A MITEL
PRODUCT
GUIDE

Unify OpenScape Fault Management

Unify OpenScape Fault Management V13, Web

User Guide
09/2023

A31003-F30D0-U121-01-7619

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

Contents

1 Preface

This chapter discusses the following aspects:

- purpose and audience of this guide
- terminology
- organization of this guide
- conventions used in this manual

1.1 Purpose

This User Guide describes the OpenScape FM Web for OpenScape FM.

1.2 Audience

This guide addresses users who want to learn how to use the OpenScape FM Web. To work with the OpenScape FM Web, it is helpful to know how the OpenScape FM Client is used. More about this can be found in the *OpenScape FM Desktop User Guide*.

1.3 Organization of this Guide

This guide is organized as follows:

- *Chapter 2, "Introduction"* provides a short overview about the structure of the OpenScape FM Web.
- *Chapter 3, "First Steps"* shows how to start, initialize and license the OpenScape FM Web.
- *Chapter 4, "Concepts"* describes the basic concepts and the user interface of the OpenScape FM Web.
- *Chapter 5, "Navigation"* describes how to navigate the data provided by the OpenScape FM Web.
- *Chapter 6, "Dashboards"* describes the various dashboards provided by the OpenScape FM Web.
- *Chapter 7, "Categories"* describes the various object categories provided by the OpenScape FM Web.
- *Chapter 8, "Reporting"* discusses the reporting features provided by the Web Client.
- *Chapter 9, "Technologies"* describes Categories that are specific for objects that represent OpenScape technology elements (like OpenScape Voice).
- *Chapter 10, "Topologies"* describes Main Views that focus on the topology.
- *Chapter 11, "Monitoring"* describes Main Views that focus on monitoring parameters provided by the System Management Plugin.

- *Chapter 12, "Detail Views for Object Types"* shows the object types known by the OpenScape FM Web for which specific Detail Views can be displayed.
- *Chapter 13, "Configuration"* shows how new objects can be added to the OpenScape FM and how existing ones can be reconfigured.
- *Chapter 14, "Administration"* introduces the administrative functions that can be performed via the web client.
- *Appendix B, "Macros"* introduces helpful macros that can be used in many places as output placeholders in e.g. notifications or self defined events.

1.4 Conventions Used in this Manual

The following font conventions are used in this document:

Bold Font: Indicates that a word is a new or important term. Bold is also used for buttons, menu names and item names

Example: **Dashboard** or **OK**.

Bold Computer Font: Indicates data to be entered by the user.

Example: **`java`**.

Computer Font: Indicates computer output, file content, an explicit directory or a file name.

Example: `prompt%`.

Italics: Indicates a reference to another manual or to a different section within the current manual.

Example: see *Desktop User Guide.*

Italic type is also used for emphasis.

Example: *All* users will be affected.

1.5 Terminology

- **OpenScape FM** means OpenScape Fault Management.
- **Server** means the OpenScape FM Server, i.e. the server where OpenScape FM Desktop has been installed.
- **Client** means the classic OpenScape FM Client.
- **Desktop** means the OpenScape FM Desktop.
- **Host** is used as a synonym for IP Node within this user guide.

2 Introduction

This chapter provides a short introduction into the OpenScape FM Web and the major keywords used in this user guide.

The OpenScape FM Web is a purely web-based user interface for the OpenScape FM. It is designed to be easy to use and to provide quick access to information that is vital for the operator. Incorporated extensive options to filter the data allows the operator to quickly focus on the relevant information.

Currently the OpenScape FM Web does support a part of the administrative tasks within the OpenScape FM. For such tasks the OpenScape FM Java Client has to be used. This client, described in the *OpenScape FM Desktop User Guide*, can be started as a standalone application or via Java Webstart without the need for a web browser.

The OpenScape FM Web runs within web browser windows which are divided into three major elements: the **Header Bar** located at the top, the **Navigation Panel** located on the left and the **Main Panel** that uses the major area located at the lower right.

The **Header Bar** displays the application‘s banner and the **Server Status** (see *Section 4.5*). It contains the **User Menu** (see *Section 4.2*) that offers the logout function and provides information about the current user and the application itself. The **Full Text Search** (see *Section 4.17*) to find and display OpenScape FM objects based on specific substrings is also located within the Header Bar. The Header Bar also contains an **overview of currently unconfirmed events**. (see *Section 4.4*).

If the Web Client is currently busy collecting or storing data, this will be displayed by an orange bar displayed at the upper edge of the Header Bar.

Main Views (see *Section 4.9*) deliver the information to the user. They can be opened by entries located within the **Navigation Panel**, from within other views or by the **Full Text Search** and are displayed within the **Main Panel**.

The **Navigation Panel** (see *Section 4.8*) provides direct access to three types of Main Views:

- **Dashboards** (see *Section 4.10*) show aggregated and reduced data to provide quick information about a specific goal or topic.
- **Categories** (see *Section 4.11*) and OpenScape specific **Technology Categories** labeled **Technologies** show complete lists of objects that meet a Category specific criterion.
    - **Status Indicators** (see *Section 4.8.2*) provide instant information about the existence of non normal objects within a Category.
    - **Severity Displays** (see *Section 4.16.1*) give an overview about the status distributions of the objects within a Category.
    - **Filters** (see *Section 4.16.2*) can be used to only display the objects that meet user defined criteria.
- **Network** (see *Section 4.13*) allow the navigation within a part of the Java Client‘s topological object structure.

To get additional information about a specific object, its **Detail View** (see *Section 4.15*) can be opened. This is generally done by clicking a link representing the object within a Main View or within another Detail View.

Depending on the type of the effected objects, **Actions** (see *Section 4.18*) can be performed for objects selected in Main Views or for the object assigned to a Detail View.

3 First Steps

3.1 Installation of the OpenScape FM Web

The OpenScape FM Web is installed automatically during the installation of the OpenScape FM Server (see *Desktop User Guide*).

3.2 Initialization of the OpenScape FM Web

No separate initialization is needed. The OpenScape FM Web is available, if the OpenScape FM Server is running. This is indicated by an *active* service OpenScape Startup Service running on the OpenScape FM Server host.

3.3 Licensing of the OpenScape FM Web

No separate license is needed for the OpenScape FM Web. It is licensed with the OpenScape FM Base License.

3.4 Launching of the OpenScape FM Web

The OpenScape FM Web can be launched by three methods:

- By using the URL
  `https://OpenScape_FM_host:3080/web`
  within a web browser.
- From the OpenScape FM Client by using the main menu entry **Client->Web**.
- By starting the OpenScape Fault Management landing page with the URL
  `https://OpenScape_FM_host:3043`
  and selecting the button **Web**.

In the URLs for the first and third method `OpenScape_FM_host` has to be replaced with the IP or hostname of the machine on which the OpenScape FM Server and its Wildfly Server are running and whose data should be used.

4 Concepts

This section describes the basic functions and components of the OpenScape FM Web.

Mainly the following topics are handled:

- The user **Authorization** (see *Section 4.1*), the **Starting of other Clients** (see *Section 4.6*) and **Online Help** (see *Section 4.7*).
- The main user interface elements **User Menu** (see *Section 4.2*), the self monitoring of the OpenScape FM (see *Section 4.5*), **Navigation Panel** (see *Section 4.8*), **Main View** (see *Section 4.9*), **Dashboard** (see *Section 4.10*), **Categories** and **Technologies** (see *Section 4.11*), **Reporting** (see *Section 4.12*), **Network** (see *Section 4.13*), **Monitoring** (see *Section 4.14*) and **Detail View** (see *Section 4.15*).
- Working with **Tables** (see *Section 4.16*).
- The **Full Text Search** to find objects independent of their object type (see *Section 4.17*).
- The methods to perform **Actions** on selected objects (see *Section 4.18*).
- The windows to **Create** and **Configure** objects (see *Section 4.19*).

4.1 Authorization and Authentication

This section describes the user login and logout (see *Section 4.1.1* and *Section 4.1.2*), the handling of access rights (see *Section 4.1.3*) and the changing of passwords (see *Section 4.1.4*)

4.1.1 Login

When the OpenScape FM Web is started, the login page is automatically opened. The user has to authenticate against the OpenScape FM Server by entering the login name (**User**) and a matching **Password**. The OpenScape FM server that can be reached on the host specified in **Server** via the entered **Port** checks whether the user/password combination is valid, and if valid, allows access to this server.

If the Caps Lock key is active while the password is being entered, as a warning a notice is displayed below the password entry field.

Alternatively, the logon can also be done using a Windows Single Sign On authorization, if this has been enabled as a possible logon method (see *Desktop User Guide*).

If it has been enabled and is to be used by the current user, all that needs to be done on the login page is to click the link **Use Windows session authentication**. The logon is then performed via the domain user account with which the user is currently logged on to the system.

If, in addition to Single Sign On, automatic user creation has also been enabled at the same location, the first time a user logs on with Single Sign On, the user is automatically created. A user created in this way has only the elementary User rights. Further rights must be enabled by an Administrator (see *Section 14.3*).

The **Language** that will be used within the OpenScape FM Web can be selected within the Login Page, as well as the Color **Theme** that should be used (see *Section 4.3.1*).

Important Note:
Only one session at a time can be opened per browser and OpenScape FM Server. This session is valid for all browser tabs and windows.

4.1.2 Logout

The session for the current user and the connection to the OpenScape FM Server can be terminated by using the entry **Sign Out** within the User Menu (see *Section 4.2*).

When the session is terminated, the login page is opened (see *Section 4.1.1*).

Important Note:
If the **Sign Out** function is *not* used, but only the browser page is closed, the session can remain for a few minutes. Within this period of time the session can be continued in a new browser page without entering a password.

4.1.3 Access Rights

The access rights the user has within the OpenScape FM Web correspond to the access rights the user has within the OpenScape FM Client. The user has access to the same objects and events as he has within the OpenScape FM Client.

Events or objects for which the current user has no access rights within the OpenScape FM Client will not be displayed or counted within the OpenScape FM Web. Actions for which the user has no rights within the OpenScape FM Client can also not be initiated by the user within the OpenScape FM Web.

4.1.4 Password Change

The Password of the current user can be changed by using the entry **Change Password** within the User Menu (see *Section 4.2*).

To perform a password change, the old password has to be entered as a user confirmation and the new password has to be typed twice to avoid undesired mistypes.

An entered password has to fullfil the general password guidelines of the OpenScape FM (see separate *Desktop User Guide*) to get accepted.

4.2 User Menu

The User Menu is located right most within the Header Bar. It is displayed as a green button with a gear symbol. If the browser window does not exceed a certain width, the User Menu can be found above the Navigation Panel (see *Section 4.8*).

The User Menu provides the following functions:

- The menu entry Preferences can be used to configure user dependant settings (see *Section 4.3*).
- The menu entry **Info** shows information about the current version of the OpenScape FM Web, the copyrights and trademarks.

  Pressing the button **License Information** opens a browser window that provides links to the End User License Agreements (EULA) and the Third Party Software Information.
- The starting of the classic OpenScape FM Administrator Client and the Performance Management Client by using the entry Administrator **Client** and **Performance Manager** Client (see *Section 4.6*).
- The menu entries **Help Web** and **Help Overview** can be used to open the Online Help (see *Section 4.7*).
- For Users with Administrator or Operator rights the menu entry **Administration** opens a new browser page (see *Chapter 14*) in which Administrators can configure the OpenScape FM and Operators can view this configuration.
- The menu entry **Change Password** can be used to change the password of the current user (see *Section 4.1.4*).
- The entry **Sign Out** is used to terminate the session for the current user and the connection to the OpenScape FM.

4.3 User Settings

The User Settings can be selected on a configuration page.

These can be opened by using the User Menu (see *Section 4.2*) entry **Preferences**.

On the configuration page, the display colors of the Web Client (see *Section 4.3.1*) and the calculation method of the Status Indicators (see *Section 4.3.2*) can be selected.

4.3.1 Display Theme

Within the User Menu under **Preferences** the selection menu **Theme** can be used to configure which color theme should be used by the Web Client.

This selection can also be made directly while logging in on the Login Page (see *Section 4.1.1*) also using the **Theme** selection menu.

The available options are:

- **Light**: This selection activates the 'classic', fairly bright, colors for the Web Client. They are especially suitable in brighter work environments (Day Mode).
- **Dark**: This selection activates a darker color palette. This selection is especially useful in darker work environments (Night Mode).

4.3.2 Status Indication

Within the User Menu under **Preferences** the selection menu **Status Indicator** can be used to configure how the values within the Status Indicators (see *Section 4.8.2*) should be calculated.

The available options are:

- **Sum of most critical States**: The number of all matching objects or unconfirmed events that are currently in the worst status (the status that is also displayed in color).
- **Sum of non normal States**: The number of matching objects or unconfirmed events that are in a status that is worse than normal (*Critical*, *Major*, *Minor* or *Warning*).
- **Sum of all States**: The number of all matching objects or unconfirmed events

4.4 Overview of Current Events

Located within the Header Bar between the Full Text Search (see *Section 4.17*) and the User Menu (see *Section 4.2*) is a two-part overview of events that are currently unacknowledged.

In the left part there are three values which show the number of still unacknowledged events that occurred in the last 24 hours (**24h**), the last 8 hours (**8h**) or the last hour (**1h**). The color of the values reflects the status of the most critical event within the respective period.

The numbers shown in the colored areas to the right indicate how many events of each status are currently unacknowledged (from left to right: *Critical*, *Major*, *Minor*, *Warning* and *Normal*).

All numbers within the overview can be clicked. This action expands the currently displayed Main View by a view listing the respective events. These views are independent from manual filters defined within the Category Events (see *Section 7.1*) and can therefore be navigated with the forward/backward browser buttons or stored as an individual URL.

Note:
Event numbers that reach or exceed 1,000 are shown in the display as `999+`.

4.5 Self-Monitoring / Server Status

The server Self-Monitoring is used to inform the user working with the Web Client that the OpenScape FM server could possibly have a pending problem.

The Self-Monitoring Indicator is located in the header to the left of the input field for the Full Text Search (see *Section 4.17*) and consists of a colored frame enclosing the product name. The color of the frame corresponds to the status of the server. If the status deteriorates, the color changes towards red and additionally the frame starts to pulsate.

Clicking on the Self-Monitoring opens the page **Server Settings->Server Information** (see *Section 14.6.4*).

However, Self-Monitoring is only displayed if the Client window has sufficient width.

Currently the Self-Monitoring checks:

- the *Memory Usage* parameter of the *Internal Monitoring* monitor on the server host system.
  This should identify threatening memory problems on the server host.
  The Server Status corresponds with the object status of the respective parameter, which is determined by the configured thresholds.
- the *Disk Usage - Disk Usage* and *Disk Usage - Installation Size* parameters of the *Internal Monitoring* monitor on the server host system.
  This should identify threatening storage size problems on the server host.
  The Server Status corresponds with the object status of the respective parameters, which is determined by the configured thresholds.
- missing or soon to be expired licenses.
  The Server Status corresponds with the status of the License Manager object.

Further monitoring checks are to be integrated in the future.

4.6 Starting Clients

From within the OpenScape FM Web, the classic **OpenScape FM Administrator Client** can be started as a Client Application. This can be done by using the entry **Client** within the User Menu (see *Section 4.2*). More about the Administrator Client can be found in the *OpenScape FM Desktop User Guide*.

With the entry **Performance Management** of the User Menu, the **Performance Management Client** can be opened. More about this Client can be found in the *Performance Management User Guide*.

4.7 Online Help

The Online Help can be opened by two entries of the User Menu (see *Section 4.2*):

- The entry **Help Web** opens the user guide for the OpenScape FM Web in a separate browser tab and with the current language.
- The entry **Help Overview** opens an index page that lists all OpenScape FM user guides in a separate browser tab. From this index page all OpenScape FM user guides can be opened in English or German language.

4.8 Navigation Panel

The Navigation Panel is located on left side of the OpenScape FM Web.

By clicking the burger icon (three white lines) that is located in the upper left of the Header Bar, the panel can be closed or opened.

It is either permanently shown, if the browser window exceeds a certain width, or else it can be opened by clicking the green button on the utmost left of the Header Bar.

The Navigation Panel is used to select the Main Views (see *Section 4.8.1*) that should be displayed. It also provides information about the current existence of critical objects (see *Section 4.8.2*).

4.8.1 Opening Views

Main Views (Dashboards, Categories, Technologies) can be opened simply by clicking the respective entry within the Navigation Panel.

Detail Views (see *Section 4.15*) for specific objects can then be opened from the displayed Main View or from inside other Detail Views. Generally this is done by using links.

4.8.2 Status Indicator

To indicate possible current problems, colored indicators are displayed to the right of the Categories and Technologies within the Navigation Panel.

The color of the indicators represent the worst severity of the objects that are currently displayed within the respective Category (red for *Critical*, orange for *Major*, yellow for *Minor* or light blue for *Warning*). If the Category contains *no* object that has a severity that is at least *Warning*, no indicator will be shown for the Category.

The indicators contain a value based on the number of objects in the given category. For the Events category (see *Section 7.1*), the value is based on the number of unconfirmed events that do not correlate with a newer event.

The current counting method can be configured in the user menu under **Preferences** (see *Section 4.3.2*).

The status distribution and the currently selected counting method are displayed in the tooltip of the Status Indicator.

Important Note:
The counter for events will always represent the number of objects as it will be displayed in the Correlated View, even if the correlated view is switched off. Therefore the displayed number may vary from the number displayed within the Category itself.

Example:
If a three is displayed within a orange indicator, then three objects within the Category have a *Major* severity. *No* objects are in *Critical* severity, else the indicator would be displayed in red.

4.9 Main View

Main Views are the central element of the OpenScape FM Web.

They are opened within the current window by clicking their name in the left pane of the window. They can also be opened in a separate browser page or browser window by right-clicking their name.

A Main View either contains the Login panel (see *Section 4.1*), a Dashboard providing aggregated information about specific topics (see *Section 4.10*) or Categories providing information about objects with a common topic or technology (see *Section 4.11*).

A Main View can also consist of elements that are found by a Full Text Search (see *Section 4.17*), or of objects that are displayed as a list within a Detail View (see *Section 4.15*).

The self-referencing link of an object within the Main View opens a Detail View (see *Section 4.15*) of the selected object. In most cases it can be found within the column *Name*.

In most cases Actions can be performed for the objects listed in a Main View (see *Section 4.18*).

4.10 Dashboards

Dashboards are Main Views that provide individual representations of data collections to fullfil a certain goal.

The data might be condensed and reduced to the data needed for the goal. Data from various technologies or aggregated data (e.g. averages over time intervals) may be contained within a single Dashboard.

For example: The Dashboard Overview (see *Section 6.1*) which has the goal to indicate possible problems only shows non normal Events and Hosts. Complete lists of Events and Hosts are displayed by the respective Categories.

A list of the Dashboards that can be directly opened from the Navigation Panel (see *Section 4.8*) can be found in *Chapter 6*.

Each segment within a dashboard is based on a Contol Center object (see *Control Center User Guide*). If this object is set to unmanaged, the corresponding segment is hidden within the web.

Important Note:
Dashboards do not react immediately if their Control Center objects are managed/unmanaged. A user will only see this, if a reload or a new login is performed.

4.11 Categories and Technologies

Categories provide a current and complete list about objects known by the OpenScape FM that are specific to a topic or technology.

They display a table containing a list of objects with a common characteristic. For example, these can be OpenScape FM events, hosts, networks or devices of a specific technology.

A Severity Display (see *Section 4.16.1*) above the table shows the status distribution of the objects or events currently displayed within the table.

The objects shown in the Main View table of an Category can be filtered by their Severity or by the contents of the table columns (see *Section 4.16.2*).

The table columns can be resized by dragging the column boarders and sorted by clicking the column header. By using the button **Automatically adjust column width** located below the table, the column widths can be automatically adjusted to the respective widest content.

Individual columns can be displayed or hidden by using the **Select the columns...** button. Checked columns will be displayed.

The link within the column **Name** (or **Description** for Events) can be used to open the Detail View (see *Section 4.15*) of the selected object.

The column **Events** shows the number of events that currently affect the object. Clicking on the number opens a table with these events. If a **! in a circle** is displayed in front of the number, there is at least one unacknowledged event for the object, if a **filled sun symbol** is displayed, there is at least one unacknowledged 'blinking' event.

A list of the Categories that can be directly opened from the Navigation Panel (see *Section 4.8*) can be found in *Chapter 7* (for general Categories) and *Chapter 9* (for OpenScape specific Technologies).

4.12 Reporting

The **Reporting Views** are special Category Views (see *Section 4.11*) that display all existing Reports (see *Section 8.1*) or all created Templates to generate Reports (see *Section 8.2*).

4.13 Network

The **Network Views** are special Category Views (see *Section 4.11*) which reflect the object structure of the OpenScape FM similar to the Classic Client.

The object hierarchy is displayed both as a Navigation Tree View (see *Section 10.2*) and as a Submap Structure (see *Section 10.1*).

4.14 Monitoring

The **Monitoring Views** are special Category Views (see *Section 4.11*) that deal with objects that are relevant to System Management Monitoring. Specifically, these are lists of the Hosts monitored by System Management (see *Section 11.1*), the active Monitor Types (see *Section 11.2*), the monitoring Profiles (see *Section 11.3*), and an overview of the active Monitors, Parameters, and System Management Agents (see *Section 11.4*).

4.15 Detail View

While the Main Views (see *Section 4.9*) generally display lists of objects that match a common criteria, the **Detail Views** display information about a specific selected object.

The Detail View for an object is opened by selecting a reference to the specific object, generally by clicking the **Name** link of a list entry representing the object within a Main View.

The header of a Detail View shows the type of the displayed object and an object identification (e. g. the name and IP of a Host). It also provides a link that can be used to display the Detail View in a separate tab or window.

Usually the information shown directly below is the **Status** of the selected object and the reason of its status. This information is available for all Object Types.

Further information is displayed depending on the type of the object and of the data the OpenScape FM has collected about the object.

Individual information blocks can be expanded or collapsed with tick symbols.

Actions can be performed for the object displayed in the Detail View and in some cases for objects displayed in information blocks (see *Section 4.18*).

The individual Detail Views for the various Object Types and the information displayed for each Object Type are explained in *Chapter 12*.

Links displayed within a Detail View can be used to show information about the linked object in a separate browser tab or window.

Individual areas of a Detail View can be expanded or collapsed with the help of arrow symbols located in front of their headings.

These areas usually also have an **Info Icon**, which is displayed to the right of the heading when the mouse icon is positioned on the heading. The Info Icon can be used to open a Detail View with further information.

4.16 Tables

Tables are used to display a set of objects with certain common properties in a compact way.

For example, the Main Views of Categories contain a table with all known Hosts or Networks. However, Tables also appear in Detail Views, e.g. to display all Interfaces of a Switch or all Hosts of a specific Network.

Within a Table, each row corresponds to a matching object or event. And each column corresponds to a value of the corresponding object or event. These values can be, for example, the name of the object or the number of associated events.

Columns whose contents name the object of the respective row (often the **Name** column) usually have a link that can be used to open the detail view of the corresponding object.

Columns that name the number of (unconfirmed) events for the respective row object (often the column **Events**) usually have a link that can be used to open a list of the corresponding events.

The common column **Last Event** contains a link to the last event received for the object described in the row. The field content consists of the time when the event occurred and a short description of the type of event. A round icon indicates whether the event is unconfirmed (exclamation mark) or already confirmed (confirmation checkmark). The color of the icon corresponds to the status (e.g. red = *critical* or green = *normal*) of the event. If there is a comment for the event, an additional comment icon (speech bubble) is displayed. If a correlated event exists, a correlation symbol (square) is displayed.

To the lower right of a table there are usually up to three symbols:

- The **Column Symbol** opens an input window in which the columns to be displayed in the table can be selected.
- The **Divider Symbol** resets the widths of the individual table columns to the default width.

- The **Use default filter Symbol** resets these to the default value if column filters are available (see *Section 4.16.2.2*).

Actions can be executed for the displayed objects of some tables (mainly the central tables of Categories or Technologies). These tables have an additional Checkbox column in which the objects for which the desired action is to be performed are selected (see *Section 4.18*).

If a checkbox is directly clicked, it is toggled. In this way, individual rows can be added to or removed from a selection. Clicking the row itself outside of a link selects this row and deselects all other rows.

The following sections describe how the status overview of the table entries works (see *Section 4.16.1*) and how the contents of tables can be restricted by search criteria (see *Section 4.16.2*).

4.16.1 Severity Display

The Severity Display for tables is located at the top of most tables (generally for Categories). If no filter is defined, it can be used to show the number of objects within the Category‘s list that have currently a specific Status (for Events) or Severity (for non Events).

If currently, considering the selected filters, no objects exist that have a specific Status or Severity, the respective marker will be filled with a white colored background instead of the Status/Severity specific color.

The display fields can also be used as a filter by clicking them. This will filter the list of object to those with the respective severity (see *Section 4.16.2.1*).

If a filter is active, the displayed numbers correspond to the objects that match the current filter.

4.16.2 Filter for Tables

Object tables, e.g. for Categories, can be filtered to show only a subset of the data.

Using filters limits the number of displayed objects to those matching the current filters, for example to only objects within a specific network or of a specific status.

Filters only reduce the number of *displayed* objects. If the filters are changed or removed, the display of the objects is instantly refreshed according to the new settings of the filters.

There are two filter methods provided that are common to Categories:

- Severity Filters (see *Section 4.16.2.1*) can be used to filter the displayed lists of events or objects by severity.
- Table Filters (see *Section 4.16.2.2*) can be used to filter the table content for entries that have matching column contents.

The current combination of the settings of both filter methods can be saved as a personal default filter for the current Category and the current User with the button **Save user-defined filter** located below the table.
This makes the filter combination the default setting when the user logs on again at a later time and it can also be reloaded/activated at any time using the **Use user-defined filter** button

The filter setting recommended by OpenScape FM can be activated at any time by clicking the **Use default filter** button. For events, this default setting displays all unacknowledged events, and for objects of other types it generally displays all objects.

