Fudo Security Sp. z o.o. Al. Jerozolimskie 178 02-486 Warszawa sales@fudosecurity.com.pl +48 22 100 67 00 NIP 5242521745 KRS 0000224900

Fudo Enterprise 5.6.1
Release Notes

Date: August 2025

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

NEW FEATURES

ROLE-BASED ACCESS CONTROL

In this Fudo Enterprise version we gladly introduce **RBAC (Role-Based Access Control)** - feature, which brings significant improvements in access management.

List of improvements within RBAC:

- **Creating custom roles** – Administrators can create roles with precisely defined permissions tailored to specific tasks, instead of relying solely on the predefined roles as before.
- **Managing selected object types** – Roles can be narrowed down to manage only selected types of objects, such as Users, Listeners, Pools, Servers, or Safes.
- **Assigning action scope on objects** – Permissions can be limited to specific actions, such as creating, modifying, exporting, deleting, or blocking particular types of objects.
- **Flexibility in assigning permissions** – Permissions can be granted globally or selectively, e.g., to all objects of a certain type (e.g., Users, Accounts, or Servers) or only to selected, specific objects.
- **Access management by specific tabs** – The ability to create roles with access limited to selected tabs within Fudo Enterprise.
- **Multi-role assignment** – Users will be able to receive multiple roles, rather than just one of the six predefined roles as was the case before.

GROUPS

We’re introducing a new object—**Group**—that adds an extra layer of control over resource access. Administrators can now create user groups to grant more precise permissions, ensuring that only

authorized users can interact with specific Safes. Additionally, it is now possible to view which Safes a user has access to through the groups they belong to.

AI SESSION SUMMARY

Fudo Enterprise 5.6 introduces a beta version of AI-powered summaries for SSH sessions. This feature allows administrators to quickly assess session context without replaying full recordings, improving audit efficiency and reducing manual review time. The feature can be easily configured with AI providers such as OpenAI, Anthropic, or a custom model using a local Ollama framework.

GRANULAR ACCESS TO REMOTE APPLICATIONS

To improve access control and reduce surface exposure, this version adds support for **restricting users to specific remote applications** without granting access to the full desktop environment. This enhancement enables more granular permission management and helps ensure that users interact only with the resources necessary for their roles.

TUNNEL LISTENERS

Fudo Enterprise 5.6 introduces a new Listener type that allows establishing an SSH tunnel for more secure connections. With this feature, administrators can safely enable access to protocols that are not encrypted by default, such as Telnet or VNC, while also adding an optional layer of encryption to other supported protocols.

ADDITIONAL NEW FEATURES AND IMPROVEMENTS

- Port Ranges: Added support for configuring Server objects with a port range, simplifying multi-port redirection and reducing manual setup.
- Added support for configuring an outbound HTTP proxy for authentication-related traffic (OIDC, SMS, DUO). Also usable for timestamping services. Support for more integrations coming in future releases.
- Added the ability to specify a remote application when establishing a session through the web client.
- Enhanced MySQL protocol support:
    - Added support for Bastion connections
    - Enabled authentication against the MySQL server
    - Supported all authentication methods, including one-step multi-factor (e.g., password+token)
    - Supported authentication plugins:

  - for communication between Fudo and the database server: mysql_clear_password, mysql_native_password, caching_sha2_password;
  - for communication between the client and Fudo: mysql_clear_password.
- Reorganized Interface Elements:
  - **Export/Import Configuration** options have been relocated from the user menu (top-right corner) to **System > Configuration** for improved visibility and accessibility.
  - The **Timestamping** settings have been moved from a standalone tab to **Settings > System,** aligning with other system-level configuration options.
  - The former **LDAP Synchronization** tab has been replaced with **User Directory**, reflecting its broader functionality and redesigned layout.
  - A new **Object Rights** subtab has been added to the editing views of Servers, Accounts, Pools, and Safes. This change, introduced with role-based access control (RBAC), enables administrators to define which users or roles are authorized to manage a given object—supporting more granular delegation of access rights.
- User mapping in the User Directory has been redesigned — users are now assigned to groups instead of safes. This simplifies configuration and enables more flexible, centralized control over user permissions.
- Nearly all configuration tabs in Fudo Enterprise have now been fully migrated to the new graphical interface. Each redesigned tab features improved clarity, faster navigation, and consistent behavior. Overview of Updated Tabs:
  - **Sessions tab** – Redesigned layout with labeled action buttons and a customizable column view. Less-used fields moved under a three-dot menu.
  - **System tab** – New *Configuration* subtab for export/import. Diagnostics split into focused subtabs for better clarity.
  - **Network Configuration tab** – Refreshed visuals and clearer layout for managing interfaces and routes.
  - **Reports tab** – Unified table view for all report types and schedules. Simplifies configuration and overview.
  - **Cluster tab** – Split into *Create cluster* and *Join cluster* tabs for more intuitive setup.
  - **Notifications tab** – Updated layout aligned with the new interface style. Improved readability.
  - **User Directory tab** – Formerly *LDAP Synchronization*. Restructured with modal windows for cleaner configuration.
  - **External Storage tab** – Updated to match the modernized UI. Minor usability enhancements.

