webdyn
Flexitron group

WebdynSunPM
Application note

Configuration Serveur SFTP

Table of contents

Doc ID sftp-server-config **Version** 1.0
Lifecycle released **Updated** 2026-02-17

1. SFTP server configuration

1.1 Objective

This document describes the parameters required on the SFTP server side to connect a WebdynSunPM with a legacy SSH stack.

1.2 SFTP client technical requirements (WebdynSunPM)

Server requirements - **compatible security profile** :

Category	Parameter to be authorized
Host key algorithms	`ssh-rsa`
Key exchange (KEX)	`diffie-hellman-group-exchange-sha256`
Encryption (ciphers)	`aes128-ctr` or `aes256-ctr`.
MAC (integrity)	`hmac-sha2-256` or `hmac-sha2-512`.
Compression	`none`

These parameters correspond to the most secure intersection between the datalogger's cryptographic capabilities and the current standards supported by modern SSH servers.

> **Warning**
>
> A server configured only with modern host keys (e.g. Ed25519 or ECDSA without RSA enabled) will prevent negotiation and the connection will fail before authentication.

1.3 Example of OpenSSH configuration

This configuration explicitly guarantees compatibility with WebdynSunPM, while maintaining modern cryptographic parameters for the rest of the connections.

1.3.1 Add a dedicated configuration file

Create a dedicated file (recommended to avoid modifying the global configuration) :

```
sudo nano /etc/ssh/sshd_config.d/sunpm-rsa-legacy.conf
```

Recommended content:

```
HostKeyAlgorithms +ssh-rsa
PubkeyAcceptedAlgorithms +ssh-rsa
KexAlgorithms +diffie-hellman-group-exchange-sha256
```

```
Ciphers +aes128-ctr,aes256-ctr
MACs +hmac-sha2-256,hmac-sha2-512
```

These directives add only the algorithms required, without disabling those already configured.

Then restart the service:

```
sudo systemctl restart ssh || sudo systemctl restart sshd
```

1.3.2 Check for the presence of an RSA Host Key

List existing server keys:

```
ls /etc/ssh/ssh_host_*
```

An RSA key must be present:

```
/etc/ssh/ssh_host_rsa_key
```

If absent, generate it :

```
sudo ssh-keygen -t rsa -b 3072 -f /etc/ssh/ssh_host_rsa_key
sudo systemctl restart ssh || sudo systemctl restart sshd
```

1.3.3 Checking for acceptance

Check the actual configuration loaded by sshd :

```
sudo sshd -T | grep -Ei 'hostkeyalgorithms|kexalgorithms|ciphers|macs'
```

The output must include :

- ssh-rsa
- diffie-hellman-group-exchange-sha256
- aes128-ctr (or aes256-ctr)
- hmac-sha2-256 (or hmac-sha2-512)

1.3.4 Other SFTP servers (AWS / Azure / third-party solutions)

The parameters in section 2 constitute the interoperability specification. Any SFTP server is compatible if it allows these algorithms.

AWS Transfer Family

- Authorize an RSA host key for the server
- Check that the security policy does not only require Ed25519/ECDSA
- The required KEX and cipher algorithms are natively supported

Azure SFTP (Storage Account SFTP)

- Enable SFTP option
- Check that the endpoint accepts RSA host keys
- No Kex/cipher settings required (managed by the platform)

Autres serveurs SFTP Generic principle :

> **Note**
>
> The server must authorize an RSA host key and at least one of the common algorithms listed in section 2.

No dependency on OpenSSH is required.

1.4 Server-side verification

Order to be executed :

```
sshd -T | grep -Ei 'kex|cipher|hostkey'
```

Check for the presence of :

- ssh-rsa
- diffie-hellman-group-exchange-sha256
- aes128-ctr (or aes256-ctr)

1.5 Connection test

From a remote station :

```
ssh -vv user@serveur -p PORT
```

Expected outcome of the negotiation :

```
Server host key: ssh-rsa
```

If this line does not appear, the server does not allow the required algorithms.

1.6 Recommended good safety practices

To limit exposure linked to RSA compatibility activation :

- restrict access to the server through IP filtering or private operator APNs
- create a dedicated datalogger account
- limit this account to an SFTP chroot folder
- disable interactive shell
- use a dedicated port

1.7 Diagnosing common errors

Message log	Probable cause	Action
no matching host key type	Unauthorized server-side RSA	activate ssh-rsa
no matching key exchange	KEX incompatible	authorize group-exchange-sha256
connection refused	closed port or firewall	open port
timeout	server unreachable	check routing / NAT