4.16.2.1 Severity Filter

The Severity Display for Tables (see *Section 4.16.1*) can also be used as a stats filter to filter the displayed objects by severity.

The Severity Filter consists on a number of buttons, one each representing the severities **Critical**, **Major**, **Minor**, **Warning** and **Normal**, and one labeled **Other** that represents all other severities like e.g. *Unknown*.

If one of these buttons is clicked, only objects with a severity that matches the severity represented by the button will be displayed in the data list.

If the button **All** is clicked, the Severity Filter will be reset.

Below the buttons besides the **All** button a **Checkbox** is displayed.

These checkboxes show whether the respective severity is currently displayed in the list.

In addition, clicking an individual checkbox toggles the display of the respective severity.

Within a user session, the settings for the individual Categories and Technologies are preserved, even if a view will be closed at some point.

Examples:

- Only *Critical* objects should be displayed:
  Clicking the button **Critical** will achieve this.
- Only *Critical* and *Major* objects should be displayed:
  Clicking the button **Critical** displays only the *Critical* objects. If the **Checkbox below the button Major** is checked, this adds the *Major* objects to the list.
- All objects that are *not Normal* should be displayed:
  This can be achieved by clicking the button **All** (all objects are shown) and by unchecking the **Checkbox below the button Normal**, which will filter out the *Normal* objects.

4.16.2.2 Column Filter

The **Table Filters** are located at the top of object tables that are displayed within many Main Views (see *Section 4.9*). They are used to filter the data displayed within the table based on the columns content.

Table Filters consist of a number of **Column Filters** that are attached to individual table columns.

A Table Filter matches to an object within the table, if *all* Column Filters match for the object.

Depending on the data type that is displayed within a column the Column Filter may consist of a Selection Menu, a Range, a Time Range or a Text Field:

- **Selection Menus** provide a multiple choice selection. A column entry matches, if the entry *exactly* matches the selection or if the menu item *All* is selected.

  Important Note:
  Generally, Selection Menus contain, besides the entry *All*, exactly those entries that currently appear at least once in the column.

- **Ranges** search for a range of values (e.g. date intervals). A column entry matches, if its value is larger or equal to the lower boundary and lower or equal to the upper boundary.
  Only entered boundaries will be checked. If e.g. no upper boundary is entered, the value matches if it is larger or equal to the lower boundary. If no boundaries are entered, all entries match.

- **Time Ranges**: Clicking the Clock Symbol opens the *Time Range Configuration Window*:

  On the **From-To** page a start time (**From**) and end time (**To**) can be specified by selecting the respective day and time. Empty fields stand for an open interval at the beginning or end.
  A start or end can be deleted with the **X** in the respective line. If both lines are deleted, all entries match.

  Alternatively, on the **Time period until now** page, a period of time in the past up to the current time can be specified (e.g. the last 5 hours).
  If the value is set to `0` (set to `1` and click on **Minus** (**-**)), all entries match.
  With the **X** at the end of the line the interval can be deleted.

- **Text Fields** search for the appearance of the entered string as a sub string within the column entry. The search for the sub string is case insensitive. If no string is entered, all entries match.
  Important Note: If string values are expected for a column, leading and trailing space characters (space, tabulator, etc.) are not taken into account for the filter input for the respective column.

There are no Column Filters for columns displaying the object status since the status is filtered by using the Severity Filters (see *Section 4.16.2.1*).

All column filters of a table can be reset to their default setting by clicking the **Use default filter Symbol** at the lower right of the table.

4.17 Full Text Search

The **Full Text Search** can be used to find specific objects by searching for a substring that is a part of any of the object‘s search indexed parameters.

The entry field labeled **Search** is generally located within the Header Bar left of the User Menu.

The search is *not* case sensitive and wildcards are *not* supported. Asterisks (`*`), interrogation marks (`?`) and dots (.) are therefore interpreted as the actual ASCII character and not as a place holder.

The search checks for matching objects of the types *Host*, *Host Container*, *Network*, *Event*, *Service*, *OpenScape Voice Cluster* and *System Management Parameters*.

Among the indexed search parameters are the *Labels* of the respective objects, the *Host Address* and the *Fully Qualified Host Name* of Hosts, the *Description* and *Source* of Events, Annotations and Comments.

The result of a Full Text Search is a Main View that contains a table with all matching objects.

4.18 Actions

For objects displayed in Main or Detail Views, actions can be performed.

Examples for such actions are the acknowledgement or deletion of events.

Actions are usually displayed in an **Action List** on the right side of the current view.

Each entry of the Action List represents a specific action.

Main Views

If actions can be performed on objects represented as table entries in Main Views (see *Section 4.9*), the respective table contains a separate **Checkbox Column**, and an **Action List** that is displayed to the right of the table.

Individual checkboxes can be checked or unchecked by clicking the respective checkbox.

Clicking the checkbox within the header of the Checkbox Column checks or unchecks all table rows.

If an Action is selected within a Main View, its Action will be performed on all objects within the displayed table for which the checkbox is currently checked.

The Actions that can be performed for the objects displayed within the various Categories are described beginning with *Chapter 7*.

Detail Views

If actions can be performed within a Detail View (see *Section 4.15*), the corresponding **Action List** can be found on the right side of the Detail View. With the green arrow besides the headline Actions the Action List can be hidden or shown.

In some Detail Views, individual blocks of information can be shown or hidden with tick symbols. If such a block contains a list, and if actions are offered for the elements of this list, then these actions are displayed below the general Actions List in another list when the block is opened. The additional list has the name of the opened information block as its heading.

If a general action is selected in a Detail View, the action is executed on the object for which the Detail View is displayed. If an action is selected that refers to an expanded list, it is executed for all objects marked in the corresponding list.

Actions that are possible within Detail Views for specific object types are described in *Chapter 12*.

4.19 Configuration Views

Configuration Views are modal windows that are used to configure new objects or to modify the configuration of existing objects.

If a configuration is triggered by a **New** or **Modify** action, such a window opens.

As long as a Configuration View is open, the rest of the Web Client is locked for input.

Configuration Views exist for Hosts (see *Section 13.1*) and Reports (see *Section 13.4*).

5 Navigation

This chapter describes the general methods and concepts that can be used to navigate through the data provided by the OpenScape FM Web.

Compared to OpenScape FM V10, the navigation has been fundamentally revised and adapted to the familiar way of navigating between web pages using an Internet browser.

Main Views

Main Views (see *Section 4.9*) are displayed via the individual entries in the Navigation Panel (see *Section 4.8*) on the left. Clicking with the left mouse button opens the desired Main View in the current browser window.

In addition, the Main View entries behave like normal browser links. They can also be opened with the right mouse button in a new window or tab, or with the middle mouse button in a new tab..

Detail Views

Detail Views (see *Section 4.15*) are usually opened by using normal browser links. They are displayed as green text and can be opened with browser functions either in the current view or in a new window or tab.

Detail Views contain a header that contains the current object type and object name. This heading is also a link.

Configuration Views

Configuration Views (see *Section 4.19*) allow the user to enter data. They are used, for example, to configure objects or define reports.

Usually these are opened for objects selected in a list or a Topology View (see *Section 10.1*).

They are modal windows that have to be closed before navigation can be continued.

Changing the Display Size of Views

Elements of individual views (e.g. the individual areas in dashboards) can be enlarged. To do this, the **Enlarge** button located on the right within the header of the respective element must be clicked.

Classic Navigation

The Web Client offers the possibility to navigate the Object Tree as in the Classic Client. This is supported both in the Submap View (see *Section 10.1*) and in the Tree View (see *Section 10.2*).

6 Dashboards

This chapter contains descriptions of the **Dashboards** provided by the OpenScape FM Web that can be directly opened from the Navigation Panel (see *Section 4.8*). They are listed under the label **Dashboards**.

Dashboards contain theme specific collections of information. The general handling of Dashboards is described in *Section 4.10*.

The Dashboard **Overview** shows a listing of currently problematic Events and Hosts (see *Section 6.1*).

The other Dashboards provide a statistical overview about problems of the last 30 days and about current problems for objects of the types:

- **Events** (see *Section 6.2*)
- System Management Monitoring Parameters (**Monitoring -** see *Section 6.3*)
- **Hosts** (see *Section 6.4*)
- **OpenScape Voice** Hosts (see *Section 6.5*)
- **OpenScape 4000** Hosts (see *Section 6.6*)
- **OpenScape Business** Hosts (see *Section 6.7*)

It is also possible for a User to create **individual Dashboards** (see Section 6.8).

6.1 Dashboard - Overview

The Dashboard **Overview** can be used as a permanently displayed Main View that may indicate important and current problems. These indications are provided by two lists that show active Events and currently non normal Hosts.

This page will also be opened when the logo located left within the Header Bar is clicked.

- The table **Unacknowledged Events** contains all Events that:
  - are currently unacknowledged
  - that not appeared during a Maintenance phase of the related object
  - would be shown in a Correlated View (see *Section 7.1*)
  - have the Severity *Critical*, *Major*, *Minor* or *Warning*
  - are accessible by the current user (Operator rights for the corresponding Source Object are needed)

  These conditions are met by Events that are allowed to be seen by the current user, that indicate a non normal state for an object not in Maintenance and that have not already been handled or identified as solved.

  The column **Source** provides a link from which a Detail View for the object the Event is assigned to can be opened.

The column **Description** provides a link from which a Detail View for the respective Event can be opened (see *Section 12.2*).

- The table **Hosts** contains all Hosts:
  - that have the Status *Critical*, *Major*, *Minor* or *Warning*
  - are accessible by the current user (User rights for the corresponding object are needed)

  The column **Name** provides a link from which a Detail View for the respective Host can be opened (see *Section 12.4*).

  The column **Events** contains a link which displays the unacknowledged Events of the selected Host.

By default the tables are sorted by *Severity* (in order *Critical*, *Major*, *Minor*, *Warning*) and within a Severity by *Date*. Therefore the last critical Event or the last Host that turned critical would always be on top of the respective list.

Above both lists are Severity/Status indicators that show how many objects of the respective Severity/Status are currently displayed within the respective list.

6.2 Dashboard - Events

The Dashboard Events shows some statistics over the last 30 days and an overview about the current events within the OpenScape FM.

- The pie chart **Unacknowledged Uncorrelated Event Status Distribution** shows the distribution of the unacknowledged events within the OpenScape FM.
- The bar chart **Unacknowledged Uncorrelated Events Over Time** visualizes the distribution of all events within the OpenScape FM over time.
- The table **Hosts With Most Critical Unacknowledged Uncorrelated Events** lists the ten Hosts with the most unacknowledged '*Critical*' events.
- The table **Hosts With Most Unacknowledged Uncorrelated Events** lists the ten Hosts with the most unacknowledged events.
- The table **Non Normal Events** contains the ten recent events that have a worse status than '*Normal*'.

6.3 Dashboard - Monitoring

The Dashboard **Monitoring** provides an overview about possible current problems concerning objects monitored by the System Management plugin.

It shows general critical System Management Parameters and the worst hosts considering a number of basic monitoring parameters (monitored by the profile „Basic Monitoring"). In detail the following data is provided:

- The table **Recent Critical Parameters** shows the last ten System Management Parameters that changed to the status '*critical*' and that are still in that status.

- The table **Top CPU Usage** lists those Hosts that are monitored by the Basic Monitoring and that have the highest CPU usage.
- The table **Top Filesystem Usage** lists those Hosts that are monitored by the Basic Monitoring and that have the highest file system usage.
- The table **Top Memory Usage** lists those Hosts that are monitored by the Basic Monitoring and that have the highest memory usage.
- The table **Top Network In Usage** lists those Hosts that are monitored by the Basic Monitoring and that have the highest incoming network usage.
- The table **Top Network Out Usage** lists those Hosts that are monitored by the Basic Monitoring and that have the highest outgoing network usage.

Important Note:
The Monitoring Dashboard is only available within the Navigation Panel, if the System Management plugin has been initialized in the OpenScape FM Server.

6.4 Dashboard - Hosts

The Dashboard **Hosts** provides an overview about possible current problems concerning hosts (IP nodes) and some event statistics over the last 30 days.

- The bar chart **IP Events Of Category „IP Manager“ Over Time** shows the distribution of events within category '*IP Manager*' by time.
- The table **IP Hosts Gone Critical** lists the last ten IP Nodes that changed to the status '*Critical*' and that are still in that status.

  The column **System** provides a link from which a Detail View for the respective Host can be opened (see *Section 12.4*).
- The table **IP Interfaces Gone Critical** provides the last ten IP Interfaces that changed to the status '*Critical*' and that are still in that status.

  The column **System** provides a link from which a Detail View for the respective Interface can be opened (see *Section 12.5*).
- The table **Non-normal Routers** lists the last ten Routers that changed to a status worse than '*Normal*' and that are still in that status.

  The column **System** provides a link from which a Detail View for the respective Host can be opened (see *Section 12.4*).
- The table **Non-normal Switches** contains the last ten Switches that changed to a status worse than '*Normal*' and that are still in that status.

  The column **System** provides a link from which a Detail View for the respective Host can be opened (see *Section 12.4*).

Important Note:
The Hosts Dashboard is only available within the Navigation Panel, if the IP Manager plugin has been initialized in the OpenScape FM Server.

6.5 Dashboard - OpenScape Voice

The Dashboard **OpenScape Voice** provides an overview about possible current problems concerning OpenScape Voice systems and some event statistics over the last 30 days.

- The pie chart **Event Status Distribution** shows the distribution of the unacknowledged events within category '*OpenScape Voice*' by status.
- The bar chart **Events Over Time** visualizes the distribution of events within category '*OpenScape Voice*' by time.
- The table **Hosts Gone Critical** provides the last ten OpenScape Voice Hosts that changed to the status '*Critical*' and that are still in that status.
- The table **Hosts With Most Unacknowledged Events** lists the ten OpenScape Voice Hosts with the most unacknowledged events.
- The table **Non Normal Events** contains the ten recent events from category '*OpenScape Voice*' that have a worse status than '*Normal*'.

Important Note:
The OpenScape Voice Dashboard is only available within the Navigation Panel, if the OpenScape Voice plugin has been initialized in the OpenScape FM Server.

6.6 Dashboard - OpenScape 4000

The Dashboard **OpenScape 4000** provides an overview about possible current problems concerning OpenScape 4000 and HiPath 4000 systems and some event statistics over the last 30 days.

- The pie chart **OpenScape 4000 Event Status-Distribution** shows the distribution of the unacknowledged events of the last 30 days for 'OpenScape 4000 systems by status.
- The bar chart **OpenScape 4000 Events Over Time** visualizes the distribution of events of the last 30 days for OpenScape 4000 systems by time.
- The table **Latest OpenScape 4000 Systems Gone Critical** provides the last ten HiPath/OpenScape 4000 systems that changed to the status '*Critical*' and that are still in that status.
- The table **OpenScape 4000 Systems With Most Unacknowledged Events** lists the ten HiPath/OpenScape 4000 systems with the most unacknowledged events.
- The table **Last Non Normal OpenScape 4000 Events** contains the ten recent events from category 'OpenScape 4000' that have a worse status than '*Normal*'.

Important Note:
The OpenScape 4000 Dashboard is only available within the Navigation Panel, if the OpenScape 4000 plugin has been initialized in the OpenScape FM Server.

6.7 Dashboard - OpenScape Business

The Dashboard **OpenScape Business** provides an overview about possible current problems concerning OpenScape Business and HiPath 3000 systems and some event statistics over the last 30 days.

- The pie chart **OpenScape Business Event Status Distribution** shows the distribution of the unacknowledged events of the last 30 days for OpenScape Business/H3K systems by status.
- The bar chart **OpenScape Business Events Over Time** visualizes the distribution of events of the last 30 days for OpenScape Business/H3K systems by time.
- The table **Recent OpenScape Business Systems Gone Critical** provides the last ten OpenScape Business/H3K systems that changed to the status '*Critical*' and that are still in that status.
- The table **OpenScape Business Systems With Most Unacknowledged Events** lists the ten OpenScape Business/H3K systems with the most unacknowledged events.
- The table **Last 10 Non Normal OpenScape Business Events** contains the ten most recent events from category 'OpenScape Business/H3K' that have a status worse than '*Normal*'.

Important Note:
The OpenScape Business Dashboard is only available within the Navigation Panel, if the OpenScape Business/H3K plugin has been initialized in the OpenScape FM Server.

6.8 Individual Dashboards

In addition to the predefined Dashboards described in the previous sections, Individual Dashboards can also be created.

In these, various display elements can be freely combined and arranged in order to provide the desired overviews for special tasks.

The individually created Dashboards are displayed in the Navigation Panel (see *Section 4.8*) below the default Dashboards and are visually distinguished by a **Wrench Symbol** behind their name.

A click on the name opens the respective Dashboard as usual. A click on the Wrench Symbol opens the **Dashboard Layout View** in which the respective Dashboard can be configured.

Configuration

The configuration of a Dashboard consists essentially of three tasks:

- The Dashboard itself has to be created and managed (see *Section 6.8.1*).
- The individual components have to be arranged within the Dashboard (see *Section 6.8.2*).

- The content of the individual components has to be defined (see *Section 6.8.3*).

6.8.1 Managing Dashboards

Dashboards can be created and edited by any User.

Each User can only see, modify or delete the Dashboards he created himself.

Create Dashboards

The creation of a new Dashboard is initiated within the Navigation Panel by clicking on the **+** symbol behind the heading **Dashboards**.

This opens the **Dashboard Layout View**. Within the top area of this view a **Dashboard Name** can be assigned. The new Dashboard can then be created by pressing the **Save** button.

Modify Dashboards

A Dashboard can be modified using the **Dashboard Layout View**. This view is opened automatically when a new Dashboard is created.

For existing Dashboards, the view is opened by clicking the **Wrench Symbol** behind the name of the desired Dashboard within the Navigation Panel.

The modification consists of the arrangement of the individual elements (see *Section 6.8.2*) and the configuration of the content of these (see *Section 6.8.3*).

Delete Dashboards

A Dashboard can be deleted by using the button **Delete** within its **Dashboard Layout View**.

6.8.2 Arranging Dashboard Widgets

If a new Dashboard is created or an existing Dashboard is modified (see *Section 6.8.1*), the **Dashboard Layout View** opens, which is the basis to configure Dashboards.

If no elements to be displayed, so-called **Widgets**, have been defined yet for the Dashboard, the Dashboard Layout View consists of a grid of squares, each containing a **+** symbol.

These squares represent a respective area within the Dashboards. They are used to arrange the individual Widgets.

Each of the squares has coordinates assigned. The square in the upper left corner has the coordinates (`X=1,Y=1`). The X value grows to the right, the Y value grows downwards.

Create and Position Widgets

Each Widget can occupy a rectangular area of squares. As its coordinates (its **X** and **Y** value) it has the coordinates of the square in its left upper corner. In addition it has the **Width** and the **Height** that corresponds to the respective number of squares.

If a **+** Symbol gets clicked, a new Widget will be assigned to this square. The Widget has therefore initially the coordinates of the clicked square and as its width and height the value `1`.

When creating a new page, the **Widget Configuration Window** opens automatically, which among other things allows changing the position, width and height on the page **General**. More about the configuration of the Widget‘s content can be found in *Section 6.8.3*.

If a Widget has been created, it will be displayed within the *Dashboard Layout View* at the defined position. Its position can now moved by dragging its representation within the *Dashboard Layout View*. Its width and height by dragging its edges or corners.

Delete Widgets

A Widget can be removed from the Dashboard in the Dashboard Layout View by clicking the Trash Can Symbol in the upper left corner of the Widget that should be deleted.

6.8.3 Configure Dashboard Widgets

For the configuration of the Widgets and hereby of the Dashboard content the **Widget Configuration Window** is used.

This window will be automatically opened when a new Widget is created. In addition it can be opened from within the **Dashboard Layout View** by clicking on the **Wrench Symbol** located in the middle of the Widget that should be configured.

The Widget Configuration Window always consists of two pages:

Page ‚General‘

The page **General** has the same structure for all Widgets.

Besides the positioning of the Widget within the Dashboard (see *Section 6.8.2*), here the **Name** of the Widget can be entered. This will be used as the header of the Widget. The size of this header can be selected within the field **Font Zoom**.

The lower part of the page shows an example look based on the current configuration.

Within the selection menu **Widget** the type of the Widget and therefore the form of representation will be defined. The configuration of the content itself will be handled on the page **Configuration**.

Page ‚Configuration‘

The page **Configuration** is used to select the information to be displayed in the widget.

Depending on the type of widget selected on the page *General*, the selection of the displayed information is usually done by selecting elements from a list of possible data sources, and/or by configuring filters to limit the displayed information.

Objects that are currently not *managed*, are not shown in selection lists.

Some widget types display data of a single parameter (e.g. as a graph or single value). Usually, these types provide an **i Icon** (an `i` in a circle) in the upper right corner of the widget. This icon is a link to the Detail View of the corresponding object (e.g. Parameter or Host.

The basic Widget Types are:

- **Table**: (e.g.: *Object Table*, *Event Table*)
  A tabular listing of OpenScape FM objects, in which each table row corresponds to an object. The current number of table entries is shown in the header of the Widget.
  The column **Name** contains links to the Detail Views of the respective objects.

  The configuration consists of three pages. On these the object properties (**Search Parameters**), the starting points of the search (**Start Objects of Search**) and the sorting/size of the result list (**Result View**) are defined.

  If no starting point is defined, the *Network Topology* Container will be used.

- **Fixed Table**: (e.g. *Fixed Object Table*)
  Corresponds essentially to the type *Table* (see above). However, the table content is not determined dynamically via a filter at runtime, but the objects it contains are fixed when the Widget is created.

  The configuration consists of a table in which the desired objects can be selected. In addition, the order of the displayed objects can be determined.

- **Graph**: (e.g. *Graph*, *Host Availability Graph*)
  A curve representing a value list. Usually the return values of a monitoring parameter.

  The configuration consists of a table in which the desired value source can be selected.

- **Status History**:
  A special case of the type *Graph*, which shows the status progression (*Normal* to *Critical*) of an object in the displayed curve.

  The configuration consists of a page where the desired object can be selected.

- **Status**, **Status Explanation**:
  A box that displays the current status of a selected object as a value, or the reason for the current status.

  The configuration consists of a object search dialog. By using the filter settings a specific object type (e.g. `IP`, `Host`) can be preselected, and then a specific object can be selected within the displayed list.

- **Counter**: (e.g. *Object Counter*, *Event Counter*)
  A box that displays the number of found objects as a value.

  The configuration consists of two pages. On these the object properties and the starting points of the search are defined.

- **String**: (e.g: *System Management Parameter*)
  A box that displays the return value of a query as text. The color of the text corresponds to the status of the monitored object.

  The configuration consists of a table in which the desired value source can be selected.

- **Percentage Value**: (e.g.: *CPU Usage*, *File System Usage*)
  A display that shows a percentage value visually and as a number.

  The configuration consists of a table in which the desired value source can be selected.

- **Textual Information**: (e.g.: *Host Availability Information*, *Status Explanation*)
  A window that displays an information text.

  The configuration consists of a table in which the desired value source can be selected.

- **Quick-Access**:
  An area which contains links to open defined web pages.

  The configuration consists of a list of web pages in the area **Quick**. Here new pages can be defined (**+**) or existing ones can be edited or deleted (**Tool Symbol**).

  For each web page a display string (**Label**) and the URL of the web page to be accessed via the display string (**Link**) are defined.

- **Topology**:
  An area which contains the submap of an selected object.

  The configuration consists of a object search dialog. By using the filter settings a specific object type (e.g. `IP`, `Host`) can be preselected, and then a specific object can be selected within the displayed list.

  The submap of the selected object will then be displayed in the widget.

  In the base settings (`Base`, `All`) the containers *System Management* and *Network Topology* are always provided.

- **Clock**: (e.g.: *Clock*)
  A window that displays the current date and time.

  The configuration consists of a selection menu in which the **Time Zone** that should be displayed can be chosen.

7 Categories

This chapter contains descriptions of the basic **Categories** provided by the OpenScape FM Web that can be directly opened from the Navigation Panel (see *Section 4.8*). They are listed under the label **Categories**.

Categories contain information about OpenScape FM Objects of a specific type (like Hosts).The general handling of Categories is described in *Section 4.11*.

7.1 Category - Events

The Category **Events** displays all events of the OpenScape FM for which the current user has the right to see them.

Each row within the Main View‘s table represents one individual event. Within the columns of the table for example the **Date** of the appearance, the **Severity**, the **Category** and the Acknowledg**e**ment state (**Info**) of the event are shown.

The column **Source** provides a link from which a Detail View for the object to which the Event is assigned can be opened.

The column **In Progress** displays, whether the attribute *In Progress* is assigned to the Event. In this case the ID of the User that has set the Event *In Progress* is displayed. Else no value is shown.

The column **Description** contains a link, that opens the Detail View of the Event itself.

If the checkbox **Correlated View**, located at the right of the Severity Filters (see *Section 4.16.2.1*) is checked, only the event that appeared last within each group of correlated events is displayed. If this is unchecked, all events will be displayed.

More about (Correlated) Events can be found in Section *Event Browser* within the separate User Guide for the *OpenScape FM Desktop*.

The Detail View for objects of the type Event is described in *Section 12.2*.

Actions

Important Note:
In Correlated View, all events correlated to the selected events are also effected by a selected Action.

- **Acknowledge**: This action sets the state of the selected Events to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Unacknowledge**: This action sets the state of the selected Events to *Unacknowledged*. They appear as currently untreated and, dependent on their Severity, may reappear within the Dashboard *Overview* (see *Section 6.1*).
- **In Progress**: Sets the *In Progress* attribute for the selected Events to the current User.
- **Not in Progress**: Removes the *In Progress* attribute from the selected Events.

- **Delete**: This action deletes the selected Events and the objects representing the Event within the OpenScape FM. Even within the OpenScape FMhis action *cannot be reverted*.
- **Submap**: This action opens the Topology View (see *Section 10.1*) of the submap of the object to which the Event has been assigned.
  This action is only displayed if at least one child object exists for the object.
- **Event Filter**: This action opens a window that lists all configured automatic actions for incoming events. This particularly includes the Ignore actions, which can be used to automatically suppress similar future events. Such actions can also be activated from within the Web Client (see *Section 12.2*).