    - **Productivity tab** – Updated to match the modernized UI. Minor usability enhancements.
- The Session Player interface has been refreshed to enhance usability. Key control buttons have been repositioned for improved visibility and a more intuitive playback experience.
- Enhanced Listener configuration for User Access Gateway. Administrators can now bind Listeners directly to the UAG address, simplifying native client connections and improving flexibility when UAG operates on multiple addresses.
- Added support for mapping OIDC configurations to Fudo domains. This allows assigning an OIDC configuration to a specific domain, resolving conflicts where users with identical user IDs originate from different LDAP/AD synchronizations.
- Added support for custom TLS certificates in OIDC configuration. Administrators can now specify the CA certificate that signed the OIDC server certificate, provide a custom server certificate, or continue using the system root CA repository as before.
- Added support for clustered environments in ShareAccess. When Fudo Enterprise instances are configured in a high-availability cluster, they can now be connected to ShareAccess as gateway nodes, ensuring redundancy and seamless failover.

API CHANGES

- The transition to APIv2 continues, bringing numerous new endpoints designed to enhance functionality and streamline the process of rewriting tabs to the new API. Consequently, this update aims to significantly improve performance and expand overall capabilities.
- We've added numerous new object specifications and endpoints to our Fudo Enterprise 5.6 APIv2, so you can now utilize it to manage:
    - Roles (RBAC)
    - Groups (RBAC)
    - Capabilities for objects (RBAC)
    - Sessions, including:
        - Timestamping
        - OCR
        - Approve/Reject actions
        - Comments
        - Last activity tracking
        - Replication
        - Restoring
        - Sharing and revoking shared sessions
        - Terminating

        - Downloading
    - User Directory (formerly LDAP Synchronization)
    - Password changers and remote applications in accounts
    - Discovery scanners and rules
    - Upgrade process
    - License management
    - Hotfix installation
    - Defined reports
    - Remote applications (new endpoints)
    - Configuration import/export
    - IPMI port configuration

DISCONTINUED FEATURES

- 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.

BUG FIXES

- Fixed an issue where changing the organization owner in ShareAccess could fail due to insufficient permissions.
- Fixed an issue where RDP authentication failed when using a native client and the system keyboard input language was set to Russian, for users with OATH enabled.
- Fixed a limitation preventing bulk account removal from safes with multiple listeners.
- Fixed an issue that could cause cluster freeze due to incorrect locking.
- Fixed an issue where a single failed Kerberos login caused multiple failed attempts in Active Directory, leading to account lockout, by adding handling for specific failure reasons such as incorrect password, locked account, or expired password.
- Implemented caching to avoid repeated attempts to contact unreachable KDC servers.
- Implemented infinite scroll in areas handling large datasets, including password changers, password verifiers, and remote applications, to ensure consistent and reliable data loading across the interface.
- Fixed a conversion error that occurred when downloading restored sessions in formats other than TGZ or text log.
- Fixed an issue where the HTTPS listener returned only the server certificate, omitting the intermediate certificate from the configured chain during SSL handshake.
- Fixed an issue where transport certificates added manually to password changer configuration were saved in an incorrect format, causing certificate parsing failures and preventing proper operation.
- Fixed an issue where timeout settings were not correctly applied, causing early logouts for User Access Gateway users and no timeout enforcement for users on the Admin Panel interface.
- Fixed incorrect visual indicators for disk statuses on the dashboard, ensuring consistent representation for "Synchronizing" and "Warning" states.
- Fixed an issue preventing users from logging out due to a missing X-CSRFToken header.
- Fixed an issue where incorrectly generated empty email files caused an internal server error in the Notification tab.
- Fixed an issue where SFTP backups to servers using RebexSSH failed with a "Badly formed packet received" error, preventing session data transfer.
- Fixed an issue where manually replicated sessions with 'database' replication only failed to play, displaying a black screen despite showing playback progress.
- Fixed an issue where removing an external AD authentication server did not delete its associated certificate, causing upgrade failures due to leftover configuration artifacts.

