

StorageGuard

Release Notes

Hotfix 9.2.7.1



Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 9.2.7.1

Document version: 1.0

Legal Notice

All products and services are licensed, sold and provided subject to Continuity Software's terms and conditions of sale supplied at the time of order acknowledgment. Customers should obtain the latest relevant product and services information before placing orders and should verify that such information is current and complete.

Continuity Software reserves the right to make corrections, modifications, enhancements, improvements and other changes to its products and services, at any time, and to discontinue any product or service without notice.

Continuity Software warrants performance of its products to the applicable specifications, at the time of supply, in accordance with Continuity Software's standard warranty. Testing and other quality control techniques are used to the extent Continuity Software deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

Except as expressly provided, Continuity Software does not grant any implied or other license under any Continuity Software patent right, copyright, mask work right, or other Continuity Software intellectual property right, relating inter-alia to any combination or process in which Continuity Software products or services are used.

Information published by Continuity Software regarding third-party products or services does not constitute a license from Continuity Software to use such products or services or an endorsement thereof. Use of such products or services may require a license from third parties under their patent or other intellectual property rights, or a license from Continuity Software under the patents or other intellectual property thereof.

Reproduction of information from this User's Guide is only permitted without modifications and with all associated warranties, notices, and qualifications, and for the sole purpose of use of the Continuity Software products and services. All other reproduction is prohibited and is an unfair and deceptive business practice and Continuity Software will not be responsible or liable for any such reproductions.

StorageGuard, design marks associated with StorageGuard, and trade dress associated with Continuity Software's products, are among the trademarks or registered trademarks owned by or licensed by Continuity Software. All other brand and product names are or may be trademarks of, and are used to identify products or services of, their respective owners.

Contacting Us

US Headquarters

5 Penn Plaza, 23rd floor

New York, NY 10001

Phone: +1.646.216.8628

Fax: +1.646.417.6171

Support: +1-646-461-6217

Toll-Free: +1-888-782-8170

Israeli Office

27 Habarzel St.

Or Towers, Building A, 10th floor.

Tel Aviv 69719, Israel

Phone: +972.3.647.0888

Fax: +972.3.644.9389

Support +972.3.600.2200

Email: support@ContinuitySoftware.com

Table of Contents

Release Notes.....	2
Contacting Us.....	3
Introduction.....	4
Enhancements and Fixes overview	4
Enhancements	4
Fixed issues	5
Renamed checks.....	12
New / Modified system properties	13
Security advisories	13
Known issues and limitations	13
Installation guide.....	13
Installing the Hotfix	13
Uninstalling the Hotfix	14
Getting help.....	15

Introduction

This document provides important information about Hotfix 9.2.7.1

Enhancements and Fixes overview

Enhancements

Id	Title	Description
SG-29837	Version update for NetApp StorageGRID API	Upgraded StorageGRID probe to API v4 to eliminate data gaps and maintain forward compatibility.
SG-29838	New Check: Required CAC/PIV domain validation (NetBackup)	Added a check “SG-C0721T217V01: Required CAC PIV domain name” to ensure the required CAC/PIV domain is used ¹
SG-29027	Expose inventory via StorageGuard public REST API	Inventory can now be retrieved through the public API
SG-29955	Configuration Compliance report generation improved	Optimized processing to shorten generation time by reducing evidence size and improving overall report delivery speed.

¹ A ‘**Required...**’ check verifies whether all **necessary** entities (NTP / DNS server, Domain, etc.) , are configured on the storage / backup system. If one or more required entities are missing from the configuration, the check fails and indicates a risk. When all required entities are defined, the check passes. An ‘**Approved...**’ check verifies whether any **unauthorized** entities (NTP, DNS, Domain, etc.) are configured on the entities configured on the storage / backup system. If one or more configured entities are not included in this approved list, the check fails and indicates a risk. If all configured entities belong to the list of approved items or if no entities are configured— no unauthorized entities are configured and the check passes.

