

Fudo Enterprise 6.3

Release Notes

Date: October 2026

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

NEW FEATURES AND IMPROVEMENTS

- **File scanning in rendered HTTP sessions** - files uploaded and downloaded in rendered HTTP sessions can now be scanned by your antivirus engine through an ICAP service before they reach the target server or the user's device.
- **Configurable file transfer in RDP Webclient sessions** - get more control over file transfers with separate upload and download settings for each safe and a configurable storage limit.
- **RDP session playback decoded in the browser.** Recordings from the new RDP implementation are now decoded directly in the browser for consistent playback, seeking, OCR, and video conversion. Servers without RDPGFX require Use legacy RDP implementation on the listener.
- **Commands list in SSH session playback** - review SSH sessions faster with a searchable list of entered commands. Click any command to jump straight to the moment it was entered.
- **Session details side panel** - review session information without jumping between pop-up windows. The session player and the `Sessions` list in the Admin Panel now include a side panel with dedicated tabs for session details, participants, access and share history, live monitoring, AI summary, and transferred files.
- **AI Live Session Monitoring for more protocols [BETA]** - AI agents now analyze Telnet, PostgreSQL and MySQL sessions in addition to SSH. Each agent runs on the protocols selected for it, and the built-in agents can be used directly once you assign them a provider and select them in a safe.
- **Signed .rdp files** — files generated for the Native client option are now signed with the listener's server certificate, so the Windows warning about an unsigned connection file can be dismissed permanently.
- **Access Gateway allowed hosts** - a new list in the system settings restricts the host names and IP addresses under which users can open the User Access Gateway.

- **TACACS+ external authentication** - added TACACS+ as an external authentication server type, with ASCII, PAP, and CHAP authentication methods. The connection to the TACACS+ server can be secured with TLS 1.3, with server certificate verification and a client certificate that can be uploaded or generated in the Admin Panel.
- **OpenID Connect Back-Channel Logout** - signing out at the Identity Provider now also ends the corresponding Fudo Enterprise sessions in the Admin Panel and the User Access Gateway across all online cluster nodes. To use this, register the *Backchannel logout URL* from the OpenID Connect configuration with the Identity Provider.
- **Password strength and complexity hints** - see how strong a new password is as you type. When password complexity is enforced, a live checklist shows which requirements are met, and the password can be saved only after all of them are satisfied. A built-in generator creates a compliant password in one click.
- **Fudo Officer pairing from the User Access Gateway** - users can now pair the Fudo Officer mobile app with their account directly from the User Access Gateway. Pairing is controlled per user by the administrator and can be removed at any time.
- **Webclient clipboard improvements** - work more naturally in SSH and RDP Webclient sessions with direct clipboard integration and familiar keyboard shortcuts.
- **Public address for Reverse Proxy listeners** - Reverse Proxy listener mappings can now define an external address and port, for example a public IP address or a DNS name behind NAT. The User Access Gateway shows them to users for native client connections instead of the remote address and port.
- **Blocking concurrent sessions through other safes** - a new safe option prevents users from having sessions through two different safes at the same time.
- **Italian and French interface languages** - Fudo Enterprise is now available in Italian and French. An updated license file is required to make them available for selection.
- **Secure secret storage in Fudo Officer** - Fudo Officer 2.4.4 release now stores 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** - Fudo Officer 2.4.4 mobile app brings 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 can view, filter and create their own personal secrets — logins, SSH keys, API keys, notes and certificates — directly in the app.
- Renamed the session cookie to `__Host-sessionid` to strengthen its protection. If your integrations or security rules rely on the previous `sessionid` name, update them, or temporarily enable the *Use legacy sessionid* option in the system settings (requires a restart).

- API v2 responses now include the `Content-Disposition: attachment` header. An API URL opened directly in a browser is now downloaded as a file instead of being displayed.
- API v2 JSON responses now declare `charset=utf-8` in the `Content-Type` header.
- The User Access Gateway now removes the stored Webclient connection and Accounts page filters from browser storage on logout, including automatic logout.

API CHANGES

The API continues to expand alongside new product features. Version 6.3 introduces new endpoints and object specifications for managing:

- File Transfer Scanning (antivirus engines and file transfer records)
- Session HTTP Requests
- User Access Gateway Allowed Hosts
- Fudo Officer pairing initiated by an administrator
- Session protocols of AI live session monitoring agents

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

- Fudo Officer pairing and unpairing by users
- Password policy retrieval

No endpoints have been removed in this version.