- Fixed an issue causing XML response parsing failures when retrieving passwords from the Delinea (Thycotic) External Password Repository, which resulted in authentication errors.
- Corrected the Russian translation of the Armenian language name in the OCR language selection list.
- Fixed an issue related to SNMP communication being resynchronized, where Zabbix connections failed after some time.
- Fixed an issue where users could not authenticate with CERB as the first factor when using the External Authentication + Duo method, preventing successful login.
- Fixed incorrect behavior of partial synchronization in environments with multiple synchronization sources and mappings, where users could be incorrectly removed from safes shortly after being added, despite valid assignments.
- Fixed an issue where users were not removed from Fudo groups after being removed from the corresponding AD groups during synchronization.
- Fixed an issue where the AD group search in User Directories did not support SSL certificate chains, preventing successful LDAP connections when multiple certificates were provided.
- Fixed an issue preventing OTP generation for forward-type accounts when users logged into the User Access Gateway via OpenID without a configured secret in MGMT.
- Fixed an issue where uploading an HTTPS certificate with an encrypted private key to the User Access Gateway or Admin Panel failed silently, with no error or warning shown in the UI or API response.
- Fixed an issue where connections failed if a server and an account shared the same name, causing the system to locate the server but not the corresponding account.
- Fixed an issue where the 'Join' button was missing when accessing a shared session link without the 'Read only' option enabled, preventing anonymous users from joining active sessions as intended.
- Fixed an issue where ldapsyncd failed to remove users from Fudo after they were deleted from the mapped Active Directory group due to insufficient SQL grants.
- Fixed an issue where configuring SMTP with certain authentication types (Login, NTLM, Digest MD5, or External) caused notifications to fail and test connections to return errors.

KNOWN ISSUES

- AI models trained on a specific version must be retrained after an upgrade in clustered environments. The issue does not occur when upgrading a single-node (master) deployment.
- When using native clients to connect through forward accounts with the "Authenticate against server" option enabled, connections may fail to establish. Disabling "Dynamic virtual channels" in Safe settings allows the connection to succeed.

- Password changer may not function correctly when `transport_bind_ip` is set to `Any`. This issue typically affects configurations that were modified in recent versions. Instances of password changers that have not been altered since earlier versions are expected to work as intended.
- Limited LAPS support: Only the Legacy version of Microsoft LAPS is currently supported. In some environments, LAPS functionality may be entirely unavailable.
- Several issues have been identified when connecting to VNC servers via the web client.
    - VNC sessions may fail to load entirely, and web client behavior is inconsistent.
    - Native connections to VNC servers using regular accounts (with stored credentials) still prompt users to manually enter credentials.
- The Upgrade Check process may experience significant delays when updating to this version.
- AAPM support has been officially removed in this release. However, some configuration options and backend components related to AAPM may still be present. These will be fully removed in a future update.
- Multiple redundant OCR processes may start after a Fudo reboot, leading to unnecessary resource usage.
- Session inactivity limit may not be enforced correctly for rendered HTTP sessions in certain scenarios.
- Loading times for the Users and Dashboard tabs may be significantly increased when using the Session Viewer role in environments with a large number of objects. This issue may also affect other roles with restricted permissions, but does not impact the Super Admin role.
- Users with the Operator role cannot view sessions created by anonymous users, even if they have the appropriate permissions for the safe, listener, and users involved.
- The system does not provide information about whether a user has access to session playback. As a result, the play button may appear active, but attempting to use it shows a spinner with no feedback, and the action fails silently.
- OIDC login flow does not support GET redirect requests. Only POST requests are currently handled, which may cause compatibility issues with some identity providers expecting GET-based redirects.
- Sessions restored from backup may not be fully removed due to incorrect ownership of the restored session directory. This can cause repeated restore attempts to fail with a “session directory already exists” error.
- When the licensed user limit is exceeded, users are unable to log in to UAG, even if they should have access.
- License dashlet display incorrect server count and show an untranslated string for active users instead of the proper label.

