. RAMP provides a complete Fault, Configuration, Accounting, Performance, and Security solution with a robust portfolio of management and provisioning tools that allow service providers and enterprises to easily perform management of their network, quickly remediate issues, leading to an improved customer experience and reduced costs.

Compatibility with Ribbon Products

Refer to the [Ribbon Application Management Platform Interoperability Matrix](#) for the latest and minimum compatible product versions supporting this release.

Ribbon Elements Supported

- Application Server
- Centralized Policy and Routing Server (PSX), and PSX Software Edition (PSX SWe)
- C20 Call Session Controller
- C3 Call Controller
- Data stream Integrator (DSI)
- Dell Servers
- Diameter Signaling Controller (DSC)
- Edge 8000
- EdgeMarc
- General Media Server (GMS)
- G5 Line Access Gateway
- G6 Universal Gateway
- G9 Media Gateway
- Layer 2 Manager (L2MGR)
- Multimedia Resource Function Processor (MRFP)
- Ribbon Media Gateway (GSX9000)
- Session Border Controller Software Edition (SBC SWe)
- Session Border Controller 5400
- Session Border Controller 7000
- Session Border Controller CNe
- Session Border Controller SWe Edge
- Session Border Controller 1000
- Session Border Controller 2000
- Signaling Gateway (SGX4000)
- SIP Load Balancer

Note

In the RAMP 24.12 GUI or documentation, any instance of the SBC Core refers to **SBC 7000/5400/SWe/CNe** and **MRFP** products, unless otherwise noted. Any instance of the SBC Edge refers to the **SBC1000/2000** and **SBC SWe Edge**.

Note

The following table lists the supported/unsupported EdgeMarc Subtypes:

Supported EdgeMarc Subtypes

- 302
- 304
- 2900
- 2900A
- 2900E
- 2900PoE
- 4550v2
- 4551
- 4552
- 4555
- 4600T4
- 4601
- 4603
- 4604T4
- 4608PoE
- 4700
- 4701
- 4750
- 4751
- 4800
- 4808
- 4806v2
- 4808v2
- 4808
- 6000
- 7301
- 7400
- 8000

Tip

When upgrading your network, ensure to upgrade each product to the most current release to take advantage of the latest features, enhancements, and fixes.

New Features and Functionalities

New Features in Release 24.12.00R001

There are no new features in this release.

Note

Beginning with the RAMP 24.12 release, the node-level postpaid reports are disabled by default, and the RAMP generates only the network-level postpaid reports. To enable the node-level postpaid reports, a new setting, "Generate Node-Level Postpaid Reports," is introduced to the LM administration page.

New Features in Previous Releases

For the list of features in previous 24.xx.xx releases, refer to the following release note:

- [New in RAMP 24.12R000](#)
- [New in RAMP 24.09R001](#)
- [New in RAMP 24.06R000](#)
- [New in RAMP 24.03R000](#)

SOAP API Deprecation Notice

The RAMP SOAP API support for the SBC Core is only supported for EMS migrations to allow backwards compatibility. The RAMP SOAP API supports the SBC functionality through the SBC release 12.x. The functionality is targeted to deprecate in Q4 2024. Users need to migrate to the REST API for the SBC API access.

Security Vulnerabilities

The following security vulnerabilities (CVEs) are fixed in this release:

Note

The severity is based on the CVSSv3.x scores. For more details about the individual CVE, refer to <https://nvd.nist.gov/vuln/search>. These are listed verified CVEs in 24.09R1 Release.

Severity	CVE numbers
Critical	CVE-2022-42889, CVE-2022-42920
High	CVE-2022-45688, CVE-2024-47554, CVE-2023-5072, CVE-2013-4002, CVE-2012-0881, CVE-2022-25647
Medium	CVE-2021-29425, CVE-2020-13956, CVE-2022-45146, CVE-2015-5262, CVE-2020-14338, CVE-2022-23437, CVE-2009-2625, CVE-2023-2976, CVE-2015-5262, CVE-2021-38153, CVE-2024-29857, CVE-2024-30171
Low	CVE-2020-8908

Hardware and Software Requirements

This section provides information about any release-specific Ribbon Application Management Platform software requirements.

Note

- RAMP 24.12R001 is minimum supported on 16 vCPU. Contact Ribbon Support team for the upgrade-related assistance.
- The disk size is changed from 130GB to 150GB for the RAMP 23.09R000 and above releases. The templates are updated to reflect this change.
- Refer to the update, Warning-23-000007983.

Software Bundles

Download the RAMP 24.12R001 software bundle from the Support Portal.

The following files are delivered as part of RAMP 24.12R001:

Files	Environment	Description
AMI ID = ami-0399176320fd6c41d templates.tar	AWS	RAMP install/upgrade on AWS
AppServices-24.12.00R001-B7796_vmCCS-1.14.3-x86_64.qcow2 AppServices-24.12.00R001-B7796_vmCCS-1.14.3-x86_64.vmdk AppServices-configDrive.img heat_template_etcd.yml AppServices-snmpMIBs.tar.gz	App Service	etcd deployment for auto switchover
InsightAllMibs.tar	Generic	MIB files
ramp-hostcheck-V24.12.00R001.tar.gz	KVM	Hostchecker tool for RAMP deployment
ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.img ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588-2025-01-09.vhd	Azure	RAMP install/upgrade on Azure
ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.qcow2 ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.qcow2.md5 templates.tar	OpenStack	Image for RAMP install/upgrade on OpenStack

Files	Environment	Description
ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.qcow2 ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.qcow2.md5 rampBootstrap-V24.12.00R001_RHEL.tar configDriveImgDeployment.img	KVM	RAMP install/upgrade on KVM
ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.vmdk ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.vmdk.md5 ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.ovf configDriveImgDeployment.img rampBootstrap-V24.12.00R001_RHEL.tar	VMware	RAMP install/upgrade on VMware
ramp-V24.12.00R001-rhv_ansible_playbooks.tar.gz ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.qcow2	RHV	RAMP install/upgrade on RHV
ramp-V24.12.00R001-SOL1-v361-Generic.csar ramp-V24.12.00R001-SOL1-v361-marketplaceStructure.zip	VNFD	RAMP deployment with VNFM
rampBootstrap-V24.12.00R001_RHEL.tar	Migration Upgrade	For the EMS to RAMP migration and upgrade

Note

- The 24.12.00R001 release supports deployment of the RAMP in Cloud Native Functionality (CNe). For the RAMP CNe installation/deployments, contact your Ribbon sales representative.
- If you are running the EMS/RAMP on the RHV platform, contact your Ribbon sales representative for upgrade/migration.

Ribbon OEM Host Operating System (ROHOS)

The minimum ROHOS version and the Dell firmware versions compatible with the RAMP 24.12.00R001 release are provided below:

ROHOS	Dell Firmware
02.08.16 or higher ¹	<ul style="list-style-type: none"> • iDRAC: iDRAC9 • BIOS: 5.00.20.10 • Firmware: 2.17.1

ROHOS	Dell Firmware
Tested Version	VERSION=02.08.26 VERSION=02.08.23

*1For ROHOS versions higher than 02.08.16, refer to the [ROHOS Release Notes](#) for supported iDRAC, BIOS, and firmware versions.