  The table displayed in the window contains a defined automatic event action per row. The table columns contain the following entries:

  - The first three columns specify the conditions that an incoming event must fulfill in order for the configured action to be executed automatically. **Event Type** indicates the type of event, **Filter** indicates the object to which the event has to be assigned (or `Any` for all objects), and **Time Schedule** indicates a defined time interval within which the event must occur (or `Any` for any point in time).
  - **Actions**: This column displays the name of the action that is executed for matching events. Using the **Delete** button deletes respective Event Filter definition.

  The description of the configuration of general event actions is provided in the *OpenScape FM Desktop User Guide* in *Chapter 8 - Event Actions*.

7.2 Category - Hosts

The Category **Hosts** displays all Hosts that are known by the OpenScape FM that would be accessible for the current user.

Each row within the Main View‘s table represents one individual Host. Within the columns of the table for example the **Status** of the Host, its **Name** and **IP Address** and the date of the last **Status Change** are shown.

The column **Last Event** contains a link to the corresponding event. There may be icons in front of the link.
The **color** of an icon indicates the status of the event,
an **exclamation mark** that the event is unacknowledged,
a **check mark** that the event is acknowledged,
a **speech bubble** that a comment is assigned to the event
and a **square** that at least one correlated event exists.

More about Hosts can be found in the separate User Guide for the *OpenScape FM IP Manager*.

The Detail View for objects of the type Host is described in *Section 12.4*.

Actions

- **Acknowledge**: This action sets the state of all Events of the selected Hosts to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Events**: This action displays a list that contains all Events of the selected Hosts.

- **Delete**: This action deletes the selected Hosts and the objects representing the Hosts within the OpenScape FM. Even within the OpenScape FMhis action *cannot be reverted*. However, events assigned to the deleted objects are maintained.
- **Manage**: This action sets *Unmanaged* Hosts to *Managed*.
- **Unmanage**: This action sets the selected Hosts to *Unmanaged*. Unmanaged Hosts are ignored by the monitoring. For example no status or configuration requests or discoveries will be performed for the respective Hosts and Events from unmanaged Hosts will not be displayed.
- **Report**: This action opens a Report Configuration View (see *Section 13.4*) to create a new Report. The selected Hosts are pre selected for the new Report.
- **New**: This action opens the Configuration View to create a new IP node within the OpenScape FM (see *Section 13.1*).
- **Edit**: This action opens the Configuration View for the selected IP nodes to modify its configuration (see *Section 13.1*).
- **Start Discovery**: This action performs a check for new child components, such as a new HTTP server. The components found are displayed in a table.
- **Configuration Poll**: This action triggers the child components of selected IP nodes to refresh their configuration data.
- **Check Availability**: This action performs a Status Poll for the selected Hosts. A Status Poll checks, if the IP Node assigned to the Host is responding to status request (ICMP/TCP/SNMP ping). If this is the case, the child components will be triggered to refresh their state and as a result the state of the Host.
- **Submap**: This action opens the Topology View (see *Section 10.1*) of the selected object‘s submap. This action is only displayed if at least one child object exists for the object.

7.3 Category - Host Types

The Host discovery can recognize the type of a host by scanning specific properties (e.g. the existence of a particular SNMP MIB). All discovered types (e.g. Switch, Router, OpenScape Business) are listed under **Host Types**. By using a link within the column **Name**, all hosts of that particular type are shown. A host can have multiple types assigned.

Actions

- **Acknowledge**: This action sets the state of all Events of *all* Hosts of the selected Types to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Events**: This action displays a list that contains the Events of all Hosts of the selected Types. This action can also be triggered by using the link within the column **Events**.
- **Report**: This action opens a Report Configuration View (see *Section 13.4*) to create a new Report. The Hosts of the selected Types are pre selected for the new Report.

Important Note:
If a Report Template is created for selected Host Types (see *Section 13.4.3*), this template does not contain the Host Types, but a list of the hosts applicable at creation time.
Hosts of the corresponding types that are added or removed later are not automatically added to tor removed from he template. Instead, the template must be redone if necessary.

- **Submap**: This action opens the Topology View (see *Section 10.1*) of a submap that contains the objects of the selected type.
  This action is only displayed if at least one child object exists for the object.

7.4 Category - Host Containers

The Category **Host Containers** shows a list of all Host Containers that are known by the OpenScape FM.

Host Containers are Virtual, Object or Topology Container, that are located within the container `Root->Network Topology` of the OpenScape FM Navigation Tree that contain at least one Host.

Such containers may have been manually generated by a user or they can be automatically created by discoveries. For example a Host Container may contain all Hosts that are of a specific technology like OpenScape 4000 or OpenScape Voice Assistants.

Each row within the Main View‘s table represents one Host Container. Within the columns of the table for example the **Status** of the Host Container and its **Name** are shown.

The **Status** of a Host Container is equivalent to the worst Status of the Hosts within the Host Container that are visible to the current user.

The column **Path** shows the location of the Host Container within the object tree of the OpenScape FM. The location is described in relation to the `Network Topology` container.

The column **Status Distribution** shows the relative distribution of the Status of the Hosts that belong to the Container. The number of the Hosts contained in the Container is shown in column **Hosts**.

By using the link within the column **Name** the Detail View of a Host Container can be opened. The Detail View for objects of the type Host Container is described in *Section 12.6*.

Actions

- **Acknowledge**: This action sets the state of all Events of *all* Hosts of the selected Containers to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Events**: This action displays a list that contains the Events of all Hosts of the selected Containers. This action can also be activated by using the respective link within the column **Events**.
- **Report**: This action opens a Report Configuration View (see *Section 13.4*) to create a new Report. The Hosts of the selected Containers are pre selected for the new Report.
- **Submap**: This action opens the Submap of the selected Host Container.
- **Delete**: Deletes the selected Host Containers. Some default container cannot be deleted.

7.5 Category - Networks

The Category **Networks** shows a list of all IP Networks that are known by the OpenScape FM.

Each row within the table of the Main View represents one individual Network. Within the columns of the table for example the **Status** of the Network, its **Network Name**, **Network Address** and **Network Mask** are shown.

The **Status** of a Network is equivalent to the worst Status of the Hosts belonging to the Network that are visible to the current user.

The column **Status Distribution** shows the relative distribution of the Status of the Hosts that belong to the Network. The actual number of the Hosts contained in the Network is shown in column **Hosts**.

The Detail View for objects of the type Network is described in *Section 12.7*.

Actions

- **New**: This action opens the Configuration View to create a new Network within the OpenScape FM (see *Section 13.2*).
- **Modify**: This action opens the Configuration View for the selected Network to modify its configuration (see *Section 13.2*).
- **Acknowledge**: This action sets the state of all Events of *all* Hosts of the selected Networks to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Delete**: This action deletes the selected Networks and all Hosts contained in these Networks that are not contained in at least one other Network.
- **Events**: This action displays a list that contains the Events of all Hosts of the selected Networks.
- **Report**: This action opens a Report Configuration View (see *Section 13.4*) to create a new Report. The Hosts of the selected Networks are pre selected for the new Report.
- **Manage** or **Unmanage**: This action sets the selected Networks and all Hosts contained in these to the state *Managed* or *Unmanaged*.
- **Discovered IP Addresses**: If IP nodes have been detected for a selected network but not created as individual objects in the OpenScape FM (see *Section 13.2.2*), the corresponding hosts can be displayed using this action. The action opens a window in which the corresponding hosts, their name and the method of their discovery are displayed in a list. By clicking the **Add Node** button a host selected in the list can be added to the OpenScape FM monitoring.
- **Submap**: This action opens the Topology View (see *Section 10.1*) of a submap that contains the objects of the selected type.
  This action is only displayed if at least one child object exists for the object.

7.6 Category - Cluster

The Category **Cluster** shows a list of all Clusters that are known by the OpenScape FM (see *IP Manager User Guide*).

Each row within the table of the Main View represents one individual Cluster. Within the columns of the table for example the **Status** of the **Cluster**, its **Name**, the **Host Status Distribution**, the number of **Events** and the number of enclosed **Hosts** are shown.

The **Status** of a Cluster is equivalent to the worst Status of the Hosts belonging to the Cluster that are visible to the current user.

Actions

- **Acknowledge**: This action sets the state of all Events of *all* Hosts of the selected Clusters to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Delete**: This action deletes the selected Cluster.
- **Events**: This action displays a list that contains the Events of all Hosts of the selected Clusters.
- **Submap**: This action opens the Topology View (see *Section 10.1*) of the submap that contains the selected Cluster.
  This action is only displayed if at least one child object exists for the object.

7.7 Category - Services

The Category **Services** shows the Services that are currently defined within the Service Impact Management of the Event Correlation Engine.

Each line within the displayed table represents one of these Services.

The column **Name** contains the name of the Service and the availability that has been calculated for the Service.

The column **Status** represents the status that has been calculated for the Service based on the availability.

The column **Events** shows the number of unacknowledged events for the Service.

The Detail View for objects of the type Service is described in *Section 12.8*.

More about the displayed Services can be found in Chapter *Service Impact Management* within the separate User Guide for the *OpenScape FM Event Correlation Engine*.

Actions

- **New**: This action initiates the creation of a new Service (see *Section 13.6.1*).
- **Edit**: This action opens the configuration window for the selected Service (see *Section 13.6.2*).
- **Acknowledge**: This action sets the state of all Events of *all* Hosts of the selected Services to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Delete**: This action deletes the selected Service.
- **Events**: This action displays a list that contains the Events of all Hosts of the selected Services.
- **Manage** or **Unmanage**: This action sets all selected Services to the state *Managed* or *Unmanaged*.

- **Dependencies**: This action opens the Dependency View of the Service. This View shows, how the Availabilty Value of the Service is calculated, which objects are part of the calculation, and the current availability values for the elements contained in the Service.

Categories

Category - Services

8 Reporting

This chapter contains descriptions of the Main Views related to the **Reporting** of selected data. They are listed under the label **Reporting**

The functions are divided into the generation of **Reports** (see *Section 8.1*) and the creation of **Templates** for Reports (see *Section 8.2*).

8.1 Reporting - Reports

The Category **Reports** shows the created Reports that are accessible by the current user. These are either Reports created by the user itself or Reports that were defined as *Public*. Reports of the formats PDF, JRPRINT or CSV can be shown by this Category.

Each line within the displayed table represents one of these Reports.

The columns display information like the **Name** of the Report, its **Creation Date** or whether it is **Public**.

The column **Status** represents the creation status of the Report.

The Detail View for Reports is described in *Section 12.9*, the configuration of Reports in *Section 13.4*.

Actions

- **New**: This action opens the Configuration View *Report* to create a report or template (see *Section 13.4.1*).
- **Delete**: This action deletes the selected Reports from the OpenScape FM Server. They will be no longer available for *any user*.
- **Download**: If only one Report is selected, it is downloaded from the OpenScape FM server to the local computer. If several Reports are selected, they are transferred together in a ZIP archive.
- **Show**: This action is only available if only a single Report is selected. It displays the selected Report in a preview window or saves the Report to the local machine.

8.2 Reporting - Templates

The category **Templates** displays the Report Templates that are accessible by the current user.

Report Templates are stored Report configurations.

Actions

- **New**: This action opens the Configuration View *Report Template* to create a report or template (see *Section 13.4.3*).
- **Modify**: This action opens the configuration window (see *Section 13.4*) for the selected Template. In this window the current Template can be edited. The window also serves to execute the Template.

- **Delete**: This action deletes the selected Templates from the OpenScape FM Server. They will be no longer available for *any user*.
- **Generate**: This action is only available if only a single Template is selected. It creates a Report based on the selected Template. The result can be viewed in the Report list (see *Section 8.1*).

  Depending on the output type selected for the Template (see *Section 13.4.1 - File and Forward*), the result will be displayed on the **Reports** page (see *Section 8.1*), and/or an email will be sent to the configured recipient.

9 Technologies

This chapter contains descriptions of the OpenScape specific Technologies provided by the OpenScape FM Web that can be directly opened from the Navigation Panel (see *Section 4.8*). They are listed under the label **Technologies**.

The general handling of OpenScape Technologies corresponds to the handling of Categories described in *Section 4.11*.

The currently supported Technologies are **OpenScape Voice** (see *Section 9.1*), **OpenScape 4000** (see *Section 9.2*) and **OpenScape Business** (see *Section 9.3*).

9.1 Technology - OpenScape Voice

The Technology **OpenScape Voice** shows the objects created by the OpenScape FM that relate to OpenScape Voice elements like OpenScape Branches, OpenScape Session Border Controllers (SBC), OpenScape Voice Switches, Branches, Border Controllers, Assistants or Endpoints.

This corresponds to the objects located within the `Root->Network Topology->OpenScape Voice` container of the OpenScape FM Navigation Tree.

The topology is represented by a tree table in which each row represents one OpenScape FM object.

The column **Name** shows the respective object labels and the triangle symbols can be used to show/hide the objects that are located on the submap of the current object.

The column **Last Event** contains a link to the corresponding event. The link may be preceded by the icons listed in *Section 7.2*.

The column **Cluster** contains a link to the Detail View of the OpenScape Voice Clusters (see *Section 12.14*).

More about the topology tree can be found in Section *OpenScape Voice Network Topology* of the *OpenScape Voice User Guide.*

Important Note:
The OpenScape Voice Technology is only available within the Navigation Panel, if the respective plugin has been initialized in the OpenScape FM Server.

The provided **Actions** consist of the general Host Actions (see *Section 7.2*).

Using the Action **New** creates a new Host using the general Host Configuration (see *Section 13.1*) but, depending on a selection, with an *OpenScape Voice*, *OpenScape Branch* or *SBC* Container added by default.

9.2 Technology - OpenScape 4000

The entry point to the **OpenScape 4000** technology can be found below the grouping **Technologies**. It shows a list of all discovered devices in an OpenScape 4000 environment, including switches, managers, APs, systems, frames etc. The list looks similar to the *Host* view under *Categrories*, but it includes additional, OpenScape 4000 specific information like System ID (Mnemonic), PBX-Id, Location or the last Alarm.

Each row within the list represents one OpenScape 4000 object. Clicking the Link within the column **Name** opens the Detail View of the Host object of the selected device/system. Selecting the Link within the column **Manager** opens the Detail View of the respective OpenScape 4000 Manager object. These Detail Views provide access to all available information about the related systems.

The column **Last Event** contains a link to the corresponding event. The link may be preceded by the icons listed in *Section 7.2*.

Important Note:
When the OpenScape 4000 Technology is added to a node, the matching SNMP-Agent Port is also added (and automatically deleted when technology is removed from the node).

Actions

Besides the general Actions for Hosts (see *Section 7.2*) Actions which give access to important OpenScape 4000 specific data.and functions on the selected devices are provided. For example, data about systems, faults and errors is available and AMO discoveries can be started.

Important Note:
The OpenScape 4000 Technology is only available within the Navigation Panel, if the respective plugin has been initialized in the OpenScape FM Server.

Using the Action **New** creates a new Host using the general Host Configuration (see *Section 13.1*) but with the *OpenScape 4000* Container added by default.

9.3 Technology - OpenScape Business

The entry point to the **OpenScape Business**/OpenScape 3000 technology can be found below the grouping **Technologies**. It shows a list of all devices discovered in an OpenScape Business environment. The list looks similar to the host view under *Categories*, but it includes additional, OpenScape Business specific information like hardware- and software-version.

Each row within the list represents one OpenScape Business object. Clicking a row or the Link within the column **Name** opens the Detail View of the Host object of the selected object. This Detail View provides access to all available information about the related systems, including gateways and controllers.

The column **Last Event** contains a link to the corresponding event. The link may be preceded by the icons listed in *Section 7.2*.

Actions

Besides the general Actions for Hosts (see *Section 7.2*) Actions which give access to OpenScape Business specific data. and functions on the selected devices are provided. For example, data about ports, features, subscribers, slots and errors is available and can be displayed for multiple systems at once.

Important Note:
The OpenScape Business Technology is only available within the Navigation Panel, if the respective plugin has been initialized in the OpenScape FM Server.

Using the Action **New** creates a new Host using the general Host Configuration (see *Section 13.1*) but with the *OpenScape* Business Container added by default.

10 Topologies

This chapter contains the descriptions of the Main Views, which provide access to part of the network topology structure of the Java Client. They are listed under the heading **Network**.

Specifically, it is possible to navigate through the object tree below the `Root->Network Topology` container. In both the Submap View (see *Section 10.1*) and the Tree View (see *Section 10.2*).

10.1 Network - Topology

This Main View shows the OpenScape FM objects that are located within the `Root->Network Topology` container of the OpenScape FM Navigation Tree.

The Topology View corresponds to the submap representation within OpenScape FM Classic Client.

Like in the classic view, objects are represented by symbols that represent the type by pictogram, the status by color and the object‘s label by a string below the symbol.

The arrangements of the symbols is identical to the representation in the classic client which includes possible background pictures.

Using **Drag&Drop** symbols can be rearranged within a submap.

Clicking a symbol shows the submap of the object represented by the clicked symbol.

Objects can be selected by hovering over the respective symbol and clicking the small **Rectangle** that is shown in the upper left of the symbol. Symbols representing selected objects are displayed with a light blue background aura. Clicking the small rectangle again deselects a selected object.

To change the size of the display, the mouse wheel has to be turned while the mouse is inside the Main View. This **zooms out** (turn mouse wheel down) or **zooms in** (turn mouse wheel up) the view of the submap. The current zoom level is displayed in a field at the top edge of the displayed submap. Clicking this field resets the zoom level to 100%.

Settings below 100% result in a smaller display of the individual symbols, but otherwise leave the display of the complete submap unchanged.

Settings above 100% result in an enlarged display of the symbols and the submap. This makes the submap larger than the Main View, and the visible section can be selected using the scroll bars at the right and bottom.

Hint:
A reset to 100% also occurs whenever the view is reopened or the browser window is resized. To avoid this, the view can be opened in a separate browser window, e.g. by using the link in the header line.

The following actions are available within the Topology View:

Actions

- **Submap Up**: Replaces the view by the parent submap of the currently displayed submap.
- **Start Submap**: Shows the submap that has been defined as the Start Submap of the current user.

- **Set Start Submap**: This sets the current submap as the Start Submap of the current user. This action will also affect the Start Submap Setting within the classic client.
- **Manage/Unmanage**: This action manage/unmanage the currently selected objects.
- **Copy**/**Paste**: The action *Copy* remembers the currently marked objects. A subsequent *Paste* action will then add a copy of these objects to the submap opened at that time. So there are now additional symbols, each representing one of these objects, on this submap.
- **Cut**/**Paste**: The action *Cut* remembers the currently marked objects. A subsequent *Paste* action moves these objects to the now opened submap. The corresponding symbols of these objects are thus removed from the original submap.
- **Remove from Submap**: This removes the selected symbols from the current submap. If there are other symbols representing the same objects on other submaps, those and their events are preserved. If there are no further symbols, the action corresponds to the action *Delete from Database*.
- **Delete from Database**: This deletes the selected objects from the database. This will also remove all symbols on other submaps that represent the same objects.
- **Show Details**: Shows the Detail View of the selected object (see *Chapter 12*).
- **Create Container**: This action adds a Container object to the current submap. During creation it is possible to specify whether it should be an *Object Container*, a *Topology Container* or a *Virtual Container*. For the latter, the filter conditions for the contained objects can also be specified. More about the container types can be found in the *Desktop User Manual*.
- **Configure Container**: This action allows to change the Name and Propagation Properties of a selected Container. For containers of the type *Virtual Container*, the filter conditions of the container can be adjusted additionally.

10.2 Network - Tree

This Main View shows the Navigation Tree of the OpenScape FM objects that are located within the `Root->Network Topology` container of the OpenScape FM Navigation Tree.

The topology is represented by a tree table in which each row represents one OpenScape FM object.

The column **Name** shows the respective object labels and the triangle symbols can be used to show/hide the objects that are located on the submap of the current object.

The column **Events** shows the number of events that currently affect the object. Clicking on the number opens a table with these events. If a **! in a circle** is displayed in front of the number, there is at least one unacknowledged event for the object, if a **filled sun symbol** is displayed, there is at least one unacknowledged 'blinking' event.

The symbols within the column **Details** can be used to open the **Detail View** or the **Submap** of the corresponding object.

Note:
The Submap-Symbol will only be displayed, if the submap contains at least one symbol.

The tree is a combination of the elements shown within the Main Views *Host Containers* (see *Section 7.4*) and *Networks* (see *Section 7.5*). But within this view the whole object tree with sub elements like e g. Interfaces or System Management components can also be browsed.

More about the network topology can be found in Section *Network Topology Management* of the *OpenScape Desktop User Guide*

Topologies

Network - Tree

11 Monitoring

This chapter contains descriptions of the System Management monitoring functions provided by the OpenScape FM Web that can be directly opened from the Navigation Panel (see *Section 4.8*). They are listed under the label **Monitoring**.

The System Management (see separate *System Management User Guide*) provides data through **System Management Agents** that collect the data with the help of so called **Monitors**. The Monitors and there configurations are contained in **Profiles** and report one or more **Parameters** (e.g. CPU Load, Memory Usage) each.

Below the Navigation Panel label **Monitoring** four entries provide access to the System Management data by opening specific Views:

- **Hosts**: Shows a list of all Hosts that are monitored by at least one System Management Agent (see *Section 11.1*)
- **Monitor Types**: Displays a list of all Monitor Types that are monitored for at least on Host (see *Section 11.2*)
- **Profiles**: Opens a list of all configured Profiles that are attached to at least one System Management Agent (see *Section 11.3*)
- **Agents** (see *Section 11.4*), **Monitors** (see Section 11.5) and **Parameters** (see Section 11.6) provide details about the respective monitoring components.

Important Note:
In contrast to the Classic Client, monitoring in the Web Client does not use the internal object database of the System Management Agents when displaying parameter values, but accesses the configured OpenScape FM database (e.g. MySQL or Derby).

11.1 Monitoring - Hosts

The Monitoring Category **Hosts** opens a View that provides an overview about all monitored Hosts and their active Monitor Profiles. The upper area aggregates the current Status of the effected Hosts and can be used to sort and filter the content of the View.

The main element of the View is a list of all Hosts for which at least one System Management Agent collects data through an active Monitoring Profile.

Each row within the table represents one individual Host. Within the columns of the table the **Status** of the Host, its **Name**, the IP **Address** and the date of the last **Status Change** are shown.

Selecting the link in the **Name** column opens a Detail View for the respective Host (see *Section 12.4*). The Detail View provides related Events, detected Technologies and additional information about all active monitoring functions.

The column **Events** shows the current number of known Events for the Host. Clicking the link in this column opens a Detail View that lists these Events.

The column **Monitoring Profiles** list the Monitoring Profiles that are active for the respective Host. The respective links open a Detail View of the selected Profile (see *Section 12.3.2*).

The columns **Reachable** and **License Assigned** indicate whether the reachability test was successful for the host and whether a System Management license has been assigned for the host.

Actions

- **Acknowledge**: This action sets the state of all Events of the selected Hosts to *Acknowledged*. They appear as treated and vanish from the Dashboard *Overview* (see *Section 6.1*).
- **Events**: This action displays a list that contains all Events of the selected Hosts.
- **Delete**: This action deletes the selected Hosts and the objects representing the Hosts within the OpenScape FM. Even within the OpenScape FMhis action *cannot be reverted*. However, events assigned to the deleted objects are maintained.
- **Manage**: This action sets *Unmanaged* Hosts to *Managed*.
- **Unmanage**: This action sets the selected Hosts to *Unmanaged*. Unmanaged Hosts are ignored by the monitoring. For example no status or configuration requests or discoveries will be performed for the respective Hosts and Events from unmanaged Hosts will not be displayed.
- **Assign License** or **Revoke License**: These actions assign or revoke a System Management License for the selected hosts. Without an assigned license, no monitoring functions are performed for a host.
- **Report**: This action opens a Report Configuration View (see *Section 13.4*) to create a new Report. The selected Hosts are pre selected for the new Report.
- **Modify**: This action opens the Configuration View for the selected IP node to modify its configuration (see *Section 13.1*).
- **Discovery**: This action performs a check for new child components, such as a new HTTP server. The components found are displayed in a table.
- **Configuration Poll**: This action triggers the child components of selected IP nodes to refresh their configuration data.
- **Status Poll**: This action performs a Status Poll for the selected Hosts. A Status Poll checks, if the IP Node assigned to the Host is responding to status request (ICMP/TCP/SNMP ping). If this is the case, the child components will be triggered to refresh their state and as a result the state of the Host.
- **Submap**: This action opens the Topology View (see *Section 10.1*) of the selected object‘s submap.

11.2 Monitoring - Monitor Types

The Monitoring Category **Monitor Types** opens a View that provides an overview about all active Monitors grouped by Type.

By clicking on a Monitor Type the Detail View of this Type will open. This View will then display all instances of the particular Type (e.g. *Disk Usage* for each host where disk usage is measured). Links within the instance list lead to further information, like e.g. host details.

The View consists of a table in which each row represents one Monitor Type. The table contains the following columns:

- **Monitor Type**: Provides the Name of the Monitor Type and a Link opening the Detail View of this Type (see *Section 12.3.1*).
- **Agent Hosts**: Shows the Names of the Hosts on which Agents controlling the Monitor Type are running. It provides a Link for up to three of these Hosts. They open the Detail View of the corresponding host (see *Section 12.4*). If there are more than three Hosts, they can be viewed using the link in the column **Monitor Type** in the detail view that opens.
- **Status Distribution**: The aggregated current Status of all active Monitors of the respective Type.

11.2.1 Monitor Types and their Configuration

This section gives a short description of some Monitor Types.

The common configuration of Monitors is described in *Section 13.5*. Here only those configuration parameters are listed that are specific for the respective type.

Important Note:
Not every monitor created in the Classic Client can be modified in the Web Client.