In the User Access Gateway RDP configuration, the `server_id` and `listener_id` attributes are deprecated and ignored.

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

- **Safe:** `http_rendered_file_quota` must be at least 1048576 (1 MiB). Smaller values are rejected.
- **User Access Gateway RDP configuration:** `server_id` and `listener_id` are deprecated and ignored. The listener and the server are derived from the OTP.

DISCONTINUED FEATURES

- The **Category** attribute of accounts (privileged / non-privileged) is currently **under review** and may be removed in a future release. If removed, the field will no longer be available in the Fudo Admin Panel, and the `category` attribute will be removed from the account object in the API. Review any scripts and integrations that set or read this attribute.

- Support for **RAW session recording** for protocols that support the **FBS recording format** is currently **under review** and may be removed in a future release. If removed, FBS will become the only supported recording format for these protocols.
- 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

- Fudo Enterprise 6.3 **no longer trusts the emSign ECC Root CA - G3 root certificate** due to compromised keys of eMudhra intermediate certificate authorities. It also removes outdated root certificates that are no longer trusted by web browsers. After the upgrade, connections to target servers and integrations that rely on any of the removed root certificates will fail. See the *Before You Upgrade* section for more information.
- Sessions established through a reverse proxy are now always recorded with the source address `127.0.9.1:22`. A location policy in *Allow connections* mode that lists only networks blocks these sessions unless `127.0.9.1` is added to the policy. See the *Before You Upgrade* section for more information.

BUG FIXES

- Fixed an issue that could cause file transfers through the web-based RDP client to perform significantly below the available network bandwidth, particularly on higher-latency connections such as VPNs.
- Fixed an issue where reverse proxy listeners bound to a specific IP address on an interface assigned to a non-default routing table were unreachable through the tunnel.
- Fixed excessive event log entries generated for RDP connections when device redirection is not enabled in the safe.
- Fixed removing a node from the cluster configuration, which left the page loading until it was refreshed and displayed an empty row on the other nodes.
- Fixed the header of the View capabilities window for roles.
- Added information in the Fudo Admin Panel that external storage is available only on physical appliances.

- Fixed just-in-time access notifications (email and Fudo Officer) showing the time in UTC instead of the configured time zone.
- Fixed keys not being forwarded correctly to virtual machine consoles opened in HTTP sessions (for example VMware or Proxmox), where Alt acted as the power button and the arrow keys did not work.
- Fixed premature email delivery errors by increasing the SMTP timeout from 5 to 120 seconds.
- Fixed the User Access Gateway login so that a verified client certificate takes precedence over Kerberos SSO again, as in versions before 5.6. Kerberos SSO is used when no certificate is presented or the certificate fails verification.
- Fixed sessions being disconnected when the user navigated back and forward in the Fudo kiosk mode browser.
- Fixed OpenID Connect authentication failing for users whose Fudo domain contains uppercase letters.
- Fixed the parent interface list in the VLAN interface edit view, which did not include LAG interfaces.
- Fixed PEM certificates pasted into constant values of password changer definitions losing their line breaks. Malformed certificate values are now rejected when the password changer is saved.
- Fixed Webclient file transfer events in the event log not being attributed to the session and user.
- Fixed converting SSH sessions to video failing when the session used bright background colors.
- Fixed a replication error in the session AI Agent.
- Database queries are no longer reported as slow statement warnings with the full SQL text. Queries taking 10 seconds or longer are logged at the debug level.
- Fixed the background color of the RDP login page in the new RDP engine, which was red instead of blue as in the legacy engine.
- Fixed the Safes page header in the German interface.
- Fixed .rdp files downloaded from the User Access Gateway opening as plain text in Firefox.
- Fixed ShareAccess certificate generation failing when connect.shareaccess.com is not reachable through the default gateway. The configured bind IP is now used.
- Fixed user directory synchronization stopping for all directories when the attribute mapped to the Fudo login contained characters not allowed in Fudo logins, such as @. Such users are now skipped and a warning is logged.
- Fixed SNMP not listening on IP label addresses.