App Service

Component	VNF	CNF
RAMP	24.12.00R001-588	24.12.00R000-78
ETCD	AppServices-24.12.00R001-B7796_vmCCS-1.14.3-x86_64	helm version: 1.4.0
		bitnami/etcd: 3.5.16
		bitnami/kubectl: 1.31.1
		OBS: 3.2.2

Key Changes:

- Updated the OS patches
- update prometheus-autoconfig to 1.8.16
- update vmCCS to 1.14.1
- PLTF-5009: update third-party containers
 - Update etcd to 3.5.16
 - Update prometheus to 2.54.1
- PLTF-5164: resize /dev/sda3 instead of /dev/sda2 after CommonOS added Secure Boot support
- PLTF-5565: AppServices - Failure to upgrade the ETCD in the IPv6 environment without persistence

Known Issues (VNF)

None.

Known Issues (CNe)

None.

Upgrade Notes

The following upgrade paths are supported in this release.

Release	Platform					
	KVM	VMware	OpenStack	AWS	Azure	CNe
23.09.00R000	Yes	Yes	Yes	Yes	Yes	No
23.12.00R000	Yes	Yes	Yes	Yes	Yes	No
24.03.00R000	Yes	Yes	Yes	Yes	Yes	No
24.03.00R001	Yes	Yes	Yes	Yes	Yes	No
24.03.00R002	Yes	Yes	Yes	Yes	Yes	No
24.06.00R000	Yes	Yes	Yes	Yes	Yes	Yes
24.09.00R000	Yes	Yes	Yes	Yes	Yes	Yes
24.09.00R001	Yes	Yes	Yes	Yes	Yes	Yes

Note

To upgrade the RAMP from a pre-23.09 release, contact the Ribbon Support team.

Migration Notes

The following migration paths are supported in this release.

Platform	EMS Release
KVM	15.X, 14.x, 13.x
VMware	15.X, 14.x, 13.x
OpenStack	15.X, 14.x, 13.x
AWS	15.X, 14.x, 13.x

Note

Reach out to Ribbon Professional Service for more information about the EMS-to-RAMP Migration process.

Note

Current and last release Resolved and Known issues listed in this Release notes. For issues fixed in previous releases, refer to the corresponding Release Notes.

Checksums and ID Details

The installation files have the following checksums:

Md5sum	Size	File Name
c9a72c2ade312559b04151656d90e882	14719057920	ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.qcow2
c53938f1777788da7d208792e4ac13c7	5897256960	AppServices-24.12.00R001-B7796_vmCCS-1.14.3-x86_64.qcow2
cf8b49355d652293360398cace421fba	3329820160	AppServices-24.12.00R001-B7796_vmCCS-1.14.3-x86_64.vmdk
33cec2c70bed47b48f6353cbeb481a32	131072	AppServices-configDrive.img
e27f843d9727593eb26cb79e0f717c37	24627	AppServices-snmpMIBs.tar.gz
c9e4c69c1bcadcf97de1aa3fa925b603	1048576	configDriveImgDeployment.img
acc64f3b7d95ec50467a2bf503842358	77199360	InsightAllMibs.tar
2441ac548a94304b527f0ba59bc18bd5	3553280	rampBootstrap-V24.12.00R001_RHEL.tar
b78eb482d46349f7104a980fd7b19844	1914209	ramp-hostcheck-V24.12.00R001.tar.gz
95cca1f55a15fbad92889fa72a3a179a	5552	ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.ovf
0fb0b511ceab303221696d0ac62a3fb5	14396068864	ramp-V24.12.00R001-RHEL-8.10.102-187-x86_64_588.vmdk
979248e199b09a04e7eb49d98acfd0ad	1879958	ramp-V24.12.00R001-rhv_ansible_playbooks.tar.gz
05d2e996dbe58d8f06faa3042ee94ceb	3122487	ramp-V24.12.00R001-SOL1-v361-Generic.csar
f9001f0e7903c850f0f2c28aebb12c2f	14581386012	ramp-V24.12.00R001-SOL1-v361-marketplaceStructure.zip
8f60a4abc2fea4bb563d8ed6858b9029	254023680	sbci_api_doc_v12_01.04.tar
425e049d2a6d381118bf210fa9765a98	153600	templates.tar
baa38a69492539bbdc429f36d7c00804	50822	heat_template_etcd.yml
3cfe654ecbb95cddd4471de9234fef68	133633282	testTools-V24.12.00R001.tar.gz

Resolved Issues

RAMP 24.12.00R001

The following issues are resolved in RAMP 24.12R1 release:

Severity 1 Issue

There are no resolved severity 1 issues in this release.

Severity 2 and 3 Issues

The following table lists the resolved severity 2 and 3 issues in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-13718	N/A	3	The <code>find</code> command for the trunk group fails for PSX 16.1.4.	Impact Statement: Unable to perform the find operation through the CLI for trunk group search. Resolution Details: A new column was added to the trunk group in PSX 16.1.4 without the required wrapper. Modified the code to resolve the issue.
AFM-13754	N/A	3	STI Service Definition: The flag, <code>Fallback to Reason Code</code> if Error Id not present on the PSX fails to work as expected.	Impact Statement: The flag, <code>Fallback to Reason Code</code> if Error Id not present on the PSX fails to work as expected. Resolution Details: Modified the code to resolve the issue.

RAMP 24.12.00R000

The following issues are resolved in RAMP 24.12R0 release:

Severity 1 Issue

The following table lists the resolved severity 1 issue in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-10746	NA	1	Unable to run the STI signing and verification on the same call.	Impact Statement: Unable to perform the STI signing and verification on the same call. Resolution Details: The RAMP 24.12 is enhanced to support STI signing and verification on the same call.

Severity 2 and 3 Issues

The following table lists the resolved severity 2 and 3 issues in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-8977	NA	3	The RAMP displays database and Kafka exceptions when users open 50 event lists.	Impact Statement: N/A Resolution Details: Modified the code to handle the exceptions.
AFM-9984	NA	3	The RAMP generates alarms for the Agent version mismatch.	Impact Statement: The RAMP generates the sonusV2VfyMgrApplVersionFailNot ification / sonusV2VfyMgrAgentVersionFailNo tification alarms when the RAMP agent restarts. Resolution Details: Removed obsolete alarms to resolve the issue.
AFM-10048	NA	3	After implementing the relocateGR on the RAMP 23.09, the node turns offline, and relocation fails (Random occurrence).	Impact Statement: Unlock for the Peer fails due to the timeout, resulting in relocation failure. Resolution Details: Increased the timeout value to 600 seconds while performing the unlock operation.
AFM-10369	NA	3	The RAMP waits five minutes to display the failure status for the Device Backup job.	Impact Statement: The User must wait five minutes to see the failure status on the GUI. Resolution Details: Modified the code to handle the error scenarios and report the errors correctly.
AFM-11142	NA	3	The Instanceup fails with the error, "Node is unregistered" when the SBC Direct Single node is started after it is unregistered from the RAMP.	Impact Statement: The Instanceup fails with the error, "Node is unregistered". Resolution Details: Modified the code to update both the node status and host status to "Partially Registered" status when the active node re-registers.
AFM-11473	NA	3	Realign the Tab key usage flow for the User Creation screen.	Impact Statement: The Tab key usage flow to navigate the User Creation screen is not correctly aligned. Resolution Details: Updated the form field elements to place the "username", "password", and "re-enter password" fields in one div element on the left hand side and the "tenant" and the "description" on the right-hand side.
AFM-11581	NA	2	The GSX Navigator and Task Configuration buttons do not respond when the network is slow.	Impact Statement: The GSX Navigator and Task Configuration buttons use a flat styling without any hover or click effect. Because of this, the user could not tell if an operation (click) was happening, giving the impression that buttons were not responding when the network was slow. Resolution Details: Removed the styling to resolve the issue.