11.2.1.1 Basic Monitoring

Basic Monitoring contains a set of fundamental Monitors to be able to have the standard monitoring of Hosts provided centrally.

Specifically, it contains the Monitors:

- CPU Usage (see *Section 11.2.1.2*),
- Filesystem (see *Section 11.2.1.3*),
- Memory Usage (see *Section 11.2.1.4*),
- Network Usage (see *Section 11.2.1.5*),
- Top Processes (see *Section 11.2.1.6*) and
- System Info (see *Section 11.2.1.7*).

This Type does not need additional configuration.

11.2.1.2 CPU Usage

Monitors the CPU utilization of all detected logical processors (e.g. multi-core processors) on the target system in percent.

This Type does not need additional configuration.

11.2.1.3 Filesystem

Monitors the file system usage for each detected file system on the target system as percentage values.

In case not all file systems should be monitored, under *Expert Settings* in the field **Filter Filesystemname** a regular expression can be entered that contains the names of the file systems that should not be evaluated.

For example, if `C:|E:` is entered, the C and E partitions are not checked.

11.2.1.4 Memory Usage

Monitors the memory usage on the target system as a percentage value.

This Type does not need additional configuration.

11.2.1.5 Network Usage

Monitors the throughput (in bit per second), the relative utilization (in percent) and the error rates (in percent) of all detected non-loopback network interfaces on the target host.

In case the interface speed cannot be determined, a **Default Speed** in bit/second can be configured under *Expert Settings*.

11.2.1.6 Top Processes

Monitors the CPU utilization of all running processes on the target host and creates a ranking of the processes with the highest utilization.

Under *Settings* the **Number of processes to be shown** can be configured.

11.2.1.7 System Info

Determines the used operating system, the logical processors, the available memory, the existing file systems and the established network interfaces.

It therefore provides basic information about the respective target host.

This Type does not need additional configuration.

11.2.1.8 IO Statistics

Monitors the I/O statistics of the configured drives.

A description of the parameters can be found in:
https://www.kernel.org/doc/Documentation/block/stat.txt

In **Operating System of Monitored Host** *Windows* or *Linux* has to be selected.

Monitored Drives configures the drives to be monitored by entering a comma separated list of drive names like e.g. `sda,sdb` or `C:,D:` .

11.2.1.9 Check Processes

Checks whether the specified processes are running on the target system.

Under *Settings*, the names of the processes to be controlled by the Monitor can be entered in the table **Monitored Processes**.

When the Monitor is executed, it checks for each of the specified names whether a matching process is currently running on the host. The output of the Monitor shows for each name how many processes with matching name are running.

In the OpenScape FM, an object is assigned to each name. This has the status '*Normal*' if at least one suitable process is running, otherwise the status '*Critical*'. If the status changes, a corresponding Event is generated.

In addition, by marking the corresponding line, it can be specified whether the **CPU Usage**, the **Virtual Memory Size**, the **Working Set Size**, the **Page Faults** and the **Thread Count** are to be monitored for the monitored processes.

11.2.1.10 TCP-Port-Monitor

Tries to open a connection to the configured TCP Target Port.

If this does not work, a Critical event is generated. If the port is reachable again, a Normal event is generated.

In addition, the monitor measures the time to open and close the port.

11.2.1.11 Host Resources

Provides system information by querying the `HOST-RESOURCES-MIB`.

The monitor combines four sub-monitors that can be configured centrally in the monitor. In the user interface, they are displayed as independent monitor symbols.

In detail, the following four monitorings are concerned. for each of which an individual **Execution Interval** can be configured:

- **System**: Displays general system information, such as the uptime, the system time and the number of users.
- **Processes**: Displays the running processes, their status, the used CPU time and the used memory.
- **Storages**: Displays the state of connected storage devices, such as hard disks, CD-ROMs or RAMs.

- **Devices**: Displays the state of connected devices, such as printers, network interfaces, drives, keyboard or CPUs.

The configuration of the SNMP connection is done on the subpage **Host Settings** of the Host Detail View (see *Section 12.4*). An exception is the selection of the **SNMP Port**, which can also be done in the monitor configuration itself.

11.2.1.12 Uptime

Monitors the system uptime of the SNMP agent in days (`sysUptime`).

The configuration of the SNMP connection is done on the subpage **Host Settings** of the Host Detail View (see *Section 12.4*). An exception is the selection of the **SNMP Port**, which can also be done in the monitor configuration itself.

11.2.1.13 Windows Services

Checks whether the specified Windows Services are running on the target system.

Under *Settings*, the names of the services to be controlled by the Monitor can be entered in the table **Monitored Services**.

When the Monitor is executed, it checks for each of the specified names whether a matching service is currently running on the host. The output of the Monitor shows for each name whether the service runs (*Service running*), it is unknown (*Unknown service*) or currently stopped (*Not running*).

In the OpenScape FM, an object is assigned to each name. This has the status '*Normal*' if the service is running, '*Critical*' if stopped or ‚*Unknown*‘ if unknown. If the status changes, a corresponding Event is generated.

11.2.1.14 Windows Hardware

This Monitor provides information about temperature, fan speed and operating voltage of the hardware of a Windows system. Exactly which data can be determined depends on the type of system.

The Monitor calls an external tool and therefore only works on the local Windows system on which the configured internal or external OpenScape FM Agent is running.

This Type does not need additional configuration.

11.2.1.15 Windows Event Log

This Monitor checks if the Windows Event Log of the target system contains errors and warnings.

The entries of the log that have been added since the last execution of the Monitor are taken into account.

In the configuration, it can be specified which event IDs or which occurring text fragments are to trigger an OpenScape FM event:

Event IDs:
Here events from the Event Log are specified comma-separated, which are to be considered by the Monitor.

The configuration of each event type has one of the following two formats:

`<Event ID>:<Source>` or `<Event ID>:<Source>:<Status>`

Example: `8019:DNS Client Events:Major`

Source and *Event ID* correspond to the contents of the corresponding columns of the Windows Event Viewer. *Status* corresponds to the status value to be assigned to the corresponding events in the OpenScape FM (e.g. `Minor`). If the status is not specified, the default setting `Critical` is used.

- **Generate Events (Event IDs)**:
  Only if a check mark is here, an event is generated, if the configuration in *Event ID* matches.
- **Event Patterns**:
  Here also events from the Event Log are specified comma-separated, which are to be considered by the Monitor. However, the hits do not result from the columns *Source* and *Event ID*, but from the event message.

  The configuration has the following two format:

  `<Pattern>:<Status>`

  Here, *Pattern* is a sub-string that is to occur in the event message. *Status* again corresponds to the status value that the corresponding events are to receive within the OpenScape FM.

  In this case, Events are generated if one of the configured sub-strings occurs in the message and a suitable Threshold has been defined in the Classic Client.
- **Generate Events (All Log Entries)**:
  If this is checked, a matching Event is generated in the OpenScape FM for each entry in the Windows Event Log.

  Warning:
  This can lead to a very large number of Events.

11.2.1.16 Linux Services

Checks whether the specified Linux Services are running on the target system.

Under *Settings*, the names of the services to be controlled by the Monitor can be entered in the table **Monitored Processes** (p_service).

When the Monitor is executed, it checks for each of the specified names whether a matching service is currently running on the host. The output of the Monitor shows for each name whether the service runs (*Service running*), it is unknown (*Unknown service*) or currently stopped (*Not running*).

In the OpenScape FM, an object is assigned to each name. This has the status '*Normal*' if the service is running, '*Critical*' if stopped or ‚*Unknown*‘ if unknown. If the status changes, a corresponding Event is generated.

11.2.1.17 Linux Hardware

This Monitor provides information about temperature, fan speed and operating voltage of the hardware of a Linux system. Exactly which data can be determined depends on the type of system.

The Monitor uses SNMP to collect the data and needs the `LM-SENSORS-MIB` (usually the packages `net-snmp` and `lm-sensors/sensors`) on the monitored system.

In detail, the following parameter are observed: `lmTempSensorsTable`, `lmFanSensorsTable`, `lmVoltSensorsTable`.

Besides that the settings for temperature, fan speed and operating voltage, can be configured individually, this Type does not need additional configuration.

11.2.1.18 Linux Uptime

This Monitor provides the monitored system‘s uptime in days using SSH.

To perform the monitors requests on the monitored system access data have to be configured.

The login date (**Login** and **Password**) is configured under **Settings**, and the SSH access parameters under **Expert Settings**.

11.2.1.19 PostgreSQL Performance

This Monitor monitors the performance data of a Postgres database.

By using a JDBC network connection from the Postgres service daemon it fetches the current Number of *Database Connections*, the *Block IO / Throughput*, the *Tablespace Sizes*, the *Cache Hit Ratio* (in percent) and the current *Transactions per Second*.

The configuration requires the username (**Login**) and **Password** of a Postgres user with the necessary rights to read the performance indicators listed above.

In addition the **JDBC Port** that should be used to collect the data, the **Execution Interval** for these collections, and the OpenScape FM **Monitoring Agent** that should be performing the collections can be configured.

Important Note:
If the Monitor should be used, it may be necessary to adjust the PostgreSQL configuration file `pg_hba.conf` (see *PostgreSQL Documentation* e.g. at `https://www.postgresql.org`).
If there are no corresponding entries in this file, only clients/users located on the same computer as the database cluster can access the database.
On Linux, before and after adjusting the configuration file, the PostgreSQL postmaster process must be stopped or started using `pg_ctl`.

11.2.1.20 Mediatrix Gateway (Media5)

Provides information about Mediatrix gateways (Media5) by querying the `mx-crout MIB` via SNMP.

The monitor combines two sub-monitors that can be configured centrally in the monitor. In the user interface, they are displayed as independent monitor symbols.

In detail, the following both monitorings are concerned. for each of which an individual **Execution Interval** can be configured:

- **Basic Info**: Displays general information like product name, MAC address, SerialNumber and interfaces.
- **Port Usage**: Displays the available and used FXS ports and the channel assignment of the ISDM interfaces.

The configuration of the SNMP connection is done on the subpage **Host Settings** of the Host Detail View (see *Section 12.4*). An exception is the selection of the **SNMP Port**, which can also be done in the monitor configuration itself.

11.2.1.21 VMWare Monitor (vCenter)

Monitors the virtual machines and host systems of a VMWare Server and provides detailed information about the status and the components of the VMWare environment through data tables.

Every host system and every monitored virtual machine is displayed as a container node. An IP Node and System Management license is necessary for the configured vCenter Server itself.

The monitor uses the Yet another VMware VI (vSphere) Java API (`yavijava.jar`), which is based on the VMware *vSphere Web Services SDK*. The version 6.0 of the SDK supports the following VMware servers:

- ESX/ESXi 4, 5, 6
- ESX Server 3.5, 3i, 3.0.x
- vCenter Server 4, 5, 6
- VirtualCenter Server 2.5 and 2.0.x

The monitor combines three sub-monitors that can be configured centrally in the monitor. They are displayed in the interface as independent monitor icons.

To access the VMWare server, the authentication for the VMWare server must first be configured under **Common Settings** (**Login**, **Password**).

The sub-monitors are the following three monitors. for each of which a separate **Execution Interval** can be configured:

- **VMWare Overview**: Gives an overview of the state of the VMWare server.
- **Virtual Machines**: Checks the reachability of the monitored virtual machines of the vCenter Server.
- **Host Systems**: Checks the accessibility of the monitored host systems of the vCenter server.

By default, all detected host systems and virtual machines are automatically monitored.

This default setting can be modified under **Expert Settings**:

- If **Hostsystems Autodiscovery** is not marked there, no automatic detection of the host systems takes place. In this case, a comma-separated list of the host systems to be monitored can be specified in the field **Host Systems**.
- The virtual machines are selected accordingly by unchecking **AutoDiscovery** and entering a corresponding comma-separated list in the field **Virtual Machines**

11.2.1.22 SNMP Agent

This monitor checks the availability of the configured SNMP Agents on the host system.

In the configuration, the **SNMP Port**, the **SNMP Version** used and, depending on the version, the **Read Community** and **Write Community** or the **Security Level** and the **Security Name** must be specified for each SNMP Agent.

Each port is configured on a separate page and a separate SNMP monitoring component is created for each configured port.

11.2.1.23 SNMP MIB-II

This monitor reads the values of the configured OIDs from the MIB-II of the monitored system.

Using **SNMP Port**, the port can be specified via which the SNMP agent can be reached (default: `161`):

In the table **SNMP OIDs** the values can be selected, which are to be read from the MIB-II. Each line corresponds to a selected value.

New lines can be added with **+** and selected lines can be deleted with **-** or modified after **double-clicking**.

If a single value should be read the OID of the value must be entered in the table.

If values are to be read from a table, the OID of the desired table column must be entered accordingly.

In both cases, an individual parameter name can be assigned to the read values by appending it to the OID separated by **:** (e.g.: `.1.2.3:myparameter`).

11.2.1.24 Secure Shell (SSH)

Monitors the Secure (Socket) Shell Server of the current host.

Only the **SSH Port** has to be entered.

11.2.1.25 OpenScape 4000 SNMP Proxy

Monitors the status of the SNMP Proxy Agent of an OS4K Manager or Assistant and the status of all sub-agents.

The monitoring agent must be running on the target system.

In the field **Service Names** all services to be monitored can be configured in the form of a comma-separated name list.

11.2.1.26 OpenScape 4000 Trunk Group Load

Measures the utilization of OpenScape 4000 Communication Trunks.

It is available as a `Telephony Monitor` under the category `OpenScape 4000`.

The monitor queries the trunk group utilization periodically by running the `AMO BUEND` on an OpenScape 4000 manager or assistant, either for all trunk groups of an OpenScape 4000 System or only for specific trunk group (configured by number). For each trunk, a System Management parameter is created and shown in the user interface which measures the utilization of its trunk group in percent.

Relevant for the calculation of the utilization are the fields `AKT`, `BELEGT` and `FREI`, respectively. The field `ANDERE` shows how many lines are currently out of order.

In the configuration, the field **System ID** (mnemonic) defines the OpenScape 4000 to be queried. If nothing is entered here, for assistants the `SYS1` will be used.

In the field **Trunk Group Numbers** a comma separated list of trunk numbers to be monitored can be entered. If this field is left empty, all trunk groups of the system will be monitored.

11.2.1.27 OpenScape Branch - License

Displays the current license state of the OpenScape Branch.

The connection to the OpenScape Branch is made via SSH (command: `licget`).

Since `root` is not allowed to log in via SSH, the Monitor performs a user switch to `root` on the target system, The user to be switched with must be configured here via the fields **SSH User (Switch)** and **Password SSH User (Switch)**.

11.2.1.28 OpenScape Branch - Channel Load

Monitors the channel load on the OpenScape Branch as percentage value via SSH and the asterisk command.

Since `root` is not allowed to log in via SSH, the Monitor performs a user switch to `root` on the target system, The user to be switched with must be configured here via the fields **SSH User (Switch)** and **Password SSH User (Switch)**.

At the same location the range for the monitored channels can be limited using the fields **First Channel Number (firstChannel)** and **Last Channel Number (lastChannel)**.

11.2.1.29 OpenScape Branch - Registered Subscribers

Queries the current number of registered subscribers of the specified OpenScape Branch nodes.

This Monitor requires access credentials for the OSB SOAP Web Service.

For this under *Settings* the fields **WebService Login**, **WebService Password** and **WebService Port** can be used to configure the respective access.

11.2.1.30 OpenScape Voice - Licences

Collects information about the current number of used or available dynamic licenses.

This monitor requires access to the OVB SOAP Web Service.

The **WebService Port** can be configured (default: `8767`).

Since the access to the OpenScape Voice for the requesting system has to be enabled on the OSV, no User/ Password access parameters are needed here.

11.2.1.31 OpenScape Voice - CAC Groups

Gathers information about the current number of concurrent calls and/or the used bandwidth of all CAC Groups / Policies.

This monitor requires access to the OVB SOAP Web Service.

The **WebService Port** can be configured (default: `8767`).

Since the access to the OpenScape Voice for the requesting system has to be enabled on the OSV, no User/ Password access parameters are needed here.

11.2.1.32 OpenScape Voice - Registered Subscribers

Gathers information about the current number of active and blocked subscribers.

This monitor requires access to the OVB SOAP Web Service.

The **WebService Port** can be configured (default: `8767`).

Since the access to the OpenScape Voice for the requesting system has to be enabled on the OSV, no User/ Password access parameters are needed here.

11.3 Monitoring - Profiles

The Monitoring Category **Profiles** opens a View that provides an overview about all Monitoring Profiles that are currently active.

A Profile (typically an XML file) defines a set of Monitors along with their configuration (e.g. execution times, thresholds etc.). The profile *Basic Monitoring*, for example, aggregates a few Monitors for important system parameters.

The View consists of a table in which each row represents one Profile.The table contains the following columns:

- **Monitoring Profile**: Provides the Name of the Profile and a Link opening the Detail View of this Profile (see *Section 12.3.2*).
- **Agent Host**: Shows the Name of the Host on which the Agent that controls the Profile is running. It provides a Link that opens the Detail View of this Host (see *Section 12.4*).
- **File Path**: The Path to the configuration file of the Profile.

11.4 Monitoring - Agents

The Monitoring Category **Agents** opens a View that provides an overview about all Monitoring Agents that are currently active.

The **Status Overview** at the top provides the distribution of the Status of all System Management Agents. This area can also be used to select or filter specific status values in the list below.

Each row of the displayed list represents one Agent and the following columns are displayed:

- **Agent Status**, **Agent Host** and **Server IP**: Display the current Status value of the Agent, the name of its Agent Host and the IP address of this Host. The link in the **Agent Host** column opens the Detail View of the respective Host (see *Section 12.4*).
- **Version**, **Monitored Hosts** and **Monitored Parameters**: The software version of the Agent and the numbers of Hosts and Parameters that are monitored by the Agent. The link within the column **Version** opens the Detail View of the respective Agent object (see *Section 12.3.5*).

The provided actions correspond to the identically named actions for the host object of the agent.

11.5 Monitoring - Monitors

The Monitoring Category **Monitors** opens a View that provides an overview about all Monitors that are currently active.

The **Status Overview** at the top provides the distribution of the Status of all System Management Monitors. This area can also be used to select or filter specific status values in the list below.

Each row of the displayed list represents one Monitor and the following columns are displayed:

- **Status** and **Monitor**: Display the current Status value and the name of the respective Monitor. The link in the Monitor column opens the Detail View of the respective Monitor (see *Section 12.3.3*).
- **Monitored Host** and **Agent Host**: Show the Host that is monitored by the Monitor and the Host on which the Agent is running that controls the Monitor. Both columns provide Links that open the Detail View of the respective Host (see *Section 12.4*) or Agent (see *Section 12.3.5*).
- **Profile** and **File Path** (initially hidden): The Name of the Profile to which the Monitor belongs and the path within the file system where the configuration file of the Profile is located.

Actions

- **Report**: This action opens a Report Configuration View (see *Section 13.4*) to create a new Report. The associated Parameters are pre selected for the new Report.
- **Execute Monitor**: This action immediately executes the associated Monitor.

11.6 Monitoring - Parameters

The Monitoring Category **Parameters** opens a View that provides an overview about all Parameters that are currently being collected.

The **Status Overview** at the top provides the distribution of the Status of all System Management Parameters. This area can also be used to select or filter specific status values in the list below.

Each row of the displayed list represents one Parameter and the following columns are displayed:

- **Status** and **Parameter**: Display the current Status value and the name of the respective Parameter. The link in the Parameter column opens the Detail View of the respective Parameter (see *Section 12.3.4*).
- **Value**: The last value calculated for the Parameter.
- **Monitored Host** and **Agent Host**: Show the Host that is monitored by the Parameter and the Host on which the Agent is running that controls the Monitor that monitors the Parameter. Both columns provide Links that open the Detail View of the respective Host (see *Section 12.4*) or Agent (see *Section 12.3.5*).
- **Monitor**: The Name of the Monitor to which the Parameter belongs. The link opens the Detail View of the respective Monitor (see *Section 12.3.3*).

Actions

- **Report**: This action opens a Report Configuration View (see *Section 13.4*) to create a new Report. The associated Parameter is pre selected for the new Report.
- **Execute Monitor**: This action immediately executes the associated Monitor.

12 Detail Views for Object Types

This chapter describes the **Detail Views** that are specific for the individual Object Types and the Actions that can be performed within these Detail Views. A general introduction into Detail Views can be found in *Section 4.15*.

Some actions are generally provided independent of the Object Type. These are described in *Section 12.1.* Starting with *Section 12.2* the information and actions dependent on the respective Object Types are shown.

12.1 Detail Views - General Actions and Displays

This section lists some common Displays and Actions that appear in the Detail Views of many object types

Displays

- **Details**: General information such as **Status**, **Host Name**, **IP** or **MAC Address**, or the **Status Poll Interval**.
- **Host Types**: The host type(s) assigned to the displayed object (see *Section 7.3*).
- **Status Explanation**: A description detailing why the object has its current status.
- **Comment**: The comment assigned to the object.
- **Status History** displays the changes of the object‘s Status. By using the respective tabs the changes of the Status over time can be displayed as a graph or as a table.
- **Object Information**: provides general information about the object that represents the Event within the OpenScape FM.

  Among others the internal name of the object, the creation and modification date and the status distribution of the child objects will be displayed.
- **Events**: Lists the unacknowledged events assigned to the current object.

Actions

The following actions are provided for all or at least a variety of Object Types:

- **Reload**: This action updates the data in the current Detail View.
- **Delete**: This action deletes the object that is displayed in the current Detail View. In general, all objects belonging to this object are also deleted. However, events assigned to the deleted object are maintained.
- **Submap**: This action displays the topology submap of the current object (see *Section 10.1*).
- **Acknowledge**: This action acknowledges all events assigned to the current object.
- **Unmanage**: This action sets the current object to *Unmanaged*. Unmanaged objects are ignored by the monitoring. For example no status or configuration requests will be performed for the respective object and Events from *Unmanaged* objects will not be displayed.
- **Manage**: This action sets the current object to *Managed*.

- **Service Impact**: This Action provides an overview about all Services (see *Section 7.7*) which contain the current object. The Action is only available for objects that are included in at least one Service.

  Each row of the displayed list represents one of these Services.

  - The column **Service** shows the name and the current availability of the respective Service and provides a link to a Detail View of the respective Service (see *Section 12.8*).
  - If the object is not located directly below the root object of the Service, the column **Component** shows the name and the current availability of the component in which the object is located. By using the link, the Detail View of the component can be opened.
  - The column **Value** shows the current availability value of the object itself that is used for the calculation of the respective Service availability.

12.2 Detail View - Event

The Detail View for Event objects shows additional information, like some object **Details**, about the Event for which the Detail View has been opened.

The list **Correlated Events** contains rows that represent the Events that are correlated to the current Event. The links within the column **Description** can be used to open the Detail View of the respective Correlated Event within a separate browser tab or window.

By using the textfield **Annotation** and the **Save** button located on the right side of the textfield, Annotations for the Event can be created or modified. The **Discard Changes** button located below the *Save* button can be used, to revoke the modifications made after the last Save.

More about *Correlated Events* and *Annotations* can be found in Section *Event Browser* within the separate User Guide for the *OpenScape FM Desktop*.

The Category *Events* that lists all current Events is described in *Section 7.1*.

Actions

Important Note:
The Actions **Acknowledge**, **Unacknowledge** and **Delete** effect the current Event and all Events that are correlated to the current Event.

- **Acknowledge**: This action sets the state of the current Event to *Acknowledged*. It appears as treated and vanishes from the Dashboard *Overview* (see *Section 6.1*).
- **Unacknowledge**: This action sets the state of the current Event to *Unacknowledged*. It appears as currently untreated and, dependant on its Severity, may reappear within the Dashboard *Overview* (see *Section 6.1*).
- **In Progress**: Sets the *In Progress* attribute for the Event to the current User.
- **Not in Progress**: Removes the *In Progress* attribute from the Event.
- **Delete**: This action deletes the current Event and the object representing the Event within the OpenScape FM. This action *cannot be reverted*, even within the OpenScape FM.

- **Ignore** and **Ignore Global**: With these menu entries events of the same type as the current event can be ignored in the future. Using **Ignore** for the object to which the current event is assigned and **Ignore Global** for all objects.
  In both cases, a check mark behind the entry indicates that a general or object-specific ignore filter exists for the current event type.
  If such a filter exists, it is deleted by clicking the corresponding button again.
  In addition ignoring events can be undone using the general overview of automatic actions for events (see *Section 7.1 - Event Filter*).

12.3 Detail View - System Management

This section describes the Detail Views for System Management objects, which can, for example, be accessed from entries within the Navigation Panel (see *Section 4.8*) listed under the label **Monitoring**. There are five different types of System Management Detail Views which can be accessed via the web user interface and provide information of one object of the specific type:

- **Monitor Types** (see *Section 12.3.1*) are mainly accessed from the Main View **Monitor Types** (see *Section 11.2*)
- **Monitoring Profile** (see *Section 12.3.2*) are mainly accessed from the Main View **Profiles** (see *Section 11.3*)
- **Monitors** (see *Section 12.3.3*), **Parameters** (see *Section 12.3.4*) and **Agents** (see *Section 12.3.5*) and are mainly accessed from the Main View **Details** (see *Section 11.4*)

12.3.1 Detail View - Monitor Type

Monitor Types define a general type of a monitoring function. Instances of Monitor Types that monitor specific Hosts are called Monitors (see *Section 12.3.3*).

The Detail View of a Monitor Type consists of two areas:

The **Status Overview** at the top provides the distribution of the Status of all active Monitors of the selected Monitor Type. This area can also be used to select or filter specific status values in the list below.

The **List of Monitors** in the lower part of the View contains one row for each active Monitor of the displayed Monitor Type. Clicking a list row opens the Detail View of the correlated Monitor.

The lists has four columns:

Status: Displays the current Status value of the respective Monitor.

Monitor: Shows the Name of the Monitor. Clicking the Links in this column open the Detail View of the respective Monitor.

