Fudo Enterprise 6.0
Release Notes

Date: April 2026

This is a major Fudo release, introducing a range of improvements and new fixes.

NEW FEATURES AND IMPROVEMENTS

- Introduced **Password Vault**, a new module that extends Fudo Enterprise with centralized secret storage and credential lifecycle management.
    - Supports secure storage of passwords, SSH keys, API keys, certificates, and secure notes.
    - Organizes secrets in a hierarchical collection structure for easier management across teams and environments.
    - Provides RBAC-based access control to collections, allowing precise delegation of management permissions.
    - Offers a dedicated view of secret-related activity to improve auditability and support security investigations.
    - Integrates with Password Changers to enable automated password rotation for stored secrets.
- Introduced a modular licensing model for Privileged Session Management and Password Vault.
- Introduced **Reverse Proxy**, enabling secure SSH reverse tunneling to publish internal services without exposing the infrastructure to inbound connections.
- Added **German** and **Uzbek** as new user interface languages.
- Complete UI refresh - The entire Fudo interface has been redesigned with a modern, clean aesthetic featuring updated typography, refined color scheme, simplified navigation structure, and enhanced visual hierarchy for better usability and professional appearance.
- Redesigned data tables interface - All tables throughout the product have been modernized with improved filtering, sorting capabilities, column visibility management, and cleaner visual presentation for enhanced user experience.

Fudo Security Sp. z o. o.
Al. Jerozolimskie 178
02—486 Warszawa
NIP 52425217
sales@fudosecurity.com

- Added CHAP and MS-CHAPv2 as a new authentication method options for RADIUS external authentication, providing enhanced security and compatibility with Microsoft Active Directory environments.
- Added support for the PostgreSQL protocol, enabling the creation of dedicated PostgreSQL servers and listeners.
- Added TLS support for VNC.
- Added support for connecting to target servers through reverse SSH tunnels.
- Added support for displaying the user who created the tunnel in SSH tunnel sessions established using an anonymous account.
- Added support for a custom hostname in RDP sessions. The new RDP Config Domain field in the RDP listener configuration defines the hostname shown in the RDP client title bar.
- Added visibility into the source of each session. The new Access channel column in the Sessions tab shows which product or client was used to establish the connection.
- Added fullscreen mode support to the Webclient for a more convenient session view.
- The Webclient clipboard now allows sensitive content to be hidden using the eye icon, so copied values such as passwords do not have to be displayed in clear text.
- Added a delay after authentication failures to help prevent brute-force attacks.
- Upgraded the operating system base to FreeBSD 14.3.
- Updated the Angular framework used by the web interface to version 21, the current stable release.
- Performed additional maintenance updates to frontend dependencies.
- Updated the FreeTDS library to support newer TDS protocol versions.
- ShareAccess improvements:
    - Improved organization owner reassignment in ShareAccess by limiting the selection to users eligible to become the new owner.
    - Added file upload support to the ShareAccess Webclient for RDP sessions.
    - Notifications in the ShareAccess GUI now include resource names for improved clarity.
- Fudo Officer mobile app improvements:
    - Added support for additional push notification types, including session start, session end, and policy alert notifications.
    - Added support for Password Vault access requests in the mobile app.
    - Added the ability to configure which Fudo Enterprise notification types are sent as push notifications to Fudo Officer.
    - Added a notification history view with detailed notification screens.

    - Added unread counters for access requests and notifications in the profile switch view.
    - Improved connection error handling in the mobile app.
- Improved the User Report and User Access Report by excluding anonymous entries that are not relevant to the purpose of these reports.
- Improved performance when adding new entries to large routing tables.
- Improved performance when loading large access account lists in UAG.
- Restored the ability to change the order of user authentication methods in LDAP synchronization settings.
- Added logging and storage of user location data during authentication. The recorded location information is currently available through the API.
- Improved performance of session filters by reducing delays in displaying the Removed toggle and updating object counts.

API CHANGES

The API continues to evolve with new endpoints introduced alongside new product features. We've added numerous new object specifications, extending APIv2 support for managing:

- Password Vault
    - Collections
    - Secrets
    - Password Vault global settings
- User notification assignments in Safes and Password Vault collections
- Reverse Proxy

We've also added a search parameter to the API, enabling text-based queries across selected object attributes.

DISCONTINUED FEATURES

- Fudo Enterprise 6.0 **no longer supports transparent and gateway modes** in the listeners configuration. All listeners still configured with transparent or gateway modes **must be reconfigured** to use proxy or bastion modes **before starting the upgrade.** Refer to the **Before You Upgrade** section for detailed guidance.
- Fudo Enterprise 6.0 **no longer supports bridge interfaces** and **network interface cards with bypass mode**. These components were closely tied to transparent and gateway modes, which were removed in version 6.0. Before upgrading, review your network

configuration and ensure that all bridge interfaces are removed and bypass mode is disabled to avoid compatibility issues after the upgrade.

