



Shared Managed File Transfer (MFT) Service

Technical Data Sheet

This data sheet provides the technical information required to connect to the SEEBURGER Shared Managed File Transfer (MFT) service. Depending on your usage scenario, the information applies either to automated file transfers using SFTP (Section 2) or to user-initiated file transfers via the MFT Portal (Section 3). Please refer only to the section relevant to your use case.

1. NETWORK / FIREWALL Configuration

If your organization restricts outbound network connections, please ensure that the public IP address specified in this document is allowlisted before your migration. Access to the SFTP service also requires the hostname and port specified below.

Parameter	Value
Hostname	bisfx-gw.seeburger.cloud
IP Ranges	85.115.5.64 – 85.115.5.95 (alternative representation) 85.115.5.64/27 and 85.115.5.192 – 85.115.5.207 (alternative representation) 85.115.5.192/28
SFTP Port	8022
HTTPS Port	443
Protocol	SFTP/HTTPS

2. Automated File Transfer (SFTP)

This section applies if files are exchanged automatically between your systems and the SEEBURGER Shared Managed File Transfer (MFT) service using an SFTP client or integration software. It also contains the supported SSH algorithms required for environments with restricted cryptographic policies.

Parameter	Value
Protocol	SFTP
Hostname	bisfx-gw.seeburger.cloud
Port	8022
Username	<provided separately>
Password	<provided separately>

Directory Structure

The following directory structure is used for automated file transfers.

Direction	Directory
-----------	-----------

Upload to SEEBURGER
Download from SEEBURGER

/My Subscriptions/TO_<Partner>
/My Subscriptions/FROM_<Partner>

Notes

- Existing FTP connections must be updated to use the new SFTP endpoint.
- User credentials are managed by SEEBURGER.
- Firewall rules may need to be updated to allow outbound connections to the new hostname and port.

Supported SSH Algorithms

The following SSH algorithms are supported for automated SFTP file transfers. They are subject to change as part of ongoing security improvements and product enhancements. Algorithms may be added, removed, or updated in future releases to address evolving security requirements and industry best practices.

Key Exchange Algorithms (KEX)
curve25519-sha256 curve25519-sha256@libssh.org
diffie-hellman-group18-sha512 diffie-hellman-group17-sha512 diffie-hellman-group16-sha512 diffie-hellman-group15-sha512 diffie-hellman-group-exchange-sha256

Host-Key Algorithms
ssh-ed25519
rsa-sha2-512 rsa-sha2-256

Encryption Algorithms (ciphers)
aes128-gcm@openssh.com aes128-ctr
aes192-ctr
aes256-gcm@openssh.com aes256-ctr

Message Authentication Code Algorithms (mac)
hmac-sha2-512-etm@openssh.com hmac-sha2-256-etm@openssh.com

3. User-Initiated File Transfer (MFT Portal)

This section applies if users manually upload or download files using the SEEBURGER Shared Managed File Transfer (MFT) Portal.

Parameter	Value
URL	https://bisfx-gw.seeburger.cloud
Protocol	HTTPS
Port	443
Username	<provided separately>
Initial Password	<provided separately>

Directory Structure

After signing in to the portal, the same directory structure is available as for automated SFTP access.

Direction	Directory
Upload to SEEBURGER	/My Subscriptions/TO_<Partner>
Download from SEEBURGER	/My Subscriptions/FROM_<Partner>

Notes

- Portal users receive their login credentials separately during the migration.
- Users can change their password according to the configured security policy.
- Files can be uploaded and downloaded directly through the web interface.
- The directory structure is identical to the one used for automated SFTP transfers.

4. Connection TEST

We are not using a separate test system for the SEEBURGER Cloud. After configuring your connection, SEEBURGER recommends verifying the new environment before switching productive file transfers to SFTP.

The following tests should be performed:

- Successful connection to the new endpoint
- User authentication
- Upload of a test file
- Download of a test file
- Verification of automated file transfers (if applicable)

If you encounter any issues during testing, please verify your local firewall and connection settings. If the problem persists, contact the SEEBURGER Service Desk.

Email:	servicedesk@seeburger.com
Service Desk Portal	https://servicedesk.seeburger.com

5. Migration Information

The migration is performed individually for each customer. During your migration window:

- The existing FTP connection and the new SFTP connection are available in parallel.
- The parallel operation is planned for 30 days.
- During this period, you should update your systems and complete all required testing.
- At the end of the migration window, the FTP connection will be decommissioned and only SFTP will remain available.

Further information about the migration process is available in the accompanying document:

FAQ – Migration to the New Shared Managed File Transfer Service