Fudo Enterprise 6.2.1

Release Notes

Date: August 2026

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

NEW FEATURES AND IMPROVEMENTS

- **AI Live Session Monitoring [BETA]** — AI agents analyze an SSH session while it is still running, and a policy can react to their findings, up to pausing or terminating the session. Disabled by default; SSH only; session content is sent to an external AI provider. After the beta stage it will be delivered as a separately licensed module.
- **Session sharing improvements**:
  - Share links now work on the User Access Gateway address, not only on the Admin Panel address. Link generation returns both addresses, built from the same key — send whichever the recipient can reach.
  - Authenticated shares — the recipient must sign in to Fudo before viewing, and their identity is recorded. Anonymous, key-only shares remain available.
  - Users can share their own live sessions from the User Access gateway (UAG), without an administrator. Enabled per safe with *Allow users to share live sessions*. Such shares always require sign-in, grant interactive access and expire when the session ends.
  - *"Until the session ends"* validity — shares of running sessions no longer need a time window.
  - Live supervision — a safe can require a set number of authenticated supervisors to watch a session. The session does not start until they connect, pauses if the count drops, and resumes automatically when it recovers. Supported for RDP, VNC, SSH shells, Telnet/TN3270/TN5250 and rendered HTTP. Anonymous viewers do not count towards the required number.
  - Access history — every viewer connection is recorded with identity or Anonymous, source IP, address used, and view, join and disconnect times. Entries survive link deactivation.
  - Redesigned sharing dialog.

- **Master key storage in an HSM.** Fudo can use a Hardware Security Module (HSM) to provide hardware-backed protection for its master key. HSM integration supports key rotation and clustered deployments. **Note:** KEK rotation is not supported for clusters in this release.
- **Oracle (TNS/TTC) protocol support [BETA]** — native monitoring of Oracle databases with session recording, playback and SQL command policies.
- **Location-based access restrictions.** Connections can now be allowed or blocked by the country and network they come from. A policy holds a list of countries and networks and is applied to users through groups, on top of a built-in global policy.
- **Custom scopes in OpenID Connect configurations.** An OpenID Connect configuration can now carry a custom scope, sent to that identity provider in addition to the standard *openid*, *profile* and *email* scopes, for providers that select which user database to authenticate against based on a scope in the request.
- **Time-based Just-in-Time approval** — a Just-in-Time safe can now skip the approval step during the hours covered by the user's Daily Access Policy, and require an approved access request only outside them.
- **Enforced reason format for Just-in-Time requests.** Administrators can now require users to provide access request reasons that match a predefined format.
- **New RDP engine (FreeRDP 3).** The RDP proxy has been reimplemented on FreeRDP 3. Existing listeners keep the previous engine after the upgrade — the *Use legacy RDP implementation* option on the listener stays selected.
- **Audio in RDP recordings.** Sound from the remote session is now captured and played back in the session player.
- **Redesigned Daily Access Policy editor** — draw, move and resize access windows directly on the weekly grid with 30-minute precision, copy a day to the whole week, and choose explicitly whether a bulk edit merges with or overrides existing schedules.
- **Time policies can now be configured for users accessing safes through groups.** Group-to-safe assignments now support the *Blocked* option and an *Access time period*, matching direct user-to-safe assignments. You can also configure an individual user's time policy from the *Access via groups* section without assigning the user directly to the safe.
- **RFC 5424 syslog log format support** — each external syslog server can now forward event log entries in either the RFC 3164 (BSD) or the RFC 5424 wire format. Existing servers keep their current behaviour.
- **The availability of the Productivity module** is determined by the license file and can be disabled at the customer's request, to comply with legal requirements restricting the monitoring of employee productivity.