- Support for the **Telnet 3270** protocol is **under review** and may be removed in a release following version 5.6. If this protocol is critical to your environment, please contact Fudo Support for more information.
- Support for the **4-Eyes** principle, implemented through the **Require approval option** in safe configuration and used to restrict user access by requiring confirmation, is currently under review and is planned for removal in a future release. Its functionality is largely covered by the Just In Time feature, which we recommend adopting instead. If this functionality is critical to your environment, please contact Fudo Support for more information.

ANNOUNCEMENTS

- Sessions established through an SSH tunnel may use an anonymous account, but they are still assigned to the user who created the tunnel and remain attributable on the Sessions list.
- In future releases, the handling of selected SSH MAC algorithms may be further aligned with the Legacy Crypto setting, which may affect their availability and behavior.

BUG FIXES

- Fixed an issue where commands cleared from the terminal during SSH sessions in Webclient were missing from text-based session recordings.
- Fixed an issue in User Access Gateway where pool names were not displayed in the Active Connections view.
- Fixed an issue where generated passwords did not fully comply with the character set restrictions defined in the password changer policy.
- Fixed multiple issues affecting recorded MSSQL and MySQL session playback, including missing queries and decoding errors.
- Fixed an issue where the Player continued to show completed live sessions as still active.
- Fixed an issue with overlapping server address ranges that could cause the wrong server configuration to be selected and block access.
- Fixed an issue where Azure users in UPN format could not be correctly mapped through OIDC based on the configured domain.
- Improved validation of uploaded HTTP certificates and keys, with clearer feedback for invalid or mismatched files.
- Restored the Connection Command display for MySQL accounts in UAG.

- Fixed an issue where master key invalidation did not correctly re-encrypt previously stored data.
- Fixed an issue where the hotfix installation confirmation window remained open after a successful installation.
- Fixed an issue where Syslog event forwarding configured with an FQDN server address did not resume automatically after reboot if DNS resolution was unavailable during system startup.
- Fixed an issue where, in configurations with multiple DNS servers, the system did not consistently use the primary DNS server first, which could cause intermittent external authentication delays or failures.
- Fixed an issue where copied LDAP Verifier password changers displayed the DN/Filter field as mandatory.
- Fixed an issue where roles could be manually assigned to LDAP-synchronized users while synchronization was enabled.
- Fixed an issue where a WinRM-based Password Changer ignored the configured transport_bind_ip value and used an incorrect outbound interface and source IP address during password changes.
- Fixed an issue that prevented organizations from being found through the search field in Sessions filters.
- Fixed an issue where filters could omit servers beyond the first 300 results.
- Fixed an issue where the *Bind Address* could not be selected when enabling Diagnostics for the first time.
- Fixed an issue in version 5.6.4 where report generation could fail in environments using specific time zones.
- Fixed an issue where LDAP group GUID values in newly created mappings could be reset during synchronization, which could interrupt further sync operations. For newly created configurations, the default GUID attribute is now set to entryUUID.
- Added support for direct upgrade from version 5.4.12 to 6.0.
- Fudo Officer: Fixed an issue with missing notification sounds on iOS.
- Fixed an issue where external storage connected through multiple additional disks on the same FC interface might not reconnect correctly after an upgrade or reboot, which could cause missing session previews and prevent new session recordings from being saved to that storage.
- Fixed an issue where password changers using templates with Transport host set to predefined did not apply the associated target server configuration, which could cause

password change operations to fail in environments requiring specific connection settings, such as Legacy Crypto.

- Fixed issues affecting manual account onboarding in Discovery, including incorrect object selection behavior when assigning safes and listeners, and a backend rule validation problem that could trigger an assertion error during onboarding or quarantine actions.
- Fixed an issue where generating a report for a single session could produce a report containing all sessions instead of only the selected session.
- Fixed an issue where passwords enclosed in curly brackets ({}) could cause authentication to fail.

KNOWN ISSUES

- Anonymous accounts associated with a tunnel listener can currently be assigned to only one safe. Scenarios requiring the same tunneled anonymous account to be used across multiple independent safes are not supported.
- It is currently not possible to set Password Vault as the authentication method for an account if a default password policy is still assigned to that account.
- Users whose account validity expires during an active Admin Panel or User Access Gateway session may retain access until the session times out. During this time, some functions may behave inconsistently, including logout, Dashboard data display, and session establishment.
- In clustered environments, the Downloads section may display session recording download links on nodes where the exported file is not locally available, which can result in unsuccessful download attempts.
- After a backup server is removed from the configuration, safes previously associated with it may continue attempting to replicate or restore sessions using that server, which can lead to errors.
- Users disabled in LDAP may still be synchronized as active, even when the Sync users block state option is enabled.
- Users who do not have permission to view the sessions list may still be able to access session data stored in raw format.
- In environments that require a specific source IP for routing or firewall policies, SMTP notifications may not work as expected when the bind address is configured using an IP label.

