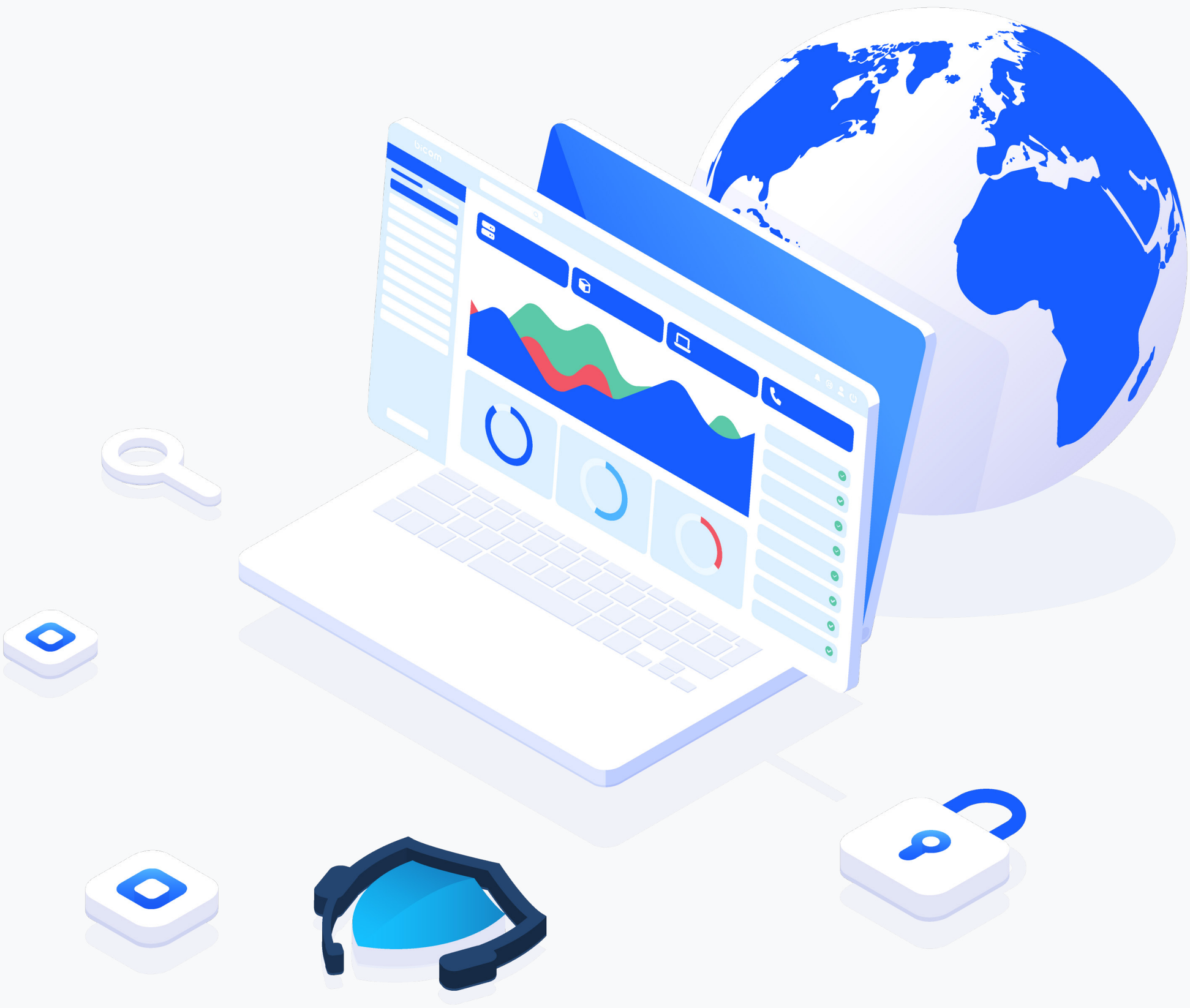


RELEASE NOTES

SERVERware 5.1.0

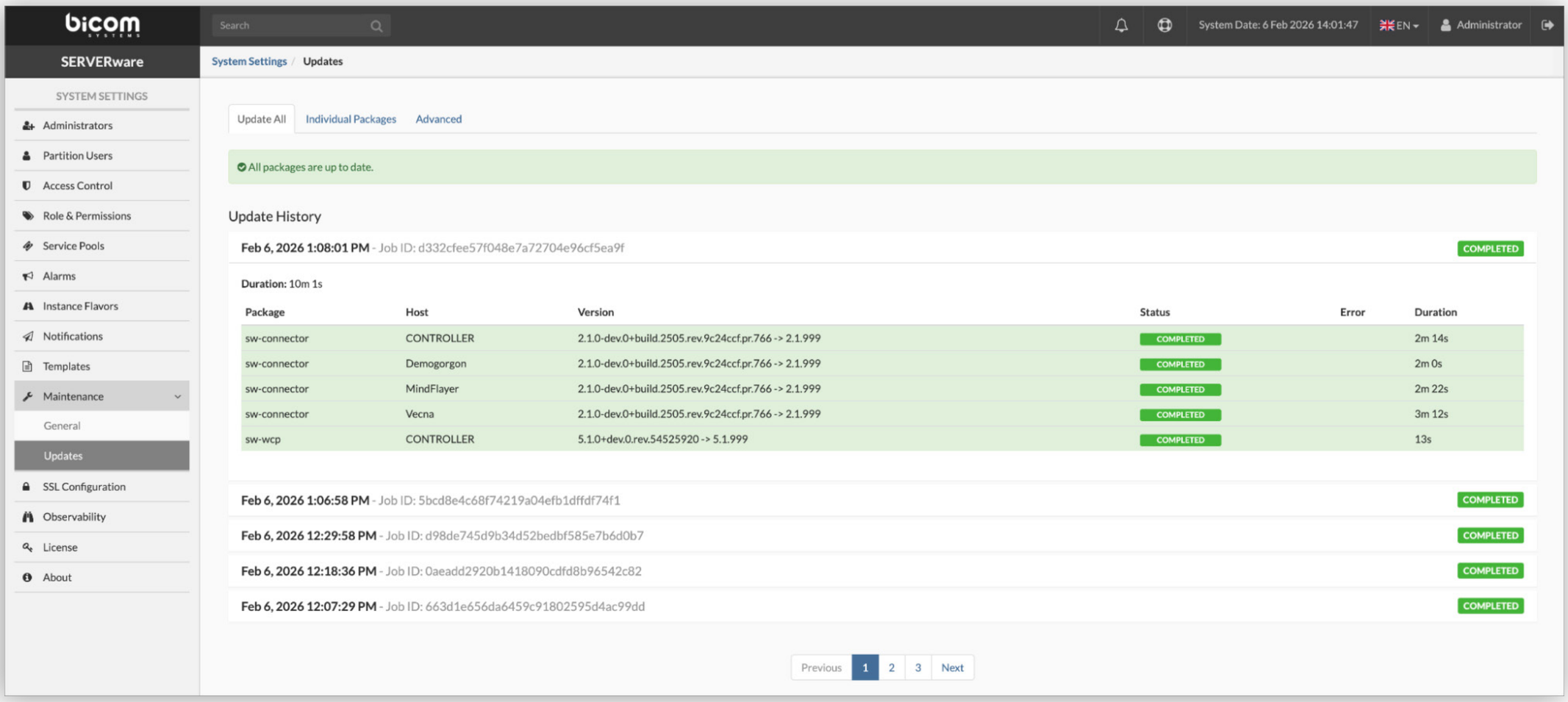
wiki.bicomsystems.com

Table of Contents

The SERVERware release v5.1 brings a set of practical SERVERware improvements aimed at making everyday operations simpler and more reliable. New features like Maintenance Mode and the Services page give administrators clearer visibility and better control, while backend hardening and workflow refinements improve overall stability. Together, these updates help reduce downtime, avoid surprises, and make system management more predictable.