SG-30018	Azure AD authentication integration hardened	Improved stability and error handling for authentication flows to reduce intermittent failures
SG-30015	End of Support (EoS) checks: accuracy and coverage improved	Updated sources and logic to increase reliability across EoS validations for Brocade FC, Cisco SAN, ECS, StorageGRID & VMAX/PMAX systems

Fixed issues

Id	System type	Title	Description
SG-29758	---	Enhanced in-UI log collection	Collect troubleshooting and investigation logs directly in the UI, without accessing underlying infrastructure
SG-29802	---	Expansion package export	The Export button now works correctly when packages are selected
SG-29805	---	Check dependency handling	Improved logic, now checks without declared dependencies no longer return a misleading Not applicable status
SG-29706	---	Golden Standard selection persistence	Fixed behavior; the previous Golden Standard choice is no longer cleared when the popup is reopened and closed without saving
SG-30049	---	Assets table performance	Improved loading and interaction speed in the Assets tab's Inventory table.
SG-29796	---	"Golden Standard" Comparison user permissions	Users with the Modify role can now view and add groups
SG-29806	---	Certain custom checks may fail to be presented in the UI after upgrade	Fixed an issue where some custom checks vanished from the UI following an upgrade

Id	System type	Title	Description
SG-29944	---	Fixed missing CI group counts	Assigning custom collections now updates CI group totals properly.
SG-29869	---	Custom check cloning issue resolved	Fixed an issue where cloned items did not receive unique identifiers
SG-29823	ONTAP	SG-C0019T187V01: "Target OS version" check inaccurate finding	Resolved an issue where SG-C0019T187V01: "Target OS version" check for ONTAP produced incorrect results
SG-29777-9	ONTAP	Multiple checks returning incorrect or insufficient information	Fixed incorrect <i>"Insufficient information"</i> status; configuration data is now correctly evaluated for: SG-C0243T187V01: "DNS server configuration", SG-C0417T187V01: "Password hash strength", SG-C0191T187V01: "NFS export ACL status"
SG-29781-4	ONTAP	Multiple checks returning incorrect or insufficient information	Fixed incorrect <i>"Insufficient information"</i> status; configuration data is now correctly evaluated for: SG-C0239T187V01: "Multi-factor authentication", SG-C0231T187V01: "Non-default local users", SG-C0121T187V01: NFS versions enabled", SG-C0033T187V01: Central authentication for CIFS SMB file share access"
SG-29786	ONTAP	Multiple checks returning incorrect or insufficient information	Fixed inaccurate or Insufficient information results across several checks, including SG- SG-C0255T187V01: "SSH MAC strength", SG-C0258T187V01: "SSH cipher strength", SG-C0448T187V01: "Trusted certificate-authority (CA)", SG-C0128T187V01: "CIFS SMB anonymous user access restriction", and SG-C0122T187V01: "CIFS SMB version enabled"
SG-29786, SG-29776	ONTAP	Multiple checks returning incorrect or insufficient information	Fixed inaccurate or Insufficient information results across several checks, including SG-C0140T187V01: Unused ports, SG-C0162T187V04: Expired SSL certificate – OU, SG-C0163T187V01: Approved AD domain, SG-C0242T187V01: NDMP

Id	System type	Title	Description
			authentication type, SG-C0307T187V01: Admin account status, SG-C0308T187V01: Diag account status, SG-C0381T187V01: HTTP service status, SG-C0430T187V01: Autosupport status, SG-C0426T187V01: "Login banner status"
SG-29916	ONTAP	SG-C0029T187V01: Centralized log server" check inaccurate finding	Fixed inaccurate detection logic.
SG-30027	ONTAP	SG-C0124T187V01: "SSHv1 status" incorrect logic	Fixed incorrect detection logic for ONTAP that identifies if a MAV rule has a sufficient number of approvers
SG-30030	ONTAP	SG-C0552T187V01: "Authorization policy rules" incorrect logic	Fixed incorrect detection logic for ONTAP that identifies if SSH v1 is enabled
SG-29927	ONTAP	SG-C0381T187V01: "HTTP service status" check wrong violation details	"Violation details" section now reflects the correct service status
SG-29928	ONTAP	SG-C0033T187V01: "Central authentication for CIFS SMB file share access" inaccuracies	Central authentication validation for ONTAP now reports results correctly
SG-29719	ONTAP	SG-C0209T187V01: "Idle session timeout – CLI" check inaccurate finding	Fixed incorrect results for zero timeout settings
SG-29937	ONTAP	NTAP-20240426-0001: NetApp cDOT detection inaccurate	Fixed incorrect detection logic, which ensures the NetApp cDOT finding NTAP-20240426-0001 is now evaluated correctly.
SG-29874	ONTAP	ONTAP API call corrected	Replaced incorrect request with the proper endpoint to ensure accurate results.
SG-29822	HPE 3PAR/Primera	SG-C0019T244V01: "Target OS version" check improved data analysis	Fixed incorrect Insufficient information status for HPE 3PAR/Primera when data is present