- **Configurable scope for automatic interface routes.** You can now decide whether routes derived from interface IP addresses are added to every routing table or only to the interface's own table.
- **French** (AZERTY) **keyboard layout** support.
- **JWT authentication support.** Fudo Enterprise can now accept a signed JWT presented in an HTTP header as the credential for a request, which lets a web application firewall or reverse proxy authenticate users at the perimeter on Fudo's behalf.
- **Optional domain appending for RADIUS authentication**. A new Append domain to username option in the RADIUS external authentication server definition controls whether the user's AD domain is appended to the login sent to the RADIUS server. **Note:** The option is enabled by default — also for definitions that existed before the upgrade — so the current behavior is preserved. Clear it when the RADIUS server expects the bare username and resolves the domain on its own.
- **Administrator control over user-managed authentication methods in the User Access Gateway** - administrators can now decide system-wide which authentication method types User Access Gateway users may add and remove on their own.
- **Modules disabled for a user are now hidden and blocked in the User Access Gateway.** A user whose PSM or Password Vault module is disabled sees the section greyed out and can no longer reach it — nor the module's API. The block takes effect immediately and no longer waits out the 30-day active-user period.
- **Reworked assignment tables.** The lists used to assign groups, pools and object rights now match the main lists and support working multi-select.
- **Password Vault improvements.** Bulk delete, move and secret changer runs now report progress object by object, show which items failed without abandoning the rest, and can be stopped part-way. Smaller fixes across the vault interface round out the release.
- **Configurable OCR confidence threshold.** A new system-wide setting controls the minimum confidence required for recognized text to be indexed. The threshold can be set from 0 to 100 and defaults to 95, preserving the existing behavior. Lower values can improve text detection in noisy sessions, with a higher chance of false matches.
- **Secure secret storage in Fudo Officer.** Fudo 6.2 adds API endpoints that issue a per-device database key. An upcoming Fudo Officer release will use it to store the app's data in an encrypted database rather than a file protected by the device PIN, removing its exposure to PIN brute-forcing.
- **Password Vault in Fudo Officer [coming shortly].** An upcoming release of the Fudo Officer mobile app will bring the Password Vault to the phone: browsing and searching accessible collections, viewing secret details, sending an access request when approval is required, and filling a matching secret into another application on Android and iOS. Users

will also be able to view, filter and create their own personal secrets — logins, SSH keys, notes and certificates — directly in the app.

- **Password Vault Browser Extension 1.1.** An upcoming release of the Password Vault browser extension will add support for viewing, adding, and deleting secrets in Personal Vault, as well as two-factor authentication (2FA) at sign-in.
- **Values of encrypted Password Changer variables are no longer returned by api/v2.** An encrypted constant is stored under the master key and decrypted server-side only, when the changer script runs. Reads now report `value_type: "encrypted"` for such a variable, the same way account and user secrets are presented; through an account, `predefined: {"value_type": "encrypted"}` with `predefined_display: "<encrypted>"`. The same marker on write means keep the stored value, so read-modify-write clients need no change. Setting a new value works as before. Credential retrieval is handled by the Password Vault module.
- TLS hostname verification for monitored servers with TLS enabled and a configured CA certificate. Fudo checks that a server's certificate covers the address it connects to, controlled per server by the new Verify hostname option.
- Updated the underlying FreeBSD base system to the latest supported 14.4 patch release, including recent security fixes.
- Added the Permissions-Policy header to responses from the web interfaces, disabling browser features that are not used by Fudo Enterprise.
- Added the Cache-Control: no-store header to application responses. The browser cache no longer has to be cleared manually after an upgrade.
- Changed the cipher preference in connections to monitored SSH servers, so that AES-GCM is offered before AES-CTR. This prevents connection failures with servers supporting only legacy MAC algorithms.

