Fudo Enterprise 5.6.3
Release Notes

Date: November 2025

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

NEW FEATURES

- **Extended AI-powered session summaries to support RDP sessions**, in addition to SSH. This enhancement enables administrators to quickly review both SSH and RDP activities using AI-generated summaries, further improving audit efficiency and reducing manual review time.
- Introduced **Kerberos support for User Directory synchronization**. When Kerberos authentication is enabled in **Settings > Authentication > Global** and the **User Directory server type** is set to **AD**, synchronization now uses the Kerberos protocol.
- Added support for converting TCP sessions to PCAP files.

IMPROVEMENTS

- Improved RDP session performance, providing better display quality and increased responsiveness.
- Improved efficiency of converted storage usage to optimize system resource utilization.
- Centralized the OTP generation logic to improve maintainability and consistency across components.
- Added legacy support for VNC environments using the RFB 3.3 protocol.
- Raised the log level for password change information in Fudo to make it more visible in system logs.
- Extended user synchronization attributes to include account expiration date and ensure access control does not rely solely on Active Directory (AD) authentication. This enhancement addresses the fact that AD does not flag expired user accounts as locked, which could result in situations where login remained possible through authentication methods independent of the domain controller. Following this change, Fudo now also synchronizes information regarding account expiration time to prevent users whose AD accounts have expired from logging in, especially in scenarios where the authentication

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

process does not directly involve the domain controller.
Note: Additional safeguards were introduced to prevent the new AD-mapping field from unnecessarily updating the expiration date during sync operations.

API CHANGES

We've added two new object specifications and group of endpoints, so you can now utilize APIv2 to manage:

- productivity
- external storage.

DISCONTINUED FEATURES

- The **Delta** button available for SCP/SFTP sessions in the Session Player view has been removed.
- Fudo Enterprise 5.6 no longer supports the **DHCP**.
- Fudo Enterprise 5.6 no longer supports the **APIv1**. All scripts using APIv1 should be rewritten to use APIv2.
- **Grant-related endpoints** have been **removed** in this release. Please update your integrations accordingly. For more information, refer to the **updated API documentation**.
- **Disabled** access to the **/api/v2/diagnostics** endpoint.
- Fudo Enterprise 5.6 no longer supports the **Application to Application Password Manager**.
- Fudo Enterprise 5.5 and 5.6 no longer supports the **Mobile Token** authentication method used to bind the Fudo Officer mobile application to a User. You must **unlink all Fudo Officer bindings** from Users configuration before the upgrade. For more details, please refer to the 'Before You Upgrade' section below.

ANNOUNCEMENTS

- Fudo Enterprise 5.6 is the **last version** supporting **transparent and gateway modes in the listeners configuration.** Listeners using these modes **must be reconfigured** to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the **transparent** and **gateway** modes, which will also be removed in version 5.7.

We recommend reviewing your network configuration to ensure compatibility with future versions.

- 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.

BUG FIXES

- Fixed an issue where upgrading directly from versions 5.5.x to 5.6.2 could result in an inability to authenticate with passwords containing some special characters (version 5.6.2 has since been withdrawn).
- Ensured that all legacy components, references, and artifacts related to the deprecated API version were fully removed after discontinuing its support, leaving the codebase clean and aligned with the current API architecture.
- Fixed an issue in Fudo Officer 2.0 on iOS devices where push notifications for new access requests were delivered without playing the notification sound, despite the app having the required permissions.
- Fixed an issue where access requests were not displayed in Fudo Officer 2.0 when accounts were not linked to a listener.
- Fixed an issue where generating a QR code in Fudo Officer 2.0 failed due to certificate errors, resulting in a 502 response.
- Fixed an issue where an incorrect message about incomplete Fudo Officer 2.0 pairing was displayed even after the device was successfully connected and functioning properly.
- Fixed an issue causing errors during session summary replication in clustered environments.
- Fixed an issue where AI models in clustered environments required retraining after an upgrade.
- Fixed an issue where files downloaded from session playback could differ from the originals transferred during the SFTP session.
- Fixed an issue in retention to ensure session data is only deleted after a successful external backup is confirmed.