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-11788	NA	3	Document the etcd upgrade procedure with the RAMP upgrade procedure.	<p>Impact Statement: The etcd upgrade procedure is not available.</p> <p>Resolution Details: Documented the etcd upgrade procedure. For more information, refer to Upgrading etcd.</p>
AFM-11871	NA	2	The EdgeMarc PCAP and Diagnostic Snapshot do not work on the public IP address setup.	<p>Impact Statement: Certain EdgeMarc features were not working when deploying the EdgeMarc with a Public IP.</p> <p>Resolution Details: Modified the code to resolve this issue.</p>
AFM-11918	NA	2	The PSX Manager <code>Jsonlp</code> file download failings after migrating to the RAMP.	<p>Impact Statement: The <code>proxyPreferredIp</code> value was missing after a migration, which caused a PSX Manager launch failure.</p> <p>Resolution Details: Modified the code to resolve this issue.</p>
AFM-11996	NA	3	Provide support in including "commas" in the exported PM CSV file.	<p>Impact Statement: The RAMP does not support including "commas" in the exported PM CSV file.</p> <p>Resolution Details: Modified the code to support including "commas" in the exported PM CSV file.</p>
AFM-12033	NA	3	RAMP 24.06R0: Security scan vulnerability.	<p>Impact Statement: The RAMP reports vulnerabilities during the security scan.</p> <p>Resolution Details: Handled all the reported vulnerabilities.</p>
AFM-12035	NA	3	A missing line item for the SBC SWe Edge HA fails License Profile creation.	<p>Impact Statement: When creating a license profile for the SBC SWe Edge, The user is unable to generate the license since the line item SBC-SWE-EDGE-INSTANCE-D contains a description that says, "SWeEdge HA is not available to select."</p> <p>Resolution Details: Modified the code to resolve the issue.</p>
AFM-12075	NA	3	Allow the CLI session to the non-SSO SBC.	<p>Impact Statement: The RAMP user can log in through the CLI as an admin user to the older version of the SBCs (pre-11.1 versions) that do not support the SSO login.</p> <p>Resolution Details: Introduced new property to both configuration file and User Interface to choose whether to enable/disable CLI access to older non-SSO SBCs based on deployment.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12098	NA	2	Data miss aligned in the RAMP Task Configurator IP Trunk Group.	<p>Impact Statement: Data that is misaligned in the RAMP Task Configurator for Selected IP Trunk Group displays incorrect data for certain fields.</p> <p>Resolution Details: Modified the code to prevent argument value misalignment when creating an IP TG while an empty argument is added to the task instance info,</p>
AFM-12105	NA	3	Unable to dump the core files since the directory, <code>/home/core</code> does not exist.	<p>Impact Statement: The directory, <code>/home/core</code> is missing in the RAMP, which results in failure to store core files during unexpected crashes.</p> <p>Resolution Details: Added the missing directory to resolve the issue.</p>
AFM-12256	NA	3	The "Apply" and "OK" buttons perform the same functionality in the RAMP GUI.	<p>Impact Statement: The functionality of the "Apply" and "OK" buttons overlap.</p> <p>Resolution Details: Removed the "Apply" button from the Create Report Schedule form since it only applies to the Edit form.</p>
AFM-12286	NA	3	Add the <code>sonusHostDiskMonHardErrorNotification</code> alarm to the RAMP documentation.	<p>Impact Statement: The <code>sonusHostDiskMonHardErrorNotification</code> alarm was not available in the RAMP documentation.</p> <p>Resolution Details: Added the <code>sonusHostDiskMonHardErrorNotification</code> alarm page to the RAMP documentation.</p> <p>For more information, refer to sonusHostDiskMonHardErrorNotification.</p>
AFM-12460	NA	3	The PM collection fails for the Edge nodes after migrating from the EMS to the RAMP.	<p>Impact Statement: The PM collection does not work on the Edge node after an EMS to RAMP migration.</p> <p>Resolution Details: Added the missing <code>id_ecdsa.pub</code> key to the <code>~/.ssh/authorized_keys</code> entry for the Insight user. The EV uses this Insight user's SSH identity to connect to the SFTP without a password.</p>
AFM-12472	NA	3	Document the Character Limitation for the Profile Name.	<p>Impact Statement: The Character limitation for the Profile Name was mentioned in the documentation.</p> <p>Resolution Details: Updated the document with a note stating that the collection profile name must contain alphanumeric characters with a maximum length of 23. For more information, refer to Define Statistics to Collect.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12484	NA	3	The RAMP generates an error message stating, "Password will Expire in -19898 day(s)."	<p>Impact Statement: The user receives a password expiry message that prevents logging in to the system.</p> <p>Resolution Details:</p> <p>Modified the code to handle the scenario. With this resolution, when the user updates the LOCAL realm value for the password nonreusable time period and password aging, the following conditions are met.</p> <ul style="list-style-type: none"> • <code>PassHistPurgeBeforeTime >= PassReusableTimePeriod</code> • <code>PassHistPurgeBeforeTime >= PassAging >= PassExpWarning</code>
AFM-12496	NA	3	The PM CSV purger script generates authentication error.	<p>Impact Statement: Unable to implement the purger job for the CSV files.</p> <p>Resolution Details: Modified the script to run with the correct permissions.</p>
AFM-12498	NA	3	RAMP JITC/FIPS: The RAMP generates errors when running the JBoss CLI commands.	<p>Impact Statement: The RAMP generates log errors while processing the JBoss CLI command. This error does not impact any RAMP functionality.</p> <p>Resolution Details: Modified the application to handle the error scenario.</p>
AFM-12507	NA	2	The RAMP SGX discovery function does not work properly	<p>Impact Statement: The SGX discovery fails after a switchover.</p> <p>Resolution Details: Modified the code to use the IPs of the second host.</p>
AFM-12508	NA	3	Enhance the <code>analyzeSystem.sh</code> script.	<p>Impact Statement: If there are multiple interfaces with similar names, the script fails since it receives network information for multiple interfaces instead of receiving it for one interface.</p> <p>Resolution Details: Modified the script to handle the scenario.</p>
AFM-12510	NA	3	Issue observed in Configuration Management Permission in Network Wide Provisioning Operations.	<p>Impact Statement: The RAMP allows the user to perform provisioning, backup, and upgrade without holding the Configuration Management permission.</p> <p>Resolution Details: Modified the code to list the nodes based on the user role.</p>
AFM-12511	NA	3	The RAMP fails to query the server error for the AD user.	<p>Impact Statement: The RAMP fails to query the server error due to a missing step in the document.</p> <p>Resolution Details: Updated the document to add the missing step. For more information, refer to Post-Upgrade Procedures for RAMP.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12549	NA	3	Fields in the inventory report contain NULL for the primary SBC node name.	<p>Impact Statement: The Inventory Report contains NULL for the primary SBC HA hostname.</p> <p>Resolution Details: Modified the code to set the correct hostname for the SBC HA.</p>
AFM-12592	NA	3	Some of the commands fail in the GSX CLI through the RAMP.	<p>Impact Statement: The Incorrect role, gsx.prov, was used for an auth check when running these commands through the GSX CLI in the RAMP, resulting in provisioning failures.</p> <p>Resolution Details: Updated the role to devices.prov.</p>
AFM-12595	AFM-10338 (24.03)	2	The RAMP performed an automatic switchover due to a healthCheck failure on the InsightHotDeploy.	<p>Impact Statement: Occasionally, the system resources memory/CPU goes high, which causes the Linux OOM killer to kick in and kill the INSIGHT JBoss process, initiating a SWACT.</p> <p>Resolution Details: To avoid a SWAT, the INSIGHT JBoss process's OOM score is reduced to "-300" whenever it is spawned. This ensures the Linux OOM killer does not pick the INSIGHT JBoss process, which avoids SWACT. Even if killed, the rest of the processes restart on the same instance within seconds.</p>
AFM-12597	NA	2	Gaps in the RAMP SBC HA communication when the SBC switchover results in node offline.	<p>Impact Statement:</p> <ol style="list-style-type: none"> 1. For a non-cloud SBC HA, when the active reboots, the automatic rediscovery fails for both hosts, and the node stays in a Registered - Offline state. 2. For a cloud SBC, even though automatic rediscovery succeeds for the new active node after an SBC switchover, the primary IP address is not updated to the currently active host IP address, and the node stays in a Registered - Offline state. <p>Resolution Details: Modified the code to add a retry for the non-cloud SBC.</p>
AFM-12685	NA	2	Improve the <code>manualBackup.sh</code> script.	<p>Impact Statement: A backup lasts a very long time because of the large number of parquet files collected in the backup.</p> <p>Resolution Details: The code is modified to include an option to skip the PM parquet files during the backup.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12761	AFM-12521 (24.03R3)	2	The PM export fails in large networks with the "Argument list too long" error.	<p>Impact Statement: Failed to export the PM data to multiple locations when the number of devices are approximately 1500 and the device names are long.</p> <p>Resolution Details: Modified the code to write the arguments to the file and pass the filename as an argument to the export script to avoid the "Argument list too long" error.</p>
AFM-12875	NA	3	The RAMP installation on Azure generates an error on the first deployment.	<p>Impact Statement: Some steps in the customer documentation are not clear or are missing, causing a RAMP installation failure on Azure.</p> <p>Resolution Details: Updated the document Instantiate a Standalone RAMP Instance on Azure.</p>
AFM-12891	NA	2	The RAMP PM statistics are not visible in the OBF backend.	<p>Impact Statement: Missing PM data in the OBF.</p> <p>Resolution Details: Modified the code to successfully copy the PM metric <code>tarball</code> file from the RAMP to the telemetry-agent's PVC without permission issues.</p>
AFM-12933	NA	3	The ETCD CNF Health Check documentation update.	<p>Impact Statement: Enhance the product documentation to include the ETCD CNF Health Check for CNF deployments.</p> <p>Resolution Details: Updated the product documentation. For more information, refer to RAMP CNF etcd Health Check.</p>
AFM-12938	NA	2	RAMP CNF: RAMP FMaaS ETSI format update.	<p>Impact Statement: Enhance alarm mapping to use the ETSI format.</p> <p>Resolution Details: Enhanced alarm mapping to use the ETSI format.</p>
AFM-12944	NA	2	The SBC API deployment failures cause a failure during the RAMP startup.	<p>Impact Statement: The RAMP startup fails because some services do not come up within the stipulated timeframe.</p> <p>Resolution Details: Modified the code to start some services in the background and increase the timeout to avoid startup failures.</p>
AFM-12949	NA	2	The Node Lock License association is missing after a migration.	<p>Impact Statement: The Node Lock License association is missing after migrating from the EMS 14.1.6 to the RAMP 24.03.R2.</p> <p>Resolution Details: Modified the code to obtain all nodes from the Auth API on the first restart after a migration to prevent the LM service from starting early before the data is available.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12951	AFM-12489 (24.03R3)	2	The RAMP fails to generate SBC PMs for the configured remote destinations, SevOne, and RA.	<p>Impact Statement: Downstream was not receiving consistent PM data from the RAMP.</p> <p>Resolution Details: The code is updated to handle the scenario where the Export service does not copy files to the RA since the exporter-service is writing a Kafka message not present in the Kafka topic due to a race condition.</p>
AFM-12984	NA	2	RAMP 24.03R2: The RAMP fails to generate post-paid reports.	<p>Impact Statement: The RAMP is not receiving the post-paid reports, resulting in a report processing failure. The RAMP failed to send the report because an OOM occurred while processing the report.</p> <p>Resolution Details: Changed the design to fetch the data in the sample so that the LM fetches the one-day data in three iterations, writes it to a file and processes it. This design allows the processing of large data without an OOM.</p>
AFM-13038	NA	2	Errors observed in TrunkGroupSummaryReport, TotalConfiguredDS0s, and TotalEnabledDS0s columns.	<p>Impact Statement: The RAMP fails to report the correct data to the user.</p> <p>Resolution Details: Modified the code to fetch and process the PM data correctly.</p>
AFM-13094	NA	2	Migration: localhost discovery fails post migration with different IP address and hostname.	<p>Impact Statement: The RAMP discovery fails with an error "Certificates do not conform to algorithm constraints".</p> <p>Resolution Details: The code is modified to restore the agent keystore from the EMS to RAMP if the keystore includes the MD5withRSA signature algorithm. If the CA-signed agent certificate is used, re-generate CSR the and re-import the certificate to the agent keystore.</p>
AFM-13198	NA	3	Update the documented procedure "Configure RAMP for TLS Communication".	<p>Impact Statement: The missing steps prevented RAMP from pushing licensing data to the SBC for a JITC-enabled RAMP.</p> <p>Resolution Details: Updated the procedure with the required steps. For more information, refer to Configure RAMP for TLS Communication.</p>

