

Fudo Enterprise 5.4.11

Release Note

Date: June 2024

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

ANNOUNCEMENTS

- Fudo Enterprise 5.4.11 is **the last version supporting the 4-Eyes** authentication for sessions approval in the Sessions tab (the 'Require approval' option). Starting with version 5.5, it will be replaced by **Just In Time** functionality. Simultaneously, the Fudo Officer mobile application will be deprecated. Users utilizing this integration will need to migrate to the new Fudo Officer version that uses the Just In Time feature.

IMPROVEMENTS

- Simplified workflow for RDP connections when using MSTSC and the RDP configuration file generated in the Access Gateway.
- Users now receive information about the reason for the rejected Access Request in mail notifications.

BUG FIXES

- Fixed an issue preventing the saving of a Telnet server configuration when 'TLS enabled' is unselected.
- Fixed a possible authentication bypass in the 'mobiletoken' method. The following conditions have to be met:
 - The user has a 'mobiletoken' authentication method attached (this is automatically attached when the user scans a QR code from the Fudo Officer mobile application).
 - The user has to successfully authenticate at least once using the 'mobiletoken' method. This occurs when the user logs in through the Fudo Officer app.
- Fixed an issue that prevented objects beyond the first 1000 from being searchable through the GUI, ensuring all objects are now accessible regardless of their position in the list.
- Resolved a memory limit issue in Fudo Player that occurred while listing a large number of files in a directory during an SFTP session.
- Fixed an issue with the inactive 'Back' button in the Access Gateway's Web Client connection option modal window.
- Fixed an issue with a disruptive log about incorrect content in 'ssh_config' component.

- Fixed an issue with Okta OpenID Connect authentication where the 'email_verified' field could not be located.
- Fixed an issue preventing the deletion of replicated or backed-up session data if it originates from another node or backup.
- Fixed an issue causing double OTP prompts for redirected RDP connections in RDS, impacting users configured with the OATH authentication method.
- Fixed an issue causing sessions to close due to clipboard handling when using an RDP client.
- Addressed an issue causing password changers to malfunction when using the SSH Key authentication method with 'Legacy crypto' enabled in the Server configuration.
- Resolved an issue related to session data replication between nodes that caused variations in session data size.
- Resolved an issue where adding another LDAP synchronization configuration caused the deletion of previously synchronized users.
- Resolved an issue with LDAP synchronization falling into a loop after manual deleting and re-adding external authentication method for synchronized user.

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.

IMPORTANT INFORMATION FOR UPGRADING FROM VERSIONS 5.2.x AND OLDER

Due to the significant changes in the database, the upgrading process from 5.2.x and older versions might take more time than usual.

There are a few things that need to be verified before the 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.

- As of Fudo PAM 5.3, Citrix, ICA, and Oracle protocols are no longer supported; it is required to remove the sessions (except those already exported) associated with these protocols.
- It is required to have the “Use root store certificates” option enabled in every HTTP server configuration.
- “Hitachi ID Privileged Access Manager” and “Lieberman Enterprise Random Password” must be removed from the External password repositories configuration.
- Users with names containing ‘#’ or ‘%’ chars must be removed or renamed.
- If there are multiple servers with the same address and port pair but different protocols, then only one of them can be left and the other must be removed.
- Remote app configuration must be removed from all the servers and accounts.
- In password changers configuration the server properties: “*protocol*”, “*secproto*”, “*ssl_to_server*”, “*ssl_v2*”, “*ssl_v3*”, “*subnet*” are no longer supported and must be removed.
- Port number 8888 is now reserved. Listeners using this port must be modified to use another port.
- Port numbers greater or equal 60000 are now reserved. Listeners using these ports must be modified to use other ports.

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.

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.

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. Upon a successful '*Run Check*' result, upgrade your Fudo by using the '*Upgrade*' button. Upon system restart, all active sessions will be terminated.

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.

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 '*Restart*', and select previous system revision from the drop-down list.

Please keep in mind any session recordings performed on a newer version will be lost upon upgrade rollback execution.

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