- Fixed an issue where revealing a password in the User Access Gateway failed when the account used an SSH key from another account.
- The password changer fails when transport_bind_ip is set to a predefined type and the specified server bind IP is not available on the active password changer node.
- Fixed an issue where the password changer failed when transport_bind_ip was set to a predefined type and the specified bind IP was unavailable on the active node.
- Fixed an issue in the User Directory configuration where changing the *Encrypted connection* checkbox did not update the Port field, causing incorrect values to persist until the configuration was recreated.
- Fixed an issue where the *Common configuration* field in RDP functionality safe configuration allowed only a single line of input, instead of supporting multiple lines as in previous versions.
- Fixed an issue where users accessing an active session via a shared link lost real-time screen updates but could still perform operations (join, pause, type, or end the session) if the link was revoked during the session view.
- Fixed an issue that limited the Common configuration field for RDP functionality in safe configuration to a single line instead of allowing multiline input.
- Fixed an issue where the session list appeared empty on the last day of the month due to an incorrect default filter date in the Sessions view.
- Fixed an issue where opening a session fragment containing a searched phrase with special characters caused the Admin Panel to freeze.
- Fixed an issue where multiple redundant OCR processes could start after a Fudo reboot, causing excessive resource usage.
- Fixed an issue where the password changer could fail when `transport_bind_ip` was set to `Any`, affecting configurations modified in recent versions.
- Fixed an issue where users could not log in to UAG when the licensed user limit was exceeded.
- Fixed an issue where sessions restored from backup could not be properly deleted due to permission errors.
- Fixed an issue where connections using native clients through forward accounts with Authenticate against server enabled failed to establish.
- Fixed an issue where assigning or loading more than 1000 objects in the Object Rights and related sections caused data to not load properly.
- Fixed an issue where users without the configuration-read privilege could not access the Backup and Retention page despite having other required permissions.
- Fixed an issue where the Sessions list did not load correctly for users with limited capabilities, causing missing or incorrectly refreshed session pages when navigating or scrolling.

- Closed the possibility to connect to an arbitrary address after successful authentication from within a rendered HTTP session.
- Fixed a missing validation in the network interfaces configuration that allowed saving multiple interfaces with the same subnet.
- Fixed an issue in Network Configuration where renaming an IP label caused a critical database error if the label was used as a bind address in multiple external authentication methods.
- Fixed an issue where LDAP synchronization did not perform incremental updates, functioning only during full synchronization.
- Fixed an issue where the Reset Authentication Failures Counter button did not work for users synchronized from LDAP.
- Fixed an issue where LDAP-synchronized users with access to safes via groups could not send access requests and received a 403 error.
- Fixed an issue where external authentication methods assigned to users synchronized through LDAP or Active Directory were lost after upgrading to a version introducing RBAC changes.

  Note: *The issue is resolved when upgrading directly from version 5.5 (e.g., 5.5.11/5.5.12) to 5.6.2. However, if an upgrade to 5.6.1 has already caused authentication methods to be lost, updating to 5.6.2 will not restore them.*
- Fixed an issue where the user list in safe configuration did not display users assigned through Fudo groups.
- Fixed an issue where actions performed by a user who joined a live webclient session were not visible in real time and appeared only after the session ended.
- Fixed an issue where clicking a safe name in the Access via groups section resulted in a 404 error instead of redirecting to the correct safe page.
- Fixed an issue where logging in through external authentication with TLS and no certificate was not possible when Kerberos was disabled.
- Fixed an issue with building the input buffer for pattern matching in terminal protocols (SSH and Telnet).
- Fixed an issue in password changer policies where password complexity options were incorrectly handled after saving, causing unchecked options to become selected.
- Fixed an issue where users could not select External address and port or provide an IP address or FQDN when User Access Gateway was set as the Local address.
- Fixed an issue where downloading the RDP file for a native client connection generated spurious log errors without affecting the connection.
- Fixed an issue where network interface configuration changes made through the UI were not persisted to the database, causing settings to appear saved until a page reload or logout.