RAMP 24.09.00R001

The following issue is resolved in RAMP 24.09R1 release:

Severity 1 Issue

The following table lists the resolved severity 1 issue in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
PLTF-4086	N/A	1	Security vulnerabilities in the RAMP (23.09).	Impact Statement: Security vulnerabilities are observed in various scans. Resolution Details: Resolved the critical vulnerabilities.

Severity 2 and 3 Issues

The following table lists the resolved severity 2 and 3 issues in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-7376	N/A	3	The RAMP CLI does not disconnect after the configured idle timeout period.	Impact Statement: The CLI session stays active even after the configured idle timeout. Resolution Details: Modified the code to disconnect the EMS CLI session when the CLI inactivity exceeds the configured disconnect time.
AFM-7461	N/A	2	The RAMP GUI session does not expire when the user performs actions on the same page after a session timeout.	Impact Statement: The RAMP GUI session does not disconnect when users perform actions on a page after a session timeout. Resolution Details: Modified the code to log the user out on a session timeout.
AFM-8412	N/A	3	Augment documentation for the ETCD operations.	Impact Statement: Missing ETCD documentation for detailed scenarios and commands to debug the system. Resolution Details: The following documents are updated: <ul style="list-style-type: none"> • Import Previously Generated TLS Certificate • GSX Upgrade Automation • RAMP GR Auto-Switchover Troubleshooting
AFM-8493	N/A	3	The <code>jboss-cli.sh</code> script requires credentials for editing without enabling the FIPS.	Impact Statement: The <code>jboss-cli.sh</code> script requires credentials to perform any operation. Resolution Details: Modified the code to enable silent authentication by default for the <code>jboss-cli.sh</code> . Also, included a script to disable the silent authentication. Updated the following documents: <ul style="list-style-type: none"> • Configure Silent Auth for Jboss CLI • Reset Admin Password for Jboss CLI • Change Log Level