# of Parameter: The number of Parameters that are checked by the Monitor.

Target Host: The Host that is monitored by the Monitor.

Agent Host: The Host that performs the monitoring.

12.3.2 Detail View - Monitoring Profile

Monitoring Profiles aggregate a predefined combination of one or more Monitors (see *Section 12.3.3*). Monitoring Profiles can be assigned to target system to perform all of their included Monitors on this system.

The Detail View of a Monitoring Profile consists of two areas:

The **Status Overview** at the top provides the distribution of the Status of all active Monitoring Profiles of the selected Profile Type. This area can also be used to select or filter specific status values in the list below.

The **List of Monitored Hosts** in the lower part of the View contains one row for each Host that is monitored by the Monitoring Profile of the displayed Profile Type.

The lists has five columns:

Status: Displays the current Status value of the respective Monitoring Profile.

Name: Shows the Name of the Host that is monitored by the Monitoring Profile. Clicking the Links in this column open the Detail View of the respective Host.

Events: The number of Events related to the Monitoring Profile. Clicking the links in this column opens a Detail View with a list of the respective Events.

Last Event: Displays the date and message of the last event for the host and provides a link to that event.

IP Address: The IP Address of the Host that is monitored by the Monitoring Profile.

12.3.3 Detail View - Monitor

A Monitor is a specific instance of a Monitor Type (see *Section 12.3.1*) that monitors one or more parameters on a target system. The Detail View of a Monitor provides the following, monitor-specific information:

Host: The agent system on which the Monitor is running. This can be different from the system which is actually monitored.

Key Path: Relative path within the topology tree where the Monitor is displayed in the client.

Target IP: The system which is actually monitored by this Monitor

File Path: The XML file which defines the related monitoring profile. A profile can define more than one Monitor, so a number of Monitors may have the same file path.

Long Message: The recent textual output of this Monitor

In addition, under **General** access to all Parameters (see *Section 12.3.4*) measured by the current Monitor is available. At a File System Monitor, for instance, these are the individual file systems monitored on a particular host.

Actions

- **Execute Monitor**: This action immediately executes the current Monitor.

12.3.4 Detail View - Parameter

A Parameter refers to a single measurement series monitored by a Monitor, for example the load of a particular CPU core. The detail view provides parameter-specific information displayed on four sub pages:

- **Overview**:
  Displays the last acquired value, a graph or a list with the history of the acquired values, and the textual output of the last execution of the parameter.
- **Events**:
  Contains a list of events associated with the parameter.
- **Details**:
  Contains information about the Parameter object (e.g. status history), as well as links to the Host or Agent Host (see *Section 12.4*) and Monitor (see *Section 12.3.3*) of the Parameter.
- **Settings**:
  Provides the possibility to edit a comment for the parameter.

Actions

- **Execute Monitor**: This action immediately executes the associated Monitor.
- **Report**: Opens the Report Configuration for the current Parameter (see *Section 13.4.1*).

12.3.5 Detail View - Agent

An Agent executes Monitors either locally or remotely and stores the acquired data. The Detail View of an Agent shows the following, agent-specific information:

Host: The system on which the Agent is running

Version: The version of this Agent. It is recommended to use the same as the server version, i.e. the Agents are updated when the server is updated.

Server Name: The host name of the server on which the Agent is running.

Server IP: The IP address of the server on which the Agent is running.

Agent UUID: A unique identifier for this Agent

Monitored Hosts: The number hosts monitored by this Agent and below a list with the monitored hosts and links to the respective elements.

Monitored Parameters: The number of parameters measured by this Agent

12.4 Detail View - Host

The Detail View for Host objects shows additional information, like some object **Details**, about the Host for which the Detail View has been opened.

The header of the Detail View contains, in addition to the **Status Display** the date of the last Status Check, Configuration Check (**C**) and Discovery Check (**D**).

If the Host could not be reached with the last Availability Check, '*not available*' will be displayed instead of the date of the last Configuration Check.

The Category *Hosts* that lists all current Hosts is described in *Section 7.2*.

Since the information for Hosts is very extensive, the additional information and possible actions are divided among the following sub-pages:

- Sub-page **Host Dashboard**:

  This page shows an overview about the condition of the Host and its sub components (see *Desktop User Guide - Status Explanation*).

  It contains:

  - the **Availability** by showing the last test result and a graph with the results of the last days and by providing a link to the respective Parameter Detail View through an **i Icon** in the upper right,
  - the current **Status Explanation**,
  - a list of the **Status Relevant** (unacknowledged) **Events** for the Host and its sub components,
  - a list of the **Status Relevant Sub-Components**,
  - a list of the **identifying characteristics** of the Host (name, IP address, type and the OpenScape FM internal characteristics object id and object name)
  - and a list of the Host specific **Monitoring Parameters**.

  Actions

  - **Check Availability**: This action performs a Status Poll for the current Host. A Status Poll confirms if the IP Node assigned to the Host is responding to status request (ICMP/TCP/SNMP ping). If this is the case, the child components will be triggered to refresh their state and as a result the state of the Host.
  - **Update Configuration**: This action triggers the child components of the current Host to refresh their configuration data.
  - **Start Discovery**: This action performs a check for new child components, such as a new HTTP server. The components found are displayed in a table.
  - **Report**: This opens the report creator (see *Section 8.1*) with a default setting for the current host.
  - **Reload**: Refreshes the displayed data.
  - **Manage**: Sets *Unmanaged* Hosts to *Managed*.
  - **Unmanage**: Sets the selected Hosts to *Unmanaged* (see *Section 7.2*).
  - **Delete**: Deletes the displayed Host from the OpenScape FM after confirmation. However, events assigned to the deleted object are maintained.

- Sub-page **Events**

  This page contains a list of Events that are currently present for the current Host.

  The content and actions of the page are essentially the same as for the Category *Events* (see *Section 7.1*), with a filter on the current Host.

  In addition, the action **Acknowledge All** is available, which acknowledges all currently unacknowledged events of the host.

- Sub-page **Monitoring**:

  This page provides an overview of the monitoring of the Host by the System Management (see *System Management User Guide*).

  It shows the reachability of the Host (**Availability (Ping)**).

  If **Basic Monitoring** has been activated for the host, the most important parameters (**CPU Usage**, **Memory Usage**, **Network Usage**, **IO Statistics**, **Top Processes** (CPU Usage) and **Filesystem Usage**) are displayed in an overview. The displayed colors correspond to the Status of the respective parameter.

  Additional Monitors active for the Host are represented by a box in the color of the respective current Monitor Status. Clicking one of the boxes opens the Detail View of the corresponding Monitor (see *Section 12.3.3*).

  The Action **Configure Monitors** can be used to configure the Monitors monitoring the current Host (see *Section 13.5*).

- Sub-page **Graphical Topology**:
  This page initially displays the Topology View of the submap on which the Host is located. From here it can be navigated as usual within the Topology (see *Section 10.1*).

  The additional Action **Back to Host** reopens the initial view and selects the Host.

- Sub-page **Sub Components**:
  This page shows the topological Tree View where the selected Host is the root object of the tree. It can be navigated as usual within a Tree View (see *Section 10.2*).

  As an additional Action, **Reload** updates the structure of the tree.

- Sub-page **Host Details**: This page shows information about the Host. These may differ, depending on the technologies or monitoring settings detected for the Host.

  Expandable sections often provide an **i Icon** in the upper right corner (an `i` in a circle), which becomes visible when the mouse pointer is hovering over the section heading. This icon is a link to a separate Detail View of the area. On this Detail View, e.g. Actions can be executed for elements of the area.

  Using the textfield **Comment** and the **Save** button located on the right side of the textfield, Comments for the Host can be created or modified. The **Discard Changes** button located below the *Save* button can be used, to revoke the modifications made after the last Save.

  The tables **Status Related Objects** and **Status Related Events** show the objects and unacknowledged events that are currently relevant for the Status of the Host.

  Status History displays the changes of the Host‘s Status. By using the respective tabs the changes of the Status over time can be displayed as a graph or as a table.

The table **Interfaces** provides a list of the Host‘s Interfaces and their key parameters like **IP Address**, **Netmask**, **MAC Address** or there current status.

Actions

- **Reload**: Refreshes the displayed data.

- Sub-page **Host Settings**:

  This page provides the option to configure some basic properties of the host:

  - Under **Network Settings** the *Display Name*, the *Host Name* and the *IP Address* of the Host can be viewed and/or configured.
  - **SNMP Connection** allows the configuration of SNMP connection settings for the default SNMP agent port 161. Other SNMP agents can be configured using the provided link (see *sub-page Monitoring*).
  - Under **Display Setting as Router**, it can be selected whether the Host should be displayed in the topology presentation as an *IPv4 Router*, *IPv6 Router* and/or *MAC Switch*. If *Auto* is selected, an attempt is made to determine the corresponding property via SNMP. According to the classification as router/switch, the Host is additionally displayed in the Network Topology Container and receives a connection to every Network in which it has an IP address.
  - Under **Status Change Notification** it can be set whether and to whom an email notification should be sent when the status of the Host changes to one of the selected values.

    The sender of the emails and the mail server to be used can be set using the administration (see *Section 14.6.1*).
    Using the link **Please click here to configure mail server...** the corresponding administration page can be opened immediately.
  - Under **Advanced Settings**, it can be specified what happens to the Host when it is detected that its IP address has changed. The placement in the Topology can either be preserved, or the discovery filter rules are applied as when the Host is newly created.

    If **IP Address Adjustment** is marked and the Host is unreachable, an attempt is made to reach the IP address of another Interface of the Host. If this can be reached, it is used for further reachability tests.

    IP Template allows to determine the IP configuration of the Host via a selected Template.
  - The link **Further settings for SNMP agents, .. Monitoring** can be used to configure the Monitors monitoring the current Host (see *Section 13.5*).

  Actions

  - **Reload**: Refreshes the displayed data.
  - **Apply** or. **Discard**: Stores or discards the changes made for the configuration.

12.5 Detail View - Interface

The Detail View for Interface objects shows additional information, like some object **Details**, about the Interface for which the Detail View has been opened.

By using the textfield **Comment** and the **Save** button located on the right side of the textfield, Comments for the Interface can be created or modified. The **Discard Changes** button located below the *Save* button can be used, to revoke the modifications made after the last Save.

Depending on technologies or monitoring settings that are discovered for the Interface, additional information may be displayed.

For example: If System Management Parameters are collected by or for the Interface, additional data will be shown.

12.6 Detail View - Host Container

The Detail View for Host Container objects displays a list in which the rows represent the Hosts that are a member of the Host Container.

For each Host its **Name**, **Status**, **IP Address** and the date of the last **Status Change** are shown in the respective table columns. Like Main View Categories the table can be filtered by *Severity* and *Table Filters* (see *Section 4.16.2*).

Using the links within the column **Name** opens a separate Detail View for the respective Host (see *Section 12.4*).

The Category *Hosts Containers* that lists all current Hosts Containers is described in *Section 7.4*.

12.7 Detail View - Network

The Detail View for Network objects displays a list in which the rows represent the Hosts that are a member of the Network.

For each Host its **Name**, **Status**, **IP Address** and the date of the last **Status Change** are shown in the respective table columns. Like Main View Categories the table can be filtered by *Severity* and *Table Filters* (see *Section 4.16.2*).

Using the links within the column **Name** opens a separate Detail View for the respective Host (see *Section 12.4*).

The Category *Networks* that lists all current Networks is described in *Section 7.5*.

Actions

The possible actions correspond to the actions in the general host overview (see *Section 7.2*), but no new hosts can be added here.

12.8 Detail View - Service

If the respective data is available, the Detail View shows two charts or tables about the measured availability of the current Service.

Availability History shows the availability at the displayed points of time and **Average Availability** shows the average availability within the displayed time intervals (e.g. per day).

To see what error sources may have caused a service to be less than optimal at a particular point in time, the **Availability History** can be used.

If this is opened in table form, the links in the column **Message (Value)** provide the possibility to open an info page. This page shows which service elements did not have the status *Normal* at the corresponding point in time.

Under **Service Model** the Detail View shows the object structure and the calculated availability of the Service for which the Detail View has been opened.

Each Service consists of **Service Components** that are responsible for the calculation of the Service‘s availability, and of **Service Objects** who are monitored by the Service and whose Status provide the base data for the calculation (see *OpenScape FM Event Correlation Engine User Guide* - Chapter *Service Impact Management* for more about Services).

The Detail View contains a tree table in which each line represents one of the objects that define the Service within the OpenScape FM.

Service Objects are represented by their **Name** (which corresponds to their label within the OpenScape FM Client) and by their **Availability** that is calculated from the current Status of the object. Usually *Normal* is represented by the Availability 100% and *Critical* by 0%. But any other assignment for each Status is possible and has to be defined within the OpenScape FM.

By using the symbols in the column **Details** the Detail View or the Submap of the corresponding object can be opened.

Service Components are also represented by their **Name**. Their **Availability** is calculated based on the underlying Service Components and Service Objects. These underlying objects are represented as child objects within the tree table and the child objects can be displayed/hidden by using the triangle shaped arrows located on the left of the Service Component within the column **Name**.

For Service Components the column **Availability** shows the calculated availability and the method by which the calculation has been performed. This can be either the **Maximum**, **Minimum** or **Average** of the availability of all child objects, or the availability of the child object whose Status has changed **Last**.

The Availability of the root object of the tree table represents the total current Availability of the Service.

The Category *Services* that lists Services is described in *Section 7.7*.

12.9 Detail View - File/Report

The Detail View for Reports shows additional information, like some object **Details**, about the Report for which the Detail View has been opened.

The view also contains action buttons to view or download the associated file.

By using the textfield **Comment** and the **Save** button located on the right side of the textfield, Comments for the Report can be created or modified. The **Discard Changes** button located below the *Save* button can be used, to revoke the modifications made after the last Save.

The Category *Reports* that lists Reports is described in *Section 8.1*.

Actions

- **Show**: Opens a window in which the report is displayed. From here it also can be saved or printed.
- **Download**: Downloads the Report PDF file to the user‘s download directory on the local host.

12.10 Detail View - HTTPS

The Detail View for HTTP/HTTPS objects shows additional information, like some object **Details**, about the HTTP/HTTPS Web Service for which the Detail View has been opened.

If the Web service has been configured successfully, the starting page of the Web Service can be opened using the link **Home Page**.

Objects of the HTTP/HTTPS type are usually detected automatically by Discoveries and added to the OpenScape FM objects.

In addition, they can be manually added to a host by accessing its configuration (see *Section 13.1*) and adding and configuring an element of the type **HTTP Server**.

More about HTTP/HTTPS objects can be found in the *IP Manager User Guide*.

Actions

- **Modify**: This action opens the configuration view for the current Web Service to edit its configuration (see *Section 13.3*). For example, a certificate can be accepted there.

12.11 Detail View - OpenScape 4000 Manager

The Detail View of an OpenScape 4000 Manager is an extended version of the Host Detail View.

It provides an additional sub page **OS4K Manager**. that is handled in this sections. The other sub pages of the Host Detail View are described in *Section 12.4*.

The OS4K Manager sub page itself consists of two tabs:

Details:

The tab **Details** provides manager information such as the status of the sub agents (table **State**), the alarms (tables **Alarms On** and **Alarms Off**) and the CMI nodes (table **Systems**).

In addition it shows the **Domain Ports** used by the manager, and it provides a link to the manager itself (**Manager Web Access**).

It also shows some information about the OpenScape FM object representing the OpenScape 4000 Manager like the objects **Status History**, some general **Object Information** and a table containing the currently **Unacknowledged Correlated Events** for the object.

Configuration:

The tab **Configuration** can be used to configure the database connection and how the OpenScape 4000 topology should be displayed for the manager.

The checkbox **Use JDBC** defines, whether a JDBC connection should be used for the manager at all.

If this is the case, the following parameters can be configured to use with this connection:

- **JDBC Login**, **JDBC Password** define the credentials to be used for the database selected in the menu **Database Name**.
- The checkbox **JDBC SSL** defines whether an encrypted JDBC connection should be used.
- The checkbox **Trunk Group Topology** defines, whether the trunk based (unchecked) or the trunk group based topology (checked) should be used.
- If JDBC is selected for the synchronization, the **KNDEF-Options** can be used to determine which of the virtual node numbers should be considered for the topological display: *None*, *All* or only those that are evaluated as *Default* by the AMO KNDEF.

12.12 Detail View - OpenScape 4000 System

The Detail View of an OpenScape 4000 System is an extended version of the Host Detail View.

It provides an additional sub page **OpenScape 4000**. that is handled in this sections. The other sub pages of the Host Detail View are described in *Section 12.4*.

The sub page OpenScape 4000 contains a number of tables the show all available information about the OpenScape 4000 system. This data includes the sections **Faults**, **Topology/Trunks**, **Hardware**, **Software** and **Discovery**.

In addition it shows some general **System Info**, and it provides a link to the manager of the system (**Manager Web Access**).

It also shows some information about the OpenScape FM object representing the OpenScape 4000 System like the objects **Status History**, some general **Object Information** and a table containing the currently **Unacknowledged Correlated Events** for the object.

12.13 Detail View - OpenScape Voice Universe

The Detail View for OpenScape Voice Universes objects shows additional information about the OpenScape Voice Universe for which the Detail View has been opened.

By using the textfield **Comment** and the **Save** button located on the right side of the textfield, Comments for the OpenScape Voice Universe can be created or modified. The **Discard Changes** button located below the *Save* button can be used, to revoke the modifications made after the last Save.

The Technology *OpenScape Voice* that contains OpenScape Universes is described in *Section 9.1*.

Actions

Most of the following actions are only available, if a correct SNMP Configuration has been made for the respective OpenScape Voice.

The actions **Active Alarm Table** and **Event Table** are only available, if an OpenScape Voice SNMP Agent has been discovered and at least one of the OpenScape Voice Switches belonging to the OpenScape Voice Cluster

- **Active Alarm Table**: This action opens a separate tab which displays all events stored in the Event Table for which a reference exits in the Active Alarm Table (`rtpArmAlarmTable`) of the OpenScape Voice Switch. The OpenScape Voice Documentation should be used for further information about the displayed data.
- **Event Table**: This action opens a separate tab which displays all events stored in the Event Table (`rtpEvtTable`) of the OpenScape Voice Switch. The OpenScape Voice Documentation should be used for further information about the displayed data. The events are requested and displayed in reverse order of their creation date, therefore the latest event will be shown topmost.
- **Endpoints**: This action lists the assigned Endpoints on a separate tab.
- **OpenScape Branches**: This action lists the assigned OpenScape Branches on a separate tab.
- **Cluster Info**: This action opens a separate tab which provides general information about the OpenScape Voice Cluster (e.g. Name, Operation Mode, IP Node1).
- **Unmanage**: This action sets the current OpenScape Voice Universe to *Unmanaged*.
- **Manage**: This action sets the current OpenScape Voice Universe to *Managed*.
- **Object Information**: This action provides general information about the object that represents the OpenScape Voice Universe within the OpenScape FM.

12.14 Detail View - OpenScape Voice Cluster

The Detail View for OpenScape Voice Clusters objects shows additional information about the OpenScape Voice Clusters for which the Detail View has been opened.

By using the textfield **Comment** and the **Save** button located on the right side of the textfield, Comments for the OpenScape Voice Cluster can be created or modified. The **Discard Changes** button located below the *Save* button can be used, to revoke the modifications made after the last Save.

The Technology *OpenScape Voice* that contains OpenScape Clusters is described in *Section 9.1*.

Actions

- **Cluster Info**: This action opens a separate tab which provides general information about the OpenScape Voice Cluster (e.g. Name, Operation Mode, IP Node1).
  This Actions is only available, if a correct SNMP Configuration has been made for the respective OpenScape Voice.
- **Unmanage**: This action sets the current OpenScape Voice Cluster to *Unmanaged*.
- **Manage**: This action sets the current OpenScape Voice Cluster to *Managed*.

- **Object Information**: This action provides general information about the object that represents the OpenScape Voice Cluster within the OpenScape FM.

12.15 Detail View - OpenScape Voice Component

The Detail View for OpenScape Voice Universes objects shows additional information about the OpenScape Voice Component for which the Detail View has been opened.

By using the textfield **Comment** and the **Save** button located on the right side of the textfield, Comments for the OpenScape Voice Component can be created or modified. The **Discard Changes** button located below the *Save* button can be used, to revoke the modifications made after the last Save.

The Technology *OpenScape Voice* that contains OpenScape Components is described in *Section 9.1.*

Actions

- **Show Event Description**: This action displays an excerpt of the OpenScape Voice Manual that contains a list of the possible alarms and their corrective actions.
- **Unmanage**: This action sets the current OpenScape Voice Component to *Unmanaged*.
- **Manage**: This action sets the current OpenScape Voice Component to *Managed*.
- **Object Information**: This action provides general information about the object that represents the OpenScape Voice Component within the OpenScape FM.

13 Configuration

This chapter describes how new objects can be added to the OpenScape FM by using the Web Client, and how objects already known by the OpenScape FM can be reconfigured.

Currently the following basic types of objects can be added or reconfigured:

- **Hosts** (see *Section 13.1*). This basically stands for every object with one or more individual IP addresses. For example switches or OpenScape 4000 systems are also added as Hosts.
- **Networks** (see *Section 13.2*). Here Networks can be added, configured or hidden.
- **HTTPS** (see *Section 13.3*). Here Web Services can be configured.
- **Reports** (see *Section 13.4*). Here Reports can be created or reconfigured.
- **Monitors** (see *Section 13.5*). Here the Monitors monitoring a specific Host can be configured.
- **Services** (see *Section 13.6*). Here Services can be created or reconfigured.

13.1 Host Configuration

With the help of the Host Configuration it is possible to add Hosts within the Web Client in the OpenScape FM, to set them up and to configure the methods of their monitoring.

In this context, *Host* stands for virtually any object that has an IP address. This includes in particular technology specific objects such as OpenScape 4000 systems.

The following sections describe how to add new Hosts (see *Section 13.1.1*), how to edit the configuration of a single Host already known by the OpenScape FM (see *Section 13.1.2*) and how to configure more than one Host simultaneously (see *Section 13.1.3*).

13.1.1 Add Hosts

The function to create a new Host object within the OpenScape FM is triggered by the Action **New**. This can be found in the action list of categories and technologies whose central list consists of Hosts.

This action opens the **Add Host** configuration window.

In this window the Host Name, an Alias or the IP Address of the object to be added to the OpenScape FM can be entered.

If an IP address is entered, the OpenScape FM tries to determine a suitable host name. If this is successful, this name is used as the name of the new IP node.

If the **Next** button is clicked, a corresponding object is created and the OpenScape FM automatically performs a standard discovery for the entered Host Name or IP Address (see *Desktop User Guide*).

The results of the discovery are displayed in the form of a list. Each row displayed corresponds to a discovery rule that matches.

Afterwards, the user has three buttons at his disposal to select the further procedure:

- **Cancel**: The temporarily created object is removed from the OpenScape FM and the configuration window is closed.
- **Save**: The new object is provided with the properties found by the discovery and the configuration window is closed. This corresponds to adding an object in the Classic Java Client. If the configuration window has been opened for a specific category or technology, a configuration block for the corresponding category/technology is automatically added to the object.
- **Edit**: The object is created as for **Save**. The *Modify Host* configuration window (see *Section 13.1.2*) is then opened automatically for further configuration of the object.

For all created host objects, the configuration can also be modified at any later time by using the Modify configuration window (see *Section 13.1.2*).

13.1.2 Configure Individual Host

The function for the configuration of an existing Host object within the OpenScape FM is triggered by the action **Edit**. This can be found in the action bar of Categories and Technologies, whose core list consists of Hosts. If multiple Hosts were selected, the multiple configuration page opens instead (see *Section 13.1.3*).

The action opens the **Modify Host** configuration window for the currently selected Host object.

In the upper part the window contains the name of the affected Host (**Hostname**) and its Display Name (**Display Name Format**).

Underneath is always the general block **Settings**. This block is present for each Host, cannot be deleted and contains settings that correspond to the IP Parameter configuration of the Classic Java Client (see I*P Manager User Guide*).

If a general technology, such as OpenScape 4000 or OpenScape Business, has been detected for the Host, an additional technology-specific block is displayed, in which further specific parameters can be configured.

The configuration data of the **Blocks** can be shown or hidden by using the **>** symbol on the left side of the corresponding block.

When the data display is expanded, technology-specific blocks can be removed using the red trash can icon located to the right of the block header.

Which properties of the Host are monitored or should be monitored can be viewed or set on the **Monitoring page** of the Host. This is opened using the button **+ Configure Monitoring**.

The Monitoring page consists of two areas:

- On the left, a list of all **Available Monitors** is displayed. Each of these Monitors corresponds to an independent Monitor Type. Mostly, but not always, these are actually System Management Monitors (see *Chapter 11*).

  If a check mark is displayed in the column **Active**, this Monitor Type is currently already set up for the Host.

- On the right, the configuration of the Monitor currently selected on the left is done.

  For some Monitor Types, such as monitoring *SNMP Agents* or *Web Servers*, multiple Monitors can be set up for a Host. These are each configured in a separate tab on the right. By clicking **+ Add** a new Monitor can be added, by clicking the **X** in front of the respective tab name an existing Monitor can be removed.

  Such Monitor Types are *Active* if at least one corresponding Monitor has been set up for the Host.

  For other Monitor Types, such as *Basic Monitoring* or the monitoring of *Windows Services*, only at most one Monitor can be set up for a Host. These types are set up and thus *Active* if the **Check Mark** is set in front of the heading of the configuration area within the header of the right-hand area.

For example, an HTTPS-based Web Service can be set up for the monitoring on the Host by pressing the button **+ Configure Monitoring** and selecting **Web Server** from the list of **Available Monitors**.
Via **+ Add** a new Web Server can then be added on the right and its monitoring can be configured.

Important Note:
Depending on the Discovery Rules, some Monitors may be created automatically when the next Discovery of the Host is performed, even if they were previously manually removed during configuration.

Once the configuration is complete, it can be confirmed using the **Save & Close** button.