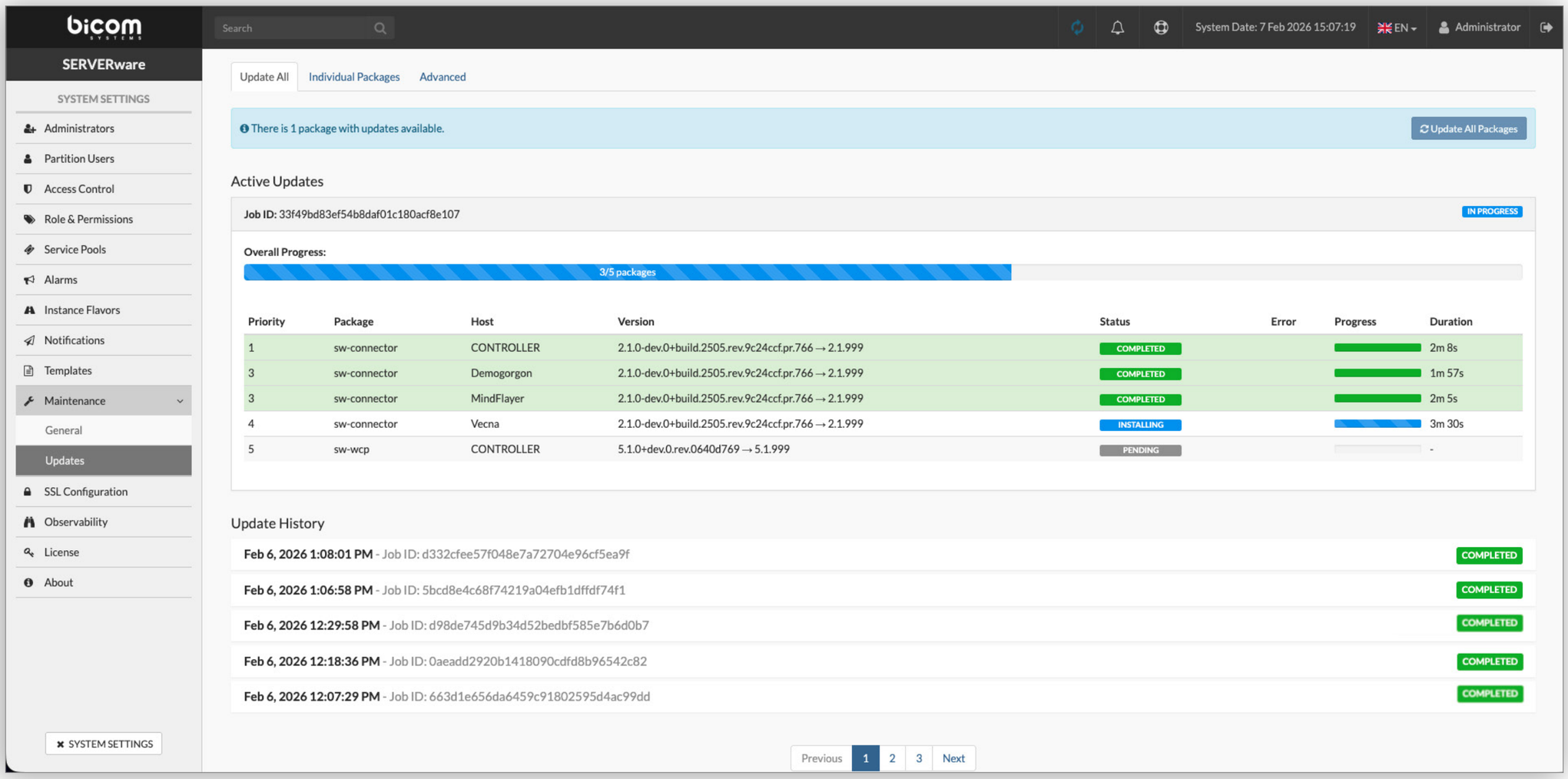
SERVERware Update Manager

This release adds a new, streamlined GUI update process that lets administrators start a full system update with a single click and follow its progress in real time.



The existing update workflow remains unchanged and is now available under Maintenance → Updates → Individual Packages, while a new All Packages tab shows the overall update status and provides an Update All Packages button when updates are available.

When an update is running, an Active Updates view shows the update job along with detailed information for each package and host, including progress, duration, status, and any errors. An icon in the navigation bar also alerts administrators that an update is in progress and provides quick access to the update view.

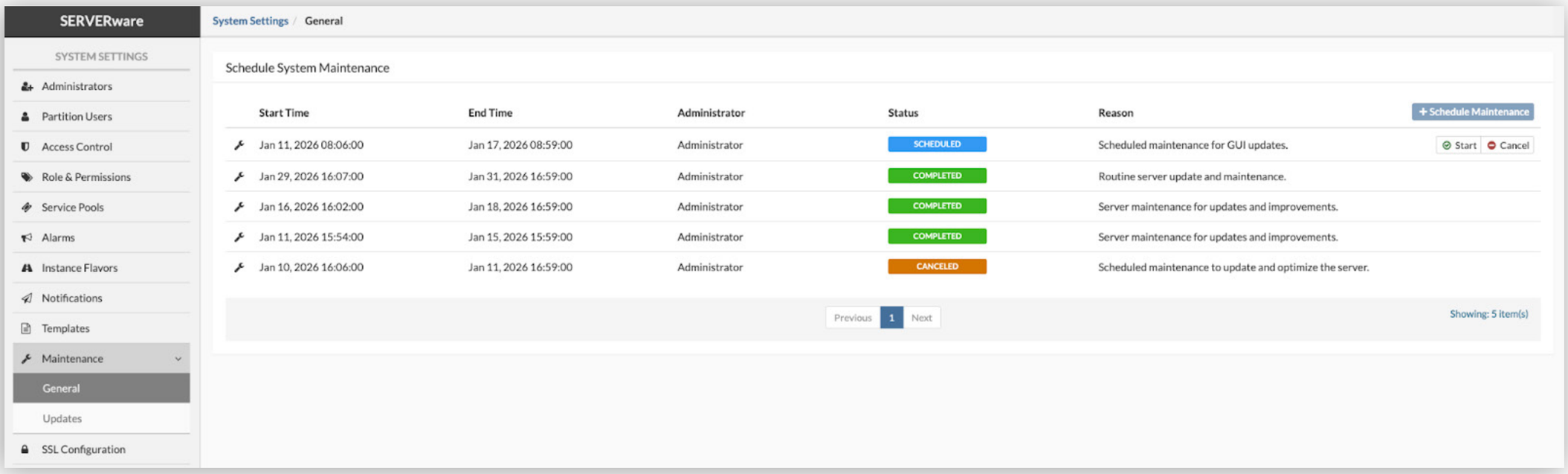


Once the update finishes, it moves into a new Update History section with pagination and complete job details. The package catalogue is refreshed automatically, and new updates cannot be scheduled during an active update.

The legacy GUI update option has been retained and renamed to Individual Packages, and a new All Packages view has been added for bulk updates. Update availability is now shown in both views, and audit logs are recorded for every update job and item.