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-10328	N/A	2	Generate the CSR with RSA key size of 4096 bit.	<p>Impact Statement: Users cannot generate a CSR with a key size of 2048 bits.</p> <p>Resolution Details: Modified the CSR configuration <code>manageCert</code> script to generate CSRs with a key size between 2048 and 4096 bits.</p>
AFM-10338	N/A	3	Automatic switchover occurs due to high Insight CPU usage (random occurrence).	<p>Impact Statement: An automatic switchover occurs due to a high Insight CPU usage (random occurrence).</p> <p>Resolution Details: The code is modified to reduce the memory usage in the FM, disable the <code>settroubleshootd</code> service, and reduce the Insight process OOM score to ensure the OOM killer does not pick it up in case of intermittent high system memory.</p>
AFM-10393	N/A	3	The GSX timer-based alarm on the RAMP does not clear automatically.	<p>Impact Statement: A few alarms from the legacy devices do not clear automatically.</p> <p>Resolution Details: Modified the code to support the timer alarms. These alarms clear automatically.</p>
AFM-10408	N/A	2	Certificate-based authentication for the REST API in the RAMP.	<p>Impact Statement: Use the certificate-based authentication for the REST API in the RAMP.</p> <p>Resolution Details: The product documentation is updated to provide more information on using certificate authentication for the REST APIs. For more information, refer to:</p> <ul style="list-style-type: none"> • Example API Requests and Responses • Importing Third Party Certificates
AFM-10511	N/A	2	The <code>HostSwapUsageRisingThreshold</code> alarm stays in the idle state.	<p>Impact Statement: The RAMP generates <code>HostSwapUsageRisingThreshold</code> alarm during an idle state.</p> <p>Resolution Details: This is an expected Red Hat Linux behavior and does not affect any RAMP functionality. The severity of the alarm is reduced to "Informational".</p>
AFM-10560	N/A	2	The RAMP switchovers from Source to Target due to high CPU usage.	<p>Impact Statement: The RAMP switches over due to high CPU usage.</p> <p>Resolution Details: Modified the code to reduce the memory usage in the FM. Disabled the <code>settroubleshootd</code> service and reduced the Insight process OOM score to ensure the OOM killer does not pick it up during intermittent high system memory.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-10725	N/A	2	The RAMP fails to export all interval data to Ribbon Analytics.	<p>Impact Statement: The RAMP fails to export all the interval data to the RA if the export time is extended.</p> <p>Resolution Details: Modified the code to schedule the failed tasks immediately instead of waiting for the next interval.</p>
AFM-11097	N/A	2	RAMP 24.06: Cipher package Nessus scan vulnerabilities.	<p>Impact Statement: Vulnerabilities are observed in various scans.</p> <p>Resolution Details: Resolved critical vulnerabilities.</p>
AFM-11229	N/A	2	Observed the <code>sonusV2VfyMgrApplVersionFailNotification / sonusV2VfyMgrAgentVersionFailNotification</code> alarm after migrating from the EMS.	<p>Impact Statement: A few legacy VfyMgr alarms are present after migrating from the EMS.</p> <p>Resolution Details: Removed the legacy alarms since the RAMP automatically rediscovers a node if it goes offline and returns. These alarms are no longer needed.</p>
AFM-11355	N/A	2	RAMP support for all EdgeMarc devices.	<p>Impact Statement: A few EdgeMarc device versions were missed in the RAMP.</p> <p>Resolution Details: Added support for the EdgeMarc 7400 model.</p>
AFM-11370	N/A	3	The RAMP fails to retain the Force Password Change option after a migration.	<p>Impact Statement: The user settings of the Force Password Change option are not retained/updated after the migration from the EMS to the RAMP.</p> <p>Resolution Details: The RAMP uses double negation to understand the EMS DB equivalent field, <code>exempt_aging forcepasswordchange</code> value in the RAMP. The EMS-mapped field is <code>password_change</code>. If the Force Password Change option is enabled on the EMS, <code>password_change</code> is 3 in the EMS DB. However, the RAMP migration script always mapped the field with <code>!= 0</code> and set it to "True" for the <code>forcepasswordchange</code>. An explicit check in the RAMP migration script is performed to check for the values and fix them.</p>
AFM-11378	N/A	3	Schema mismatch causing FM to restart after an upgrade from 23.09 to 24.03.	<p>Impact Statement: When the RAMP is upgraded from 23.09 to later versions, a Kafka message schema compatibility issue is observed, as the old schema is registered with the schema registry. This schema gets registered with the schema registry when the UI operations are performed on the alarms received from the SBC and the DSC.</p> <p>Resolution Details: The fix for this issue is communicated through a bulletin and provided a patch to apply after the upgrade from 23.09 to 24.03 and before GR setup.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-11381	N/A	3	The RAMP GUI TLS certificate (2k vs 4k).	<p>Impact Statement: The user cannot generate the CSR with a key size greater than 2048.</p> <p>Resolution Details: The script <code>manageCert</code> is modified to support the CSR generation with a key size between 2048 and 4096 bits. The key size is configurable in the CSR configuration.</p>
AFM-11473	N/A	2	Modify the User Creation tab to make it more user-friendly.	<p>Impact Statement: After entering the password in the Password field, the user must press the Tab key multiple times to navigate to the Re-Enter Password field.</p> <p>Resolution Details: Changed the form field elements to place the Username, Password, and Re-Enter Password fields in the left div and Tenant and Description fields in the right div.</p>
AFM-11573	N/A	2	Duplicated Resource Groups are present in the user Interface.	<p>Impact Statement: Duplicated Resource Groups are present in the user interface.</p> <p>Resolution Details: Modified the code to disable the Save button once it is clicked and enable when the API response is complete.</p>
AFM-11638	N/A	3	The RAMP fails to populate the Trunk Group when selecting the Daily PM.	<p>Impact Statement: The PSTN Index/trunk group name is not loaded in the PM reports page when the user selects the granularity "Hourly" for GSX Nodes.</p> <p>Resolution Details: The user's parquet included data with empty trunk group names. The <code>dropna</code> method call on the dataframe did not/will not remove these empty columns/rows. Hence, <code>getIndexValues.py</code> returned an empty <code>trunkgroupname</code> for all PSTN Indexes. Replaced the empty strings with 'NaN' values so that the <code>dropna</code> method drops those rows.</p>
AFM-11653	N/A	3	The PM Administration fails to work after migrating from the EMS 13.2.3 to the RAMP 24.06.	<p>Impact Statement: The PM Administration-related values were not migrated.</p> <p>Resolution Details: Updated the migration process to include these values during the migration.</p>
AFM-11713	N/A	2	The EMS alarm's <code>varbind</code> order differs from the order defined in the MIB.	<p>Impact Statement: The <code>varbind</code> order mismatch leads to the NBI issue.</p> <p>Resolution Details: Modified the code to align the <code>varbind</code> order correctly.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-11771	N/A	2	Generate the <code>authKey</code> and <code>privKey</code> using the RAMP.	<p>Impact Statement: The <code>snmpkey</code> package is missing from the RAMP.</p> <p>Resolution Details: Added <code>snmpkey</code> package to the RAMP.</p>
AFM-11778	N/A	2	Agent - PSX CNe PIPE container restarts on a fresh install.	<p>Impact Statement: The PIPE container restarts while registering to the RAMP during orchestration. The PSX was not registered to the RAMP, resulting in a PIPE container restart during the deployment. The cash used to modify the agent password occasionally exited, which led to registration failures. During the PSX registration process with the RAMP, the <code>sonusAgent</code> running on the PSX occasionally failed to log in using the given credentials. The login sequence takes more time (3-15 seconds) due to a network-induced delay. Also, the JVM parameters to set the Initial <code>Heapsize</code> and <code>Max</code>. The outdated <code>Heapsize</code> does not work in Java 8 in the <code>jash</code> script.</p> <p>Resolution Details: Modified the code to contain the proper JVM arguments supported in Java 8 in the <code>jash</code> script.</p>
AFM-11780	N/A	2	The LDAP server FQDN resolution fails from the IPv6 RAMP when the LDAP is configured with the dual stack.	<p>Impact Statement: The RAMP CNe to LDAP server FQDN resolution fails on IPv6 deployments when the DNS resolution for the LDAP returns both the IPv4 and IPv6 addresses.</p> <p>Resolution Details: Modified the code to prefer the IPv6 address in case of IPv6 deployment.</p>
AFM-11869	N/A	2	The PM YAML files for the DSC need a refresh/update.	<p>Impact Statement: The DSC <code>Linkset</code> statistics were empty after an upgrade from DSC 22.0 to 23.0.</p> <p>Resolution Details: Added a few new attributes to the Linkset statistics related to Unit Data Service (UDTS) and Extended Unit Data Service (XUDTS). Added new YAML for the DSC version 23.0 that includes the new attributes.</p>
AFM-11871	N/A	2	The EdgeMarc PCAP Diagnostic Snapshot fails to work in the public IP setup.	<p>Impact Statement: The RAMP with a public IP different from the private IP, the PCAP, and the diagnostic snapshot were not consumed by the device.</p> <p>Resolution Details: Updated the EV service code to send public IP to the device where the device can send PCAP and diagnostic snapshot information.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-11891	N/A	2	Authorize the Configure action only through the Configuration Management Permission.	<p>Impact Statement: The RAMP permits the Configure action only if the Device Administration permission is enabled. There is no option to enable only the Configure action without allowing the other actions for the node, such as Register, Discover, Edit, Unregister, and Delete.</p> <p>Resolution Details: Modified the code to enable the Configure action if the user holds the operator permission for the Configuration Management.</p>
AFM-11939	N/A	2	Object store does not stabilize on the VMware RAMP.	<p>Impact Statement: This issue is not reproducible on all the RAMP VMware installations. The <code>entropy_avail</code> value in the specific RAMP VMware installation was relatively low, causing the random number generation failure in the object store service, which led to a stagnant state.</p> <p>Resolution Details: Object store service thread was stuck due to low entropy when using the <code>SecureRandom</code> <code>getInstanceStrong</code> method. Modified the code to remove this.</p>
AFM-11940	N/A	3	Document the new script added for AFM-11823.	<p>Impact Statement: Update the Administration Guide since allowing the algorithm HMACSHA1 is incorporated with a few other cryptographic algorithms in a new script, <code>updateSystemCryptoPolicy.sh</code>.</p> <p>Resolution Details: Updated the following documents:</p> <ul style="list-style-type: none"> Legacy Device Management: Created this page with a procedure to support managing legacy devices, Federal Information Processing Standards (FIPS) are disabled. Migrate Insight EMS to RAMP: For users having the GSX, after an upgrade and migration, before discovering GSX, run the script: <code>/opt/sonus/ems/conf/updateSystemCryptoPolicy.sh</code>. For more information, refer to Legacy Device Management. Post-Upgrade Procedures for RAMP: After a RAMP upgrade, to discover the GSX, refer to Legacy Device Management.

