



White Paper

Fabasoft on Linux - SELinux Support

Fabasoft Folio 2022

Copyright © Fabasoft R&D GmbH, Linz, Austria, 2022.

All rights reserved. All hardware and software names used are registered trade names and/or registered trademarks of the respective manufacturers.

No rights to our software or our professional services, or results of our professional services, or other protected rights can be based on the handing over and presentation of these documents.

Contents

| | |
|--------------------------|---|
| 1 Introduction | 4 |
| 2 Software Requirements | 4 |
| 3 Prerequisites | 4 |
| 4 Installation | 4 |
| 5 Update | 5 |
| 6 Port Types | 5 |
| 7 File Types | 6 |
| 8 Configuration Booleans | 7 |

1 Introduction

This white paper describes how to install and configure the SELinux policy.

2 Software Requirements

System environment: All information contained in this document implicitly assumes a Linux environment.

Supported platforms: For detailed information on supported operating systems and software see the software product information on the Fabasoft distribution media.

Descriptions in this document are based on the following software:

- Red Hat Enterprise Linux 7.9 (x64)

3 Prerequisites

Fabasoft Folio provides an SELinux policy that covers supported use cases with default resource locations (database, file system paths). The policy is based on the SELinux targeted policy, which is the default in a Red Hat Enterprise Linux SELinux environment.

For Fabasoft SELinux support to work, SELinux must be enabled in the system. The configuration is defined in

```
/etc/sysconfig/selinux
```

The variable value of `SELINUX` must be set to `permissive` or `enforcing`.

Additionally, the following RPMs must be installed:

- `libselinux`
- `libselinux-utils`
- `policycoreutils`
- `selinux-policy-targeted`

All installation steps are designed to be executable in enforcing mode, switching to `permissive` is not required.

4 Installation

In case of a new single-machine installation, the feature “Fabasoft Folio SELinux Policy” can be selected. By doing so, the Fabasoft Folio Setup installs the `fsc-selinux-policy` RPM, which automatically installs the policy on the system. Additionally, the setup process registers ports and file system contexts required for selected services.

Rules are available for following services:

- Fabasoft Folio Web Management Services
- Fabasoft Folio Backend Services
- Fabasoft Folio Web Services
- Fabasoft Folio Conversion Services
- Fabasoft Folio E-Services

- Fabasoft Folio AT Services
- Fabasoft Folio IMAP Services
- Fabasoft Integration for Mindbreeze Services
- Fabasoft iArchive Services
- Fabasoft iArchiveLink Services

In case of a distributed installation on multiple machines, ports of services on remote machines cannot automatically be registered by the Fabasoft Folio Setup and must therefore be configured manually. Before being able to do so using `semanage` or a custom policy, the Fabasoft Folio policy must be installed before installing relevant Fabasoft Folio Services.

The policy must be installed via the `fsc-selinux-policy` RPM, which automatically registers and enables the policy.

The Fabasoft Folio policy defines the port types that must be configured in case of remote services local services depend on. Configure these ports accordingly (using `semanage` or a custom policy) before starting the installation process. Otherwise, one or more installation steps (e.g. steps requiring access to Fabasoft Folio Backend Services) might fail due to SELinux denies.

The license file and the installation kit must be labeled with one of the following SELinux types:

- `cifs_t`
- `iso9660_t`
- `tmp_t`
- `user_home_t`
- `user_tmp_t`

5 Update

Updating a non-SELinux enabled Fabasoft Folio installation or enabling SELinux for an existing installation requires special care because the policy installation causes the policy to become active (may deny resource access), which can affect the installation process as well as the availability of Fabasoft Folio Services.

For an update to a SELinux enabled Fabasoft Folio version, proceed as follows:

1. Perform a standard update of Fabasoft Folio using the Fabasoft Folio Setup (permissive mode).
2. Install the Fabasoft Folio SELinux Policy using the Fabasoft Folio Setup (permissive mode).
3. Configure ports and file contexts that are specific to the installation.
4. Enable auto-relabeling (`touch /.autorelabel`) and restart the system.
5. Switch from permissive to enforcing mode.

Future updates can be performed in enforcing mode.

6 Port Types

The following port types are defined in the Fabasoft Folio SELinux Policy:

- `fsc_archive_port_t`
Ports for iArchive Centera/XAM support, required for accessing archiving systems via TCP/UDP.

- `fsc_coomm_port_t`
Ports required for management service access via TCP. Must be registered for clients and the server.
- `fsc_coost_db_port_t`
Ports required for database access via TCP for COO services. Must be registered for the server. In case the Fabasoft Folio Kernel requires access to the database, the ports must be defined on servers running the kernel as well.
- `fsc_coost_port_t`
Ports required for COO service access via TCP. Must be registered for clients and the server.
- `fsc_imap_port_t`
Ports required for IMAP service access via TCP. Must be registered for clients and the server.
- `fsc_mmcst_port_t`
Ports required for MMC service access via TCP. Must be registered for clients and the server.
- `fsc_ooo_port_t`
Ports required for LibreOffice access via TCP in case of conversions. Must be registered for the server.
- `fsc_external_port_t`
Ports required for external service access via TCP. Must be registered for the clients.
- `fsc_iarchivelink_port_t`
Ports required for iArchiveLink web service access via TCP. Must be registered for clients and the server.
- `fsc_web_port_t`
Ports required for web service access via TCP. Must be registered for clients and the server.
- `fsc_wmc_port_t`
Ports required for web management console access via TCP. Must be registered for the server.

7 File Types

The following file types are defined in the Fabasoft Folio SELinux Policy:

- `fsc_archive_t`
File type for iArchive file system support, required for accessing archiving systems via mounted file systems.
- `fsc_coost_dtmlog_t`
File type for COO service DTM log locations, required for accessing DTM log data via mounted file systems.
- `fsc_mmcst_area_t`
File type for MMC service area locations, required for accessing area data via mounted file systems.
- `fsc_etc_krb5_keytab_t`
File type for Kerberos key table file in case of Kerberos authentication, located at `/etc/fabasoft/krb5.keytab`.
- `fsc_tls_t`
File type for the directory containing key and trust files for SSL/TLS for Fabasoft services.

8 Configuration Booleans

The Fabasoft Folio SELinux policy provides the following Booleans that can be changed to modify policy rules without actually changing the policy itself:

- `bool allow_fsc_smbd_userdata_access` (default: false)
Grants read/write access for MMC areas to the Samba daemon. By default, no domain outside of Fabasoft Folio can access data in MMC areas.
- `bool fsc_coomk_can_network_connect_coost_db` (default: false)
Grants direct connections from the Fabasoft Folio Kernel to the COO service database (its configured port as defined by `fsc_coost_db_port_t`). By default, access is disabled.
- `bool fsc_coomk_can_network_connect_http` (default: false)
Grants connections from the Fabasoft Folio Kernel to HTTP servers (their configured port as defined by `http_port_t`). By default, access is disabled.
- `bool fsc_coomk_can_network_connect_http_cache` (default: false)
Grants connections from the Fabasoft Folio Kernel to HTTP servers (their configured port as defined by `http_cache_port_t`). By default, access is disabled.
- `bool fsc_coomk_can_network_connect_smtp` (default: false)
Grants connections from the Fabasoft Folio Kernel to SMTP servers (their configured port as defined by `smtp_port_t`). By default, access is disabled.