Note:
If Status Poll relevant settings have been changed, a Status Poll (see *IP Manager User Manual*) is automatically executed.

The button **Cancel** discards the changes made. If the Host was newly created immediately before the configuration, **Cancel** returns to the Discovery window (see *Section 13.1.1*).

13.1.3 Configure Multiple Hosts

The function for the configuration of an existing Host object within the OpenScape FM is triggered by the action **Edit**. This can be found in the action bar of Categories and Technologies, whose core list consists of Hosts. If only a single Host was selected, the individual configuration page opens instead (see *Section 13.1.2*).

The page allows to set various parameters for all selected Hosts at the same time.

If a certain property has the same value for all Hosts (e.g. Polling Time), this value is displayed. Otherwise, the corresponding field is empty.

To change a particular property, the **checkbox** in front of the property must be marked. When the user interface is closed by clicking the button **OK**, the marked properties are then set for the selected Hosts.

The configuration page consists of three sub pages:

IP Parameters

Here the IP parameters for the selected Hosts can be configured.

The possible entries correspond to the entries for the default settings of IP parameters (see *Section 14.7.1*).

SNMP Parameters

Here the SNMP parameters for the selected Hosts can be configured.

The possible entries correspond to the entries for the default settings of SNMP parameters (see *Section 14.7.2* and *Section 14.7.3*).

Which SNMP configuration of a Host is changed is determined by the following logic:

- If *no* SNMP configuration has been assigned to a Host so far, the new selection becomes the default setting for the Host.
- If *exactly one* SNMP configuration is assigned to a Host, this is replaced by the new selection.
- If *multiple* SNMP configurations are assigned to a Host, only a configuration that affects SNMP port `161` is overwritten by the new selection.

Display Name Format

Here it is defined how the symbol label for newly discovered hosts should look like.

Hint:
Macros can and should be used, otherwise the same label would be assigned to all selected Hosts.

13.2 Network Configuration

With the help of the Network Configuration it is possible within the Web Client to change the settings of Networks or to add new Networks to the OpenScape FM monitoring.

The following sections describe how to add new Networks (see *Section 13.2.1*) and how to edit the configuration of Networks already known by the OpenScape FM (see *Section 13.2.2*).

13.2.1 Add Networks

The function to create a new Host object within the OpenScape FM is triggered by the Action **New**. This can be found in the action list of the category **Networks**.

This action opens the **Add Network** configuration window.

In this window the network address (IPv4 or IPv6), the net mask or prefix length and a name for the network to be added to the OpenScape FM can be entered.

For all created networks, the configuration can also be modified at any later time by using the Modify configuration window (see *Section 13.2.2*).

Important Note:
If a network mask or a prefix length is entered, the entered address will be adjusted accordingly, if necessary.

If the **Scan network** check box is selected, after the network has been created, an address range can be selected in a new window that will be automatically scanned for the existence of hosts with a corresponding IP address.

For all created networks, the configuration can also be modified at any later time by using the Edit configuration window (see Section 13.2.2).

Important Note:
Excluded from later editing is the function **Scan network**. This function can only be initiated once when the network is created. However, a regular scan can be configured by using the **Modify** action (see *Section 13.2.2*).

13.2.2 Configure Networks

The function to configure an existing Network object within the OpenScape FM is triggered by the **Modify** Action. This can be found in the Action List of the Categories **Networks**.

The Action opens the **Modify Network** configuration window for the selected Network object.

Its entries essentially correspond to the **Add Network** window described above (see *Section 13.2.1*)

The function of the initial network scan is replaced by selecting a **Discovery Type**. This determines whether and how the affected network should be regularly scanned for contained hosts.

The following four settings are available:

- **Auto discovery off**: No automatic discovery is performed for the network at all.
- **Discover and add new hosts**: A discovery is performed regularly and newly discovered nodes are automatically created as objects to be monitored by the OpenScape FM.
- **Discover but don‘t add new hosts**: Like the previous item. However, newly discovered nodes are not created, but are merely recorded in a list of new IP nodes. For an affected network, this list can be viewed in the **Networks** category and added to the monitoring manually if desired (see *Section 7.5*).
- **Ignore address range**: This action completely removes the network or subnetwork from monitoring. Using the procedure described in the *IP Manager User Guide* (see *Adding an IP Network - Ignore Address Ranges*), such a network can be displayed again.

Checking the **Auto Delete** checkbox specifies that the IP network container will be deleted automatically when the last IP node of the network is deleted.

13.3 HTTPS Configuration

With the help of the HTTPS Configuration it is possible within the Web Client to change the settings of HTTP based web services or to add new web services to the OpenScape FM monitoring.

The following sections describe how to add new HTTPS objects (see *Section 13.3.1*) and how to edit the configuration of such objects already known by the OpenScape FM (see *Section 13.3.2*).

13.3.1 Add Web Service

Many HTTP/HTTPS based Web Services are automatically detected, configured and assigned to the host running the service by the OpenScape FM during a Discovery.

Such web services can be created manually via the **Configuration Window of the respective Host** (see *Section 13.1.2*).

To do this, the type **HTTP Server** has to be selected once for each Web Service.

The following parameters can then be configured:

- **Port**: The port on which the Web Server listens.
- **HTTPS**: This checkbox determines whether the server uses the HTTP (unchecked) or HTTPS communication protocol (checked).
- **Accept Certificate**: If the HTTPS communication protocol is selected, this checkbox can be used to specify that self-signed certificates are to be accepted automatically by setting the check mark.
- **HTTP Login**, **HTTP Password**: These two text fields are used to define the access values to be used.

If the **Test** button is clicked, the OpenScape FM tries to contact the service on the specified port. This attempt is considered successful if any reply is received from the service. Since rejections are also considered as successful, HTTP login, HTTP port and possibly existing certificates are ignored.

13.3.2 Configure Web Service

A HTTP/HTTPS based web service already known by the OpenScape FM can be configured in the following two ways:

- From the **Configuration Window of the Host** on which the Web Service is running (see *Section 13.1.2*):

  Here a block of the form **HTTP(S)-Server Port** with the corresponding port number is found for each configured Web Service.
- From the **Detail View for the Web-Service** itself (see *Section 12.10*):

In both cases, the same parameters can be changed as for a new creation (see *Section 13.3.1*). However, the assigned **Port** uniquely defines the Web Service and remains fixed after the creation.

13.4 Report Configuration

Reports can be created or modified using the Report Configuration.

A new report is usually created by triggering the action **Report** for a selected object. This can be done for selected list elements or from Detail Views. Alternatively, this can be done using the Navigation Area, selecting **Reporting->Reports** (see *Section 8.1*), and executing the action **New**.

A report saved as a Template (see *Section 13.4.3*) can be modified by selecting the item **Reporting->Templates** (see *Section 8.2*) in the Navigation Panel, selecting the desired Template in the list that opens and executing the action **Modify**.

In both cases, the **Report Center** opens where the Report can be customized and executed.

The Report Center consists of a subpage each for defining the desired Report (see *Section 13.4.1*), for displaying the newly created Reports (see *Section 13.4.2*) and to create Templates (see *Section 13.4.3*).

13.4.1 Create Report

Reports can be created on the subpage **Report Configuration** or, if the page is opened for a Template (see *Section 8.2*), Report Templates can be modified.

The list of **Report Objects** displays the objects that are to be considered in the Report. This list is only displayed if the report was created for one or more specific objects.

The Report Type to be created can be defined in the **Report Selection** menu.

In the area below, the period to be taken into account for the displayed values is selected. Either a start time (**From**) and an end time (**To**) or alternatively an interval up to the current time under **Time period until now** can be defined.

Either *PDF* or a comma-separated value list (*CSV*) can be selected as the output **Fileformat**.

The menu below **Database Source** determines whether all collected individual data is to be taken into account for the Report (*Raw Data Absolute*) or whether the data will be aggregated as average values over time intervals (*Hourly*, *Daily*, *Weekly*, *Monthly*).

This data is sufficient to display the standard information of the selected Report Type.

If *None (Raw Values)* is selected as **Calculation Type**, two additional displays can also be selected:

If the checkbox **Show Summary** is set, additional top10 host summaries are added to the Report. These include diagrams with the 10 systems with the highest last values, the highest average values, the highest maximum values and the lowest minimum values.
This summary is only possible for parameters with numeric values and it is assumed that the parameters use the same unit for all hosts.

- If the checkbox **Show additional TOP 10 Values per Parameter** is set, additional top10 host summaries are added to the Report. These include diagrams with the 10 systems with the highest last values, the highest average values, the highest maximum values and the lowest minimum values.
  This summary is only possible for parameters with numeric values and it is assumed that the parameters use the same unit for all hosts.
- If the checkbox **Show additional table** is checked, the collected value histories are also added to the Report.

Other selections in the **Calculation Type** menu leads, depending on the selection, to an overview of the maximum, minimum or average values (or all three) within the intervals selected under **Period Type**.

Under **Show colored Severities** it can be specified whether only the most extreme three values per parameter or all values are to be displayed in their status color. This option does not apply if the calculation is based on averages, as in this case a status could be assumed for which there was not a single actual value determined.

Entries in the **Report Comment** area are inserted on the first page of the created Report.

If **Show Host Comments** is marked, possible existing comments for the handled host object will also be displayed.

Under **File and Forward** it can be set whether the result of the report execution should be stored as a file (**Store Report** is checked), and/or whether it should be sent as an email attachment (**Email Forwarding** is checked and configured).

The button **Generate Report** creates the corresponding Report. Depending on the selection of the output type described above, the result is displayed on the Show Report subpage (see *Section 13.4.2*), or an email is sent to the specified recipient.

If the configuration page has been opened for a Template (see *Section 8.2*), adjustments can be saved using the button **Save Template**.

If the configuration page has been opened for a Report, it can also be saved as a Template using the button **Save as New Template**.

The button **Close** closes the configuration window without saving any changes.

Note:
All reports are created in UTF-8 format.

13.4.2 Show Reports

The subpage **Show Reports** lists the just created Reports.

Reports indicated by a green (*normal*) status bubble are finished.

Reports indicated by a light blue (warning) status are also finished but contain no data.

By using the action icons, finished Reports can be downloaded or displayed on screen.

A list of all Reports visible for the current user can be found in the Navigation Panel using **Reporting->Reports** (see *Section 8.1*).

13.4.3 Create Template

If the report just created on the **Create Report** subpage (see *Section 13.4.1*) should be executed at a later time, it can be saved as a Template on the **Create Template** page.

To do so, a descriptive name must be assigned in **Template Name** and the **Save Template** button has to be clicked.

If the Report should be triggered by a Time Schedule, an email sender and recipient can also be defined. If several recipients should be notified, their addresses can be separated with a semicolon.

Saved Templates can be found in the Category **Reporting->Templates** (see *Section 8.2*). Here they can be opened, modified and the defined report can be executed.

Important Note:
The list of affected hosts is not flexible for all Reports!
While e.g. Templates for Networks determine the hosts during the creation of the Report, the identification of the hosts for Host Types is done once during the creation of the Template.

13.5 Monitor Configuration

The Monitor Configuration can be used to configure the individual Monitors that monitor a selected Host.

Important Note:
In order to run a Monitor on a target system, appropriate access rights are required (see *Section 13.5.2.1*).

The Monitor Configuration can be opened from within the Detail View of the respective Host (see *Section 12.4*).

It is started from the page **Monitoring** using the action **Manage Monitors**.

13.5.1 Overview Table

On the left, the configuration page contains a list of the **Available Monitors**.

Monitors marked in the column **Active** are currently active for the current host. The other monitors are not currently performed for the host.

The name of the Host is displayed in the column **Monitor**. If an **asterisk** (*) is displayed behind the name, the corresponding Monitor has been reconfigured and the change has not yet been saved. If the name is additionally displayed in **red**, the Monitor has been deactivated.

Save & Close stores the changes of the Monitors marked with a asterisk, **Cancel** discards the changes.

13.5.2 Configuration

If a Monitor gets clicked within the Overview Table, its configurations settings appear in the right half of the configuration page.

In the topmost row the selected Monitor can be activated or deactivated (**Activate**).

If it is activated, the rest of the settings can be modified.

The possible settings are dependent on the respective Monitor. But a number of settings are identical or very similar.

The following sections describe these settings. Monitor specific parameters are handled in *Section 11.2.1*.

13.5.2.1 General Settings

Almost all Monitor configurations start with the same first elements:

- A **Start/Stop Button** allows to pause or restart the regular execution of the Monitor.
- A **Description** introduces the function of the monitor.
- A block named **<Name of the Monitor> Settings** that contains:
  - A menu to select the **Monitoring** System Management **Agent**.

- The **Execution Interval**. This determines the time intervals at which the Monitor should be executed.

  If a termination interval should be defined for the execution of a monitoring script, this can be done in the Expert Settings (see *Section 13.5.2.4*).

- The checkbox **Data Export for Reporting** determines whether the monitor data should be exported (e.g. to evaluate them within a report at a later time).
- The fields **Login** and **Password** to select the credentials to be used when running the Monitor.
- In some cases a **Test** button is provided for a configuration block. Pressing the button checks the current configuration by performing a trial run.

If a Monitor collects the data for different Parameters, there may be individual configuration blocks for these. The structures described here are then available for each of these blocks.

In this case there can be a default block as a preset for all Parameters. This then has the name **<Name of the Monitor> Common Settings**.

13.5.2.2 History / Value Storage

In the area **History / Value Storage**, it can be defined how many data records are to be kept in the database for the monitor. If the corresponding number is exceeded, new results replace the oldest result still stored.

- **History**
  The number of result values stored for each Parameter of the Monitor.

  Default setting: 288. This corresponds to the data of one day if the Monitor is executed every 5 minutes.

- **History - Hourly Average**
  The number of calculated hourly averages stored for each Parameter of the Monitor.

  Default setting: 168. This corresponds to the data of one week.

- **History - Daily Average**
  The number of calculated daily averages stored for each Parameter of the Monitor.

  Default setting: 90. This corresponds to the data of three months.

- **History - Weekly Average**
  The number of calculated weekly averages stored for each Parameter of the Monitor.

  Default setting: 52. This corresponds to the data of one year.

- **History - Monthly Average**
  The number of calculated monthly averages stored for each Parameter of the Monitor.

  Default setting: 72. This corresponds to the data of six years.

- **Monitor History**
  The number of Monitor return values stored for the Monitor.

  Default setting: 288. This corresponds to the data of one day if the Monitor is executed every 5 minutes.

13.5.2.3 Thresholds

The area **Thresholds** determines how the result values of a Monitor affect monitoring

The area consists of a table, which contains one rule per line. Each of these rules consists of a parameter selection, a threshold condition, a status value and an associated message text.

With **+** and **-** new table lines can be created or the selected line can be deleted.

If the monitor measures a new value for one of its parameters, all rules are taken into account that apply to the parameter according to the parameter selection and for which the threshold condition applies according to the currently measured parameter value.

The 'most critical' status value of all these considered rules is assigned as status to the parameter. In addition, if the status differs from the previous status of the parameter, an event is generated with the configured message text of the corresponding 'most critical' rule.

,'More Critical' in this context simply stands for the importance of the status value
(*Critical* > *Major* > *Minor* > *Warning* > *Normal*)

A rule consists of the following components:

- **Parameter Name**
  The *name of the measured parameter* that should be compared, or *All*, if the rule should be used for all parameters.
- **Value**
  Specifies which value is to be taken into account in the threshold query. This is either the current parameter value itself, or an average of the last parameter values.
- **Comparison**
  The method with which the expression is compared with the value.
- **Threshold**
  A specific numerical value with which to compare.
- **Trigger at**
  Determines how many times the threshold condition must apply to the parameter in immediate succession before this threshold applies.
- **Reset at**
  If the threshold previously applied to the parameter, this value determines how often the threshold condition may no longer apply to the parameter in immediate succession so that this threshold no longer applies.
- **Status**
  The status that will be assigned to the Parameter if the threshold matches.
- **Message Text**
  The text of the generated event when the status of the Parameter changes.

If the monitor has already been executed once and parameters exist, a selection list is offered for the **Parameter Name** column in the corresponding configuration field, in which the individual parameter names can be selected

Important Note:
The preset thresholds usually apply to all Parameters of a Monitor (**Parameter Name**: `All`).
If an individual parameter is to be configured separately, new entries can be created in the table for it using the **+** button, the corresponding **Parameter Name** selected and the desired **Threshold Condition** configured.
Since only the first applicable condition is executed when evaluating the table, conditions for specific parameters should be placed ahead of the general conditions in the table.

This leads to the following behavior:

If the name of the measured parameter corresponds to the ***[Parameter Name]*** and the ***[Value]*** matches the ***[Threshold]*** according to the *[comparison operator* ***Comparison]*** for the ***[Trigger at]***-th time in succession, the parameter is assigned the status ***[Status]*** if no 'more critical' rule also applies. If the parameter previously had a different status, an event with the message ***[Message Text]*** is generated

If the ***[Threshold Condition]*** on it does not match ***[Reset at]***-times in a row, the threshold no longer applies to the Parameter, else it stays valid.

13.5.2.4 Expert Settings

The area **Expert Settings** contains access options for SSH parameters for an authenticated data transfer and directly for the Monitor's configuration file.

For some Monitor Types further type specific parameters can be configured (see *Section 11.2.1*).

SSH Authentification

In a number of fields the connection data for an authenticated data transfer via SSH can be configured (see tooltips of the corresponding fields).

For example, the path to the SSH Key File or the SSH Gateway Host to be used can be set here.

Configuration File

The button **Edit XML** opens a window containing the configuration file of the Monitor. This XML file contains, among other things, the values that were set for the Monitor during the configuration described above.

The window allows manual editing of this file. However, this should only be done in special exceptional cases and with caution.

Timeout

If a script is executed for a Monitor, a maximum runtime can be defined for this script. If this runtime is exceeded, the execution of the script is aborted.

The entry in the field **Timeout** defines after how many seconds runtime a script should be aborted.

The runtime has a default value of 60 seconds, and an allowed minimum of 2 seconds.

If the checkmark in front of **No Timeout** is marked, the runtime control for the corresponding script is switched off.

13.6 Service Configuration

The following sections describe the creation of a new Service (see *Section 13.6.1*) and the editing of the configuration of a Service already known by the OpenScape FM (see *Section 13.6.2*).

13.6.1 Add Service

To create a new Service, on the overview page of the category **Services** (see *Section 7.7*) the action **New** can be selected.

This action opens a creation window where a **Name** for the new service can be defined. This name should be unique and should clearly identify the service.

In addition, the menu **Target Container** can be used to specify where the new service should be created within the object tree. This makes it possible to sort the individual services within a user-defined object structure.

Displayed is the topology container `root->ECE`, and all topology containers below this container.

If a service has been newly created, the further configuration corresponds to the editing of an already existing service (see *Section 13.6.2*), and the corresponding configuration window is automatically opened.

13.6.2 Edit Service

The Service Configuration opens when a new Service has been created (see *Section 13.6.1*), or a Service has been selected in the Category **Services** overview (see *Section 7.7*) and the action **Edit** has been executed.

The Service Configuration consists of the following three pages:

- A Service is a collection of objects that have a logical relationship to each other and are to be evaluated and monitored together.

  Depending on the configuration of the object context, a value for the current availability of the Service is determined based on the current status values of the objects contained in the Service. The value is a percentage value from `0` (poor) to `100` (perfect).

  The definition takes place on the page **Service Elements** (see *Section 13.6.2.1*).

- From the determined current overall availability of the Service, a current status of the Service itself is determined.

  How this should be done is defined on the page **Service Status** (see *Section 13.6.2.2*).

- In addition, the average availability of Services within defined time intervals can be determined.

  The definition of these time intervals and the determination of the server status for these time intervals is done on the page **Average Availability** (see *Section 13.6.2.3*).

13.6.2.1 Service Elements

On the page **Service Elements** it can be defined which objects are to be monitored by the Service and how the status of the entire Service is to be determined from the status values of the individual monitored objects. In addition, the Name of the Service can be changed here.

The central element of this page is the service tree, which displays all elements of the service and their evaluation rules.

A service and therefore also the service tree always consists of two types of service elements:

- **Service Components** each determine their *Availability Value* from the Availability Values of their child objects. In the column **Availability**, a **selection menu** is used to determine how this calculation is to be made. In addition, the current Availability Value is also displayed in this column.

  The *root node* of a service tree is always a Service Component. This component represents the Service itself. The Availability Value of the root node thus corresponds to the Availability Value of the entire service.

  A status for the Service itself is determined from the Availability Value calculated for the root node. How this is done is defined on the page **Service Status** (see *Section 13.6.2.2*).

  The **Names** of the Service Components should be chosen in such a way that the purpose of the component is recognisable. The Name of the root node corresponds with the **Name of the Service**.

  The **i symbol** in the column **Details** can be used to open the detailed view of the corresponding Service Component. This contains, among other things, a list view of the child objects of the component.

- **Monitored Objects** are any OpenScape FM objects from whose status the availability value of the Service should be calculated.

  In the column **Status** there is a **pencil symbol** for each object to be monitored. If this is clicked, a window opens in which it can be determined for the object which object status should correspond to which Availability Value of the object.

Adding Service Components

Service Components are added by selecting an existing Service Component in the Service Tree (clicking on the corresponding row) and executing the action **Service Component**.

A name and method for the availability calculation can now be selected.

The new Service Component is entered into the service tree as a child object of the previously selected component.

Changing Service Names

To do this, only the **Name** of the root node of the Service must be changed.

Adding Monitored Objects

Monitored Objects are added by selecting an existing Service Component in the Service Tree and performing the action **Monitored Object**.

An object selection window opens in which one or more objects can be selected.

The selected objects are entered into the Service Tree as child objects of the previously selected component.

Deleting Service Elements

Service elements, whether Service Components or Monitored Objects, can be removed from a Service by selecting them in the service tree and executing the action **Delete**. This removes the selected element and all child elements from the tree.

Example*:*

A WebStore service should be monitored. The service consists of two redundant database servers (Database1 and Database2) and two redundant web servers (Web1 and Web2).
The service is functional when at least one database server and at least one web server is running.
The service shall have the following status:
Critical: Both database servers and/or both web servers are in the status *Critical*
Minor: One of the two database servers and/or one of the two web servers is in status *Critical*
Normal: All four servers are in status *Normal*.

For this example, it makes sense to combine the two database servers and the two web servers each under a separate Server Component, which is located directly under the root node. The rule *Average* can be used for both components. The components then only become *Critical* if both servers are *Critical*, and also only become *Normal* if both servers are *Normal*.

For the root node itself, the *Minimum* rule should be set here, as the service will fail if only one of the two server groups fails.

13.6.2.2 Service Status

On this page, it can be configured how the availability of the Service affects the Service Status.

For each status from *Critical* to *Normal*, it can be defined for which availability value the Service Components of the Service are to assume this status. The availability value of the root node then also provides the status of the entire Service using this configuration..

The table always covers all values from `0` (poor) to `100` (perfect).

Clicking on one of the greater than or less than buttons changes it from e.g. less than/equal to less or vice versa. The respective counterpart in the neighboring row is adjusted accordingly.

The desired percentage values can be entered manually in the number fields. Here, too, the matching counterpart in the neighboring row is adjusted in each case.

If a status should only be assumed for an exact availability value, this value can be entered simultaneously as less than/equal and greater than/equal in the corresponding line.

If a status should never be assumed at all, the value can be entered simultaneously as smaller and larger in the corresponding line.

13.6.2.3 Average Availability

This page defines how an average availability should be calculated for the Service over predefined time intervals. The page is divided into three sections:

- In the section **Average Availability Calculation** is configured how the individual intervals should look like.

  The menu **Calculation Period** determines how long the respective intervals should be. If *Deactivated* is selected, no calculation of the average availability over time intervals takes place for the Service.

  Depending on the selection of the period length, the following four lines define when exactly the respective interval should start. For example, it can be specified that the interval should always start monthly on the third day of the month at 3.30 am. Or weekly always on Tuesday at 2 o'clock.

  The line **Refresh** specifies how often within the respective interval the current availability should be evaluated and taken into account for the average.

- The section **Next Intervals** shows what the current interval and the two following intervals would look like if the specifications in the first section were valid. This section serves to check whether the specifications in the first section correspond to the desired result.

- In section **Avarage Availability Event Status**, it can be defined how the average availability value determined for a time interval is to be converted into a status for the Service. The configuration corresponds to the procedure for determining the status for current availability values (see *Section 13.6.2.2*).

14 Administration

This chapter describes the administrative tasks and configurations that could be handled through the OpenScape FM Web Client.

To define these tasks and configurations, Administrator rights are needed.

To just view the configuration settings, *Operator* rights are sufficient. For actions an Operator cannot access (like e.g. *New* or *Delete*), a respective error message will appear.

The next section provides an introductory overview about the basics of the administrative options within the Web Client. The following sections elaborate on the individual options.

14.1 Overview

The administration of the OpenScape FM within the Web Client is performed on a dedicated Administration page. This is automatically opened in a separate browser page when the menu entry **Administration** is clicked from within the User Menu (see *Section 4.2*) of the Web Client. The User Menu of the Administration Page corresponds to those of the normal Web Client view.

Reversely, the 'normal' Web Client can be opened in a new page from the user menu of the administration page by using the menu entry **Web Client**.

The individual main areas of the administration are accessed via the **Navigation Panel** located on the left. The main views of the respective areas can be opened via the individual entries located in the Navigation Area:

Assistants opens the starting page of the Administration (see *Section 14.2*). The page provides fast access to some basic administrative tasks. This page will also be opened when the logo located left within the Header Bar of the administration page is clicked.

Access & Rights enables the creation and configuration of Users and User Groups (see *Section 14.3*).

Monitoring allows the configuration of System Management Parameters for general monitoring (see *Section 14.4*).

Notification Center enables the configuration of automatic actions for incoming Events (see *Section 14.5*).

Server Settings allows the configuration of basic OpenScape FM parameters like e.g. the mail server to be used or of certificates (see *Section 14.6*).

IP Settings can be used to define the default IP and SNMP settings and to set the polling intervals (see *Section 14.7*).