Id	System type	Title	Description
SG-29826	HPE 3PAR/Primera	SG-C0432T244V01: "NTP server redundancy" check inaccurate finding	Fixed incorrect detection logic for HPE 3PAR/Primera that identified only one NTP server instead of all configured servers
SG-29827	HPE 3PAR/Primera	SG-C0294T244V01: "Virtual lock license" check inaccurate finding	Fixed incorrect logic for HPE 3PAR/Primera, which ensures the check now produces the expected result.
SG-29828	HPE 3PAR/Primera	SG-C0039T244V01: "LDAP server configuration" check inaccurate finding	Fixed incorrect detection logic for HPE 3PAR/Primera, which ensures configured LDAP servers now produce the correct result.
SG-29829	HPE 3PAR/Primera	SG-C0038T244V01: "Kerberos status" check inaccurate finding	Fixed incorrect detection logic for HPE 3PAR/Primera, which ensures configured Kerberos realms now produce the correct result
SG-29831	HPE 3PAR/Primera	SG-C0047T244V01: "KMIP status" check inaccurate finding	Improved detection and handling of KMIP/EKM configuration gaps
SG-29980	HPE 3PAR/Primera	"SG-C0381T244V01: HTTP service status" check inaccurate data collection	Fixed incorrect "Insufficient information" status; The data is now correctly handled to guarantee correct analysis
SG-29830	HPE 3PAR/Primera	SG-C0239T244V01: "Multi-factor authentication" wrong violation value	Fixed incorrect key/value rendering for MFA violation details in the UI
SG-29799	HPE Primera/3PAR	HPE Primera/3PAR scan timeout fixed	Event log collection has been disabled (currently unused).
SG-29759	NetBackup Flex Appliance	NetBackup Flex security collection expanded and accuracy improved	The relevant data now captured and displayed reliably, fixing prior incomplete reporting.
SG-29686	NetBackup Flex Appliance	SG-C0397T234V01: "Remote support configuration" check inaccurate finding	Resolved an issue where "SG-C0397T234V01: Remote support configuration" produced incorrect results
SG-29842	Data Domain	SG-C0116T061V01: "Unapproved admin	Fixed incorrect logic for Data Domain; admin usernames containing hyphens are now detected correctly.

Id	System type	Title	Description
		users” check inaccurate finding	
SG-29845	Data Domain	SG-C0163T061V01: “Approved AD domain” check inaccurate finding	Corrected handling when AD domain is not configured. Violation details fixed
SG-29850	Data Domain	SG-C0269T061V01: “Maximum repeated password characters” check updated	Removed the unused check parameter to ensure accurate and clear validation
SG-29851	Data Domain	SG-C0162T061V01: “Expired SSL certificate – Data Domain” check inaccurate finding	Fixed incorrect handling, expired SSL certificates on Data Domain systems are now detected properly
SG-28854	Data Domain	SG-C0031T061V01: Authentication server configuration inaccurate logic and description	Improved check quality and renamed the check to SG-C0031T061V01: Kerberos configuration
SG-24414	Data Domain	SG-C0001T061V01 and SG-C0509T061V01 checks removed	SG-C0001T061V01 “Audit logging status” and SG-C0509T061V01 “Audit logging status” were removed since they duplicate SG-C0029T061V01: “Centralized log server”
SG-29949	Data Domain	SG-C0024T061V02: “Authentication server redundancy – Kerberos” check inaccurate finding	Adjusted evaluation, now the results correctly reflect wildcard use and cases where Kerberos is not configured
SG-29792	VMAX/PMAX	SG-C0205T121V01: “Host access list” check inaccurate finding	Host access list validation now properly excludes relevant PowerMax models on which this feature is unsupported
SG-29821	VMAX/PMAX	SG-C0019T121V02: “Target OS version – Enginuity” check inaccurate finding	Fixed incorrect results when validating Enginuity OS version on VMAX/PowerMax systems
SG-29922	VMAX/PMAX	SG-C0366T121V01: “SYMAPI encryption” check inaccurate finding	Refined evaluation logic to better interpret SYMAPI encryption status and ensure consistent results

