Fudo Enterprise 5.6.4
Release Notes

Date: January 2026

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

NEW FEATURES AND IMPROVEMENTS

- Improved Discovery configuration by allowing empty server pools to be selected as targets for newly discovered domain accounts, enabling their use as placeholders even when no servers are assigned yet.
- Restored the previous behavior of grouping nested SSH sessions under the main session in the sessions list and system reports, replacing the separate-session view.
- Improved Web Client keyboard handling for single open connections, ensuring the TAB key is consistently passed to the target session and not intercepted by the browser, preventing focus loss or unintended autocomplete behavior.
- Improved web application security with Content Security Policy headers to protect against cross-site scripting attacks.
- (Beta) Introduced Rendered HTTP functionality in ShareAccess.
  Note: Using this feature requires accepting a self-signed certificate.

DISCONTINUED FEATURES

- Removed support for PyMySQL libraries for Python.
- 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

- **Certificate chain verification** – Fudo now verifies the entire certificate chain during server connections. See details later in this document.
- 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 with certificate chain validation where TLS verification could fail when the configured Root CA was not the direct issuer of the server certificate (longer trust chains). This affected scenarios such as External Authentication or RDP server connections with TLS enabled, where using a Root CA certificate could prevent successful authentication or session establishment.
- Fixed an issue where, during the first-login password change flow for an AD-synced user, removing the AD login from the external authentication method mid-process could cause a crash in the authentication flow and prevent the password from being updated in Active Directory.
- Fixed an issue where, when more than 100 Listeners existed, only the first 100 listeners were displayed when linking an account to a listener in a safe, making listeners beyond this limit invisible.

- Fixed an encoding issue in filter handling where entering special characters such as % or parentheses () in the Search field could trigger a 400 error and leave the UI in a loading state, regardless of whether matching objects existed.
- Fixed an issue where RDP sessions initiated via the xfreerdp client failed to start for RemoteApp connections or were immediately terminated for standard RDP sessions.
- Fixed an issue where opening the session player without sufficient privileges resulted in an indefinite loading spinner with no feedback.
- Fixed an issue where a deleted IP label was still visible and selectable in IP address dropdowns across the management interface.
- Fixed an issue where the system startup could be significantly delayed by becoming stuck in the Starting data state during reboot. Startup handling has been improved to reduce excessive delays and ensure a reliable transition to the RUNNING state.
- Fixed an issue where Sound Redirection, configured in Safe settings, worked only when Dynamic Virtual Channels (DVC) were enabled.
- Fixed an issue where RDP sessions could be randomly terminated after ending a SIP connection when Dynamic Virtual Channels (DVC) were enabled.
- Fixed an issue where files larger than 50 MB downloaded from Downloads → Files lost their original filename and extension after being transferred via SCP.
- Fixed an incorrect label in Sensitive logs retention settings.
- Fixed an issue where credential injection could fail on certain websites due to an unhandled error message, causing the browser script to stop instead of proceeding to load the page.
- Fixed a missing translation in the Scheduled Access Request popup for Just-in-Time access, which previously prevented the request from being displayed correctly.
- Fixed an issue where the vote counter for access requests displayed an incorrect number of votes when approvers lacked capabilities to the voter objects.
- Fixed incorrect handling of popup windows and external application prompts in rendered HTTP sessions by redirecting them to the main session window, restoring proper behavior of standard refresh and navigation shortcuts.
- Restored the **Select all** option in the **Sessions** tab, which was no longer available starting from version 5.6.1.
- Remove deprecated /api/v1/ endpoints related to Discovery functionality that have been replaced by /api/v2/ equivalents, and update the frontend to use the existing /api/v2/ endpoints instead.
- Fixed an issue in the Servers list where the All sub-tab did not display all available servers for the selected protocol.