BEFORE YOU UPGRADE

It is highly recommended to perform the *'Upgrade check'* before the proper upgrade. The result of the failed check may contain information about configuration changes that needs to be done by a Fudo administrator to successfully upgrade Fudo.

There are a few things that need to be verified before this upgrade can be applied:

- Make sure your Fudo instance isn't undergoing any system-wide process, such as storage rebuild, or the system isn't under full-load.
- In a cluster configuration, make sure all nodes are synchronized and upgrade the slave node first.
- Make sure you have an active Premium or Standard Support maintenance contract.

Transparent and Gateway Modes Discontinuity

Starting with this version, transparent and gateway modes have been removed from the listeners configuration. To ensure a successful upgrade, review your configuration in advance and replace all listeners using these modes with proxy or bastion mode equivalents.

Licensing Changes

Starting with version 6.0, the licensing model has been updated. The previous Fudo Enterprise license, which covered the core PAM functionality, is **now represented as the Privileged Session Management (PSM)** module. **Password Vault (PV)** is licensed separately. **ShareAccess** continues to use a separate license.

After upgrading to version 6.0, your existing license will enable Password Vault in the BASIC version with limited functionality. To use the FULL version of Password Vault, contact your partner.

Also note that the active user counting model for the PSM module has changed. A user is now counted as active if they have established a session within the last 30 days. Users active within that period continue to consume a license slot until the activity window expires.

> **Note:** Now logging into the Admin Panel is always allowed. This prevents administrators from being locked out of the system due to license limits.

If the licensed limit has already been reached, only users who were already active within the last 30 days can continue to establish sessions. Users who have not been active during that period cannot start new sessions until a license slot becomes available.

Network Routing With Multiple Routing Tables (FIBs)

Due to the FreeBSD upgrade, subnet routes derived from interface IP addresses are no longer automatically propagated across all routing tables. Services that do not allow specifying a bind address (e.g. DNS) will only use routes available through the default routing table (FIB 0).

RECOMMENDED UPGRADE PATH

Before proceeding with the upgrade, please verify the version number of your Fudo Enterprise instance. Depending on the version number, you will need to follow a specific upgrade path. To learn more, please refer to the Fudo Enterprise Product Upgrade Path article.

> **Note:** Fudo Enterprise **5.4.12** introduced a new upgrade barrier in the Product Upgrade Path. If you are upgrading from an earlier Fudo Enterprise 5.4.x release, upgrade to version 5.4.12 first before proceeding to any newer version.

HOW TO UPGRADE YOUR FUDO

1. Login to your Fudo Admin Panel.
2. Select **Settings > System** from the main menu on the left-hand side and go to the **Upgrade** tab.

> **Note:** If your Fudo is running in a cluster, start the upgrade on the Slave node, and only when the upgrade finishes successfully start upgrading the Master node. When both systems are running the same Fudo version cluster communication will be restored.

3. Select **Upload** from the top right side and upload the previously downloaded and unzipped upgrade package file.
4. Select **Run Check** to determine if your upgrade file is correct and can be applied to the existing Fudo configuration. Refresh your browser window to see **Upgrade check** current progress.
5. **Review the Upgrade Check results** to confirm that the upgrade file can be applied the existing Fudo configuration.
6. Upon a successful **Run Check** result, upgrade your Fudo by using the **Upgrade** button. Upon system restart, all active sessions will be terminated.

Note: In case of an unsuccessful check do not upgrade your system, double check your upgrade file checksum. If you encounter any problems, get in touch with us and we will assist you.

HOW TO IMPORT SYSTEM CONFIGURATION

Note:

- Importing a configuration file and initiating system with imported data will delete all existing session data.
- Export/import can be performed only between Fudo Enterprise instances with the same serial number and version.
- It is not possible to export configuration in a clustered setup.

1. Login to your Fudo Admin Panel.
2. Select **Settings > System** from the main menu on the left-hand side.
3. Go to the **Configuration** tab.
4. Upload the *'Master key'* file and *'Configuration file'* exported from another Fudo instance and click **Import** to proceed with initiating the system with the imported data.

Note: For more details, please refer to the 'Exporting/Importing System Configuration' section of the Fudo Enterprise documentation.

THE ROLLBACK PROCEDURE

If you are experiencing issues with the newly installed version, you have an option to roll back to the previous version of Fudo running on this machine. To do so, click the user menu on the top right, select **Reboot**, and select previous system revision from the drop-down list.

Note: Rollback will result in the **loss of all sessions recorded** in the newer system version and **any system configuration changes** (including changes to RBAC roles or groups and password changers activity). Any object configurations created, modified, or recorded between the current and the previous system versions will be deleted. Please refer to *'Restoring Previous System Version'* for details.

CONTACT US

If you have questions or concerns, please get in touch at support@fudosecurity.com or by phone: +48 22 100 67 09.

Sincerely,

Fudo Security Team

Fudo Security Sp. z o. o.
Al. Jerozolimskie 178
02—486 Warszawa
NIP 52425217
sales@fudosecurity.com