Unsupported public key authentication algorithm SshRsa (ssh-rsa)? Here's how to fix it.

As every good System Administrator already knows, an extremely interesting research paper published in 2023 by Keegan Ryan, Kaiwen He, George A. Sullivan, and Nadia Heninger, mathematically proved yet another weakness with RSA keys, which are often used as host keys by/for SSH/SFTP servers, or to authenticate SSH users via PKI.

For such reason, starting from Syncplify Server! v6.2.26 the `ssh-rsa` algorithm is **no longer among the default active ones**. Please understand that we have done so to protect our customers and users and ensure that we can keep the reputation we earned in the last decade as **the only enterprise-grade SSH/SFTP server on the market that's never been hacked**.

Yet, more often than we thought, we receive emails and support tickets informing us that some SSH/SFTP clients attempting to connect to our server software are receiving an error message like this: "Unsupported public key authentication algorithm SshRsa (ssh-rsa)". So, what to do about it?

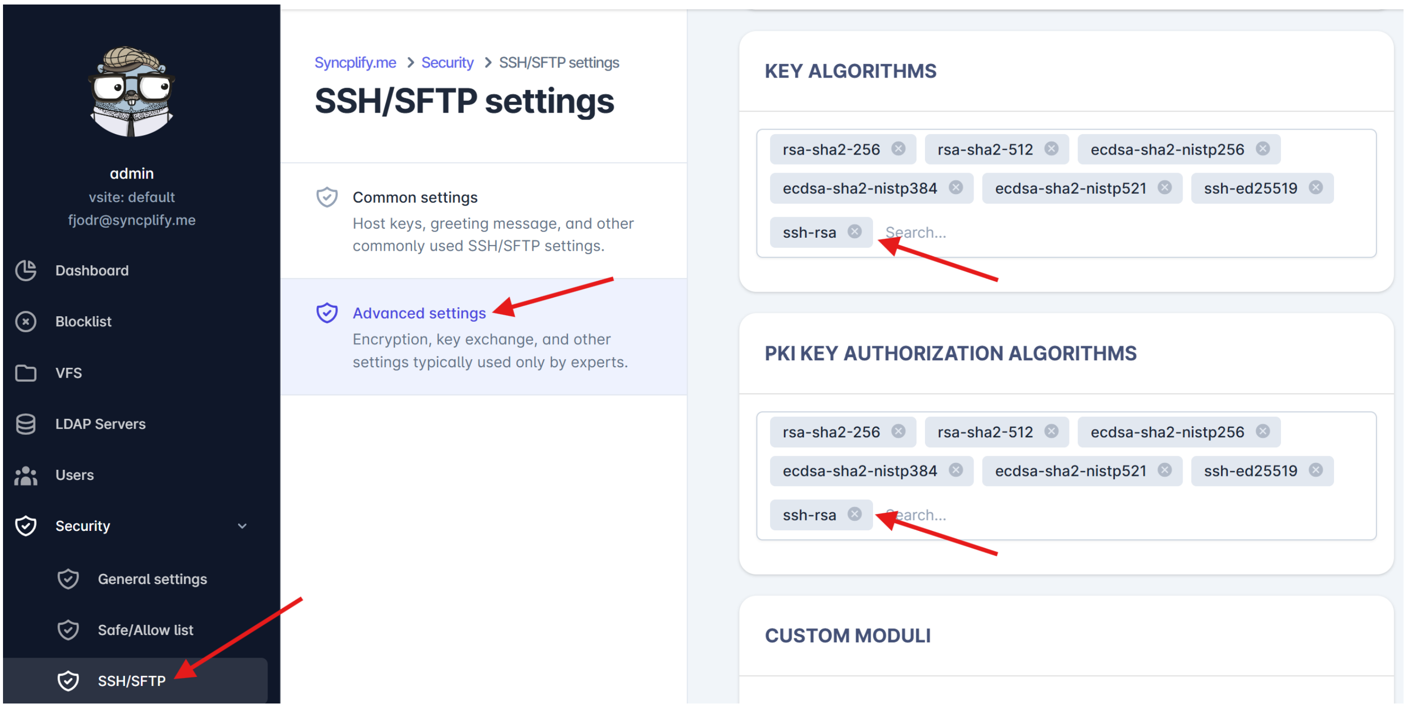
Well, there are two roads you can follow, one that is formally and actually correct and ensures your server's safety and security, and one that *works* but weakens the overall safety and security of your server for every one of your users. Let's explore them both.

The correct way to fix this

The only correct way to fix this is to **ditch RSA keys completely**. They should appear absolutely nowhere in your server's configuration, no RSA host key, no RSA keys to authenticate your users, and no `ssh-rsa` host-key or PKI algorithm enabled. Then configure all of your clients to use alternative algorithms (Ed25519 is strongly recommended) when they connect to your server. Yes, it's a hassle and it requires a lot of reconfigurations of a lot of moving parts, but no effort is too big compared to the cost (legal, monetary, and material) of being hacked.

The quick-and-dirty (and insecure) way to fix this

You can, of course, keep your RSA keys (host key and user keys) and enable the `ssh-rsa` algorithm in your server as shown in the screenshot here below:


admin
vsite: default
fjodr@syncplify.me
Dashboard
Blocklist
VFS
LDAP Servers
Users
Security
General settings
Safe/Allow list
SSH/SFTP
Syncplify.me > Security > SSH/SFTP settings
SSH/SFTP settings
Common settings
Host keys, greeting message, and other commonly used SSH/SFTP settings.
Advanced settings
Encryption, key exchange, and other settings typically used only by experts.
KEY ALGORITHMS
PKI KEY AUTHORIZATION ALGORITHMS
CUSTOM MODULI
Search...

KEY ALGORITHMS: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519, ssh-rsa

PKI KEY AUTHORIZATION ALGORITHMS: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519, ssh-rsa

Please keep in mind that **any change to the security algorithms of your SSH/SFTP server will only take effect after you restart your Virtual Site** from the SuperAdmin UI.

> **WARNING**: While we offer this option for your convenience, it’s important to understand that it does not provide the same level of security as our recommended approach. Syncplify cannot be held responsible for any security breaches that may occur as a result of using this option. We strongly advise selecting the secure option to protect your system, users and data.

Revision #3
Created 9 August 2024 09:12:25 by DevTeam
Updated 9 August 2024 09:35:52 by DevTeam