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12006	N/A	2	A few of the SBC nodes take longer than expected to display online on the RAMP.	<p>Impact Statement: If more than one SBC discovery is in progress, it takes a long time for all of them to complete and for the nodes to go online. The REST client connection pool in the Device Manager only allows two connections per route. Many requests go internally to other microservices and use the same route through Apache. One of these requests did not release the connection, which led to blocking other requests waiting for a thread.</p> <p>Resolution Details: Added the missing "close" action to ensure the thread gets released. Also increased the number allowed connections per route to account for the number of requests that use Apache.</p>
AFM-12042	N/A	2	The RAMP fails to establish the connection when launching the PSX Manager since the RAMP FIPS is enabled.	<p>Impact Statement: The RAMP fails to provision the PSX.</p> <p>Resolution Details: Modified the code to launch the PSX manager with FIPS enabled.</p>
AFM-12070	N/A	2	The Retry Mechanism for the SBC <code>setConfigStore</code> to handle the failure case.	<p>Impact Statement: At the end of a dynamic SBC node discovery, the <code>config store</code> parameter is set to enable the SBC to upload the configurations to the RAMP. If this fails, the configuration upload fails without indication, and there is no upload reattempt. A network interruption or other cause that allows a subsequent attempt to succeed can lead to this failure.</p> <p>Resolution Details: Added the <code>config store</code> parameter setting to the discovery retry mechanism to ensure if the upload fails, another discovery attempt is made. If the upload fails, but the maximum number of discovery retry attempts is reached, the failure reason indicates that the config store parameter setting failed.</p>
AFM-12130	N/A	2	Gaps with RAMP SFTP pull of GSX PM statistics files in the GSX streaming Mode.	<p>Impact Statement: The SFTP collection fails if the DSI NFS is not mounted.</p> <p>Resolution Details: Added SFTP support to the GSX PM statistics in the streaming mode, so mounting the NFS is no longer necessary.</p>
AFM-12136	N/A	2	All GSXs indicate "registered offline" due to token expirations.	<p>Impact Statement: All GSXs indicate "registered offline" with a stale-session/expired token after the user issues a "discover-all" command.</p> <p>Resolution Details: Modified the code to log the user out on a session timeout.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12160	N/A	2	The SBC SWe Edge firmware upgrade using the RAMP fails.	<p>Impact Statement: The SBC SWe Edge firmware upgrade using the RAMP fails when the image contains the string ".build".</p> <p>Resolution Details: Modified the code to allow ".build" in the 1k/2k build filenames.</p>
AFM-12161	N/A	2	(RAMP CNF) RAMP SSH access support using Active Directory.	<p>Impact Statement: The Samba packages were missing from the RAMP after migrating from the EMS.</p> <p>Resolution Details: Added the following libraries:</p> <ul style="list-style-type: none"> • samba • samba-common • samba-winbind • samba-client • samba-winbind-clients • authconfig.
AFM-12203	N/A	2	The PM collection issue exists on the SGX 10.0.6R0.	<p>Impact Statement: For SGX version 10.0.6R0, the memory usage-related counters in the PM statistics are not pegged or pegged as "0." This is a known issue in the SGX 10.0.6R0 release, and the fix is available for a higher release. Ribbon previously provided a script in the EMS to run as a cron job to collect memory information from the SGX. This is also needed in the RAMP CNF for the SGX 10.0.6R0 to retrieve memory information.</p> <p>Resolution Details: The script <code>/opt/sonus/ems/conf/sgx-mem-collector.sh</code> is added in the RAMP CNF to run as an Insight cron job every 15 minutes in RAMP by default.</p>
AFM-12244	N/A	2	Missing support for the old versions of PSX APIs.	<p>Impact Statement: The user holds the PSX version 14.1.3 and provisions through the RAMP API with the PSX WSDL version r07_03_02.</p> <p>Resolution Details: The RAMP is enhanced to support the older versions of PSX APIs (from 7.0.x to 8.2.x).</p>
AFM-12244	N/A	2	Support the old PSX API version.	<p>Impact Statement: The support for 07_00_00 and above versions were missing in the RAMP.</p> <p>Resolution Details: Added the support from 07_00 to 08_02_00 in the RAMP.</p>
AFM-12296	N/A	2	The RAMP fails to launch the SBC Manager GUI.	<p>Impact Statement: The RAMP fails to launch the SBC Manager GUI when the .KF file is generated using the DES algorithm since the SBC Manager in the RAMP does not support the DES algorithm.</p> <p>Resolution Details: Support for the DES algorithm was added in the SBC Manager.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
AFM-12361	N/A	2	Error logs are generated in the <code>ems_trace_log</code> when the PSX API provisioning is accomplished.	<p>Impact Statement: When the Application Config -> Utils -> Enable CLI/API username logging is set to True, an exception is observed in the logs, and the connection is not freed. When the flag is set to True, the <code>nodeId</code> is passed into <code>freeConnection</code> as "<code>nodeId+userName,</code>" causing an exception when trying to retrieve the provisioning PSX.</p> <p>Resolution Details: Added a <code>freeConnection</code> to match the <code>getConnection</code> and handle the extra username parameter.</p>
AFM-12369	N/A	2	SBC CNe: The SBC Manager GUI connection through the RAMP window relaunches.	<p>Impact Statement: The SBC GUI running on the RAMP frequently runs a REST call to the SBC on port 443 to check if the SBC is up and running. Occasionally, the REST call fails with an error "Connection reset by peer (connect failed)", leading the SBC GUI to consider that the SBC is down, and the GUI relaunches with only limited functionality. After an interval, the REST call succeeds, and the GUI is relaunched with complete functionality.</p> <p>Resolution Details: Implemented the retry mechanism to address the failure while connecting to the device before reporting failure to the SBC Manager GUI.</p>
AFM-12399	AFM-12456 (24.06)	2	Allow MAC and KEX algorithms on the RAMP 8122 CLI.	<p>Impact Statement: A few deprecated MAC and KEX algorithms were removed as part of security updates. However, these algorithms are required while connecting to older devices using the RAMP CLI.</p> <p>Resolution Details: The RAMP is enhanced to read the MAC and KEX algorithms from <code>/opt/sonus/ems/weblogic/sonusEms/data/cli/framework/resources/Listener.properties</code> file.</p>
AFM-12407	N/A	2	The RAMP fails to export the <code>DspResDspUsageIntervalStats</code> to the IT systems due to an SBC7K upgrade.	<p>Impact Statement: The SBC7K device fails to process <code>DspResDspUsageIntervalStats</code>. The <code>mdjson</code> file used by the PM Persister component is missing a few expected fields for SBC 11.2.x devices.</p> <p>Resolution Details: This issue is resolved in the previous version of the RAMP and verified in RAMP 24.09.</p>