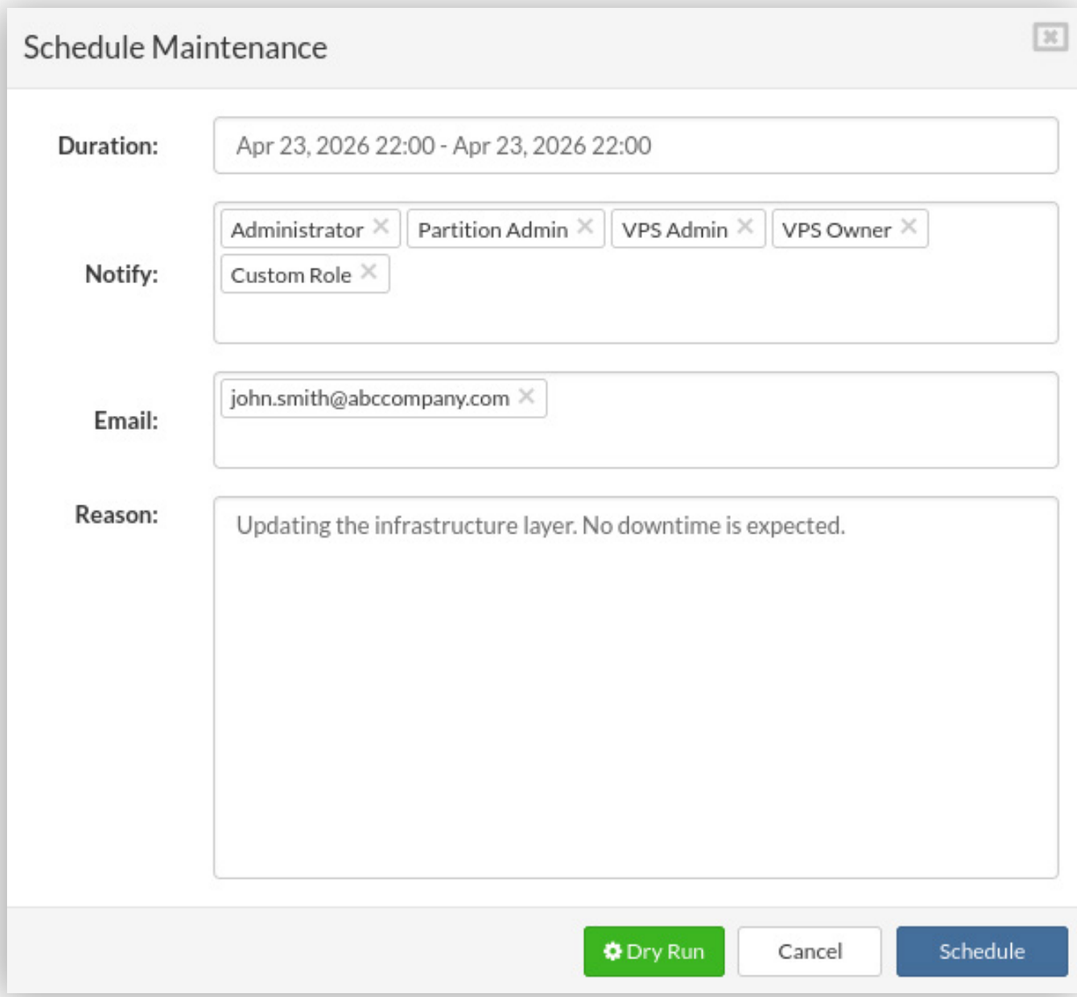
Maintenance Mode

SERVERware introduces Maintenance Mode, a feature that provides administrators with control and visibility during system maintenance.

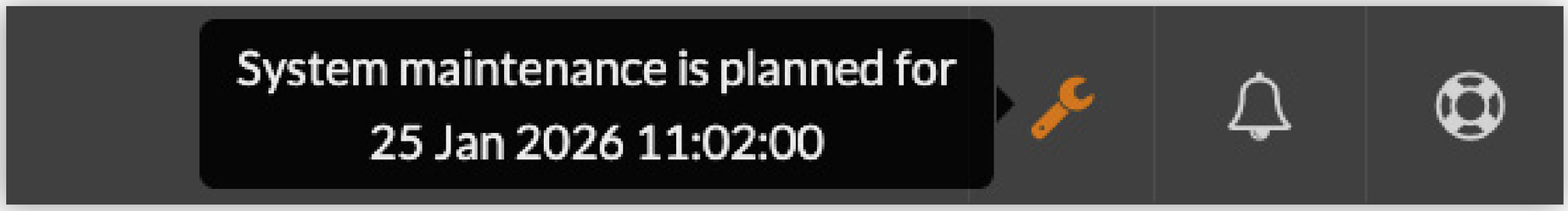


With this feature, administrators can schedule maintenance ahead of time, ensuring that users are informed and that critical operations are prepared in advance.

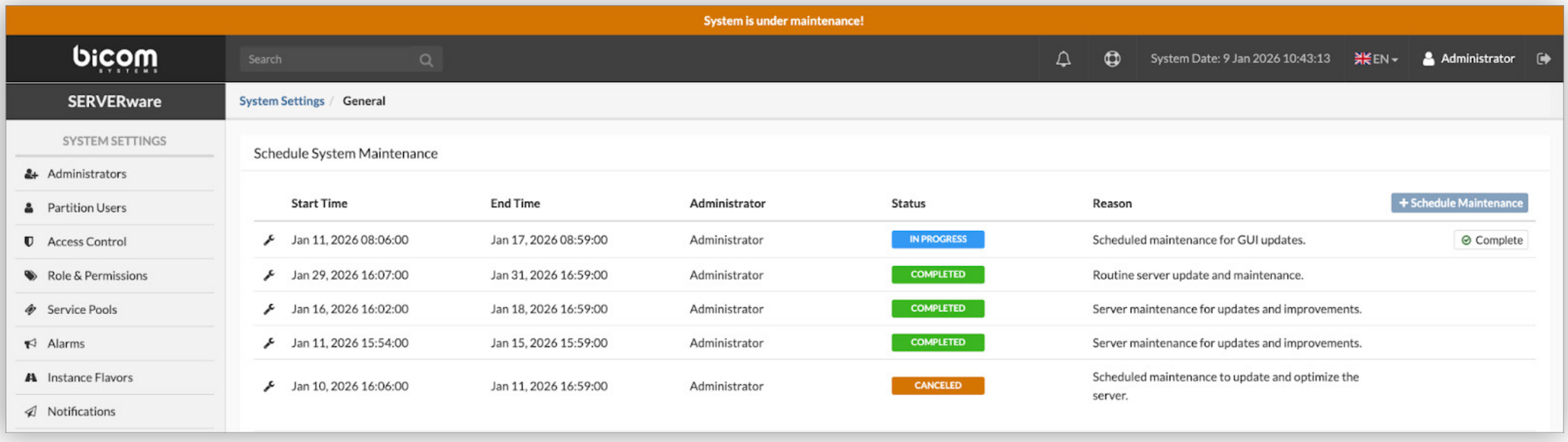
Before scheduling maintenance, it is strongly recommended to perform a Dry Run to identify and stop services that could cause issues during the process. Once maintenance is started from the GUI, all users except the administrator that scheduled the maintenance are safely logged out. Remaining administrators can re-log into the server, while other users (Partition Admin, VPS Admin, and VPS Owner) are prevented from logging in. Operations such as backup, GR replication and Site monitoring are temporarily disabled until maintenance is completed.



A clear status display keeps everyone informed, and administrators retain the ability to manually control maintenance at the host level.



Administrators who are logged out due to maintenance will receive a clear message (after logging in) indicating that the system is under maintenance, allowing them to act accordingly.