- Fixed an issue where the Retention module attempted to remove session replicas stored on external backup servers, resulting in warning logs and skipped sessions.
- Fixed an issue where certain fields were missing from email notifications, including management URL and user details for session join and leave events.
- Fixed an issue where users were no longer notified about already active sessions after upgrading to version 5.6.1.
- Fixed an issue where only one network interface was displayed in redundancy group configuration instead of all properly addressed interfaces.
- Fixed an issue where TDS sessions were not indexed.
- Fixed an issue where fetching the destination server certificate failed when using a labeled IP address.
- Fixed an issue in the RDS implementation where external connections through UAG were not properly recognized, causing dropped connections after redirection from the RDS broker.
- Fixed an issue where saving group option changes took an unusually long time and checkbox selections behaved inconsistently.
- Fixed an issue where the Object Rights table displayed Role name instead of User name in the Assign user view.
- Fixed an issue where the list of authentication methods for local users displayed only hostnames or IP addresses instead of method names, making it difficult to identify the correct method.
- Fixed an issue where the Search function did not filter Policies or Regular Expressions, preventing users from sorting results.
- Fixed an issue in the Productivity tab where the 6-month and 1-year filters in session comparison displayed data for incorrect date ranges.
- Fixed an issue where object lists in GUI filters were not sorted, causing the newest objects to appear at the top instead of in a consistent order.
- Improved the warning message displayed when modifying a time policy assigned to multiple users or groups to provide clearer guidance.
- Improved the display of revealed passwords in the User Access Gateway to properly handle multiline secrets by showing them in a text area instead of a single line.
- Fixed layout issues in the Password history view in User Access Gateway, where the Back button was misaligned for accounts with long passwords or SSH keys. Also improved the display of multiline secrets.
- Corrected Russian and Ukrainian UI translations to fix a few mismapped labels and ensure clarity and consistency.
- Fixed an issue where files transferred via Fudo using SCP were saved with randomized names and missing file extensions.

- Fixed an issue in UAG where native client connections to accounts assigned to a server pool ignored the selected server and connected to the first host or mask in the list.
- Fixed an issue where connections handled exclusively through Fudo Share Access incorrectly consumed Fudo Enterprise licenses or restricted access despite the limited license not applying to Fudo Share Access.
- Fixed an issue where unpairing Fudo Enterprise from Fudo Share Access (FSA) removed the FSA key field, preventing re-pairing with another environment.
- Fixed an issue where Fudo Share Access failed to generate OTPs for imported Active Directory groups.
- Fixed an issue where cluster pairing failed due to a missing private EC key.
- Fixed an issue in Fudo Share Access where notification emails were missing for share confirmation and access request approval or rejection.

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.

Licensing Changes

Starting with version 5.6, license enforcement logic has been updated as part of the RBAC introduction:

- In version 5.5, superadmin users were always counted as active and had priority in login rights.
- In version 5.6, logins of users with administrative privileges to the Admin Panel are always prioritized, regardless of the current license limits. Their logins are now counted as standard authentications within the licensing scope.

Note: When the number of active users **reaches the license limit** and a new user logs into the Admin Panel, the system now **prioritizes users with management access**. In this case, the user who logged into User Access Gateway (UAG) earliest will lose access, as the privileged user is now counted as active.
Existing sessions of the user who lost access are **not terminated** — they continue to run as usual.

DHCP Discontinuity

Starting from **version 5.6.1**, DHCP is no longer supported. If DHCP is enabled in the existing configuration, the upgrade process will be blocked. To proceed with the upgrade, ensure that all DHCP-related settings are removed or replaced with static network configuration before initiating the upgrade.

External Authentication - Active Directory

In previous releases, when configuring external authentication through Active Directory with TLS enabled, it was possible to upload a server certificate. Starting from this release, Fudo only supports a CA certificate. If a server certificate is currently configured, you must change its value to *None* before upgrading.

Handling Legacy Checkout Sessions

During the upgrade to **version 5.6.1 and later**, environments containing checkout sessions that still reference the deprecated SAFE_SYSTEM_ID are automatically handled as follows:

- Deleted checkout sessions referencing SAFE_SYSTEM_ID are removed.
- A new safe is created with the ID MIGRATED_CHECKOUT_SAFE_ID (value: 200) and the name '**Migrated checkout sessions**'.
- Remaining (non-deleted) checkout sessions are reassigned from SAFE_SYSTEM_ID to MIGRATED_CHECKOUT_SAFE_ID.

These changes ensure that the upgrade process completes successfully in environments previously migrated to Fudo 4.3.

Note: The safe '**Migrated checkout sessions**' is created only if the sessions described above exist in the system.

Mobile Token

Note: Fudo Enterprise 5.6 no longer supports the **Mobile token** authentication method used to bind Fudo Officer mobile application to a User. Please ensure that the mobile application is unlinked from any User configuration. Otherwise, the upgrade will fail, and the script UPG000685 will return a list of users who have the mobile application linked.

To unlink the Fudo Officer mobile application, please edit the user configuration, then:

1. Go to the 'More' tab, and in the 'Fudo Officer' section, unlink the application using the 'Cancel binding' button.
2. Alternatively, go to the 'Settings' tab, in the 'Authentication' section find the 'Mobile token' method and remove it using the 'Delete' button.

