Nimsoft® Unified Management™ Portal

User Documentation

6.0
Legal Notices

Copyright © 2012, CA. All rights reserved.

Warranty
The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses
The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend
If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks
Nimsoft is a trademark of CA.
Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.
Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.
Java(TM) is a U.S. trademark of Sun Microsystems, Inc.
Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.
Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.
Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.
UNIX® is a registered trademark of the Open Group.
ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.
All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
Contact Nimsoft

For your convenience, Nimsoft provides a single site where you can access information about Nimsoft products.

At [http://support.nimsoft.com/](http://support.nimsoft.com/), you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- Nimsoft Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about Nimsoft product documentation, you can send a message to support@nimsoft.com.
## Contents

### Chapter 1: Welcome

Getting Started with UMP ................................................................. 15
The Portal .................................................................................. 15
Create a Page ........................................................................... 18
Managing Pages ........................................................................ 18
Error Console ............................................................................ 19
Welcome to Unified Management Portal Help .................................... 20
How to Navigate the Help Topics ......................................................... 20
How to Print Multiple Help Topics ......................................................... 21

### Chapter 2: Account Admin

Account Admin Pane .......................................................................... 23
Edit ACLs Dialog .......................................................................... 24
New Account/Edit Account Dialog ......................................................... 26

### Chapter 3: Change Password

### Chapter 4: Alarm Console

Alarm Console Toolbars ........................................................................ 29
General Bar .................................................................................. 29
Command Bar ............................................................................. 30
Alarm Filter Bar ........................................................................... 31
History Bar .................................................................................. 32
Alarm Console Table ........................................................................ 34
Popup Menus .................................................................................. 36
Toolbar Popup Menu ....................................................................... 36
Alarm Console Table Popup Menu ......................................................... 37
Dialogs ............................................................................................ 39
Actions Dialog ............................................................................. 39
Adobe Flash Player Settings Dialog ......................................................... 40
Alarm Filter Dialog ....................................................................... 40
Alarm Filter Expression Dialog ............................................................. 40
Alarm History Dialog .................................................................... 41
Assign To Dialog ........................................................................... 41
Attach Notes Dialog ....................................................................... 41
Chapter 7: Dashboard Designer

Managing Alarms in Dashboards

Chapter 6: Custom Dashboards

SSO Credentials Configuration

Chapter 5: Cloud User Experience Monitor

Cloud User Experience Monitor Configuration

Chapter 4: Troubleshooting Alarm Console

Troubleshooting Alarm Console

Chapter 3: Deploying Widgets

Deploying Widgets

Chapter 2: Creating Dashboards

Create Dashboard

Chapter 1: Introducing Dashboard Designer

Configuring a Widget to Use External DB Data
Contents

Chapter 8: Discovery Status ......................................................... 129
Viewing Discovery Status .......................................................... 129
Discovery Status Pie Chart .......................................................... 129
Pie Chart Detailed View .............................................................. 130
Discovery Status Table ............................................................... 132

Chapter 9: Dynamic Views .......................................................... 135
View a Dynamic View ................................................................. 135
Understanding the Dynamic Views Tree ........................................... 136
Data Sources for Dynamic Views .................................................. 137
  Customize Data Sources for Systems ......................................... 137
View System Information in USM .................................................. 139
MiniMap Tool ............................................................................. 139
Viewing the Data as a Performance Report ..................................... 140
Customizing the Dynamic View Templates ...................................... 140
  Template Names ........................................................................ 140
  Supported Variables ................................................................... 142
  Edit a Dynamic View Template ................................................. 144
Troubleshooting Dynamic Views .................................................. 144
  Dynamic Views May Display Redundant Tree Nodes .................. 144
  Duplicate Data Series are generated ........................................ 145
  Dynamic View is not Displayed ................................................ 145
  No Access Error ........................................................................ 146
  No Existing Interfaces Error ...................................................... 146

Chapter 10: Flow Analysis ............................................................ 147

Chapter 11: List Designer ............................................................... 149
Design a List ................................................................................ 150
User Tags .................................................................................... 152
**Chapter 12: List Viewer** 169

Drilling Down in List Viewer ................................................................. 169
List Viewer Window .................................................................................. 170
Preferences Dialog .................................................................................... 171
Open View Dialog ..................................................................................... 171

**Chapter 13: Maintenance Mode** 173

Using Maintenance Mode .......................................................................... 173

**Chapter 14: My Tickets** 175

User Types .................................................................................................. 175
Requests List .............................................................................................. 176
Viewing Tickets ......................................................................................... 176
Add a Note to a Ticket (Self Service Users) ............................................... 176
Add an Attachment to a Ticket ................................................................. 177
Add A Work Log Item to a Ticket (Agent or Admin Users) ...................... 177

**Chapter 15: Nimsoft Remote Admin** 179

Migration for Legacy Users ....................................................................... 180
Troubleshooting Nimsoft Remote Admin ................................................... 180
USM Templates Do Not Deploy .................................................................. 181

**Chapter 16: Performance Reports Designer** 183

Understanding Performance Data .............................................................. 183
Viewing Raw Performance Data ............................................................... 184
QoS Selection Tabs .................................................................................... 185
Filters Tab .................................................................................................. 186
User Tags .................................................................................................... 187
Charts Pane ................................................................................................ 188
Automatic Replacement of Fields in PRD Templates ................................. 193
## Troubleshooting Report Scheduler