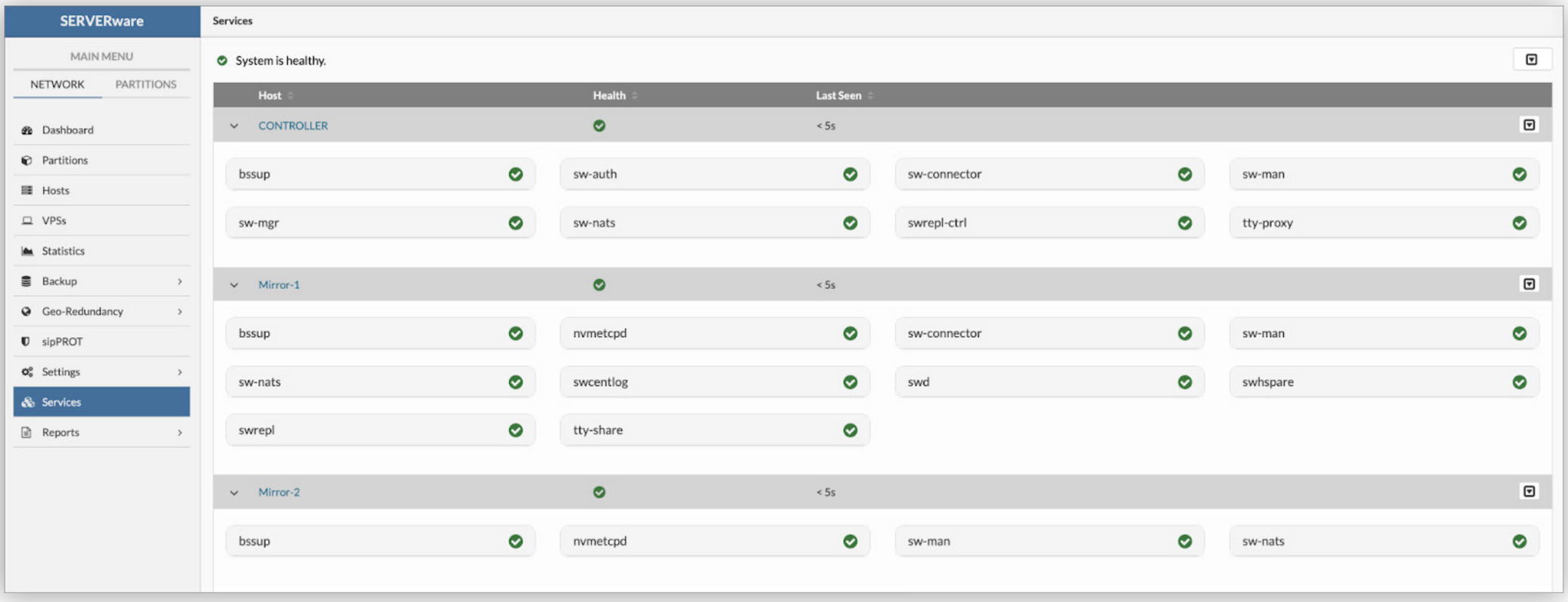


Maintenance Mode makes system upkeep safer, more predictable, and fully transparent, minimizing downtime and enhancing operational confidence.

SERVERware Services Page

The new Services Page in the SERVERware GUI provides a clear overview of all services running across servers, making it easier to monitor system health and quickly identify any issues. The page updates automatically every five seconds to show the latest status, giving real-time visibility into the user's environment.

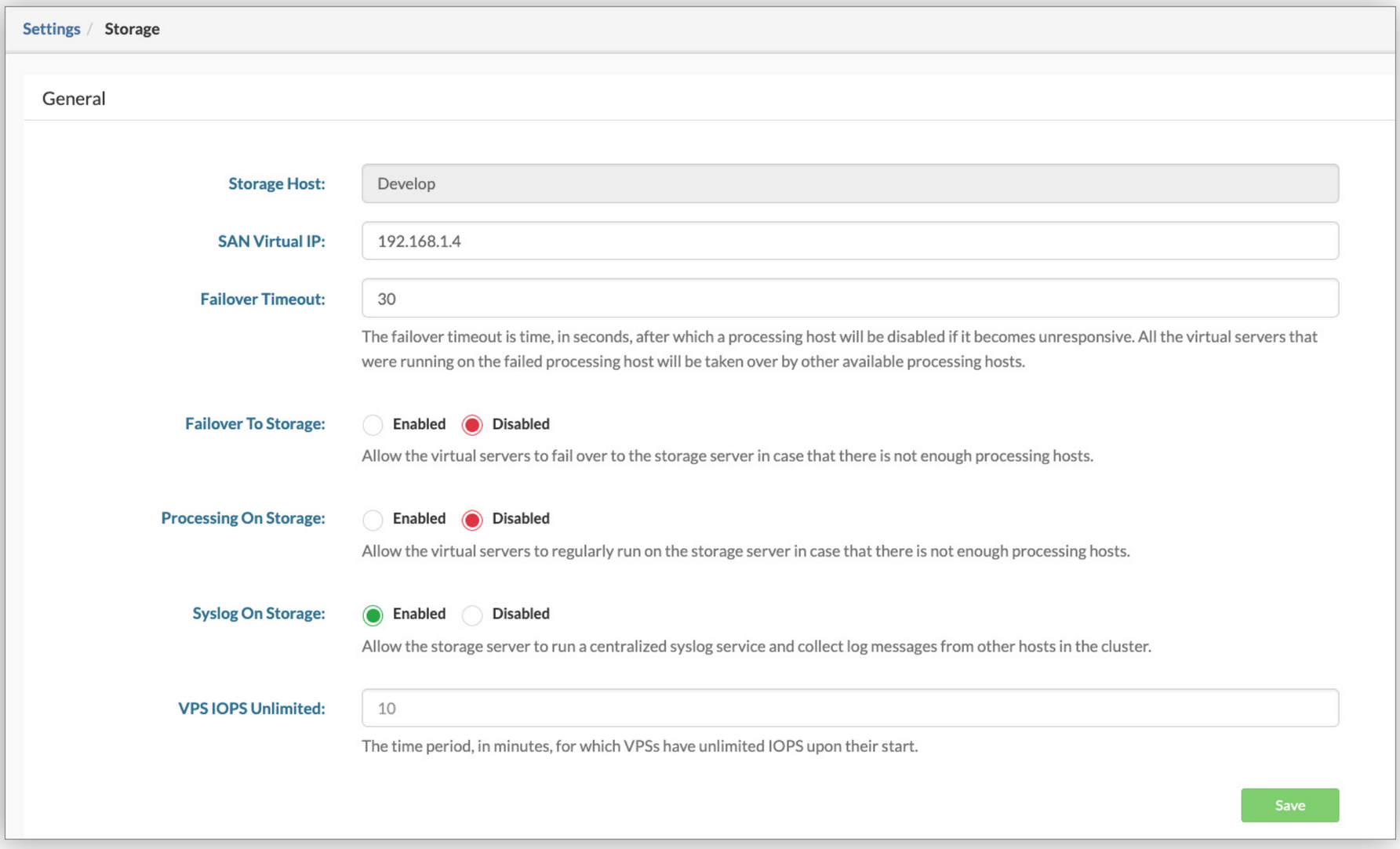
Hosts and services display intuitive status indicators, with warning icons highlighting any components that are not running as expected.



Service cards change color when a service is down, and the "Last Seen" column shows when each host or service last reported its status, with healthy components displaying <5s for up-to-date monitoring.

Storage Settings Redesign

The General and Advanced sections are now combined into a single “General” section, with a Save button that applies all changes at once.



Input validation ensures that invalid values are highlighted with a red border and warnings, and the Save button is disabled until all entries are correct. Fields that cannot be changed, such as storage host names when applicable, are now clearly greyed out.