Certificates is used to show and configure the used certificates (see *Section 14.8*).

Maintenance Windows can be used to define or view maintenance windows (see *Section 14.9*).

Logfiles allows to read the content of some of the logfiles (see *Section 14.10*).

14.2 Assistants

Assistants opens a window that contains a number of fast accesses to create new objects.

The different buttons each open a new browser tab in which the appropriate configuration window for a new addition is open.

This allows a quick creation of a **Dashboards** (see *Section 6.8*), a **Host** (see *Section 13.1*), a **Network** (see *Section 13.2*), a **Report** (see *Section 13.4*), a **User** (see *Section 14.3.1*) or a **Group** (see *Section 14.3.2*).

For the Technologies **OpenScape Voice** (see *Section 9.1*), **OpenScape 4000** (see *Section 9.2*) and **OpenScape Business** (see *Section 9.3*) quick access buttons exist to create Hosts of this specific Technology.

14.3 Access and Rights Management

The Access and Rights Management of the Web Client enables the creation and configuration of User Accounts (see *Section 14.3.1*) and User Groups (see *Section 14.3.2*).

More about Users and Groups can be found in *Chapter 14 of the Desktop User Guide*.

14.3.1 Users

A **User** defines a single Account which can be used to connect to the OpenScape FM Server.

Each User has a personal set of Access Rights that can be expanded individually or by assigning Groups (see *Section 14.3.2*).

The configuration of a User can be handled on the page **Access & Rights->Users**.

The page contains a list in which each row represents an existing User.

The action **Delete** can be used to delete a marked User.

The action **Change Password** can be used to set a password for a marked User.

The action **Lock** locks the marked user, denying the access to the OpenScape FM. The action **Unlock** withdraws such a lock respectively.

The actions **New** and **Edit** create a new User of allow the modification of a marked existing User. In both cases the configuration window for Users will be opened.

Configuration:

- **Login**:
  The fields **Login** and **Password** (2x, only for new Users) are mandatory and define the name of the account and the password to access the account.

  Bei einer Neuanlage kann hier **Empty until first login** markiert werden. Ist dies der Fall, muss der Anwender bei seiner ersten Anmeldung kein Passwort angeben, dieses aber während der ersten Anmeldung festlegen.

- **Info Data**:
  The following fields are used to enter individual describing parameters for the User. Here e.g. the name, title, email address or phone numbers can be stored.
- **Password Rules**:
  Here it can be defined whether the password should be valid as long as desired (**Password Never Expires** marked), or whether it should have a minimal (**Min Time**, not allowed to be changed before) or maximal (**Max Time**, has to be changed as the latest) expiration time.
- **Locked**:
  If this is marked, the User is currently locked (see above: Actions *Lock* and *Unlock*).
- **Assigned Group**:
  The menu provides a list of all Groups (see *Section 14.3.2*). *One* group can be selected within the list and thus been assigned to the User. Hereby the User gets all access rights that are assigned to this Group.

  Important Note:
  If the Group *Administrator* or any other Group with administrator privileges is assigned to the User, he/she gets, for example via the *Notification Center* feature (see *Section 14.5*), the possibility to start commands on the OpenScape FM server with administrator/root privileges. Such Groups should therefore **only be assigned to trusted persons**.

  Note:
  If more than one Group should be assigned to a User, this can currently only be done through the User Administration of the Java Client (see *Desktop User Guide*).
- **Start View**:
  The menu **Start View** can be used to select the submap that will be shown first to the User when logging in. Here the *Root* node of the Navigation Tree (*Root*), the individual View of the User (*Personal View*), the Network Topology Container (*Network Topology*) or the Start View of the selected Group (*Group View* - (Default)) can be selected.

  If the Group View gets selected, then the control fields **Group Autostarts**, **Group Toolbar** and **Group Favorites** are active.

  If they get marked, respectively the Group Autostart, Group Toolbar or Group Favorites will be used instead of the individual User settings.

14.3.2 Groups

A **Group** is a collection of Users (see *Section 14.3.1*), to which a set of Access Rights is assigned.

In general, in addition to his personal Rights, each User is automatically granted the Rights of all Groups to which he belongs. If Group Rights are changed, this change affects all members of the Group, without having to change the Rights of the Users individually.

A sensible approach is therefore to define tasks, set up a Group with appropriate Rights for each task, and assign a User all the Groups that correspond to the tasks the User should perform.

The configuration of a Group can be handled on the page **Access & Rights->Groups**.

The page contains a list in which each row represents an existing Group.

The action **Delete** can be used to delete a marked Group.

The actions **New** and **Edit** create a new Group of allow the modification of a marked existing Group. In both cases the configuration window for Groups will be opened.

Here for a new creation the **Group Name** can be defined, and in both cases the Group‘s **Description** can be modified.

Group Rights

The permissions of a Group result from a set of objects marked in the **List of Assigned Objects** and **List of Assigned Administrative Permissions**.

- **List of Assigned Objects**

  This list grants permissions for the objects selected in the list and all their child objects within the object tree (see *Section 10.2*).

  The two filters below the header of the list restrict the currently displayed objects to those matching the selection.

- **List of Assigned Administrative Permissions**

  This list grants permissions to all objects that belong to a specific task or technology.

In both cases the following rights can be assigned to the selected objects, and thus also to their child objects:

- **Administrator**: Full read and write permissions allow the use and configuration of the corresponding objects.

  Important Note:
  With Administrator rights, a Group and thus its members can, for example via the *Notification Center* feature (see *Section 14.5*), be given the option to start commands on the OpenScape FM server with administrator/ root rights. Groups with Administrator rights should therefore **only be assigned to trusted persons**.

- **Technical Administrator**: Corresponds to the *Administrator* right with the restriction of the rights management.

- **Operator**: Full read permissions allow working with the corresponding objects while restricting the object configuration and the rights management.

- **User**: Only the viewing of the object hierarchy is possible.

When an object is newly **Marked** in one of the lists, the Group receives the permission selected in the menu **Standard Group Permissions** for the marked object and its children.

If already **Marked**, an individual permission can be assigned within the lists using the column **Permission** and selecting the respective permission within the context menu.

Unmarking a list entry, revokes any rights for the respective object.

By marking A**dd selected objects to start view of group** the root nodes of the selected subtrees are added to the Group Start View

Group Users

The area **Assigned Users** of the configuration page contains a list of all Users that belong to the Group.

The assignment of Users to Groups is handled on the configuration page of the respective User (see *Section 14.3.1*).

Important Note:
For each right (*Administrator*, *Technical Administrator*, *Operator*, *User*) there is initially a Group with a corresponding name, which grants the corresponding right for all objects. From within the Web these Groups can neither be deleted nor modified.

14.4 Monitoring

The Monitoring Administrative Management of the Web Client allows the configuration of the MIBs used by the OpenScape FM and how incoming events for these MIBs should be handled (see *Section 14.4.1*).

14.4.1 SNMP-MIBs

The page SNMP-MIBS contains a table with all (uploaded) MIB definitions known by the OpenScape FM. It can be opened using **Monitoring->SNMP-MIBs**.

Each row within the table represents one MIB known by the system.

The columns show among others the name (**MIB Nam**e) and a short **Description** of the respective MIB.

The column **Activated** indicates whether the MIB is currently taken into account by the OpenScape FM, the column **Version** indicates whether the original MIB definition (`Original`) or a reconfigured MIB definition (`Modified`) is used for the evaluation.

Within the list, selected MIBs can be activated for monitoring by the OpenScape FM or deactivated to end the monitoring (Actions: **Activate** or **Deactivate**). In addition, it is possible to modify for individual MIBs how the OpenScape FM should react to events defined within the MIB (Action: **Modify** - see *Section 14.4.2*).

To find out, for example, in which MIB a certain event is defined, the **Search Field** located above the MIB list and filters can be used.

If this is used, the MIBs are searched for substrings that match the input.

What is being searched for is:

- the OID of variables
- the name of traps or MIBs
- the data type of variables
- the description of traps, variables or MIBs

After the search, the MIB list is limited to the applicable MIBs. The individual MIBs can then be marked to get a display using the action **Explain**, which provides justification as to why the respective MIB was 'found'.

Actions

- **Modify**: Opens the SNMP MIB Configuration for the marked MIB (see *Section 14.4.2*). The MIB has to be *activated* and must contain at least one *Event Type definition*.
- **Delete**: Deactivates the marked MIB definitions and then deletes them.
- **Activate**: Leads to taking the corresponding MIB definitions into account by the OpenScape FM.
- **Deactivate**: The selected MIB definitions are no longer activated. All settings that were made for the corresponding MIB definitions are deleted. Furthermore, all MIB objects that were created based on the corresponding MIB definition will be deleted. However, the MIB definitions remain available and can be reactivated later.
- **Restore Factory Settings**: This action discards all changes made for the event types of the MIB and resets the MIB configuration to the settings that were in place when the MIB was installed.
- **Explain**: After a search (see above) this action opens a window which shows the reason why the marked MIBs were found by the search.

14.4.2 SNMP MIB Configuration

If a MIB gets selected for modification within the SNMP MIB Overview (see *Section 14.4.1*), a configuration window opens for this MIB.

This window shows which traps are defined by the MIB and how the OpenScape FM will treat this traps.

It can also be configured whether the OpenScape FM should create Events within the OpenScape FM for traps of the individual trap types, how these Events should look like, and whether other Events should be automatically be acknowledged by the newly created Events.

The configuration window contains a table in which each row displays the settings for one trap type defined by the MIB.

The parameters shown in der columns are divided into four groups: General parameters, parameters for the creation of Events, parameters to acknowledge other Events and parameters to suppress similar Events.

Important Note:
More about the configuration of trap reactions and the macros that can be used can be found within the *Desktop User Guide,* Chapter*: Event Actions,* Section: *Event Configuration Browser*.

General Parameters

- **Event Type**: The name of the trap type.
- **OID**: The OID that identifies the trap type.

Event Creation

- **Active**: If this is *not* marked, the OpenScape FM ignores events of this type and will not create a respective Event.
- **Message**: The text that will be shown within the column *Description* for events of this type within event tables.

- **Category**: The *Category* that will be assigned to events of this type.
- **Severity**: The *Severity* of the Events created for the Event Type.
- **Flash**: If this is marked, the symbol of the respective object is blinking, if an unacknowledged matching event exists.
- **Client Massage**: If this is marked, a Client Message is generated when a respective event is created.

Acknowledgement of other Events (Expert Options)

- **Name Format**: In order to be able to acknowledge events automatically by later incoming matching events, all events are automatically provided with a key. The *Name Format* describes how the key is to be created from the properties of an event. Each new event automatically confirms all older events with the same key.
- **Name Format Separator**: If more than one key should be generated for an event, the *Name Type Separator* field can be used to specify a symbol with which the string from the *Name Format* field will be split.
- **Reset Name Format**, **Reset Name Format Separator**: Corresponds to the previous two Parameters. If instead of them the Reset Parameters are configured, the current Event will also be acknowledged.

Suppression of Duplicate Events (Expert Options)

- **Duplicate Format**, **Duplicate Time**: Events get a Duplicate Key evaluating the *Duplicate Format*. Within the *Duplicate Time* interval, Events with the same Duplicate Key will be ignored.

Actions

The action **Modify** opens a configuration window in which the parameters described above can be modified for the marked Event Type. The definitions of the parameters may contain macros (see *Section 14.6.2.2*).

14.5 Notification Center

The **Notification Center** can be used to define automatic Notifications for Alarms and/or Events. These Notifications can be an E-Mail, an SMS or the start of a program or script, the contents of which can be determined by the triggering Events.

For each Notification, it can additionally be defined whether it should be triggered again when the triggering Event is acknowledged.

The basic functionality corresponds to the MAR Plugin known from the Java Client (see separate *Mobile Alarm Reaction Plugin User Guide*) and is consistent with it. Actions defined in MAR can therefore also be edited within the Notification Center.

As in MAR, Notifications can also be created within the Notifications Center and assigned to Host Event Types. In addition, they can also be defined simply for an Event Type and thus be valid for all Hosts.

A Notification is triggered when the following conditions are met:

- A matching triggering Event assigned to the Notification is received (or acknowledged) for a configured Host, or for any Host, respectively.

- The Notification is set to **Active** and the triggering time matches the Time Filter assigned under **Execute** (see *Section 14.5.1*).

Note:
During the installation of the Web Client one Notification each of the Types *E-Mail*, *SMS* and *Start Program* will be created. These are meant as examples and *cannot* be deleted.
The examples contain useful configurations and can therefore be utilized as a basis for new Notifications by using the action **Duplicate**.

The Notification Canter consists of the three configuration elements described in the following:

- The page **Notifications**, on which the configured Notifications are displayed, and on which existing Notifications can be modified and new Notifications can be created (see *Section 14.5.1*).
- The page **Events**, on which defined Notifications can be connected independent of the Host to *all* Events of selected Event Types (see *Section 14.5.2*).
- The page **Hosts**, on which defined Notifications can be connected with selected Event Types and selected Hosts (see *Section 14.5.3*).
- The page **Activity Log** on which the automatic logging of safety-relevant activities can be configured (see *Section 14.5.4*).

14.5.1 Notifications

Notifications are actions that can be automatically triggered by an Event. This action can e.g. be the sending of an E-Mail or SMS, or the automatic execution of a Program.

For each Notification it can additionally be defined whether it should also trigger if the triggering Event gets acknowledged.

The configuration for Notifications is displayed by using the page **Notification Center->Notifications**.

This page contains a list of all currently defined Notifications and enables the creation of new ones or the editing of the already defined Notifications. This includes Notifications that were created using MAR.

A Notification can only be executed if it is either connected to a general Event Type (see *Section 14.5.2*) or more specific to an Event Type for a selected Host (see *Section 14.5.3*). How many of such connections exist is shown in the columns **Assigned Events** and **Assigned Hosts**. The respective numbers also provide a link to the lists of the affected Events or Hosts.

For the configuration of Notifications the following actions are available:

New: Creates a Notification of the Type **E-Mail** (see *Section 14.5.1.1*), **SMS** (see *Section 14.5.1.2*), **Start Program** (see *Section 14.5.1.3*), **Syslog** (see *Section 14.5.1.4*), **SNMP Trap** (see *Section 14.5.1.5*) or **Logfile** (see *Section 14.5.1.6*), which is selected at the start of the creation.

Modify: Opens, according to the type, the editing window for the selected Notification. These correspond to the editing windows for the new creation and are preset with the current configuration. The same action can also be triggered by clicking on the link in the **Name** column.

Delete: Permanently deletes the selected Notifications and removes any assignments of these Notifications to Events or Hosts.

Duplicate: Creates a duplicate of the selected notification. The name of the duplicate is extended by the appendix *Copy*. This function can be used, for example, to quickly create 'similar' notifications that should differ for example only in the recipient or the message.

Last Output: Shows the execution result of the last triggering of the selected Notification.

Common Configuration:

Independent of the Type of a Notification, all configuration windows always contain the following parameters:

- **Active**: Only if this is checked, the Notification will be considered for execution.
- **... also on event acknowledge**: If this is marked, another Notification will be send when the Event that triggered the original Notification gets acknowledged.
- **Test**: Creates a Notification according to the configuration. Macros are taken into account and resolved as far as possible.
  Note:
  Macros can access elements of the triggering Event. In this case, the corresponding macro cannot be resolved for the test, and the macro name itself is displayed for the test instead.
- **Name**: Here the name is defined under which the Notification is listed in the selection lists. This should be a unique name and as descriptive as possible.
- **Execute**: If a configured Time Interval is selected here, only Events that occur during the selected Time Interval are taken into account. The selection '*Always*' leads to a consideration of all Events.

Note:
For the actions **Save & Close** or **Test** *Administrator*-Rights are needed.

14.5.1.1 Notifications - Type: E-Mail

By using the configuration window for E-Mail Notifications respective Notifications can be created or modified. It opens automatically when such an action is triggered (see *Section 14.5.1*). This section also describes the general configuration parameters.

E-Mail specific configuration:

- **From**, **To**: The sender and receiver of the E-Mail that will be send.
- **Subject**, **Body**: The subject and content of the actual message (both fields may contain macros).
- **Configure the SMTP server**: This link opens the respective **Server Settings** (see *Section 14.6.1*).

14.5.1.2 Notifications - Type: SMS

By using the configuration window for SMS Notifications respective Notifications can be created or modified. It opens automatically when such an action is triggered (see *Section 14.5.1*). This section also describes the general configuration parameters

SMS specific configuration:

- **Phone Number**, **Message**: The target phone number and the actual text message (may contain macros).
- **COM Port**: The COM Port that should be used to deliver the message.
- **PIN**, **SMS Center**: The PIN number and the number of the SMS Center (both optional).

14.5.1.3 Notifications - Type: Start Program

By using the configuration window for Start Programm Notifications respective Notifications can be created or modified. It opens automatically when such an action is triggered (see *Section 14.5.1*). This section also describes the general configuration parameters

Start Program specific configuration:

- **Program**: The program that will be executed. Including the path, if needed.

  Important Note:
  For security reasons, programs or scripts can only be started from within the following directory:
  `<OpenScape FM Server Installation Directory>\server\start_prog`
  If this restriction should be deactivated, within the folder
  `<OpenScape FM Server Installation Directory>\startup\conf`
  the file `OpenScapeFM.properties` has to contain the entry `enforce.prog.start.directory=false`.

- **Arguments**: The program's transfer parameters (may contain macros).

14.5.1.4 Notifications - Type: Syslog

By using the configuration window for Syslog Notifications respective Notifications can be created or modified. It opens automatically when such an action is triggered (see *Section 14.5.1*). This section also describes the general configuration parameters

Syslog specific configuration:

- **Syslog Host**, **Protocol**, **Target Port**

  The remote **Syslog Host** to which syslog events are send. Either a host name or an IP address can be specified. The **Protocol** in which to send (`UDP`, `TCP` or `TCP_TLS`) and the **Target Port** (default `514`).

  Important Note:
  The OpenScape FM Server itself should never be entered as syslog Host. This could cause a feedback-loop via the build-in syslog server of OpenScape FM.

- **Facility**

  The syslog **Facility** to use (e.g. `USER`, `LOCAL0`, `LOCAL1`).

- **Application**, **Message**

  The **Application** name to be used for the entries in the logging and the **Message** that should be entered.

  The message may contain macros. By using the link **Macro examples...** examples for macros can be displayed (see *Section B.2.4*).

- **Critical**, **Major**, **Minor**, **Warning**, **Normal**

  The severity with which events with the corresponding Status (*Critical*, *Major*, *Minor*, *Warning* or others) should be entered into the logging (`ERROR`, `WARN`, `INFO`).

  Default:
  `Normal` or `Warning` to `INFO`
  `Minor` or `Major` to `WARN`
  `Critical` to `ERROR`

14.5.1.5 Notifications - Type: SNMP-Trap

By using the configuration window for SNMP-Trap Notifications respective Notifications can be created or modified. It opens automatically when such an action is triggered (see *Section 14.5.1*). This section also describes the general configuration parameters.

All events, no matter of which technology (e.g. OS4K, OS Voice, Server, Switches) can be transformed into one, uniform SNMP trap output format. This provides the means for an easy integration into upstream event processing systems or umbrella management, since only one single SNMP trap format has to be configured on the target side.

The standard SNMP MIB definition of the Trap Forwarder SNMP Trap can be found in the *Event Gateway User Guide - Appendix B, "SNMP Trap MIB Definition"*.

SNMP-Trap specific configuration:

- **Target Host**, **Target Port**, **Community**

  The **Host** and its **Port** to which the SNMP-Traps should be send, and for v1 or v2c traps the **Community** that should be used.

- **Version**, **V3... Parameters**

  The SNMP **Version** that should be used, and the **Parameters** needed for v3 version traps.

- **Only Custom Variables**

  By default the generated traps will send a number of **Standard Trap Variable Bindings** followed by the variable bindings of the original received trap (see *Event Gateway User Guide - Chapter 7, "Trap Forwarding"*).

  If **Only Custom Variables** is checked, the traps to be sent consist only of the Custom Variables defined (see below).

- **Trap OID**

  The enterprise OID of the trap to be sent. For more about the macros that can be used here, see *Section B.2.5*.

- **Custom Variables**

  Up to twenty Custom Variables can be defined in this table, that will be added to the traps sent.

  The buttons **+** and **-** can be used to add variables and to remove selected variables from the configuration.

  The macros that can be used for this variables are shown in *Section B.2.6*.

14.5.1.6 Notifications - Type: Logfile

By using the configuration window for Logfile Notifications respective Notifications can be created or modified. It opens automatically when such an action is triggered (see *Section 14.5.1*). This section also describes the general configuration parameters.

All events, no matter of which technology (e.g. OS4K, OS Voice, Server, Switches) can be transformed into one, uniform logfile-entry output format

Logfile specific configuration:

- **Logfile**

  The path and name of the logfile to write to.

  For security reasons, only files under `OpenScapeFM/event_logging` or in the TMP directory of the operating system can be created by default.

  Other directories can be unlocked using `OpenScape.properties`.

- **Log Entry Text**

  The definition of the log entry text to write to the file. This definition supports macros like `${severity}` or `${description}` which will be replaced by the related event attributes when written to the file.

  The macros that can be used for this variables are shown in *Section B.2.7*.

- **Rotate Files**

  If this is marked, the number of logfiles and the size of these files can be configured.

  - **File Size**

    If this size is reached, the file is moved to `<filename>_1.suffix` and a new logfile is opened. Other older logfiles are renamed accordingly.

  - **Files to keep**

    Defines the maximum number of older logfiles to keep. If the number is exceeded, the oldest logfile will be deleted.

14.5.2 Events

If Notifications (see *Section 14.5.1*) should be triggered for all occurrences of a specific Event Type, this can be configured on the page **Events**.

The page contains a list of all Event Types on the left.

A list of all currently defined Notifications is shown on the right. The link **Add or edit notifications** can be used to navigate directly to the configuration page for notifications (see *Section 14.5.1*).

Event Types marked on the left can be assigned to the respective Notifications by marking them on the right, or an assignment can be revoked by removing the corresponding mark.

In addition, configured assignments are shown in the left table within the column **Notifications**.

The setting or removing of marks always effect all selected Event Types.

For multi selection the box will be marked for all Notifications that are assigned to at least one of the selected Event Types.

Note:
If a specific Notification should be assigned to all selected Event Types, and if this Notification is already assigned to at least one of the selected Event Types, the respective mark on the right has to be removed and reset to ensure the goal.

14.5.3 Hosts

If Notifications (see *Section 14.5.1*) should be triggered for all occurrences of a specific Event Type *for a specific Host*, this can be configured on the page **Hosts**.Assignments that are valid for *all* Hosts are handled on the page Events (see *Section 14.5.2*).

The page contains a list of all **Host**s, for which at least one host specific Notification has been assigned. In addition it will also be shown which **Notifications** has been assigned to the Host for at least one Event Type.

For the configuration of Notifications the following actions are available:

New: This action creates an assignment of Notifications for selected Event Types for one or more Hosts.

The first step is a query whether the Notifications should be for all Hosts, for specific Hosts or for selected Components of specific Hosts. In the first case, a reference is made to the general Event Type configuration (see *Section 14.5.2*).

In the other two cases, the second step is to select the Hosts, and the third step is to assign the Notifications to the possible Event Types or to the Event Types for the individual Components.

> **Important Note**:
> If a new assignment is made for a host for which Notifications were already assigned, the old settings are discarded.

Modify: This action is basically the same as creating a new assignment. The existing assignments for the marked hosts are displayed and there is no need to select the hosts, since they are already defined by the marker.

Delete: This action deletes all Host specific assignments of Notifications for the marked Hosts.

14.5.4 Activity Logging

The OpenScape FM allows automatic logging of security-relevant processes.

How exactly these should be logged can be configured on the page **Activation Logging**.

Default Logging

Activities of each activity type that has a check mark in the column **Logging** are automatically logged.

The default logging is done within the log file `Activity.log`, which for example can be viewed in the Classic Client within the Root Navigation Tree under `Root->Logging->Activity` (see *Desktop User Manual, Chapter: Logging*).

Events

If a check mark is set in the column **Event** of an activity type, corresponding activities trigger the creation of an event of the event type *Access Logging*.

How exactly the event should look like for each activity can be configured, as for other Event Types, under **Server Settings->Event Types** (see *Section 14.6.2*).

The link **Configure Event Creation** leads directly to the configuration page for events of the **Category** *Activity Logging*.

Automatic Reaction to Events

For events of the **Category** *Activity Logging*, as for any other events, automatic reactions can be triggered. For example, an email can be created or a program start can be executed.

The corresponding configuration can be opened via the link **Configure Notifications/Forwarding**. This link opens the page **Events** (see *Section 14.5.2*), prefiltered appropriately to the **Category** *Access Logging*.

14.6 Server Settings

Under **Server Settings**, general default settings of the OpenScape FM Server can be configured.

Here the **Default Mail Server** can be set up (see *Section 14.6.1*), it can be defined which **Events** should be handled how (see *Section 14.6.2*). the **Password Manager** can be opened (see *Section 14.6.3*), the **Server Information** can be displayed (see *Section 14.6.4*), the Server **Properties** can be set (see *Section 14.6.5*), the **Backup** can be managed (see *Section 14.6.6*) and the **Databases** can be configured (see *Section 14.6.7*).

14.6.1 Mail Server

On the page **Server Settings->Mail Server** the mail server to be used by the OpenScape FM as default can be configured.

If an **SMTP protocol** should be used, the following information is required:

- **Protocol**: The SMTP protocol to be used (`SMTP`, `SMTPS` or `SMTP_STARTTLS`).

- **Mail Server** and **Port**: the host name or IP address of the mail server and the port to be used.
- **Default Sender Address**: The mail address, which is always used as sender if no individual sender has been specified for the specific case.
- **Login** and **Password**: The authorization parameters for sending mail.

Alternatively, **Microsoft Azure** can be used to send the emails.