API CHANGES

The API continues to expand alongside new product features. Version 6.2 introduces new endpoints and object specifications for managing:

- Hardware Security Modules
- Location Policies
- JWT authentication providers
- Safe access policies for users accessing safes through groups
- Session sharing and session access
- Secret audit
- SCIM configuration
- Per-domain DNS servers

- Fudo Officer mobile database keys

The **User Access Gateway API** has also been extended with support for:

- Session sharing, including creating, retrieving, deleting, and resolving session shares
- Session comments
- Live session information
- Password changes

The following deprecated endpoints have been removed:

- `GET /objspec/discovery`
- `PATCH /account/<account_id>/discovery`
- `PATCH /server/<server_id>/discovery`

The following changes to existing object specifications are not backwards compatible:

- **User:** `pubkey_ec`, `pubkey_rsa`, `pubkey_fingerprint`, `pubkey_trusted_by`, `pubkey_trusted_at`, `invite_code`, `invite_code_expires_at`, `invited_by` and `fudo_network` are gone from the `UserModel`. They are replaced by `fudo_network_status`, `fudo_network_username`, `fudo_network_method_id` and `fudo_network_pubkey_fingerprint`, and by the `fn_*` attributes of the `fnet` authentication method.
- **Secret:** secret names are no longer required to be unique within a collection. Integrations that identify a secret by name must use its identifier.
- **Secret Change Policy:** `rsa1024` was dropped from the values of `ssh_keytype`.
- **User Access Gateway access request:** `reason` is no longer required - a request may instead carry `reason_format_id` with `reason_fields`.

DISCONTINUED FEATURES

- Starting with version 6.3, RAW session recording will no longer be available for protocols that support the FBS recording format. For these protocols, only FBS recordings will be supported.
- 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

- OpenID Connect users are now matched by UPN against the user's AD domain. A single OpenID Connect configuration can now serve users from any number of AD domains, which removes the need for one configuration — and one login button — per domain. As a consequence, the Fudo Domain field of an OpenID Connect configuration is no longer treated as the UPN suffix, and the suffix is taken from the AD domain field of the user account instead. Deployments that sign users in by name or UPN must have an AD domain set on those user accounts. See “Before You Upgrade” for the details and the required preparation.
- The new FreeRDP-based RDP implementation introduced in version 6.2 records sessions exclusively in the FBS format and does not generate RAW recordings. As a result, timestamping is not available for sessions recorded using the new RDP implementation in version 6.2, because timestamping currently operates on RAW recording files. Starting with version 6.3, timestamping will support both RAW and FBS recordings.
- S3 Buckets Are No Longer Created Automatically for Backup Targets.

For more information about these changes and other topics to review before upgrading, see the **Before You Upgrade** chapter.

BUG FIXES

- Fixed an issue where duplicating a browser tab during an HTTP session in Webclient disconnected the session. A message informing that tab duplication is not supported is now displayed instead.
- Fixed misleading field descriptions in the Password Verifier configuration, which suggested that the entered login belonged to the account used to change the password instead of the account being verified.
- Fixed an issue in the Session Player where the Next action button worked only once after opening a session.
- Fixed an issue where users without User menu and Power permissions could still access the user menu and see options to restart or shut down the device.
- Fixed an issue where, under heavy OCR workload, *fudoocrd* could fail to maintain the configured number of worker processes, causing the OCR worker pool to shrink and impacting OCR processing.
- Fixed an issue where the upgrade check status in System did not update automatically and required a manual page refresh.
- Fixed an issue causing screen flickering and image artifacts in RDP sessions in Webclient when dynamic virtual channels were enabled and session recording was set to none.