SERVERware Hardening

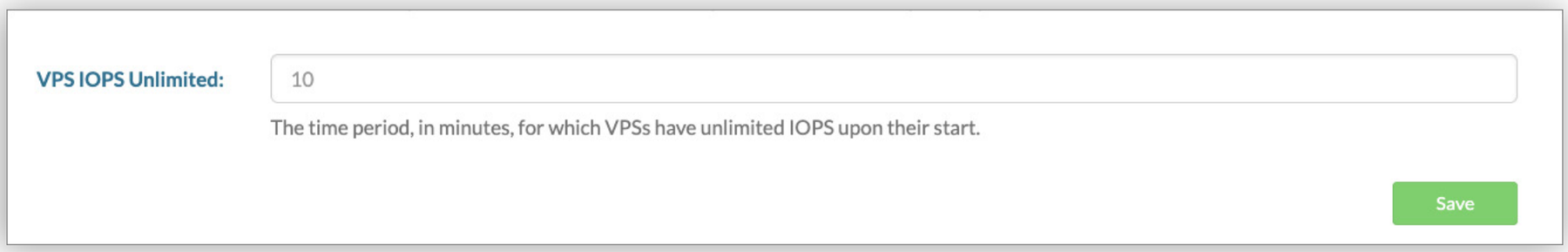
The release v5.1 focuses on strengthening system stability, improving operational reliability, and enhancing transparency across core SERVERware functionalities. Several internal mechanisms have been refined to reduce edge-case failures, improve recovery behavior, and provide administrators with better control and visibility.

Dynamic allocation of unlimited IOPS during VPS start

SERVERware now automatically allocates unlimited IOPS to a VPS when it is started. This ensures that critical internal processes such as filesystem checks or database recovery can complete without being throttled. Unlimited IOPS are applied temporarily and automatically reverted after a configurable timeout (10 minutes by default), restoring the IOPS limits defined by the VPS flavor or administrator. This behavior applies consistently across all start actions, including host moves and restores, and has been validated under load, evacuation, and reboot scenarios to ensure host stability.

GUI control for unlimited starting IOPS

To complement the automatic IOPS allocation, administrators can now control this behavior directly from the GUI (Settings>Storage). A global option allows enabling or disabling unlimited IOPS on VPS start and configuring the timeout duration.



Additionally, this setting can be overridden on a per-host basis, allowing finer control depending on host capabilities or workload requirements. By default, hosts inherit the global configuration.

Core upgrade reliability improvements

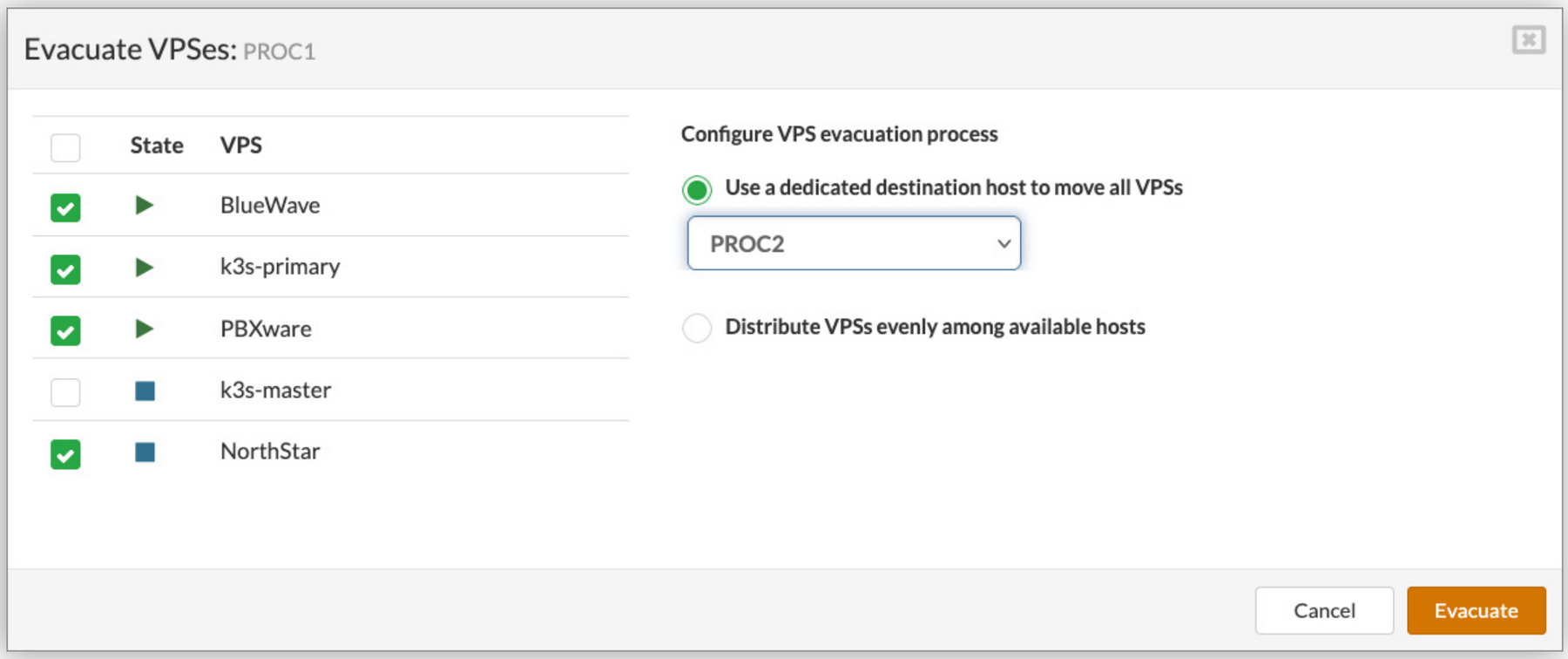
Several enhancements have been made to the core upgrade process. The upgrade script now verifies that sufficient disk space is available before execution, preventing unclear failures and providing administrators with explicit feedback when requirements are not met. Additionally, detailed upgrade logs are now generated and preserved across reboots, stored in a dedicated location with clear version-based naming to simplify troubleshooting.

Template refactoring and cleanup

The VPS template system has been refactored to resolve long-standing issues affecting restore, takeover, clone, and snapshot operations. Template information is now stored in a unified text-based format within the VPS database, reducing dependencies on multiple template-related tables. As part of this change, unused links, columns, and legacy fields have been removed, and API documentation has been updated accordingly. These changes improve consistency while preserving existing functionality.