Id	System type	Title	Description
SG-29895, SG-29900	VMAX/PMAX	SG-C0119T121V01: “Unapproved user groups” check inaccurate collection and finding	Fixed incorrect detection for PMAX user groups. Fixed regex logic, now full user and group values on PMAX systems are captured and evaluated correctly.
SG-29859	Commvault	SG-C0284T049V02: “Password history – Enabled” check inaccurate finding	Fixed detection logic, now enabled password history is reported correctly for Commvault
SG-29860	Commvault	SG-C0295T049V01: “Snapshots status” check inaccurate finding	Improved handling of missing snapshot configuration indicators to ensure expected result
SG-28484	Commvault	SG-C0274T049V01: “Password complexity” wrong evidence	Fixed detection logic and API parsing to accurately report password complexity
SG-29871	Commvault	SG-C0390T049V02: “TLS level - SDK” check inaccurate finding	Fixed detection, now TLS level is correctly reported for Commvault SDK
SG-29875	Commvault	Commvault checks enhanced for missing values	Added support for using defaultValue when the value field is not provided in Commvault responses.
SG-24953	StorageGRID	Updated StorageGRID API usage	Replaced deprecated private endpoint with supported calls
SG-30040	StorageGRID	SG-C0351T193V01: “SNMPv3 read-only user” improved logic	Updated logic marks the SG-C0351T193V01 “SNMPv3 read-only user” check as Not Applicable when SNMP is not configured
SG-29863	StorageGRID	StorageGRID vulnerability coverage	Added several StorageGRID security advisories that were not included
SG-29862	StorageGRID	Stabilized NetApp StorageGRID API	Reduced errors and timeouts during API requests
SG-30062	StorageGRID	New check SG-C0155T193V01: “SNMP service disabled” added	Added a new check verifying if SNMP service is enabled or disabled on the system
SG-29887	Pure Storage	Corrected serial number display for Pure arrays	Pure storage systems now show the correct serial number in the Assets tab and configuration compliance report

Id	System type	Title	Description
SG-29877	Pure Storage	CLI commands syntax handling	Improved command parsing and execution to prevent intermittent errors during data collection
SG-29864	Pure Storage	FlashArray: PureFA-CVE-2025-2327 incorreceted link	Fixed a broken reference link for the PureFA-CVE-2025-2327 vulnerability
SG-29873	Pure Storage	SG-C0230T199V01: "Non-default local admin" check inaccurate finding	Improve detection logic, local admin usernames containing special characters are now identified correctly
SG-29891	Brocade FC	Brocade permission handling inaccurate finding	Fixed incorrect results when Brocade commands returned Permission Denied.
SG-29820	Brocade FC	SG-C0019T031V01: "Target OS version" check inaccurate finding	Fixed incorrect handling of Permission Denied outputs
SG- 28849	Brocade FC	SG-C0030T031V01: "Centralized authentication service status" check removed	Removed as a duplicate of SG-C0031T031V01: "Authentication server configuration" for Brocade.
SG-29936	Brocade FC	"SG-C0428T031V01: "MOTD message" check inaccurate finding	Updated logic causes RBAC access limitations to lead the check to return <i>Insufficient Information</i> .
SG-29793	ECS	ECS post-upgrade scan failure fixed	Resolved an issue where ECS scans failed after upgrading to a newer SG version, ensuring scans run normally.
SG-29818	ECS	SG-C0019T067V01: "Target OS version" check inaccurate finding	Resolved an issue where "SG-C0019T067V01: Target OS version" check produced incorrect results
SG-29879	Cisco Switch	SG-C0031T037V01: "Authentication server configuration" check inaccurate finding	Corrected handling, now the check no longer returns Insufficient information when valid authentication server data is available.
SG-29888	Cisco Switch	SG-C0437T037V03: "Approved identity provider servers -	Fixed incorrect Missing input status when RADIUS parameters are configured.