The information required in this case is:

- **Protocol**: The protocol to be used (`GRAPH`).
- **Default Sender Address**: The mail address, which is always used as sender if no individual sender has been specified for the specific case.
- **MS365 Tenant**, **MS365 Client-ID** and **MS365 Client-Secret**: The credentials to use the MS Azure REST API (Microsoft Graph).

To use this protocol, the following requirements are needed in the MS Azure tenant.

- App registration with a corresponding secret key.
- API permission with the right to send mails (`Mail.Send`).
- Internet access to the Microsoft Graph REST-API `https://login.microsoftonline.com:443` or `https://graph.microsoft.com:443` .

14.6.2 Event Types

On the page **Server Settings->Event Types** it can be defined which source events depending on their type should be handled by the OpenScape FM and how these events should be displayed.

The created OpenScape FM events are additionally assigned to the object to which they best fit. Usually, this is a child object of the IP node whose IP can be assigned to the event. Therefore, for example, an interface event is usually assigned to the appropriate interface object of the IP node to which the interface belongs.

Hint:
In some cases, events can be assigned to multiple objects. For some technologies, for example, specific events are assigned to a component and the parent IP node.
If such an event is acknowledged, the acknowledgement will affect all objects to which the event has been assigned.

If an event cannot be assigned to a specific child object of an IP node, the child object **Events** is used by default.

The Event Types Configuration provides a list of all possible source events and the option to generate OpenScape FM events based on the values of these Event Types.

By default, the OpenScape FM provides predefined Event Types Configuration for the many internal and integrated events.

The customization is handled by two pages that open sequentially. First the Event Type Source Selection has to be used to select an event source (see *Section 14.6.2.1*), and then the Event Type Configuration to define the individual events for the selected source (see *Section 14.6.2.2*).

14.6.2.1 Event Type Source Selection

As mentioned before, to configure the Event Types, an event source must first be selected in the **Event Types Source Selection** page. The page can be opened using **Server Settings->Event Types**.

The configuration page contains a list of the possible sources of events. Each source for internal or integrated events is generally represented by the name of the plugin that generates the events. For external sources (SNMP traps) one entry for each Enterprise MIB definition file that has been loaded into the OpenScape FM is shown.

Marking a source and using the action **Modify** or clicking on one of the source links opens the page **Event Type Configuration** for the selected source (see *Section 14.6.2.2*).

14.6.2.2 Event Type Configuration

The Event Type Configuration Page is used to define how source events should be handled and displayed by the OpenScape FM. Each Event Type Configuration Page is opened for a single source of events as described above (see *Section 14.6.2.1*).

The page contains a table where each row represents one Event Type defined by the respective source. In the case of external events, these are the events defined by the corresponding definition file.

The column **Trap** contains the names of the different source Event Types. All other entries can be configured by marking them and using the action **Modify** or by clicking on their name.

All text fields may include macros which will be replaced when an event of the type is received. Macros start with a dollar symbol (’$’) followed by a string defining the content. The possible macros are shown in the following table.

`$1` - `$99`	value of the respective trap or event variable
`$#`	number of the variables
`$*`	all trap or event variables
`$@`	the time in seconds when the event was generated
`$T`	the system time of the SNMP agent system, when the trap was sent (for external events)
`$x`	the time as a formatted character string, when the event was generated
`$R` or `$r`	the source IP
`$e`	the Enterprise OID of the event
`$h`, `$H`	the hostname / fully qualified hostname, or if unknown, the IP address of the event’s source

Table 1 Macros

The field **Message** configures the definition of the string that will be displayed for events in the column *Description*. The column **Category** defines the content of the column of the same name.

The field **Severity** configures the severity of the event which is displayed in the column *Severity*. Here one of the constant values from the selection menu (e.g. ’*Normal*’, ’*Critical*’) can be chosen.
For external events: If a ressource key has been defined within the MIB Editor it will be displayed here.

The checkbox **Active** defines whether respective events should be evaluated at all.

The checkbox **Flash** defines whether the affected object should flash in the OpenScape FM, if a respective unacknowledged event exists.

The checkbox **Client Massage** defines whether a Client Message should be generated when respective events are created.

Events: Automatic Acknowledgement

The OpenScape FM has a default mechanism that ensures that new incoming events automatically acknowledge all existing 'similar' events. This is to ensure that e.g. traps reporting positive events automatically acknowledge the associated problem traps.

To make this possible, at least one key is automatically assigned internally to each incoming event. Already existing events, with one of these keys, are automatically acknowledged at this moment. The type of these events does not matter.

The fields **Event Type Format** and **Event Type Format Separator** define, how the key will be generated for the selected event type.

The field **Event Type Format** defines the format template which is used to generate the key. The macros listed above can be included in this template.

If more than one key should be generated for an event, the **Event Type Format Separator** field can be used to specify a symbol with which the string from the Event Type Format field will be split. All keys generated in this way are associated with the corresponding event.

Example:

A trap is received and the trap variables $3, $4 and $5 contain the values ’100’, ’15’ and ’36’.

If the *Event Type Format* is defined as ’XTrap $3 $4’ and no separator was defined, the key for this trap will be: ’XTrap 100 15’.

If the *Event Type Format* is defined as ’XTrap $3 $4&XTrap $3 $5’ and the separator ’&’ was defined, the keys for this trap will be: ’XTrap 100 15’ and ’XTrap 100 36’.

If the current new event should be confirmed in addition to the already existing events with the same key, the fields **Reset Type Format** and **Reset Type Format Separator** can be used instead. In this case, the fields for the Event Type Format have to remain empty.

Example:

For the trap `Link-Down` the *Event Type Format* `$r:Down:$1` has been defined.

For the trap `Link-Up` the *Reset Type Format* `$r:Down:$1` has been defined.

If a `Link-Down` trap is received for which `$r` will be replaced by `192.168.1.1` and `$1` by `4`, the key `192.168.1.1:Down:4` will be attached to the event generated by the trap.

If at a later time a `Link-Up` trap is received for which `$r` is also replaced by `192.168.1.1` and `$1` also by `4`, then the chosen Reset Type Format generates an identical reset key and the `Link-Down` event of the first trap and the new matching ‚positive' `Link-Up` event will be acknowledged.

If neither an Event Type Format nor a Reset Type Format is assigned for an event type, a default format is used. This format composes the key from the source of the event and the name of the Event Type. This ensures that events automatically confirm existing events of the same type for the same object.

For many Event Types useful configurations will be entered automatically during the installation of the OpenScape FM.

Usually these defaults ensure that events with status '*Normal*' acknowledge all content-matching events of the same source with a different severity.

Events: Duplicate Suppression

The fields **Duplicate Format** and **Duplicate Time** can be used to prevent the evaluation of duplicated source events (e.g. to prevent the double evaluation of an event that is send from two monitoring sources).

The *Duplicate Format* is handled like the keys described above. Based on the format, a *Duplicate Key* will be created for each incoming event for which a *Duplicate Format* has been defined. It will then be checked whether another event of the same type that has the same *Duplicate Key* has been received within the time interval defined by the *Duplicate Time*. If this is the case, the event gets tagged as a duplicate and will be ignored by default.

Note:
Incoming events are handled by the Event Correlation Engine Plugin. Within the ECE the handling of events marked as Duplicates can be modified (see separate *Event Correlation Plugin User Guide*).

14.6.3 Password Manager

The page **Server Settings->Password Manager** provides an easy overview of the passwords currently configured in the OpenScape FM. In addition, the configurations and the passwords itself can be adjusted on the page.

The displayed table contains one row per configured password with the following column values:

- **Object**
  The label of the object to which the password was assigned.
  The *Object* results from the content of the *Host* column if an object matching the *Host* is known by the OpenScape FM.
  The usual functions for objects can be accessed via the context menu of the respective row.

The combination of *Host*, *Port* and *Type* defines the unique destination for which a password is assigned. Each combination of these three values can therefore occur only once within the table.

- **Host**
  The IP address of the desired object. A Fully-Qualified Host Name (FQN) can also be specified here.
  If a password should be globally valid for all hosts, a `*` can be entered here as a wildcard symbol.

- **Port**
  The port number for which the entry should apply. If the default port is to be used for the entry, `0` can be entered here. Within the table the default port is then displayed as an empty string.
- **Type**
  The function for which the access data is used. This can be e.g. `SSH`, `SNMP_Write`, `SystemManagementAgent` or `HTTP`.

The following values define the credentials to be used to access the objects of the combination described above.

- **User**
  The account through which the login should take place.
- **Password**
  This parameter does not have its own column, it can be viewed only on the detail view (Action **Modify**). On the modify page the eye symbol to the right of **Show configured password** has to be clicked and the password of the current user has to be entered.

All column contents (with the exception of the column *Object*) can be modified for selected rows by using the Action **Modify**.

The Actions **Delete** and **New** can be used to delete a selected row or to create a new one.

If a new object is created in the OpenScape FM, e.g. SNMP for a host, it is checked whether a matching entry already exists in the password manager. If this is the case, the corresponding access parameters are used for the new object.

A Java keystore is used to store the values. The format of the file is `PFX`. The file is stored in `<install_dir>/server/database/password.pfx`. The password for the file is generated on first access and is stored in `<install_dir>/server/database/password.pfx_secret`.

The access to this file is restricted to administrators.

Whether a user has read or write permission for a row, or whether he can view passwords, depends on which permissions the user has for the respective object that is displayed in the *Object* column.

- Rows without read permission are not displayed.
- Parameters for rows without write permission cannot be modified.
- For the display of passwords write permission is required and access must be confirmed by entering the user password.

Important Note:
Currently, users with Single-Sign ON login cannot display passwords.

During the installation of the OpenScape FM, default entries for `SNMP_Read`, `SNMP_Write` and `SystemManagementAgent` are created if they are not already defined..

If the database is reset, the `password.pfx` is kept by copying it back from the created directory `dabase_old`.

14.6.4 Server Information

The page **Server Settings->Server Information** contains information about the data that is needed for the Server Self Monitoring (see *Section 4.5*). It contains the following overviews:

- **License Status**
  The current licensed OpenScape FM components, their license periods and the respective currently installed version.
- **License Details**
  The licensed and current number of licensed objects (such as Hosts or Ports.
- **Installation Size**
  The disk space occupied by the OpenScape FM on the installation partition of the OpenScape FM. The remaining disk space is also displayed here.
- **Memory Usage**
  A chronological overview of the memory usage on the host of the OpenScape FM server.
- **Disc Usage**
  A chronological overview, of the allocation of the installation medium in percent and in physical size.

14.6.5 Properties

On the page **Server Settings->Properties**, a few general settings of the OpenScape FM server can be configured:

- **Maximum Event Number**
  The maximum number of events to be kept in the event browser.
- **Event Deletion Policy**
  Which events should be deleted when the maximum number of events is exceeded:
  - **Oldest**
    The oldest event is deleted.
  - **Oldest Acknowledged**
    The oldest acknowledged event is deleted, if there are no acknowledged events, then the oldest unacknowledged event is deleted.
  - **Oldest Acknowledged By Severity**
    The oldest acknowledged *Normal* event is deleted, if there is none, the oldest acknowledged *Minor* event is deleted, and so on until the oldest acknowledged *Critical* event is deleted. If there are no acknowledged events, according to the same procedure, the oldest of the existing events with the least severe status is deleted.
- **Acknowledgement resets processing state**
  If checked, an acknowledgement will cause a removal of the status *Unacknowledged* to also remove the status *In Process* (see *Section 7.1*).

- **Display unknown traps**
  Generates an event for a trap even if there is no active MIB containing the trap type.

14.6.6 Backup

The page **Server Settings->Backup** allows the configuration of the Backup Manager module using the interface of the Web Client. This module is responsible for managing the backups of the registered backup applications.

The main task of the module is to create backups and initiate restore operations.

Important Note:
The backups are saved as ZIP archives with password protection. Therefore, to create and restore a backup, a ZIP tool with password support is required on the OpenScape FM Server host.

If the page Server **Settings->Backup** is accessed, a list of all registered backup applications is displayed. The first part of the application name always consists of the **Label** of the host on which the application is running. The Label can be customized within the Host Configuration (see *Section 13.1.2*)

Perform Backup

For selected backup applications, the following actions can be carried out for this purpose:

- **Settings**
  Here the backup behavior for a selected backup application can be defined.:
  - How often should a backup be performed (**Backup every**)?
  - When exactly is it to be executed (**Nest start at**)?
  - How many backups should be kept (**Number of Backups kept**)?
    the selected number is exceeded, the oldest backup is deleted.
  - How often should a failed backup be retried (**Number of max. Retries**)?
  - Where on the file system should the backup be stored (**Backup to**)?
  - Should an automatic backup be carried out for the application at all (**Automatic Backup enabled**)?
- **Manual Backup**
  Immediately performs a backup for the selected backup application according to its individual settings.

The action **Global Settings** can be used to define default settings for future applications in the same way as the **Settings** for individual applications described above.

If the checkmark **Apply for all backups** is set here, the current global settings will also be applied to all existing applications.

The actions **Deactivate**, **Activate** or **Delete** set the selected applications to the status *Unmanaged*, remove the status *Unmanaged* or delete the application.

Restore Backup

If the application is to be restored to the state it was in at the time of a backup, the corresponding backup can be restored.

To do this, the desired application must first be selected and the action **Backups List** must be executed. Alternatively, the link of the application can be clicked in the column **Application**.

This opens a page containing a list of all existing backups of the selected application.

If one of the backups is selected in the list, it can be restored with the action **Restore**.

Save Backup Externally

To do this, the desired application has to be selected and the action **Backups List** has to be executed or, alternatively, the link of the application within the column **Application** can be clicked.

The action **Download** creates a ZIP archive of the selected backup, and creates it as a download on the local host. This action requires entering the root password and setting a password for the ZIP archive that will be created.

In the name, the created ZIP archives contain the affected application and the date when the backup was created using the form `YYYYMMDD-hhmmss`.

The action **Upload** can be used to make a saved ZIP archive of a backup of the selected application available to the OpenScape FM again. For this action, the ZIP archive must be selected in the file system of the local host (**Upload File**) and the root password and the password of the ZIP archive to be uploaded must be specified.

14.6.7 Databases

The page **Server Settings->Databases** allows the configuration of the OpenScape FM database connections.

The tab **Monitoring Database** allows the configuration of the database connection to the database where the values for the event, status-changes and system management parameter will be exported.

The tab **Performance Management** can be used to configure the database connection used for the Performance Management Plugin. If the same database as for the monitoring should be used, the checkbox **Use same database...** can be checked.

14.7 IP Settings

Under **IP Settings**, default settings for the IP parameters (see *Section 14.7.1*) and SNMP parameters (see *Section 14.7.2*) can be configured. On an additional page SNMP V3 specific default parameters can be set (see *Section 14.7.3*).

These settings will be used as a default for newly discovered Hosts and for the discovery of Hosts and Host components.

14.7.1 IP Parameters

On the page **IP Settings->IP Parameters** basic settings for conducting host discoveries can be made:

Host Availability

Here it is specified how often a host should be checked for reachability and what should happen to its object if it can no longer be reached.

- **Execution Interval**, **Ping Method**, **TCP-Port**, **Retries** and **Timeout** define how often a host should be checked and with which method the check should be done.
- **Offline Status** determines which status a host object should assume if the host could not be reached.
- **Expiration Time**, **Expiration Time Action** and **Preserve Topology** define after which period of unreachability a host should be considered as "lost", and what should happen to the host object in this case.
- **IP Address Adjustment** specifies whether alternative IP addresses should also be used for testing the reachability of a host.
- **Auto Discovery** defines whether an auto-discovery should be performed at all and with which change options.
- **Delete empty network automatically** defines whether a net object should be deleted when the last host contained in it is automatically deleted.

Host Configuration Update

Here it is defined how often a check for already known components of a host should be performed to determine whether changes have been made for these components.

Host Discovery

This specifies how often a check for the presence of new sub-components for a host should be performed.

Display Name Format

Here it is defined how the symbol label for newly discovered hosts should initially look like.

14.7.2 SNMP Parameters

The page I**P Settings->SNMP Parameters** allows the configuration of the basic SNMP parameters for the default configuration.

Specifically, these are the maximum number of **Retries** for a send, the maximum **Timeout** per attempt, the **SNMP Version** to use, the **Read Community**, and the **Write Community**.

SNMP V3 specific settings are made on the page *SNMP V3 Trap* (see *Section 14.7.3*)

14.7.3 SNMP V3 Trap

The page **IP Settings->SNMP V3 Trap** allows the configuration of SNMP V3 specific parameters.

The basic SNMP parameters can be configured on the page *SNMP Parameters* (see *Section 14.7.2*).

Depending on the selected **Security Level**, parameters like the **Authentication Protocol**, the **Privacy Protocol** and the respective passwords can be configured that should be used for the SNMP default settings.

14.8 Certificates

Under **Certificates**, certificates can be viewed or configured.

The individual subpages allow:

- the configuration of the certificates for the Internal **Web Server** of the OpenScape FM (port `3043`) and the WildFly application of the OpenScape FM (port `3080`) (see *Section 14.8.1*),
- setting the trust status of the SSL **Certificates** known to the OpenScape FM (see *Section 14.8.2*),
- the configuration of rules to generate **Expiration** warnings for certificates with near-time expiry (see *Section 14.8.3*),
- and the definition of general **Settings** for the certificate management (see *Section 14.8.4*).

14.8.1 Web Server

The OpenScape FM allows the configuration of its own certificates. This can be done, according to the ports used, for the *Internal Web Server* on the page **Certificates->Web Server 3043** and for the *WildFly application*, which is required for the web interface, on the page **Certificates->Web Server 3080**.

The two configuration pages are identical in operation and offer a number of fields in which the attributes that are to be used when creating the certificate can be defined.

The following actions can be performed on the pages:

- **Certificate Request**
  Generates a request file that can be sent to a Certificate Authority (CA) for the signing of the certificate.

  The file with the name `certificate request.pem` is stored in the download directory on the current client. It contains only the public part of the key of the self-signed certificate created in the course of this action.

  An already existing certificate is not replaced by this action. The replacement only takes place during the loading of the Certificate Response.

- **Load Certificate**
  Three different types of certificate files can be loaded and used with this action:

  - **Certificate of a Certificate Authority**
    Loads a file in `.cer`, `.pem` or `.der` format containing the certificate of the Certification Authority that signed the submitted certificate. The certificate of the Certification Authority is stored in the keystore.

    This action is only required if the Certification Authority is not already known (error message "Chain could not be taken from the response").

- **Certificate Response**
  Loads a `.pem` or `.cer` format file containing the Certificate Authority's (CA) response to a signing request (action *Certificate Request*). The loaded certificate response replaces the existing self-signed certificate. The certificate of the Certificate Authority itself may have to be loaded first (see previous selection).
- **Keystore**
  Loads a `.jks` or `.p12` format file containing a keystore that contains a complete certificate. The certificate must contain the public and private key and is used for the Web Server after loading.

  This variant can be used, for example, if the certificate was provided by the own company.

- **Selfsigned Certificate**
  Creates a new self-signed certificate based on the currently displayed configuration. This certificate will also replace any certificate already in use.
- **Change Keystore Password**
  Allows the definition of a new password for the corresponding keystore.

14.8.2 Certificates

The page **Certificates->Certificates** shows the SSL certificates discovered by the OpenScape FM.

Each row in the table represents a certificate for which its trusted state, host name, x500 name and validity range are shown.

By using the actions **Trust**, **Untrust** and **Delete**, marked certificates can be set to trusted or untrusted, or deleted from the OpenScape FM.

14.8.3 Expiration

For accepted certificates known to the OpenScape FM, it can be defined that an event is to be displayed in the OpenScape FM when the expiration date of the certificate is about to be reached.

The configuration which accepted certificates with which lead time and with which status such events should be generated for, can be done on the page **Certificates->Expiration**.

The page contains a table that lists all the rules to create expiry warnings.

It contains the following columns:

- **Network/Host**
  The IP address of the affected host or network. Or *All* if the rule applies to all certificates.
- **Mask**
  If the rule applies to a network, the subnet mask that delimits the affected area (e.g. `255.255.255.0` if the first three bytes of the IP address determine the network). Otherwise this column is empty.
- **Severity**
  The severity to be given to the expiry warning events generated by this rule.

- **Expiry**
  The time interval before the actual certificate expiration date at the beginning of which the expiration warning event should be generated (e.g. 7 days before the certificate expires).

The action **New** can be used to create a new expiry rule.

The action opens a configuration window:

- The menu **For** defines the validity scope of the rule:
  All: For all accepted certificates.
  Network: For all accepted certificates of the defined network.
  Host: For the accepted certificates of the defined host.
- The remaining fields correspond to the description of the overview table (see above).

The action **Edit** corresponds to the action *New* with regard to the possible entries. However, this action leads to the reconfiguration of the expiry rule currently marked in the table.

The action **Delete** removes the currently selected expiry rules.

14.8.4 Settings

On the page **Certificates->Settings** general settings of the certificate management can be configured:

Accept All Certificates

If this checkbox is marked, *all* imported certificates are considered trustworthy and are accepted without further verification.

Certificate Pinning

If this checkbox is selected, valid certificates (valid CA chain) are classified as untrusted. Each certificate must be manually classified as trusted.

14.9 Maintenance Windows

The page **Maintenance Windows** allows viewing and creating maintenance windows.

Maintenance Window is a convenient function that is available for each object. It puts an object (e.g. a network element) into a maintenance state for a configured period of time. During the maintenance state (e.g. as long as maintenance work on a network element continues), events for the affected object and its child objects are suppressed so that they do not appear in the default view of the event browser.

The page *Maintenance Windows* shows all defined maintenance windows.

The following actions are available:

- **New** creates a new Maintenance Window.
- **Edit** allows the definition of a time interval for a selected Maintenance Window.

- **Objects** allows the assignment of the objects that should be affected to a selected Maintenance Window.
- **Delete** removes the selected Maintenance Windows.

  Maintenance Windows whose time interval has expired (inactive Maintenance Windows) are automatically deleted.

14.10 Log Files

Under **Logfiles** selected log files of the OpenScape FM can be viewed.

By default, a file browser is open that displays the main log file of the OpenScape FM.

Additional browsers can be opened using the **Add Window** button.

For each of the opened browsers, it can be selected in the header whether the main log file (*OSFM*), the exception log file (*OSFM_EXCEPTIONS*) or the Wildfly log file (*WILDFLY*) should be displayed.

The buttons in the upper right corner can be used to close individual browsers or refresh their contents.

A Access Rights

The OpenScape FM Web uses the Access Rights of the OpenScape FM (*see OpenScape FM Desktop User Guide*).

The are no separate Access Rights for elements of the OpenScape FM Web itself.

What objects a user can see and which action a user may perform is defined by his Access Rights defined in the OpenScape FM.

B Macros

In numerous places in the OpenScape FM, macros can be used instead of fixed texts.

For example, specific data of the triggering event can be included in the message of an automatic reaction.

This appendix lists many of these possible macros (see *Section B.1*) and in another paragraph shows some exemplary use of macros (see *Section B.2*).

B.1 General Macros

ToDo: Macros for Emails

ToDo: Macros for SMS

ToDo: Macros for Programs

ToDo: Macros for Syslog

ToDo: Macros for Traps

ToDo: Macros for Logfiles

All macros start with the dollar symbol ('$'). The following list provides an overview over the implemented field macros. A list of the possible functions is included in *the OpenScape FM Desktop User Guide*.

- `${enterpriseid}`: The enterprise id connected to the event.
- `${date}`: The date of the event given in string format. The local time zone is used for this.
- `${time}`: The time of the event given in string format. The local time zone is used for this.
- `${generic}`: XXX
- `${specific}`: XXX
- `${datetimeseconds}`: The time when the event occurred. The time is given in seconds since midnight of January 1st, 1970.
- `${datetimemillis}`: The time when the event occurred. The time is given in milli seconds since midnight of January 1st, 1970.
- `${snmpdateandtime}`: XXX
- `${sourceTimeStamp}`: The time of the event as it is reported by the source.
- `${category}`: The category of the event as it is displayed in the Event Browser.
- `${severity}`: The severity of the event (e.g. '*minor*', '*major*').

- `${severityinteger}`: The severity of the event as a number (’*unknown*’ = `1`, ’*normal*’ = `2`, ’*warning*’ = `3`, ’*minor*’ = `4`, ’*major*’ = `5`,’*critical*’ = `6`).
- `${eventid}`: XXX
- `${acknowledged}`: Is replaced with the value ’`false`’ when a reaction for a new event is performed. It is replaced with the value ’`true`’ when an acknowledgement reaction for an already known event is performed.
- `${flashing}`: XXX
- `${serverIp}`: XXX
- `${source}`: The source name of the object to which the event is connected.
- `${description}`: The text displayed in the Event Browser column Description.
- `${label}`: The automatically generated label of the object connected to the event.
- `${eventkey}`: XXX
- `${sourceip}`: The IP address of the source which triggered the event (e.g. the IP address of a HiPath 4000 Manager).
- `${hostname}`: The host name of the source that triggered the event.
- `${fullqualifiedhostname}`: The fully qualified hostname (e.g. pc123.materna.de) of the source that triggered the event.
- `${weblink}`: The URL that points to the Detail View of the effected object (e.g. Host Details).
- `${var.length}`: The number of variables attached to the event.
- `${objectcomment}`: The comment defined for the current object.
- `${annotation}`: The annotation of the event.
- `${var[<X>]}`: The content of the (X+1)th event variable. E.g. `${var[4]}` will correspond to the content of the fifth variable.
- `${java.rmi.server.hostname}`: The name or IP address of the OpenScape FM Server.
- `${oid[<X>]}`: The oid of the (X+1)th event variable. E.g. `${oid[4]}` will correspond to the oid of the fifth variable.

B.2 Macro Examples

XXX

B.2.1 Examples for Emails

ToDo

B.2.2 Examples for SMS

ToDo

B.2.3 Examples for Program Starts

ToDo

B.2.4 Examples for Syslog

ToDo

B.2.5 Examples for Trap-OIDS

ToDo

B.2.6 Examples for Trap-Vars

ToDo

B.2.7 Examples for Logfiles

ToDo

Index

P

R

S

T

U

V

W