Redesigned evacuate functionality

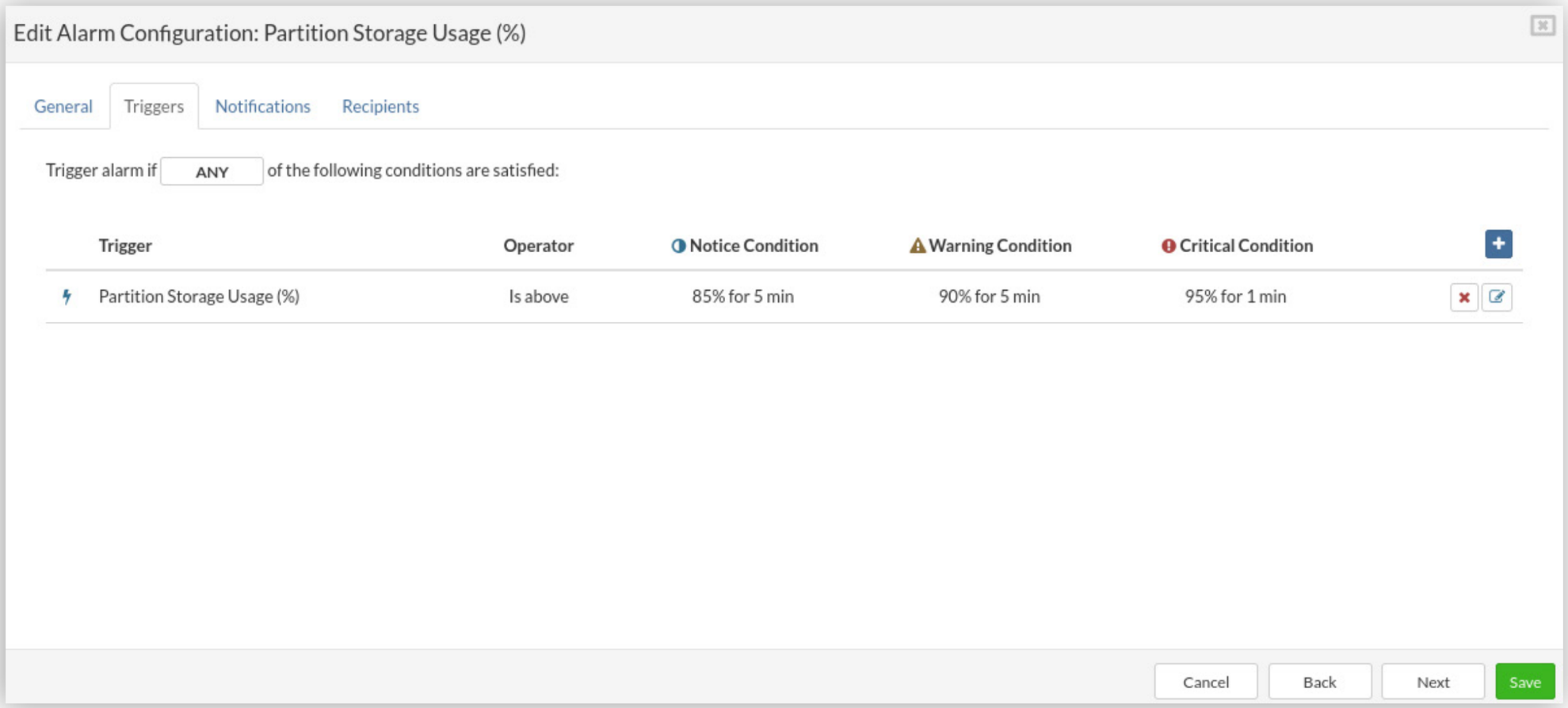
The evacuation workflow has been redesigned to provide greater control. Administrators can now select specific VPSs to evacuate from a host or choose to move all VPSs at once.



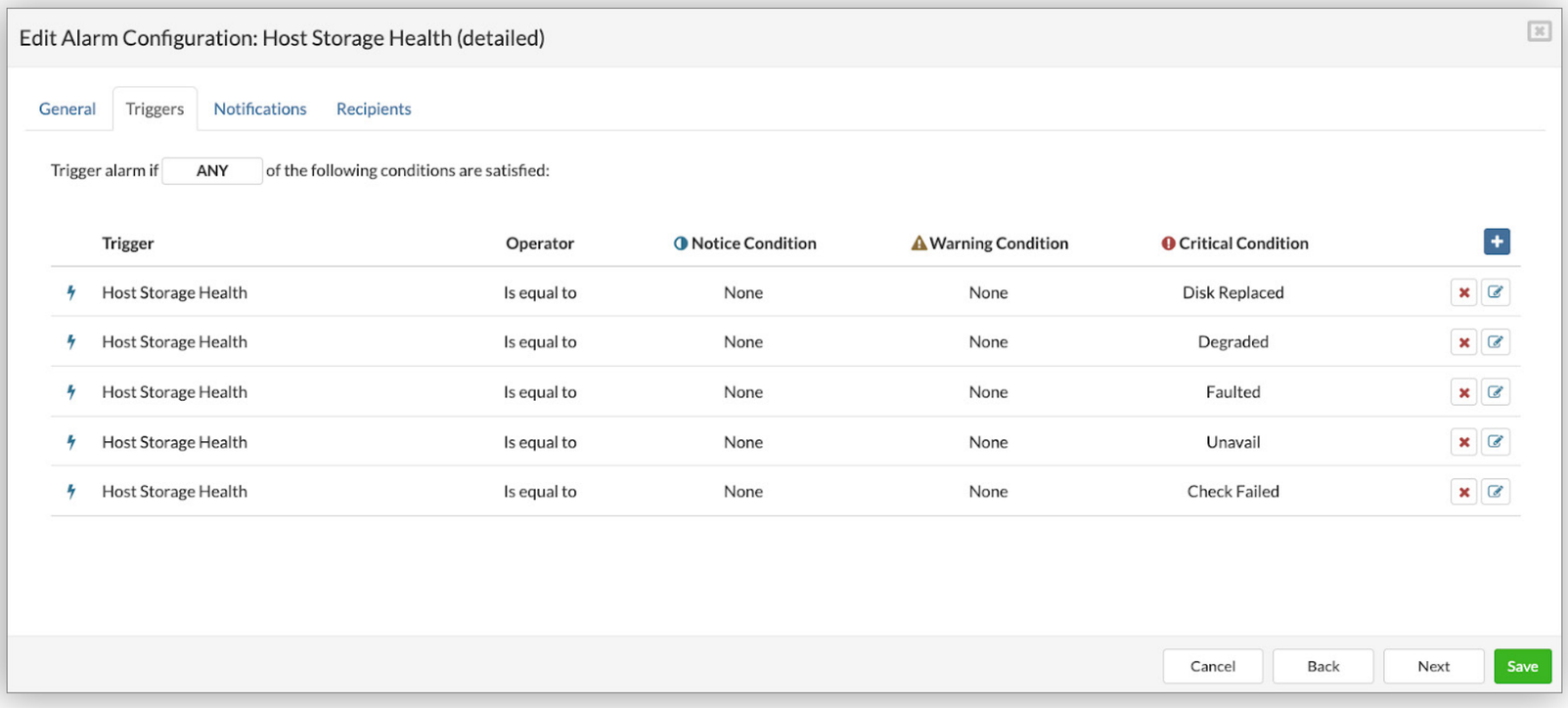
The selection dialog clearly separates running and stopped VPSs, and bulk evacuation targets can be defined explicitly. Existing undo functionality remains unchanged.

