

File Management

DESCRIPTION

Copyright

© Ericsson AB 2014, 2015. 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

1	Introduction	1
2	Functions and Concepts	3
2.1	Types of Operation	4
3	Managed Object Model	7
4	Configuration Management	9
5	Fault Management	11
6	Security Management	13





1 Introduction

This document provides an overview of the management model and concepts associated with the File Management managed area.

A managed area is represented by a group of Managed Object Classes (MOCs) within the Managed Object Model (MOM).





2 Functions and 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=NODE06ST, 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
```

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.

Three predefined file groups exist, as follows:

- 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 *Fault Management*.

- 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 *Fault Management*.

- 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.

The predefined file groups cannot be deleted. No preventive maintenance must be configured for these predefined file groups since their files are subject to internal preventive maintenance.

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*.

2.1 Types of Operation

File Management supports the following operations:

- 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 6 on page 13.

- 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 6 on page 13.

- 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 can be 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 ME raises the alarms *File Management, Number of Files in FileGroup Exceeded* and *File Management, Max Size in FileGroup Exceeded* to indicate these conditions.

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 Managed Object Model

The File Management managed area is represented in the *Managed Object Model (MOM)* as follows:

```
ManagedElement
+-SystemFunctions
  +-FileM
    +-FileGroupPolicy
      +-ThresholdMonitoring
    +-LogicalFs
      +-FileGroup
        +-FileGroup
```

For general information about the MOM, MOCs, MOs, cardinality, and related concepts, refer to *Managed Object Model User Guide*.

The File Management MOCs are described in Table 1.

Table 1 File Management Managed Object Class Descriptions

Managed Object Class	Description
<i>FileM</i>	The root of the File Management model.
<i>FileGroupPolicy</i>	Contains the preventive maintenance rules for file groups.
<i>ThresholdMonitoring</i>	Contains the configured monitoring thresholds.
<i>LogicalFs</i>	The root of the logical file system.
<i>FileGroup</i>	Contains the file groups. A file group can contain another file group or a file. Represents a directory in the logical file system.





4 Configuration Management

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

The following operations can be performed by the user and are described in Operating Instructions using the ECLI:

Manage Files

- *Fetch File in Logical File System*
- *Delete File in Logical File System*
- *List File Groups and File Information in Logical File System*

Manage File Group Policies

- *Configure Preventive Maintenance Policy Deleting Files in Logical File System*
- *Configure Preventive Maintenance Policy Reporting Alarms for Logical File System*





5 Fault Management

The File Management alarm is described in Table 2.

Table 2 File Management Alarm

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





6 Security Management

Access to the logical file system is configured through security management rules. For more information, refer to *Security Management for ECLI, NETCONF, and SFTP Users*.

The permission types in Table 3 can be applied by setting rules to *FileGroup* instances.

Table 3 Permission Types

Permission Type	Description
NO_ACCESS	The file group is invisible to the user.
R (read)	The file group and its contained <i>FileInformation</i> instances are visible to the user. The user can export files from the group.
RW (read and write)	The file group and its contained <i>FileInformation</i> instances are visible to the user. The user can set writable attributes of a <i>FileGroup</i> instance. The user can import and export files into/from the group.
RWX (read, write, and execute)	The file group and its contained <i>FileInformation</i> instances are visible to the user. The user can set writable attributes and execute actions of a <i>FileGroup</i> 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.