Fudo Enterprise 6.1
Release Notes

Date: June 2026

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

NEW FEATURES AND IMPROVEMENTS

- Added support for sudo command control:
  - Added a new sudo policy type for defining allowed sudo command execution rules.
  - Added a sudo plugin that checks sudo commands against the configured policy before execution.
  - Added Fudo Officer notifications for executed sudo commands, available in Fudo Officer 2.3.32 and later.
- Improved Password Vault capabilities:
  - Added password audit for compromised passwords, allowing administrators to upload a password list and warn users when a Password Vault password is found on that list.
  - Added support for SSH key rotation with Secret Changers, including SSH key target configuration and SSH key type selection in Secret Change Policies.
  - Updated related UI terminology from Password Changer/Verifier to Secret Changer/Verifier to better reflect support for different secret types.
- Added the Password Vault browser extension for desktop versions of Chrome, Firefox, Edge, and Safari. The extension lets users access and search Password Vault secrets, autofill recognized login forms, request access to restricted secrets, and use granted exclusive checkout directly from the browser.
- Expanded Kerberos authentication support:
  - Added Kerberos authentication for Discovery, Secret Change, and Secret Verification operations.
  - Added support for Kerberos authentication in multi-domain Active Directory environments.

Fudo Security Sp. z o. o.
Al. Jerozolimskie 178

02—486 Warszawa
NIP 52425217
sales@fudosecurity.com

    - Added separate configuration switches for RDP, external authentication, and LDAP synchronization. Added options to disable fallback to NTLM and LDAP simple bind for stricter authentication control.
- Added LDAP channel binding support for User Directory, LDAP Discovery, and LDAP-based Secret Changers.
- Added optional TOTP code reuse for OATH authentication methods. When enabled, the same valid time-based one-time password can be used for multiple parallel connections within its current time window, supporting automation and bulk access scenarios.
- Added SCIM 2.0 provisioning support with Fudo as a service provider:
    - Renamed *User Directory* to *User Sources* and added a dedicated *SCIM Provisioning* tab for configuring SCIM integration with external identity providers.
    - Added SCIM API key generation, rotation, and provisioning disable options.
    - Added *Managed by* information for users and groups, including new columns and filters for identifying objects managed by SCIM, Fudo, or User Directory.
    - Added clearer status and blocking information for SCIM-managed users and groups, including local blocking behavior in Fudo and external management indicators.
- Improved rendered HTTP sessions:
    - Enhanced Kiosk Browser mode with configurable URL bar behavior: hidden, read-only, or editable.
    - Added an optional browser tab limit with a notification that lets users open a link in the current tab when the configured limit is reached.
- Added Azure Key Vault as a new External Password Repository type.
- Added support for uploading and downloading files in RDP sessions.
- Added self-service authentication method management in the User Access Gateway, allowing users to manage their own static password, SSH key, OATH, and Passkey (FIDO2) authentication methods.
- Added support for FIDO2 authentication in the Admin Panel and User Access Gateway, enabling users to sign in with registered security keys.
- Improved LAPS and password operation handling by adding support for modern JSON-based LAPS password formats with fallback to legacy formats, clearer password retrieval errors, enhanced certificate configuration forms, and stronger logging across password change and verification operations.
- Improved syslog server configuration:
    - Added TLS support for sending logs to syslog servers over TCP.

    - Added a dedicated Syslog Servers view in the Events Log section for reviewing configured syslog servers and their connection details.
- Improved API key management by adding friendly names, configurable expiration times, and key hints that make it easier to identify existing API keys without revealing the full value.
- Updated the Webclient side toolbar for RDP, SSH, and VNC sessions. The toolbar is now displayed on the right side of the session window with a refreshed visual design.
- Improved cluster network configuration by allowing administrators to choose whether the local bind address should also be used as the node address. This provides greater flexibility for cluster deployments in environments with NAT or custom network routing.
- Improved PDF report generation reliability by replacing the previous HTML-to-PDF conversion mechanism with a dedicated PDF rendering engine.
- Restored visibility of users assigned to a specific external authentication method, making it easier for administrators to review dependencies before managing authentication configuration.
- Enhanced certificate validation for remote server connections to include hostname and address matching when CA verification is enabled, providing more precise server identity matching.
- Restored connectivity validation notifications for DNS and NTP configuration, so administrators are informed when configured servers are unreachable or non-functional.
- Added support for assigning the same anonymous account and tunnel listener combination to multiple Safes. Sessions established through such tunnels are now correctly associated with the user who created the tunnel, while existing restrictions for non-tunnel listener configurations remain enforced.
- Improved bulk operations across tables with object selection options, progress visibility, and clear completion status with issue details when needed.
- Added new columns to the user list: Auth Methods, External Authentications, and Managed by, making authentication details and management source easier to review directly from the table.
- Improved AI model synchronization in clustered environments to ensure trained models remain available across nodes after rollbacks and when new nodes join a cluster.
- Added timestamp verification scripts to TGZ session downloads for Windows and macOS, enabling users to verify session timestamping information.
- Added DMZ Gateway as a virtual appliance for Reverse Proxy deployments, available on customer request. Customers can deploy a dedicated FreeBSD-based VM image on their hypervisor to expose sshd(8), which Fudo uses to establish a reverse SSH tunnel.