Alarm Improvements

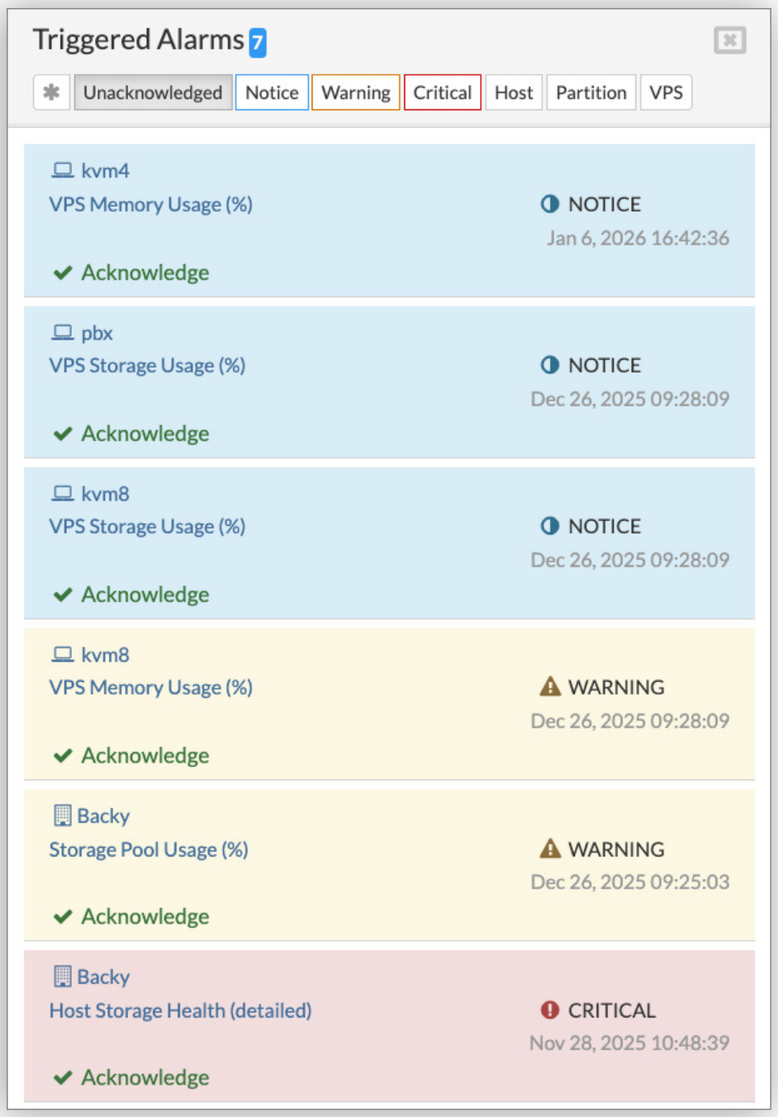
SERVERware hardening introduces several enhancements to the alarm system for better visibility and control. A new alarm has been added for partition storage usage, alerting administrators when a partition is nearing full capacity to prevent VPSs from moving to read-only mode.



The default triggers for host storage health alarms have been expanded, providing more granular notifications for different pool states, with configurable notification frequency.

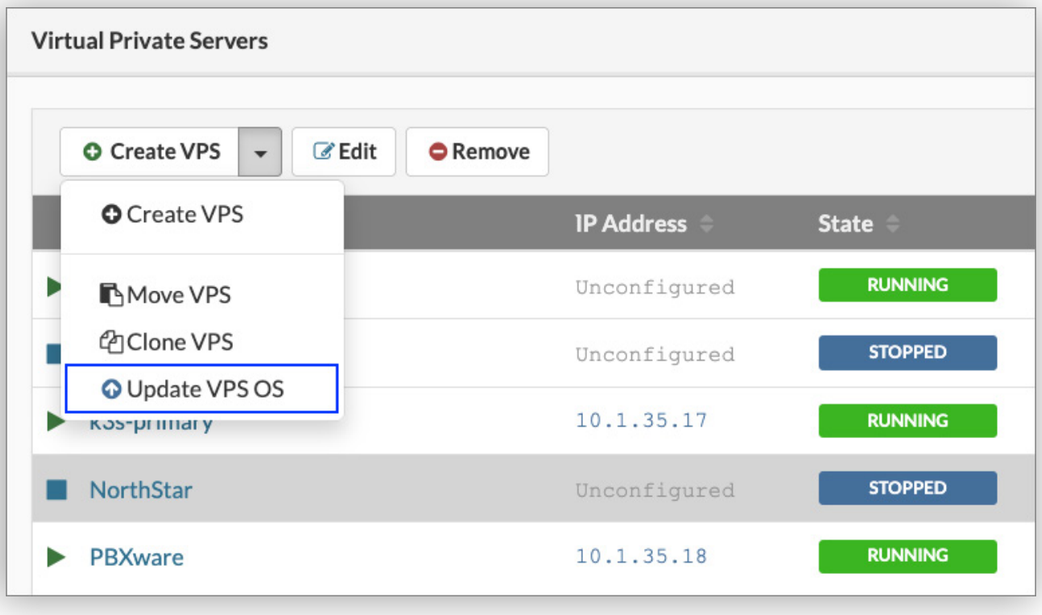


Alarm notifications now support improved filtering in the side panel, allowing administrators to filter by acknowledgment status, condition (notice, warning, critical), or type, with clear counts displayed on both the notification bell and alarm view. Multiple triggers for alarms have been corrected, ensuring that notifications are sent when any trigger condition is met, including state changes for already acknowledged alarms.



Base OS Update for PBXware VPS

SERVERware now allows administrators to update the base operating system of PBXware VPS instances directly from the GUI. To perform the update, the VPS must be stopped and must not be involved in any ongoing tasks. The update process is based on Artix Linux community templates.



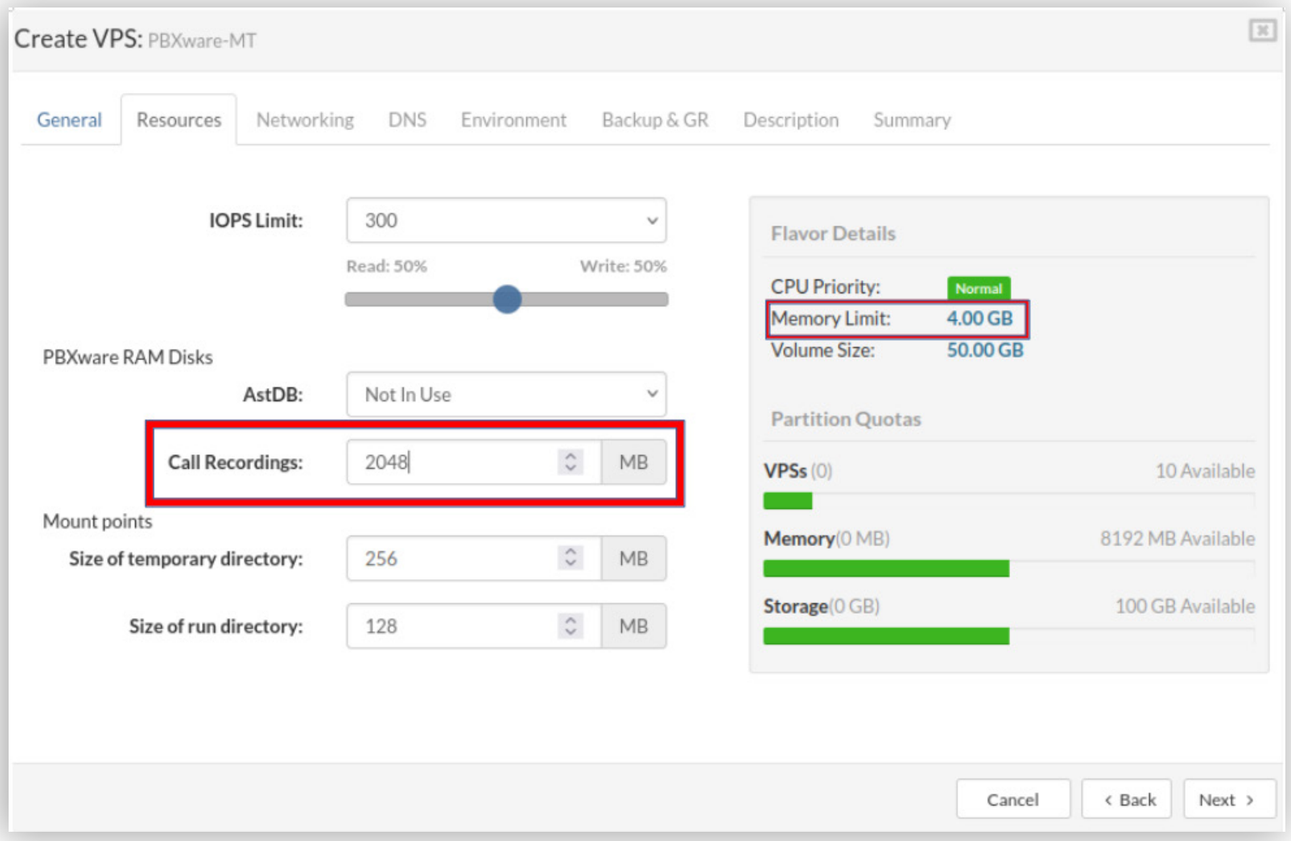
Important system files and credentials are preserved during the update, ensuring continued access with the same users and permissions after completion.