Fudo Security Sp. z o.o. Al. Jerozolimskie 178 02-486 Warszawa sales@fudosecurity.com.pl +48 22 100 67 00 NIP 5242521745 KRS 0000224900

- Live SSH sessions paused due to a policy violation may not resume immediately after being unpaused. Multiple pause and unpause actions may be required for the session to resume properly.
- The object assignment form allows selecting only the 30 visible items per page when using the “select all” checkbox, making it difficult to assign all filtered or matching objects at once.
- RDP sessions using the *xfreerdp* client do not start when connecting to RemoteApp.
- There is currently no functionality to copy an existing role along with its assigned privileges. A role duplication feature should be implemented.
- In the User Directory configuration, changing the Encrypted connection checkbox does not update the Port field as expected. The incorrect port value persists even after a page refresh, forcing users to delete and recreate the configuration.
- The Events Logs tab experiences performance issues when a large number of logs are present in the selected time range. Actions like loading, filtering, and applying filters may be slow or unresponsive.
- Leading or trailing spaces in server or user names (e.g. server_login) are not trimmed automatically, which may result in failed login attempts due to mismatched connection strings.
- It is not possible to change the password verifier without first modifying the password policy.
- Issues may occur with cluster connection and data replication between nodes, leading to instability and potential inconsistencies in shared data.
- 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.
- The authentication process may crash when attempting to change a password via Active Directory external authentication without valid AD credentials.
- Notifications configured in a Safe do not work even when all settings are correctly defined. Emails are not sent despite triggering the expected events.
- Connections using a regular account with a password sourced from another account fail when accessed via URL. Users are prompted for additional credentials and receive an incorrect credentials error.
- During external authentication via LDAP, the server certificate is not verified.
- When connecting to MSSQL through the system, canceling a query from the client does not terminate it on the destination server. The operation continues until completion or until manually killed on the server side.
- In the User Access Gateway, when an account uses an SSH key sourced from another account, the password reveal option does not work correctly.
- Installing the OVA image on Nutanix or VMware may result in an error that prevents successful deployment. A workaround is available; please contact Technical Support for detailed instructions.

- LDAP Synchronization may not perform incremental updates, while full synchronization works correctly.
- Downloaded files from the SFTP player may differ from the original version.
- When different users log in to the portal using the same browser, a new connection may incorrectly reuse the previous user's session. The issue does not occur when using different browsers or incognito mode.
- Fudo retention may remove session data from disk without verifying that a backup to an external resource has been completed.
- HTTP authentication may not work for rendered HTTP sessions, causing errors when auto-login is configured.
- Users with an account validity period may retain access to the Admin Panel after the validity has expired if they logged in before expiration.
- Special characters are not recognized during session indexing.
- Native connections in User Access Gateway for accounts assigned to a server pool may use the first host from the pool list instead of the server displayed in the Server Address field when no server is selected manually.
- Users synchronized with LDAP cannot be assigned manually to safes.
- In Webclient sessions, actions of a user who joins a live session are not visible on the timeline until the session is finished.
- External authentication with TLS (without certificate) may fail when Kerberos authentication is disabled.
- Object lists in GUI filters are not sorted, with newest objects displayed at the top, which may hinder searching by name or logical order.
- The Reset Authentication Failures button does not work for LDAP-synchronized users.

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.

DHCP Discontinuity

Starting with this version, DHCP support has been removed. To ensure a successful upgrade, review your configuration in advance and replace all DHCP-related settings with static network configuration.

Handling Legacy Checkout Sessions

During the upgrade to **version 5.6.1**, 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.
- 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.

Fudo Security Sp. z o.o. Al. Jerozolimskie 178 02-486 Warszawa sales@fudosecurity.com.pl +48 22 100 67 00 NIP 5242521745 KRS 0000224900

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.

Fudo Security Sp. z o.o. Al. Jerozolimskie 178 02-486 Warszawa sales@fudosecurity.com.pl +48 22 100 67 00 NIP 5242521745 KRS 0000224900

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 note that if upgrading from version 5.5 or earlier, 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