Issue ID	Original Issue	Sev	Problem Description	Resolution
PLTF-4305	N/A	2	Deprecated SSH cryptographic ciphers.	<p>Impact Statement: The SSH cipher vulnerabilities are reported in the Qualys scan. When the Crypto policy is set to DEFAULT/FIPS, the deprecated ciphers are enabled in those configuration files, and vulnerabilities are reported.</p> <p>Resolution Details: Added strict MACs and Ciphers on the RHEL7 in both the <code>/etc/ssh/ssh_config</code> and <code>/etc/ssh/sshd_config</code> files.</p>
PLTF-4478	N/A	2	RAMP 24.06: etcd upgrade support.	<p>Impact Statement: The etcd upgrade-related documentation is not available.</p> <p>Resolution Details: Created the documents for different upgrade configurations. For more information, refer to:</p> <ul style="list-style-type: none">• Upgrading etcd• Upgrading etcd on KVM• Upgrading etcd on VMware• Upgrading etcd on Openstack• Upgrading etcd on Kubernetes

Known Issues

Severity 1 Issues

There are no severity 1 known issues in this release.

Severity 2 and 3 Issues

The following table lists the severity 2 and 3 known issues in this release:

Issue ID	Sev	Problem Description	Impact/Workaround
AFM-4461	2	When the active RAMP goes down in an Active/Active scenario), the Standby registers a "relocate" action while the Active becomes active again, resulting in loss of functionality.	Impact Statement: The RAMP server goes down, and manual intervention is required to bring it up. Workaround: N/A
AFM-6966	2	Retain all the passwords after a restore (Upgrade/Migration).	Impact Statement: <ol style="list-style-type: none"> 1. Linux Insight user (insight) - Reset post restore 2. Linux Admin user (admin) - Reset post restore 3. Insight DB user - Retained 4. Insight Postgres DB user - Reset 5. Insight Agent (admin) - Retained 6. Insight GUI Admin user (admin) - Reset 7. Insight REST API user (restuser) - Retained 8. Insight GUI Admin User (admin) - Reset Workaround: Set the password again.
AFM-7086	3	Localhost Auto discovery failed (CNF).	Impact Statement: The Localhost registration failed. The PM and other functionalities are impacted. Workaround: Navigate to the DM page and manually re-discover the local host.
AFM-7320	3	The SBC CNe nodes are not registered in the extended IPv6 format.	Impact Statement: No functionality impact. IPv6 addresses display in short form. Workaround: N/A
AFM-7578	3	The node service must stop if the reachability consumer stops due to an exception.	Impact Statement: The node management application starts even if the KAFKA consumer reachability stops due to an unexpected error, which results in an inconsistent system state. Workaround: If the node status is not updated according to the reachability polling results, follow these instructions to restart the dynamic node services. <ol style="list-style-type: none"> 1. Log on as an insight user. 2. Run the following commands: <pre>cd /opt/devMgmt/bin ./dynamicNodeService stop ./dynamicNodeService start</pre>

Issue ID	Sev	Problem Description	Impact/Workaround
AFM-7891	3	The SBC SWe Edge configuration fails on the RAMP.	<p>Impact Statement: The RAMP fails to launch the SBC GUI configuration on the SBC SWe Edge. This is a rare occurrence attributed to a tunnel creation failure.</p> <p>Workaround: Reboot the SBC SWe Edge instance.</p>
AFM-8483	2	The <code>PeerIPAddress</code> field contains the worker node IP address instead of the RAMP IP address in the SNMP receiver.	<p>Impact Statement: The <code>PeerIPAddress</code> field contains the worker node IP address and port. The <code>PeerIPAddress</code> field must contain RAMP's eth1 IP address instead of the worker node IP address because the worker node IP address changes when the pod is moved from one worker node to another.</p> <p>Workaround: N/A</p>
AFM-8777	3	The SBC registration fails with <code>emsIpAddressOverride</code> .	<p>Impact Statement: The SBC registration fails with <code>emsIpAddressOverride</code> if the RAMP IP address is changed.</p> <p>Workaround: Remove the Node ID from the SBC User Data and resend the Registration Request.</p>
AFM-9595	3	Legacy devices such as GSX PM metrics are not available in the Prometheus if the number of devices is greater than 15.	<p>Impact Statement: The RAMP CNF observability performance issues limit the capacity of the observability component to process the GSX metrics.</p> <p>Workaround: Export the PM data to an external server.</p> <p>Note: Maximum of 10,000 metrics are exported to Prometheus.</p>
AFM-9658	3	Missing clearing event <code>sonusHARACProcessUPNotification</code> for problem event <code>sonusHARACProcessDownNotification</code> for FM processes restarted by the openSAF.	<p>Impact Statement: The clearing event does not occur through the FM process.</p> <p>Workaround: Run the <code>emsMgmt</code> command to verify the state of the FM process.</p>
AFM-10033	3	The RAMP fails to fetch the complete <code>oam</code> , <code>snmp</code> , <code>trapTarget</code> using the CLI in IPv6.	<p>Impact Statement: The RAMP CLI issue occurs when the RAMP fails to display the complete response if the response size exceeds 80 characters for the particular column. The window size is truncated whenever it reaches 80 characters. This applies to all tables.</p> <p>Workaround: N/A</p>
AFM-11210	3	Performance Load: When all the nodes go offline, the RAMP takes time to bring up all the nodes online as reachability timeout is high, which results in waiting for the threads.	<p>Impact Statement: When a huge number of nodes goes offline, the RAMP takes time to bring all the nodes back online.</p> <p>Workaround: N/A</p>

