

# Handling Files

## DESCRIPTION

**Copyright**

© Ericsson AB 2016, 2017, 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Understanding File Management</b>	<b>1</b>
1.1	Key File Management Concepts	1
<b>2</b>	<b>Basic File Management Procedures</b>	<b>3</b>
<b>3</b>	<b>Advanced File Management Procedures</b>	<b>4</b>
3.1	Security Management	4
<b>4</b>	<b>File Management-Related Alarms</b>	<b>5</b>





# 1 Understanding File Management

## 1.1 Key File Management Concepts

File Management provides a management interface to a logical file system in the Managed Element (ME).

The logical file system exposes files produced by functions on the ME, for example, performance measurement report files and alarm logs. In addition, files can be imported to the logical file system. Such files are located in directories, which are exposed as file groups on the logical file system.

A file group can contain other file groups forming a file group subtree.

File Management enables a mapping between a Managed Object (MO) Distinguished Name (DN) and a path on the logical file system, for example, as follows:

— DN:

```
ManagedElement=N0DE06ST, SystemFunctions=1, FileM=1, LogicalFs=1, FileGroup=MyService
```

For example:

```
FileGroup=MyService  
[...]  
    files=MyFile.log  
[...]
```

— Corresponding path on the logical file system:

```
/MyService/MyFile.log
```

The **FileM** Managed Objects Classes (MOCs) can be found in the Managed Object Model (MOM). For general information about the Managed Objects, cardinality, and related concepts, refer to [Managed Object Model User Guide](#).

A preventive maintenance policy is a routine that can automatically delete files or raise alarms when limits are exceeded. A preventive maintenance policy can be associated with one or more file groups, it is applied recursively to all files and file groups within a file group. File deletion applies either to the newest or the oldest file.

There are six predefined file groups. Four of the six file groups have system-controlled preventive maintenance policies; these file groups are:

— **AlarmLogs**

Contains alarm log files. The log has a preventive maintenance policy in which the maximum number of alarm log files is 11 and the size of each alarm



log file is restricted to 500 KB. The log is a wrap log where the oldest file is overwritten at log wrapping. This is controlled by the log service housekeeping policy. For more information on alarms, refer to [Handling Alarms](#).

— AlertLogs

Contains alert log files. The log has a preventive maintenance policy in which the maximum number of log files is 11 and the size of each alert log file is restricted to 500 KB. The alert log is a wrap log where the oldest file is overwritten at log wrapping. This is controlled by the log service housekeeping policy. For more information on alerts, refer to [Handling Alarms](#).

— InServicePerformance

Contains ISP XML report files. The ISP functionality regularly creates ISP XML report files and keeps them for 6 months. As a preventive maintenance policy the system automatically cleans the old ISP reports. This activity happens once per month at the time of creation of a new ISP XML report.

— PerformanceManagementReportFiles

Contains the Performance Management (PM) report files. The report file has a default preventive maintenance policy in which the maximum number of PM report files is 1000. If the preventive maintenance limit is exceeded, the oldest file is automatically deleted. This provided by PM internal housekeeping.

There are two additional predefined file groups; however, these files groups do not have any system-controlled preventive maintenance policies. A preventive maintenance policy can be specified separately for these file groups:

— BackupAndRestoreManagementFiles

The files in this file group are managed by the Backup and Restore function. It is possible to set limits on the number of Manual Backups files and the number of scheduled backups files stored in the file group.

For more information on backup and restore and preventive maintenance policy, refer to:

- [Backup and Restore](#)
- [Change Maximum Number of Manual Backups](#)
- [Enable Automatic Deletion of Manual Backups](#)
- [Set Maximum Number of Scheduled Backups](#)

— SoftwareManagement

Contains the software upgrade packages that have been downloaded into SoftwareManagement file group. A File Management preventive maintenance policy can be applied to this file group.



File Management policies are only to be applied to file groups that are not already subject to specific system controlled or user-defined preventive maintenance policies.

The files and file groups in the logical file system can be accessed through the Ericsson Command-Line Interface (ECLI), NETCONF, and the standard SSH File Transfer Protocol (SFTP).

**Note:** Special characters, such as + in filenames, appear as ?? in the ECLI. For more information, refer to *Interwork Description Ericsson Command-Line Interface*.

## 2 Basic File Management Procedures

File Management is accessed using NETCONF or the ECLI to manipulate the Management Information Base (MIB):

- Access to a logical file system through the MOM, based on security rules

Depending on security rules, a user can create or delete file groups and manually delete files in the logical file system. For more information, see Section 3.1 on page 4.

- Access to a logical file system over SFTP, based on security rules

This operation can be used by Northbound Interface (NBI) clients (such as OSS, LCT, and CLI script), which must fetch files from the logical file system. The procedure in *Fetch File in Logical File System* provides further details on how to perform this operation. Depending on security management rules, all or part of the SFTP protocol operations can be allowed. For more information, see Section 3.1 on page 4.

- Definition, modification, and deletion of preventive maintenance file group policies

The following file group policies can be defined:

- Automatic deletion, where files are deleted automatically when a limit is exceeded. Files can be deleted when the number of files in a file group subtree, or the size of a file group subtree reaches or exceeds a limit.
- Automatic deletion, where each file in a file group subtree is kept a maximum specified time.
- Automatic alarm reporting, where an alarm is raised when a limit defined in a configured monitoring threshold is exceeded. An alarm is raised when the number of files in a file group subtree, or the size of a file



group subtree exceeds a limit. The alarm informs the user that manual maintenance is required.

The procedures in [Configure Preventive Maintenance Policy Deleting Files in Logical File System](#) and [Configure Preventive Maintenance Policy Reporting Alarms for Logical File System](#) provide further details on how to perform these operations.

## 3 Advanced File Management Procedures

### 3.1 Security Management

Access to the logical file system is configured through security management rules. For more information, refer to [User Management](#). By setting rules to [FileGroup](#) instances, different permission types can be applied.

Table 1 File Group Permission Types

Permission Type	Description
NO_ACCESS	The file group is invisible to the user.
R (read)	The file group and its contained <a href="#">FileInformation</a> instances are visible to the user. The user can export files from the group.
RW (read and write)	The file group and its contained <a href="#">FileInformation</a> instances are visible to the user. The user can set writable attributes of a <a href="#">FileGroup</a> instance. The user can import and export files into/from the group.
RWX (read, write, and execute)	The file group and its contained <a href="#">FileInformation</a> instances are visible to the user. The user can set writable attributes and execute actions of a <a href="#">FileGroup</a> instance. The user can import and export files into/from the group. When using SFTP for transfer of files, all operations offered by the protocol are possible to execute without restrictions.





## 4 File Management-Related Alarms

Table 2 File Management Related Alarms

Alarm	Description
File Management, Number of Files in FileGroup Exceeded	Raised when the total number of files in the FileGroup subtree has exceeded a configured threshold.
File Management, Max Size in FileGroup Exceeded	Raised when the size of the FileGroup subtree has exceeded a configured threshold.