PROXEDO

API SECURITY

Proxedo API Security

Release notes for PAS 4.4.0

DISCLAIMER

Balasys is not responsible for any third-party websites mentioned in this document. Balasys does not endorse and is not responsible or liable for any content, advertising, products, or other material on or available from such sites or resources. Balasys will not be responsible or liable for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through any such sites or resources.

2023-05-03

The following new features, bug fixes and improvements have been completed for Release 4.4.0 Proxedo API Security.

Features

- **New base operating system**
  The PAS containers and host now run the Ubuntu 22.04 operating system to allow system administrators to apply the latest security and reliability updates, and enable the use of more advanced encryption capabilities.

Bug Fixes

- **Miscellaneous fixes**
  - The names of configuration elements in PAS are immutable, but the UI permitted editing these names, resulting in an error when saving the component. This UI now does not enable changing the name of a component when editing.
  - The *Request Code* and *Response Code* dropdown menus of the *Error Policy* brick were not scrollable when more than one error category was expanded. This has been corrected.
  - The *Failure Policy Code* dropdown menu of the *Endpoint* service was not scrollable when more than one error category was expanded. This has been corrected.
  - The *Header* matcher caused an unexpected error when the configured *Header* was not present in the traversing API call. This has been corrected.
  - Replacing the contents of a file brick resulted in an error. This has been corrected.

Improvements

- **Support for using the UI in multiple browser tabs**
  The PAS UI can now be opened in multiple browser tabs without re-authentication to allow the user to revisit other configuration elements while finalizing a configuration.
- **List usability improvements**
  Visual enhancements and inplace editing capabilities were added to lists, such as the *Backend* service's *Servers* list and the *Monitoring Manager's SNMP v3 Users* list.
- **The type of file bricks is now displayed**
  The list of *File* bricks now displays the brick's file type.
- **Default TLS options for Syslog TLS bricks**
  PAS now supplies a strict default for the TLS options when configuring *Syslog TLS* bricks.
- **Performance improvements in endpoint selection**
  When using the PAS's basic API aggregation capabilities, the *Endpoint* selection for a requested API subtree is performed faster.
- **Container debugging tools**
  PAS now ships tools and documentation on how to perform debugging tasks within the container infractructure of the product.
- **Reduced container sizes**
  PAS now ships with reduced container sizes.

Notable changes

- **Syslog TLS bricks now only support recent TLS versions**
  PAS now only support TLS versions that are considered relatively secure. While using TLS 1.3 is strongly recommended in all scenarios, support for TLS 1.2 has been kept for compatibility purposes.

- **Restricted access to internal services**
  PAS now restricts network access to containers that are used for configuration management and secure storage.
- **Unattended upgrades have been disabled explicitly**
  To avoid unscheduled service interruptions, PAS now disables the base operating system's unattended upgrade mechanism explicitly. The VM installation package now conflicts with the unattended-upgrades package.