- Fixed changing the Active Directory password in the User Access Gateway when the user's logon name (`sAMAccountName`) differs from the user principal name (UPN), or when the Fudo login is synchronized from another AD attribute.
- Fixed secret fields of configured backup targets appearing empty instead of showing masked values.
- Fixed SSH connections being dropped by servers that strictly enforce the RFC 8308 message order, such as some Bitwise SSH Server versions.
- Fixed recorded SFTP sessions being terminated when the server returned a status message with empty text.
- Fixed the time period and time policy columns in the Direct access table of a safe always showing All.
- Fixed the Sessions page failing to load when a session field contained a control character.
- Fixed finished sessions occasionally remaining listed as active when session data was being saved at the moment the session ended.
- Fixed the syslog server form showing port 6514 for a TCP server saved with port 514, and port 514 for a UDP server saved with port 6514.
- Fixed the External address and port option missing from the form of SSH listeners in Tunnel mode.
- Fixed the SNMPv3 engine boot counter resetting on every reboot, which made monitoring tools such as Zabbix reject the responses.
- Fixed replication between cluster nodes stopping after an upgrade because the same configuration setting was created on each node with a different identifier.

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.
- 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.

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.

Session Cookie Name Change

In Fudo Enterprise 6.3, the session cookie of the Fudo Admin Panel and the User Access Gateway is renamed from `sessionid` to `__Host-sessionid`. After the upgrade, integrations, scripts, and security rules (for example, WAF rules) that rely on the `sessionid` cookie stop working. Before upgrading, update them to use the `__Host-sessionid` cookie.

Note: If you cannot update your network setup right away, enable the **Use legacy sessionid** option in the **Settings > System > General** tab > **Maintenance and Supervision** section after the upgrade and restart Fudo. Treat this option as a temporary measure.

Location Policies and Reverse Proxy Sessions

In Fudo Enterprise 6.3, sessions established through a reverse proxy are recorded with the source address `127.0.9.1:22` instead of the client address. Because the reverse proxy tunnel ends inside Fudo, the original client address is not known. The same source address is displayed in the session list and session details.

As a result, location policies evaluate all reverse proxy sessions as originating from 127.0.9.1. An *Allow connections* location policy that contains only networks blocks these sessions unless 127.0.9.1 or 127.0.0.0/8 is included.

Once 127.0.9.1 is added, the policy allows all reverse proxy sessions for the user, regardless of the client location.

Note: After upgrading, add 127.0.9.1 to the *Allow connections* location policies of users who connect through a reverse proxy.

A policy that also contains countries allows these sessions even if 127.0.9.1 is not included, because a loopback address is not associated with a country.

Note: Location policies cannot restrict sessions established through a reverse proxy based on the client location.

File Scanning Network Configuration

In Fudo Enterprise 6.3, connections to file scanning providers use the default network configuration of the node. The source address and the routing table used for these connections cannot be selected, so make sure that every node can reach the providers through its default route.

Trusted Root Certificates

Fudo Enterprise no longer trusts **emSign ECC Root CA - G3** (eMudhra) in any of its trust stores, because the keys of eMudhra intermediate certificate authorities were compromised. For the same reason, the AAA Certificate Services root certificate (Comodo), which cross-signed some of these intermediate certificate authorities, is no longer trusted for TLS connections.

The list of trusted root certificates has also been updated to the current Mozilla list, which removes old root certificates that web browsers no longer trust, including DigiCert Global Root CA, DigiCert High Assurance EV Root CA, DigiCert Assured ID Root CA, GlobalSign Root CA, Baltimore CyberTrust Root, QuoVadis Root CA 2, QuoVadis Root CA 3, and COMODO Certification Authority.

After the upgrade, connections that Fudo verifies against public certificate authorities fail if the certificate chain of the remote server ends at one of the removed root certificates. This applies to servers with certificate verification against public certificate authorities, OpenID Connect

providers, AI summary providers, Password Vault integrations, and LDAP servers connected over TLS without an uploaded CA certificate.

Note: Before upgrading, make sure that these servers present a certificate chain that ends at a current root certificate, for example DigiCert Global Root G2, or upload the issuing CA certificate in the Fudo Admin Panel, in the configuration of the affected server, OpenID Connect provider, External Password Repository, or User Directory. Certificate chains that end at current public root certificates, such as Let's Encrypt, DigiCert Global Root G2, or GlobalSign R3 and R6, are not affected.

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 or later** from a version earlier than 5.5.12, you must first upgrade to version 5.5.12 before proceeding to the target version.

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