Issue ID	Sev	Problem Description	Impact/Workaround
AFM-11222	3	Multi-Tenancy: Limit the Resource Group access within the tenant hierarchy.	Impact Statement: The user can edit/delete the resource group above the tenant hierarchy. Workaround: N/A
AFM-11239	3	The RAMP CNe fails to perform the Restore Revision because it cannot download the complete configuration file (Random occurrences).	Impact Statement: The RAMP fails to perform Restore Revision because it fails to download the complete configuration file. Manually downloading the configuration file fails partially. Workaround: Restart the SBC.
AFM-11349	3	The Cluster Management table does not navigate to the previous page after deleting a cluster from the last page (RAMP GUI).	Impact Statement: The user cannot view the existing clusters. However, the table is loaded if clicked again. This problem is observed only if the cluster is deleted from the last page, not from the first page or an intermediate page. Workaround: Visit the Cluster Management page and return to the current page.
AFM-11718	3	TrunkGroupDataExporter reports are incomplete and slow.	Impact Statement: The TG reports for ALL GSX are slow. For each GSX, it takes approximately three hours to receive the TG data for the TrunkGroup CSV. Workaround: N/A
AFM-12061	2	The EMS CLI Port 8122 drops the first character.	Impact Statement: When performing a copy/paste of multiple CLI commands in the RAMP CLI port 8122 (SSH), the first command runs correctly, but the subsequent commands fail because the first character is dropped. Workaround: Add an empty line between each command and then run the script.
AFM-12063	3	24.09 (FM): Unable to load the FM Administration page (Single occurrence).	Impact Statement: Due to an FM administration page issue, the FM REST Service generates the error "Error Loading Administration Page." Workaround: Restart the FM REST Service.
AFM-12357	3	The RAMP switchover is not triggered when the OpenSAF is down (Negative scenario).	Impact Statement: The RAMP fails to perform a Switchover in the GR (Rare negative scenario). Workaround: Trigger the switchover manually.
AFM-12449	3	Email address support for the RAMP GUI certificate.	Impact Statement: Missing email address when creating a CSR for the RAMP GUI. Workaround: N/A
AFM-12482/ CHOR-12687	3	The RAMP fails to launch the SBC SWe Edge configuration page after an upgrade.	Impact Statement: Unable to launch the SBC SWe Edge device page on the upgraded RAMP server. Workaround: Reboot the SBC SWe Edge device.

Issue ID	Sev	Problem Description	Impact/Workaround
AFM-13080	2	The RAMP fails to migrate the Mediation Server for the Lawful Interface.	<p>Impact Statement: The Mediation Server configuration are not carried to the RAMP during the EMS to RAMP migration.</p> <p>Workaround: Re-configure the Mediation Server after an EMS to RAMP migration.</p>
AFM-13100	3	RAMP CNF: Handling the timestamp format (ISO8601 format) correctly in the RAMP logs.	<p>Impact Statement: Enhancement to handle the timestamp format (ISO8601 format) correctly in the RAMP logs.</p> <p>Workaround: N/A</p>
AFM-13112	2	The CliFramework fails to create a connection to the SBC if the username does not end with "admin".	<p>Impact Statement: Unable to process the CLI command for the SBC.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Create a user in the SBC with a name ending with 'admin'. For example, emsdiscoveryadmin. 2. Register an SBC with this newly created NETCONF user to ensure the CLI functionality runs correctly.
AFM-13166	2	Address the PM export issues for large loads in single export profile for each device type.	<p>Impact Statement: The GSX statistics data is lost when the PM export is enabled with many GSX devices in a single export profile.</p> <p>Workaround: Create multiple PM export profiles for the GSXs and assign them equally to the GSX devices.</p> <p>Note: Do not configure more than 100 device per export profile when the PM export mode is set to Per Node Export.</p>
AFM-13206	2	Export fails in large networks with the error "Argument list too long" for perNodeExport.	<p>Impact Statement: The perNode export fails in the large network when:</p> <ol style="list-style-type: none"> 1. A large number of devices are registered in the RAMP (more than 400) 2. Node Name of the device is too long (more than 20 characters) 3. All devices are part of one single PM export profile. <p>Workaround: Ensure that an export profile does not contain more than 100 devices.</p>

Issue ID	Sev	Problem Description	Impact/Workaround
AFM-13210	2	Include re-generating CSR in post-migration steps.	<p>Impact Statement: Discovery fails on the RAMP after a migration.</p> <p>Workaround: Added note in Migrate Insight EMS to RAMP. If the user holds a CA-signed agent certificate on the EMS with MD5withRSA signature algorithm, perform the following procedure after migrating from the EMS to the RAMP, before discovering the nodes:</p> <ol style="list-style-type: none"> 1. Re-generate the CSR. For more information, refer to Generate Certificate Request for Agent. 2. Re-import the certificate to the agent keystore. For more information, refer to Import Certificates for Agent. 3. Restart administration service: <pre># sudo su - insight # cd /opt/devMgmt/bin/ # ./administrationService stop;./administrationService start</pre>
AFM-13229	2	RAMP 24.12: The Calea user does not hold permission to access the DM UI after a migration.	<p>Impact Statement: By default, the Calea user does not hold permission to access the DM UI after a migration.</p> <p>Workaround: The user needs to add the permission manually.</p>
AFM-13339	3	The RAMP generates Active Directory Configuration issues during the upgrade and non-cloud deployment.	<p>Impact Statement: Active Directory configurations are not retained during the upgrade, causing login failures in non-cloud deployment.</p> <p>Workaround: Perform Post-Upgrade Procedures for RAMP and Reconfiguring Active Directory.</p>
AFM-13365	3	In multiple interfaces configured on the SBC setup, if the primary interface is disabled, the RAMP discovery fails for SBC after a switchover.	<p>Impact Statement: If one of the interfaces is disabled on the SBC that is returned as the first interface by the SBC, the disabled interface is updated as the primary IP address. If there is an SBC switchover, the node does not come online on the RAMP.</p> <p>Workaround: Update the Host IP address fields from the UI after every SBC switchover and do not discover the node after that.</p>

Known Limitations

The following limitations exist in this release:

1. Dual-stack RAMP deployment is not supported in the RAMP.
2. IPv6 deployment is not supported on the Azure and AWS platforms.
3. RAMP does not support High Availability redundancy.
4. RAMP supports only standalone deployments on the Azure and AWS platforms.
5. AMP does not support the REST API provisioning for SBC versions less than 11.1.
6. UI dashboard and other FM/PM UIs have issue with Multi-tenancy. They are GUI issues and will be address in Release 25.X release.
7. The following items are not restored as part of the RAMP restore operation.
 - a. Platform-related configurations
 - b. Custom Cron jobs configured by users
 - c. Custom scripts or jobs deployed at the Linux level