Id	System type	Title	Description
		RADIUS" check missing input handling	
SG-29836	Cisco Switch	Cisco MDS scan requirements corrected	Updated requirements and corrected commands to prevent invalid command errors
SG-29868	Cisco Switch	Cisco vulnerability applicability	Fixed a vulnerability check that incorrectly flagged MDS systems with an issue relevant only to Nexus devices
SG-29465	Unisphere for PowerMax	Unisphere scanning reliability	Improved handling to make systems that verify successfully can also be scanned without interruption
SG- 29946	IBM Storage Protect	SG-C0215T169V01: "Authenticated users minimum permission" check removed	Removed a duplicated check to ensure clean and accurate validation
SG-29945	IBM Storage Protect	"SG-C0166T169V01 Command approval is disabled" and "SG-C0470T169V01: Command approver user is not defined" checks clarification and improvement	Remediation and Impact fixed

Renamed checks

The following section highlights checks that were renamed:

System type	Old name	New name
ONTAP	SG-C0065T187V02: Data at-rest encryption	SG-C0065T187V02: Data at-rest encryption (disk)
ONTAP	SG-C0065T187V01: Data at-rest encryption	SG-C0065T187V01: Data at-rest encryption (logical)
Data Domain	SG-C0031T061V01: Authentication server configuration	SG-C0031T061V01: Kerberos configuration

New / Modified system properties

The following section highlights key system properties that were added or modified:

None.

Security advisories

Added fix for [Continuity Software Security Advisory \(Apache\) - October 29, 2025](#).

Known issues and limitations

Please refer to the relevant section in [9.2.7 Release Notes – Help Center | Continuity Software](#)

Installation guide

Installing the Hotfix

You can install HF 9.2.7.1 only from version 9.2.7.x. If a system has an earlier version of the product installed, you must upgrade to version 9.2.7.0 before installing this hotfix.

Installation procedure:

- Download **ContinuityPlatform_9.2.7.1.exe** and copy it to the Master server.
- On the Master server, stop the Continuity web server using the following steps:
 - Open a command line window running with administrator privileges.
 - Enter the following commands:

```
# net stop TomcatWatchDog
# net stop tomcat10
```
- Take a snapshot of the Master server.
- Take a DB backup.
- Locate the webapps folder. By default, it is in the path:

```
C:\Program Files\Apache Software Foundation\Tomcat 10.1\webapps\
```

 - Make a copy of the webapps folder and store it in another location (do not store the copy under the tomcat tree). The hotfix updates files in this folder, if you need to revert to the unpatched version, you will need the original folder.

- Locate the file named "header.iss". By default, it is in the path:
[drive]:\Program Files\Apache Software Foundation\Tomcat 10.1\conf
 - Make a copy of the header.iss file and store it in another location (do not store the copy under the tomcat tree). The hotfix updates files in this folder, if you need to revert to the unpatched version, you will need the original folder.
- Go to the folder where you saved the patch. Find **ContinuityPlatform_9.2.7.1.exe** and double-click it.
- Follow the steps in the wizard to install the hotfix.
- On the master server, start the Continuity web server using the following steps:
 - Open a command line window running with administrator privileges.
 - Enter the following commands:
net start tomcat10 (only if it hasn't started already)
net start TomcatWatchDog
- Login to Continuity application.
- Verify that the build number is correct. On the main screen, click "About".

Uninstalling the Hotfix

- Locate the copy of the pre-patched webapps folder (backup done in step 4 of -Installing this Hotfix).
- On the Master server, stop the Continuity web server using the following steps:
 1. Open a command line window running with administrator privileges.
 2. Enter the following commands:
net stop TomcatWatchDog
net stop Tomcat10ss
- Locate the webapps folder. By default, it is in the path:
C:\Program Files\Apache Software Foundation\Tomcat 10.1\webapps\
 1. Delete the webapps folder.
 2. Copy the backed-up folder to its original location.
- Locate the "header.iss" file located at: "[drive]:\Program Files\Apache Software Foundation\Tomcat 10.1\conf".
 - Copy the backed-up file to its original location, replacing the existing file.
- Using sqlplus connect to the SG database user (typically rguser) and run this command:
 - SQL> truncate table system_setting;
- On the Master server, start the Continuity web server using the following steps:
 1. Open a command line window running with administrator privileges.

2. Enter the following commands:

```
# net start tomcat10
```

```
# net start TomcatWatchDog
```

- Confirm that the system shows the correct version in the UI (before the HF)

Getting help

If you have a current maintenance agreement, you may access Technical Support information here:

<http://www.continuitysoftware.com/support>

Customer service information is available here:

<https://www.continuitysoftware.com/contact/>