- Fixed an issue where opening a single session set an incorrect placeholder start date in the session filter, which was then included as the time range in generated reports.
- Fixed an issue where password checkout in the User Access Gateway could fail in cluster environments if the active secret changer node was unavailable.
- Fixed an issue where SSH session indexing could fail when generated search data was too large, causing repeated errors in system logs.
- Fixed an issue where the upgrade from version 6.0.1 could fail during database migration and prevent Password Vault objects from being created.
- Fixed an issue where session backup to an Azure SFTP server did not work.
- Fixed an issue where the encrypted property of constant variables in Password Changers could not be edited.
- Fixed an issue where the callhomed service did not start automatically in support mode, which hindered remote diagnostics.
- Fixed an issue where adding multiple IP addresses to a network interface could fail with a CPU time exceeded error.
- Fixed an issue in the RemoteApp Web Client where context menus in SSMS could become unresponsive and remain open after right-clicking an item.
- Fixed an issue where e-mail notifications about access requests were not delivered to operators and were received only by superadministrators.
- Fixed an issue where users from multiple Active Directory domains could not be mapped through OIDC using a single configuration when no domain was defined in it.
- Fixed an issue where the download button for session recordings was not available after an upgrade due to leftover entries of previously removed cluster nodes.
- Fixed LDAP password rotation for GUI-created password changers with a secret target by updating the outdated template variable from %%account_new_secret%% to %%new_secret_value%%.
- Fixed an issue where events forwarded to a SIEM server contained a duplicated syslog header.
- Fixed a memory leak in SFTP traffic inspection that interrupted large file transfers and caused them to be recorded as several separate sessions.
- Fixed an issue where the upgrade to version 6.1.x could fail during database migration if password changer variable identifiers were outside the identifier range of the node.
- Fixed issue where session archiving to an S3 backup target failed on AWS regions other than *us-east-1*; the bucket must now already exist, as it is no longer created automatically.
- Fixed excessive RDP session recording sizes when screen animations were captured, which caused significantly higher traffic and packet counts for sessions routed through Fudo.

- Fixed issue where a pending access request could still be accepted after the requesting user's account had expired.

KNOWN ISSUES

- Removing a VLAN interface from the network configuration may leave the interface list in an inconsistent state. When this happens, subsequent attempts to apply any configuration change fail until the affected entry is corrected.
- For RDP sessions, the Session inactivity limit defined on a safe is applied as a maximum total session length rather than as an idle timeout. Affected sessions are disconnected once the configured number of minutes elapses, regardless of user activity. Other protocols are not affected.
- File transfer through the web-based RDP client may be noticeably slower than the available network bandwidth would suggest. Transfer speed depends mainly on network latency between the client and the Fudo instance, so connections with higher latency (for example over VPN) are affected the most.
- The maximum file size for transfers in the web-based RDP client is fixed at 128 MB and cannot be changed from the administration panel.
- Opening a virtual machine console from the Nutanix admin panel may fail when the Nutanix panel is accessed through an HTTP session in Fudo.
- 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.
- Fudo may fail to start properly if duplicated *fudoocrd* processes are started during boot.
- Rendered HTTPS sessions may fail when the target server's bind address uses a different routing table than the DNS resolver.

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.

Review RBAC Roles for New Permissions

When upgrading Fudo Enterprise, new permissions introduced in the release are granted automatically only to the Superadmin role. Existing built-in and custom RBAC roles are not updated with these permissions automatically.

After the upgrade, review your RBAC roles and assign any new permissions as appropriate for your organization. This prevents existing users from receiving additional privileges without an explicit administrative decision.

OIDC User Matching Behaviour Change

What changes

The **Fudo Domain field** of the OpenID Connect configuration is **no longer treated as the UPN suffix**. When it is set, it only narrows the match to users with that Fudo domain — its intended role of telling apart same-named accounts that come from different identity providers. Previously, matching a UPN required the configured domain to be appended to the user name, which effectively made that field act as the UPN suffix.

When the claim used to identify a user contains @ — a UPN such as jan@domain1.com — Fudo Enterprise matches it against the user name combined with the AD domain of the user account. This happens whether or not the OpenID Connect configuration has a domain set, so one configuration now handles users from any number of AD domains within a tenant.

Who is affected

OpenID Connect configurations **that have a Fudo Domain set and identify users by name or UPN** — that is, username mapping pointing at a claim such as preferred_username or upn, where

the value contains @. For such a configuration, a user whose AD domain field is empty, or holds a value other than the suffix of their UPN, can no longer be identified, and their first sign-in fails.

Who is not affected

- Users who signed in successfully before the upgrade. After a first successful sign-in Fudo Enterprise stores the sub claim received from the identity provider and matches the user by it, not by name.
- Configurations that identify users by e-mail address. Matching by e-mail address does not use domains.

Note: For every user who signs in through OpenID Connect by name or UPN, set the **AD Domain** field of their account to the suffix of their UPN — for example domain1.com for jan@domain1.com. If the UPN suffix has so far been kept in Fudo Domain only, copy it to AD domain.