Artix Linux is used for PBXware VPS operating system updates as a replacement for the previously used Gentoo-based system. This change simplifies package management and the installation of additional software while maintaining a non-systemd environment, and enables more efficient delivery of security updates and newer library versions, reducing maintenance effort and keeping systems up to date.

As a result, Artix Linux is the default operating system used for PBXware VPS deployment within SERVERware. Ubuntu remains available as an option for deploying PBXware outside of SERVERware environments.

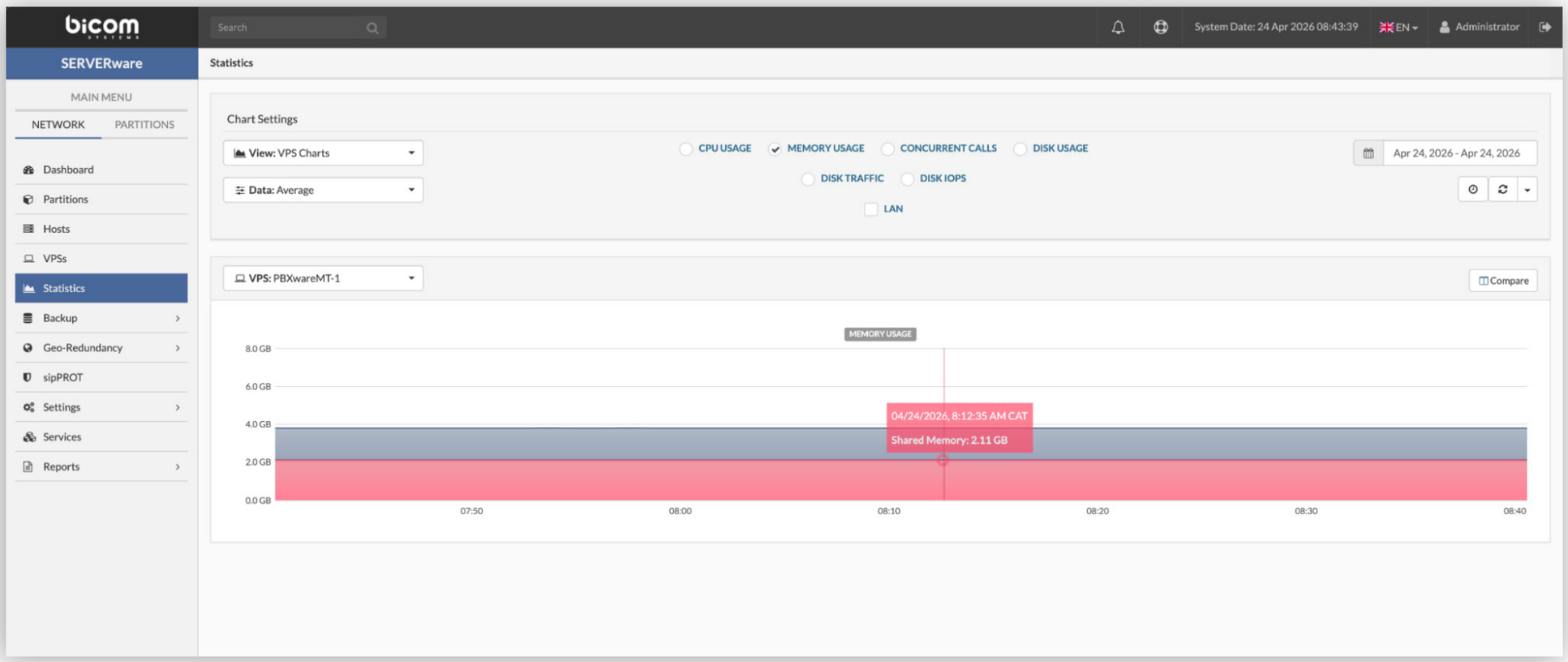
Call Recordings Memory Size

With the new AI voice features and the increased resource consumption for call recordings, the call recording memory size (tmpfs) can now be configured to scale within the VPS's memory, up to a maximum of 50% of the VPS's RAM. A safe upper limit is retained to ensure that other VPS services are not at risk of running out of memory.



Improved Statistics

As part of this improvement, stats collection and display are now in place, allowing administrators to easily track resource usage on the Statistics page. Memory used for call recordings appears in the VPS charts under Memory Usage, with the Shared Memory (red) section indicating the portion consumed by call recordings.



sipPROT

This release introduces several improvements to make sipPROT safer, more transparent, and easier to operate in clustered environments.

sipPROT Excluded From Backup Hosts

sipPROT is no longer installed on backup hosts, since these hosts do not run VPSs. This prevents backup hosts from unnecessarily consuming sipPROT host licenses that should be used by active production hosts.

For existing deployments, when updating or upgrading to this version:

- If the destination host is a backup host, any existing sipPROT instance will be automatically stopped and removed.
- This avoids situations where sipPROT accidentally occupies a license and leaves an active host unprotected.

Additional Notifications When Firewall Protection is Disabled

sipPROT now sends notifications whenever firewall protection is disabled on a host, helping administrators immediately detect unprotected systems.

A notification is sent to all configured recipients whenever firewall protection is disabled on a host. The notification follows the standard sipPROT format and includes the affected host name, the controller IP address, and the time the event occurred.

Alerts for Unhealthy Hosts

If the sipPROT daemon unexpectedly stops or crashes on a host, the system will now detect this condition and send an additional notification. This ensures administrators are alerted even when sipPROT does not shut down cleanly.

Improved sipPROT Configuration Logging

sipPROT logging has been enhanced to provide better visibility into configuration changes.

Configuration changes are now logged in greater detail, with particular emphasis on GeoIP policies and country settings. Logs may include individual configuration changes or the complete active configuration, improving auditability and troubleshooting.

CONTACT BICOM SYSTEMS TODAY

to find out more about our services

Bicom Systems (USA)

2719 Hollywood Blvd
B-128
Hollywood, Florida
33020-4821
United States
Tel: +1 (954) 278 8470
Tel: +1 (619) 760 7777
Fax: +1 (954) 278 8471
sales@bicomsystems.com

Bicom Systems (CAN)

Hilyard Place
B-125
Saint John, New Brunswick
E2K 1J5
Canada

Tel: +1 (647) 313 1515
Tel: +1 (506) 635 1135
sales@bicomsystems.com

Bicom Systems (UK)

Unit 5 Rockware BC
5 Rockware Avenue
Greenford
UB6 0AA
United Kingdom

Tel: +44 (0) 20 33 99 88 00
sales@bicomsystems.com

Bicom Systems (FRA)

c/o Athena Global Services Telecom
229 rue Saint-Honoré – 75001
Paris
Tel : +33 (0) 185 001 000
www.bicomsystems.fr
sales@bicomsystems.fr

Bicom Systems (ITA)

Via Marie Curie 3
50051 Castelfiorentino
Firenze
Italy

Tel: +39 0571 1661119
sales@bicomsystems.it

Bicom Systems (RSA)

12 Houtkapper Street
Magaliessig
2067
South Africa

Tel: +27 (10) 0011390
sales@bicomsystems.com

Follow us

www.bicomsystems.com