# permissions Module

**Miklos Tirpak**

**Edited by**
**Miklos Tirpak**

**permissions Module**

Edited by and Miklos Tirpakand Miklos Tirpak



Revision History

Revision $Revision: 1.1 $ $Date: 2003/07/24 18:11:47 $

# Table of Contents

**1. User's Guide** ..... **1**
1.1. Overview ..... 1
1.2. Dependencies ..... 1
1.2.1. SER Modules ..... 1
1.2.2. External Libraries or Applications ..... 1
1.3. Exported Parameters ..... 1
1.3.1. `allow_file` (string) ..... 2
1.3.2. `deny_file` (string) ..... 2
1.4. Exported Functions ..... 2
1.4.1. `allow_routing()` ..... 2
**2. Developer's Guide** ..... **3**
**3. Frequently Asked Questions** ..... **4**

# List of Examples

1-1. Set allow_file parameter ........ 2
1-2. Set deny_file parameter ........ 2
1-3. allow_routing usage ........ 2

# Chapter 1. User's Guide

## 1.1. Overview

Permissions module is used to determinate if a call has appropriate permission to be established. Permissions can be menaged in configuraton files simular to hosts.allow and hosts.deny:

The search stops at the first match:

- Routing will be allowed when a (FROM, Request URI) pair matches an entry in the /usr/local/etc/ser/permissions.allow file.
- Otherwise, routing will be denied when a (FROM, Request URI) pair matches an entry in the /usr/local/etc/ser/permissions.deny file.
- Otherwise, routing will be allowed.

A non-existing permission control file is treated as if it were an empty file. Thus, permission control can be turned off by providing no permission control files.

FROM header and Request URI are always compared with regular expressions! For the syntax see the sample file: config/permissions.allow

> **Note:** Create your own configuration files /usr/local/etc/ser/permissions.allow and /usr/local/etc/ser/permissions.deny! Samples can be found in the config directory.

## 1.2. Dependencies

### 1.2.1. SER Modules

The following modules must be loaded before this module:

- *No dependencies on other SER modules*.

### 1.2.2. External Libraries or Applications

The following libraries or applications must be installed before running SER with this module loaded:

- *None*.

# 1.3. Exported Parameters

## 1.3.1. `allow_file` (string)

File for the allow rules.

*Default value is "/usr/local/etc/ser/permissions.allow".*

**Example 1-1. Set `allow_file` parameter**

```
...
modparam("permissions", "allow_file", "/etc/permissions.allow")
...
```

## 1.3.2. `deny_file` (string)

File for the deny rules.

*Default value is "/usr/local/etc/ser/permissions.deny".*

**Example 1-2. Set `deny_file` parameter**

```
...
modparam("permissions", "deny_file", "/etc/permissions.deny")
...
```

# 1.4. Exported Functions

## 1.4.1. `allow_routing()`

Returns true if the (FROM, Request URI) pair in the received sip message has appropriate permission according to the configuration files.

**Example 1-3. `allow_routing` usage**

```
...
if (allow_routing()) {
    t_relay();
};
...
```

# Chapter 2. Developer’s Guide

The module does not provide any sort of API to use in other SER modules.

# Chapter 3. Frequently Asked Questions

**1.** Where can I find more about SER?

Take a look at http://iptel.org/ser.

**2.** Where can I post a question about this module?

First at all check if your question was already answered on one of our mailing lists:

- http://mail.iptel.org/mailman/listinfo/serusers
- http://mail.iptel.org/mailman/listinfo/serdev

E-mails regarding any stable version should be sent to `<serusers@iptel.org>` and e-mail regarding development versions or CVS snapshots should be send to `<serdev@iptel.org>`.

If you want to keep the mail private, send it to `<serhelp@iptel.org>`.

**3.** How can I report a bug?

Please follow the guidelines provided at: http://iptel.org/ser/bugs