- Added SBOM generation capability, allowing a Software Bill of Materials for Fudo components to be provided upon customer request.
- Upgraded the operating system base to FreeBSD 14.4.
- Upgraded OpenSSH to version 10.2.
- Added TLS 1.3 support for management, UAG, ShareAccess, and Fudo Officer connections to improve compatibility with modern security standards.
- Updated SSH message authentication algorithm configuration by moving UMAC-64 and UMAC-64-ETM to legacy options, preserving backward compatibility with existing SSH implementations while keeping the primary algorithm list aligned with current security recommendations.
- ShareAccess improvements:
    - Improved the Gateway pairing process with Fudo Enterprise by adding clearer setup guidance and validation of key requirements before the connection is established.
    - Connect Region selection for Gateways with latency measurement and automatic indication of the fastest available region.
    - Support for Server Pools synchronized from Fudo Enterprise.
    - Changed domain verification during organization onboarding from mandatory to optional.

API CHANGES

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

- Session commands for monitored sessions
- Machine Learning session scoring and anomaly detection
- Machine Learning model profiles for SSH and RDP protocols
- Disc probe for VM disk size changes
- User dashboard layouts and widget configurations
- External syslog servers
- User Access Gateway authentication confirmation
- User profile authentication methods

Selected Updates to Object Specifications:

- **Safe:** Added HTTP kiosk mode attributes: `http_rendered_kiosk_url`, `http_rendered_kiosk_max_tabs`.

- **User:** Added SCIM support with `scim_managed`, `scim_blocked`, and `scim_username`, and FIDO2 authentication support with `fido2_user_handle`.
- **User Authentication Method:** Enhanced API key support with `apikey_hint` and `apikey_expires_at`, and added full FIDO2/Passkey support.
- **Password Change Policy:** Added SSH key type configuration with the `ssh_keytype` attribute.
- **Policy**: Added 'sudo' policy type support.
- **External Password Repository**: Added 'Azure Key Vault' type support.
- **Server:** Added new RDP attributes: `rdp_nla_enabled` and `rdp_public_key`, and TLS certificate store support.

DISCONTINUED FEATURES

- 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

- DSA SSH keys are no longer supported. Review the *Before You Upgrade* section and replace affected SSH keys before upgrading to Fudo Enterprise 6.1.
- The **recommended upgrade path** has been **updated** for Fudo Enterprise 6.1. Before upgrading, verify your current version and review the Recommended Upgrade Path section for the required intermediate upgrade steps.

BUG FIXES

- Fixed an issue where connecting to a Windows server through Fudo using RDP could unexpectedly change the server time zone in environments with time zone redirection enabled.
- Fixed an issue where a saved password verifier could not be changed unless the password policy was modified first.

- Fixed an issue where users whose account validity expired during an active Admin Panel or User Access Gateway session could retain access until the session timed out. Expired users are now logged out correctly, preventing inconsistent behavior related to logout, Dashboard data display, and session establishment.
- Fixed an issue in clustered environments where the Downloads section could display session recording download links on nodes where the exported file was not locally available, which could result in failed download attempts.
- Fixed an issue where listener uniqueness validation could allow duplicate bind address and port combinations when IP labels and their corresponding IP addresses were used interchangeably. The validation now correctly prevents conflicting listener configurations.
- Fixed an issue where saved filters in the Sessions view could be migrated inconsistently during system upgrades, resulting in missing filters or incomplete filter criteria, such as session status.
- Fixed an issue where Safes could continue using a removed backup server for session replication or restore operations, which could result in errors after the backup server was removed from the configuration.
- Improved import error messages for Secret Changer and Secret Verifier JSON files when an object with the same name already exists.
- Fixed an RDP display scaling issue that could occur in multi-monitor setups after authentication when using all monitors for a remote session.
- Fixed an issue where redirected RDS sessions could fail when launched from the User Access Gateway using an OTP native client with a regular account that had empty credentials.
- Fixed an issue where RDS redirection could fail when the listener address was set to User Access Gateway, causing the connection to use an incorrect destination server address after redirection.
- Fixed an issue where sessions restored from backup could not be fully removed due to incorrect directory ownership, which could later cause repeated restore errors.
- Fixed an issue where session playback in the Admin Panel was not recorded in the event log. Playback actions are now properly logged for audit purposes.
- Fixed an issue where SSH and RDP sessions could remain marked as active after being disconnected by the user or terminated by an administrator.
- Fixed an issue where SMTP notifications could fail in environments requiring a specific source IP when the bind address was configured using an IP label.