This can be done before or after the upgrade, but it has to be in place before a user who is not yet linked signs in for the first time.

The Fudo Domain field of the OpenID Connect configuration **can stay as it is** — it still narrows the match by Fudo domain — **or be cleared** if it is not needed to tell users apart.

Known Limitations of the New FreeRDP 3 Engine

Non-TLS connections (Standard RDP Security with target key pinning) and Kerberos hardening are supported only by the previous engine. Keep *Use legacy RDP implementation* selected on those listeners — clearing it is not blocked and will break such connections.

Live view of an RDP session on the new engine degrades as the session gets older: opening it can take up to a minute and a half, the picture runs several seconds behind the target, and *Join* and *Pause* may not work or may not return to the live edge. Playback of finished sessions is not affected.

In this release, AI-generated session summaries cannot be generated for sessions using the new RDP engine (RDP3).

HSM Configuration Requirements

Fudo Enterprise requires a CPU supporting the x86-64-v2 microarchitecture level (SSE4.2, SSSE3, POPCNT, CMPXCHG16B). Every physical x86 CPU since ~2009 (Intel Nehalem, AMD Bulldozer)

supports x86-64-v2. If you are unable to see the "Set up HSM configuration" button in *System > Settings*, the hypervisor is presenting a generic vCPU model that masks these instructions.

Configuration change after upgrade — authentication methods in the User Access Gateway

Fudo Enterprise 6.2 introduces administrator control over the authentication method types that User Access Gateway users may add and remove on their own. The new setting is **disabled** after an upgrade, so self-service enrollment and removal in the User Access Gateway stops working until an administrator enables it.

Existing authentication methods are not affected. They remain on the users' lists, users can still log in with them, and changing an existing method — including a password change — remains available regardless of this setting.

> **Action required after the upgrade:** Go to *Settings > Authentication > Global tab > User-managed methods* in User Access Gateway, select the method types your users are allowed to manage, and click Save. In a cluster, apply the setting on one node only — it replicates to the remaining nodes.

Session Sharing Links

After the upgrade, **existing anonymous share links** become **reachable from the User Access Gateway** address as well, not only from the Admin Panel address. Review the links that are still active if the gateway is exposed more widely than the Admin Panel interface.

Disabled Modules Now Hidden in the User Access Gateway

The "inactive users only" rule was never enforced outside the Admin Panel, so installations may contain users who are active and yet have a module disabled. After the upgrade those users lose access to the module immediately, where previously they kept it for up to 30 days.

S3 Buckets Are No Longer Created Automatically for Backup Targets

Fudo no longer creates the bucket of an S3 backup target. If the bucket configured on the target does not exist, archiving fails with `*NoSuchBucket*` instead of the bucket being created silently. This also fixes S3 backup on AWS regions other than `us-east-1`, where archiving previously failed for every session.

Note:

- Before upgrading, go to *Settings > Backup and retention* and review each S3 backup target. Make sure the configured bucket exists in your S3 provider. If it does not, create it.
- The account configured on the target no longer needs the s3:CreateBucket permission.

Password Changer Encrypted Variable API Changes

Encrypted constant variables of Password Changers are now reported as `value_type: "encrypted"` instead of a value, and as `predefined_display: "<encrypted>"` when read through an account. A variable with nothing stored still reports `value_type: "none"`. Stored values are unchanged and no migration is required. Scripts and integrations that consumed the value returned for such a variable need to be adjusted to take the secret from another source.

Sending `value_type: "encrypted"` for a variable that is not an existing encrypted constant, for example when copying a changer or clearing **Encrypted**, is rejected with HTTP 400 and the whole request is rolled back.

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: Version **5.5.12** is required as an intermediate upgrade step in the product upgrade path. If you are upgrading to Fudo Enterprise 6.2 from a version earlier than 5.5.12, upgrade to version 5.5.12 first before proceeding with the upgrade to version 6.2.

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