Create new application or operating system accounts
Account configuration options include account expiry, allowed SSH keys, associated SSL certificates.

State lock-in home folders and automate new home folder creation.
Create and configure groups - allowing for bulk administration options.

Determine settings by group - from authentication to home folders.
Detailed configuration options available for SFTP / SCP based services.
Detailed configuration options for FTP / FTPES / FTPIS based services

**General**

- **Status**
- **Past activity**
- **Reports**
- **Keys and Certificates**
- **Review changes**

**Configuration**

**Server**

- **Services**
- **Transfers**
- **Resources**
- **Authentications**
- **Databases**
- **Locations**
- **Groups**
- **Accounts**
- **Roles**
- **Administrators**
- **Event Handlers**

**Explicit FTPS**

- **Enable Explicit FTPS support.**
  When this is enabled, the service allows Explicit FTPS connections.

- **Force secured authentication**
  When this is enabled, unencrypted login requests are not accepted.

- **Force secured command channel**
  When this is enabled, no commands are processed over unencrypted command channel.

- **Force secured data channel**
  When this is enabled, no unencrypted data transfer is processed.

- **Idle data connection timeout**
  Number of seconds after which idle data channel connections are disconnected. Set to 0 to disable disconnecting idle connections. This does not affect command channel connections, they are configured in **Connections configuration**.

- **Enable password based authentication**
  This allows authentication based on username and password.

- **Enable SSL certificate based authentication**
  This allows authentication based on username and SSL certificate. No password required.

- **Ignore ASCII data type mode.**
  Configures the FTP service to pretend that ASCII mode is supported, while doing the actual transfer in BINARY/IMAGINE mode.

- **Use ASCII data type mode as default.**
  Configures the FTP service to use the ASCII mode, when a data type is not explicitly requested by the client.
Detailed SSL/TLS configuration options available for FTPES / FTPIS
HTTP / HTTPS options available for web browser file transfer manager
Review changes to any components before application.
Once changes are applied, find out which components and changed configuration require a restart.
Authentication options available including anonymous, LDAP bind and IP time ban authentication.

### Configure authentication method "IP time ban authentication"

<table>
<thead>
<tr>
<th>Enable at startup</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this authentication method at server startup.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Identifier**
e4e41ed5-d0d7-4a1b-9a6a-d2b67add8d73 Cannot be changed at runtime.

**Name**
IP time ban authentication

**Type**
Source IP Address Temporary Ban Cannot be changed at runtime.

**Description**
Ban certain IPs from trying to access the file transfer resources

### Source IP time ban configuration

<table>
<thead>
<tr>
<th>Ban interval</th>
<th>604800</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of seconds for which authentication requests from the source IP are denied.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ban after</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of consecutive failed authentications which will result in blocking the source IP.</td>
<td></td>
</tr>
</tbody>
</table>

[Review and apply]
Add custom authentication methods including authentication over remote HTTP
Add copy or move transfers to manage your file transfer operations.
Configure detailed transfer rules according to requirements

Add custom scripts for any additional transfer actions
Configure resource "Trigger Email Alert for Mail_Transfer_Admin"

Identifier: bf02a022-7b42-457c-9878-305b35819a15
Cannot be changed at runtime.

Name: Trigger Email Alert for Mail_Transfer_Admin
A short name to identify this resource.

Type: Email Client
Cannot be changed at runtime.

Description: For transfers that have failed, trigger the email alert.
Free text description for this resource.

Email client specific configuration

Address/Port: 127.0.0.1:25
Address (or domain name) and port number of the remote server.

From email address: no-reply@yourcompany.com
Email address used in the 'From' field of the messages sent to this server.

Username: mail_transfer_admin
Username for the server. Leave blank for anonymous authentication.

Password: ***************
Password for the server.

Add email resources for custom email alerts
Set up detailed event handlers to attach specific actions based on server events.
Set up a custom email alert system using event handlers.
AAA (Authentication, Authorization and Accounting) system support for accounts.

Whitelist by file types, allocate permissions on a per-account or per-path basis.
Set a home folder structure according each group

Define permissions per-group and per-path

AAA (Authentication, Authorization and Accounting) system support for groups
Access detailed audit logs or view on Local Manager. Browse past activity and filter based on search terms, users, peers, events or date and timestamps.
Access the status of all services, transfers, authentication methods, resources and event handlers.

Locate potential problems before they reach your users.
Troubleshoot potential issues related to the server via the Local Manager (shown) and the detailed text audit trail.
Determine which components require any further action
Add databases to handle the audit trail - meet monitoring and logging requirements for compliance and other obligations.
Generate new SSH keys easily and quickly

Web-browser interface available to configure SSL / SSH services

---

### SSL / SSH Keys Management

<table>
<thead>
<tr>
<th>Generate New SSH Key</th>
<th>Convert/Read Existing SSH Key</th>
<th>New SSL Key and CSR</th>
</tr>
</thead>
</table>

**Type:** RSA

**Size:** 2048

Size of the new SSH Key. DSA/DSS keys have a fixed size of 1024 bytes.

**Private Key Password:** Enter key password

Optional password used to encrypt newly created private key. Leave empty if you want to encrypt the private key. If you set a password, be sure to store it carefully.

---

When handling the public key, make sure it is stored as a single line.

---

**OpenSSH Private**

Download

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED

---
Generate new SSL keys and CSR on demand

- Generate New SSH Key
- Convert/Read Existing SSH Key
- New SSL Key and CSR

**Size**
Size of the new SSL Key.

**Private Key Password**
Optional password used to encrypt newly created private key. Leave empty when you don't want to protect generated private keys with a password.

**Common Name**
*yourcompany.com*
In general this is the fully qualified domain name (FQDN) for the server attached to this CSR. If you are generating a CSR for a wildcard certificate your common name must start with an '*', for example: *.domain.tld

**Alternative Name**
Optional alternative name associated with the CSR. For example, DNS:www.fs.domain.tld or IPv4:192.168.7.1 or combined DNS:www.fs.domain.tld, IPv-192.168.7.1

**Email Address**
admin@yourcompany.com
Optional email address associated with the CSR.

**Organization**
YourCompany Inc
Full legal company or personal name, as legally registered in your locality.

**Organization Unit**
IT_Department
Optional branch of your company which is ordering the certificate (accounting, marketing, etc).
Do you need help?
Email us at sales@proatria.com or chat with us on sftpplus.com

Send us feedback via our feedback survey