- Fixed a memory leak in RDP sessions that could cause long-running sessions to freeze or disconnect due to memory allocation failures.
- Fixed an issue where mouse-based copy and paste in the SSH Webclient could stop working after an upgrade.
- Fixed an issue in TN5250 connections where the Fudo Authentication username field could capture only the last typed character.
- Fixed an issue where account validity could be configured with an end date earlier than the start date.
- Improved error handling and logging for rendered HTTP authentication, providing clearer information about failed connection steps and preventing unclear critical errors.
- Fixed an issue where users disabled in LDAP could still be synchronized as active even when the Sync users block state option was enabled.
- Fixed an issue where Password Vault could not be selected as the account authentication method while a default password policy was still assigned to the account.
- Fixed an issue where users without permission to view the sessions list may have been able to access session data stored in raw format.
- Fixed an issue where using browser back and forward navigation after login to the Admin Panel or User Access Gateway may have allowed access to previously entered credentials or an active session if a workstation was left unattended.
- Fixed an issue where navigating from System > License to Backup and Retention could cause the Admin Panel UI to become unresponsive.
- Fixed an issue where login data may not have been cleared after a failed HTTP authentication attempt using the Other method, allowing users establishing the connection to preview the submitted credentials.

KNOWN ISSUES

- The upgrade check status in System > Upgrade may remain displayed as In progress even after the check has completed. Refresh the page manually to view the current upgrade check result.
- WinRM Secret Changers may fail when TLS validation with a CA certificate is configured and the target server does not support legacy TLS versions.
- In some rendered HTTP sessions, the inactivity limit may not end the session when the webpage contains dynamic elements, such as a blinking cursor or animated content, that continue generating activity.

- In specific RDS published application scenarios, launching an application through RD Web may fail, and the related session recording may be incomplete or display a black screen during playback.
- When ML is enabled, a node may gradually consume increasing amounts of memory over time, which can eventually lead to memory exhaustion and a node restart.
- Fudo may fail to start properly if duplicated *fudoocrd* processes are started during boot.
- Opening a virtual machine console from the Nutanix admin panel may fail when the Nutanix panel is accessed through an HTTP session in Fudo.
- Users without User menu and Power permissions may still be able to access the user menu and see options to restart or shut down the device.
- Under heavy OCR workload, *fudoocrd* may not sustain the configured number of worker processes, which can cause the OCR worker pool to shrink and affect OCR processing.
- UAG password change may fail for synchronized Active Directory users when the UPN differs from the *sAMAccountName*.
- Password checkout in the User Access Gateway may fail in cluster environments when the node marked as the active secret changer node is unavailable.
- SSH session indexing may fail when the generated search data is too large, which can result in repeated errors in system logs.
- When editing a static password authentication method in the User Access Gateway, users may be required to provide a description even though the field should remain optional.
- Upgrading to version 6.1 may fail during runcheck if a Safe contains a User access policy with an invalid time range, for example when the start time is the same as or later than the end time.
- Renaming an IP label used as a listener bind address may cause the *rename* operation and subsequent network configuration saves to stop responding.
- LDAP password changers with a secret target that are created from the GUI fail on each rotation attempt with *KeyError: 'account_new_secret'*, making secret rotation against Active Directory effectively non-functional. The template variable was renamed from *%%account_new_secret%%* to *%%new_secret_value%%*, but the GUI still hardcodes the LDAP script fieldValue to *%%account_new_secret%%*.

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.

DSA SSH Keys No Longer Supported

Before upgrading to 6.1, you must replace all DSA (ssh-dss) SSH keys with a supported algorithm (e.g. ED25519 or RSA). This applies to listeners, accounts, servers, user authentication methods, and reverse proxies. If any DSA keys remain in the configuration, the upgrade will be blocked with error FSE0611, listing the names of the objects that must be fixed first.

Support End Date Included in License Files

Starting with version 6.1, the licensing model has been updated with support license information. The license file now includes the **technical support end date**, which is displayed in the License tab and used to verify whether the system is eligible for upgrade to newer versions.

Existing license files remain valid in Fudo Enterprise 6.1. If the license file does not include the support end date, the support status is displayed as *Unknown*.

> **Note:** An expired support end date or *Unknown* support status blocks upgrades to future Fudo Enterprise versions.

Before upgrading beyond Fudo 6.1, contact Fudo Presales team to obtain a license file that includes the support end date.

Syslog Configuration Migration

During the upgrade to Fudo Enterprise 6.1, existing syslog configuration is automatically migrated to the new syslog server model as UDP syslog servers.

> **Note:** Syslog server configuration is local to each node and is not replicated between cluster nodes. In clustered environments, administrators should verify and configure syslog servers separately on each node after the upgrade.

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:** Starting with Fudo Enterprise 6.1, version **5.5.12** is required as an intermediate upgrade step in the product upgrade path. If you are upgrading to Fudo Enterprise 6.1 from a version earlier than 5.5.12, upgrade to version 5.5.12 first before proceeding with the upgrade to version 6.1.

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 secret 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