- Fixed an issue where IPv6 addresses configured in Network configuration were not available for selection in the Local address dropdown when creating listeners or servers.
- Fixed an issue where a failed upgrade from version 5.6.x due to configuration problems could freeze the upgrade process, preventing further upgrade checks or re-uploading the .upg file.
- Fixed an issue where popup windows and external application prompts during HTTP sessions were not handled correctly and remained open instead of integrating with the main session window. All popups are now redirected to the main window, ensuring consistent behavior. Users can reload redirected pages using the standard browser refresh shortcut, and keyboard navigation shortcuts for going back or forward now work as expected.
- Improved upgrade reliability by automatically fixing invalid LDAP Synchronization configurations during upgrade, removing redundant External Authentication assignments that could cause errors and block subsequent upgrades.
- Fixed an issue where the upgrade check did not clearly report failures when upgrade conditions were not met. The check now displays an explicit error message, allowing administrators to clearly identify incompatible upgrade scenarios.
- Share Access: Verified and stabilized ShareAccess synchronization by correcting expiration date handling; synchronization now completes successfully without parsing errors.

KNOWN ISSUES

- In versions **5.6.0, 5.6.1, and 5.6.3**, the upgrade check does not clearly indicate a failure. This is particularly relevant when attempting to upgrade using an image with an **older kernel version**, where the check appears inconclusive instead of explicitly reporting that the upgrade is not supported.
- Deleting an LDAP/AD mapping that has no Fudo group assigned may incorrectly remove all LDAP-synchronized users from the system. As a result, users are re-created as new objects during the next synchronization, and users from the deleted mapping may still be synchronized once despite the mapping no longer existing.
- After upgrading from 5.5.x to 5.6.3, adding a public TLS certificate to an RDP listener may fail with the error `tls_certificate is not a valid X509 certificate chain`, due to improvements in certificate chain validation.
- Users assigned to a Safe through group membership may not receive email notifications for ńaccepted or rejected Just-in-Time access requests, even if they have the required role and capabilities.

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.

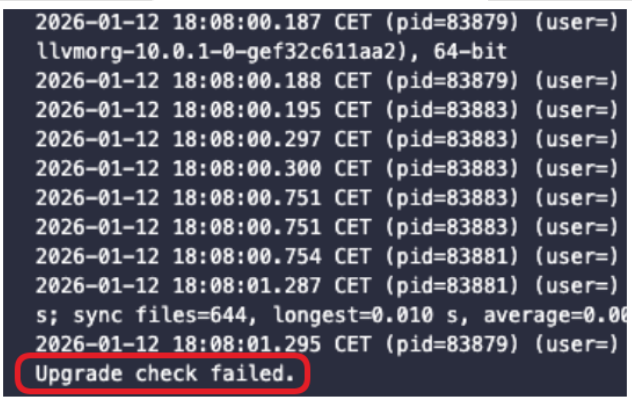
There are a few things that need to be verified before this upgrade can be applied:

- 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.

Upgrade Check Failure Reporting

In versions **5.6.0, 5.6.1, and 5.6.3**, the upgrade check **does not clearly indicate a failure**. In such cases, the check may appear inconclusive instead of explicitly reporting a failure, regardless of the underlying reason (for example, an unsupported kernel version).

Please **carefully review the upgrade check outcome** to ensure that the upgrade image is compatible with the current system configuration. This is particularly important when attempting to upgrade using an image with an older kernel version, where the check may appear inconclusive instead of explicitly reporting a failure.



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

TDS Kerberos Delegation

For Kerberos authentication to work correctly, the server configuration must use the **Host** option in the **Destination** section. Configurations using an IP address will fail because Kerberos relies on hostname-based SPN (Service Principal Name) resolution.

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.

AI Models Retraining in Clustered Environments

When upgrading a clustered deployment, AI models trained on a previous version **must be retrained** after the upgrade. This limitation does not apply to single-node deployments, where existing models continue to work correctly without retraining.

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.

CA Certificate Verification for MySQL and HTTP Servers

In versions **5.6.0, 5.6.1,** and **5.6.3**, server certificate verification was not properly enforced when establishing TLS connections to MySQL or HTTP servers using CA-based authentication.

The configured CA certificates (Root CA or Sub CA) were not correctly used to verify the server certificate during connection establishment, allowing connections to succeed even when the server presented a certificate not signed by the configured CA.

Note: This behavior affects only MySQL and rendered HTTP connections where a CA certificate is configured for server verification. Users of **other protocols are not affected**. **Other protocols are not affected**. Servers **with server (leaf) certificate configured are not affected**.

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

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: 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