Transition to RBAC After Upgrade

Note: In the RBAC model, the *-read privilege grants visibility into a specific tab of the interface, and consequently, into **all objects** of that type in the system—not just those for which the user has capabilities. This privilege provides **view-only access** and does not permit editing, deletion, or any other actions.

- **Listener Access Model Updated:** With the introduction of RBAC, users now either have access to all listeners or to none. Granting access to individual listeners is no longer possible.
- **Access Request Voting:** Now requires both `access-request-read` and `access-request-vote` privileges, as well as `read` access to the associated user, safe, and account.
- **Superadmin, Admin, and Operator Roles After Upgrade:** These roles are preserved during the transition to RBAC, with their permissions mapped to ensure comparable access as before. Note that some exceptions apply, and the mapping may not reflect a one-to-one correspondence in all cases. Selected examples include:

- After the upgrade, an **admin** who has a capability assigned to an object will automatically gain full permissions for that object.
- Since listeners are considered a global and network-level configuration, after upgrading to version 5.6, **admin** users no longer have permissions to create them.
- The **Authentication** tab is now available to users with the **admin, safe admin** and **operator** roles by default (`extauth-read` privilege) to be able to see or assign external authentication to other users.
- The **admin, safe admin** and **operator** roles now have access to the **External Password Repositories** tab (`passvn-read` privilege) to be able to see or assign external password repositories to accounts.
- The **admin, safe admin** and **operator** roles now have access to the **Cluster** tab (`cluster-read` privilege) by default, allowing them to send sessions to other nodes.
- The **operator** role now includes the `listener-read` privilege by default. However, due to RBAC changes, operators can currently view all listeners, not just those explicitly granted.
- A user with the **session viewer** role can now access the **Download > Files** tab and download files listed there. This permission is required for the correct display of SFTP/SCP sessions.
- The **session viewer** role now includes access to additional interface elements, such as new tabs (e.g., Users, Servers, Accounts, Safes) and the ability to add the Active Users dashlet from the Dashlet Marketplace, depending on the assigned capabilities.
- Operators, session viewers, safe admin, and other custom roles will now be able to see all existing anonymous sessions as well as any new sessions initiated by anonymous users.

- The predefined **user** and **service** roles have been removed.
  - After upgrading to version 5.6, any users who previously had this role assigned will no longer have any role.
  - Before the upgrade, customers who previously had multiple users assigned to the *service* role must remove all but one of them.
  - SNMP settings previously configured for that user will be transferred to the System tab and applied globally.

Note: The predefined roles serve as a transitional starting point and are fully editable (with the exception of **superadmin**). The automatic mapping of legacy roles is a one-time compatibility step performed only during the upgrade from a version without RBAC. These predefined roles are not intended to replicate previous permissions one-to-one, but rather to provide a starting point for adaptation. We recommend reviewing all assigned privileges after the upgrade to ensure they reflect your security requirements.

MySQL Listeners

TLS is now **required** for MySQL listeners. In previous versions, TLS could not be enabled for MySQL listeners or servers. As a result, any existing MySQL listeners will become non-functional after the upgrade. To restore connectivity, administrators must manually enable TLS and configure a valid certificate for the listener.

Kerberos Support for User Directory Synchronization

If you plan to use Kerberos authentication for User Directory synchronization, ensure the following before upgrading:

- Port **88 (Kerberos)** is open on the firewall — otherwise, synchronization will fail.
- The **Fudo hostname** includes the appropriate domain suffix (for example, fudo.qa.kerberos).
- The **DNS server** from the same domain is properly configured.
- The **controller address** matches the **SPN (Service Principal Name)** of the LDAP server defined in the domain.

If your current configuration uses an **IP address** instead of a hostname, update it to use the correct hostname before upgrading.

Note: If you **do not intend to use Kerberos**, disable it in the **Settings > Authentication > Global** tab to continue using **simple bind** for synchronization.

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 introduces a new upgrade barrier in the Product Upgrade Path. If you are upgrading from any version of Fudo 5.4, please ensure you upgrade to version 5.4.12 first before proceeding to 5.6.

HOW TO UPGRADE YOUR FUDO

3. Login to your Fudo Admin Panel.
4. 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.

5. Select **Upload** from the top right side and upload the previously downloaded and unzipped upgrade package file.
6. 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.
7. 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: Please keep in mind that both session recordings and any changes to RBAC roles or groups made in the newer version will be lost after rollback.

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