### Administering Report Scheduler

#### Chapter 19: Report Scheduler

- Service Level Agreement Reports
- Quality of Service Reports
- Reports Overview

#### Chapter 18: Reports

- Launching the Relationship Viewer using the WebContent Portlet
- Defining Reports with a URL
- Troubleshooting PRD
- Performance Reports May Convert Incorrectly to PDF

#### Chapter 17: Relationship Viewer

- Overview
- About the Relationship Viewer
- Accessing the Relationship Viewer
- Using the Relationship Viewer
- Changing What You See
- Relationship Viewer Control Bar
- Viewing Object Details
- Launching the Relationship Viewer using the WebContent Portlet

#### Chapter 16: Relationship Viewer

- Viewing the Relationship Viewer...
Report Scheduler: Removing an Account User’s Access .................................................. 239
Report Scheduler Shifts Time Axis in PDF Format ....................................................... 240
Report Scheduler Does Not Display Estimated Values .................................................. 240
Java Exception Displayed When Scheduling Reports .................................................... 240
Some Scheduled Jobs are Not Running ........................................................................ 241
Unexpected Character Appears in Reports .................................................................... 241
Note Icon Does Not Display in Report Scheduler Reports ............................................ 242

**Chapter 20: Service Desk** 243
Create Tickets from Alarms ............................................................................................ 244
  Automatically Create Tickets from Alarms ................................................................. 244
  Manually Create an Incident from an Alarm ............................................................... 244
CMDB Integration ......................................................................................................... 245
Reports with Integrated Data .......................................................................................... 245
Users in Service Desk ................................................................................................... 246
  Create NM Users ........................................................................................................ 246
  Create Service Desk Users ........................................................................................ 246

**Chapter 21: SLA Reports** 249
Introduction to SLA Reports .......................................................................................... 249
  Viewing SLA History .................................................................................................... 250
  Understanding SLA Reports ....................................................................................... 251
  Viewing SLA Reports .................................................................................................. 251
SLOs ............................................................................................................................... 252
QoS Objects .................................................................................................................. 252
Preferences Dialog ........................................................................................................ 253
Saving Information as a PDF ......................................................................................... 253

**Chapter 22: SLM** 255
SLM Overview ............................................................................................................. 255
  Introduction to SLM ..................................................................................................... 255
  What is Service Level Management? ......................................................................... 256
  SLM Concepts ............................................................................................................ 258
  SLM Database Structure ......................................................................................... 260
  SLA Engine ................................................................................................................ 262
  Data Engine ............................................................................................................... 263
Setting Up a Probe to Deliver Quality of Service Data .................................................. 265
Setting Permissions to Use SLM ................................................................................... 265
Compliance Calculation ............................................................................................... 266
  Definition of Compliance Percentage ....................................................................... 266
Chapter 23: Unified Reports 357
Running Unified Reports .................................................................................................................. 357
Preconfigured Reports ..................................................................................................................... 357

Chapter 24: Unified Service Manager 363
Permissions in USM .......................................................................................................................... 366
Navigating in USM ........................................................................................................................... 366
  Views ........................................................................................................................................... 366
  Search for Computer Systems ....................................................................................................... 370
  Pop Out Graphs ............................................................................................................................. 373
  Launch Relationship Viewer ......................................................................................................... 373
Automatic Agent Deployment ........................................................................................................ 373
  Deploy Agents Automatically ......................................................................................................... 374
  Deploy Agents to Systems Listed in a File ..................................................................................... 375
  View the Status of Agent Deployment .......................................................................................... 386
Getting Started with Service-Oriented Configuration .................................................................... 386
  Set Up Service-Oriented Configuration ....................................................................................... 387
SOC Probes Configuration Reference ............................................................................................. 388
Working with Groups ...................................................................................................................... 388
  Create a Group ............................................................................................................................... 389
  Automatic Groups ......................................................................................................................... 390
  Filters ........................................................................................................................................... 392
  View Group Assignments .............................................................................................................. 399
  Servers Group ............................................................................................................................... 399
  Delete a Group ............................................................................................................................... 399
Working with Monitors .................................................................................................................. 400
  Local vs Remote Monitors ............................................................................................................ 400
  Understanding Precedence, Priority, and State ............................................................................ 401
  Applying Monitors to Groups ........................................................................................................ 405
  Reapply a Monitoring Template ................................................................................................... 409
  Applying Monitors to Systems ...................................................................................................... 410
  View Monitor Status ..................................................................................................................... 413
Working with Alarms ....................................................................................................................... 414
  View Alarms ................................................................................................................................. 414
  Manage Alarms ............................................................................................................................. 421
  Working with Invisible Alarms ...................................................................................................... 421
  Filter Alarms ................................................................................................................................. 423
  Sort Alarms .................................................................................................................................. 424
Viewing System Information ........................................................................................................ 424
  View System Properties ............................................................................................................... 425
  View Metrics ............................................................................................................................... 428
Non-ASCII Characters Stored Incorrectly in the Database .................................................................457
Numeric Login IDs Do Not Work ...........................................................................................................458
I Cannot Access the Control Panel .......................................................................................................458
Logging In Takes Me to the Login Page .................................................................................................459
CSV File is Incorrect in Chinese or Japanese .......................................................................................459

Index 461
Chapter 1: Welcome

This section contains information about getting started with the Unified Management Portal (UMP) and about using the UMP online help.

For the complete set of documentation for Nimsoft products, see the Nimsoft Library.

This section contains the following topics:

- Getting Started with UMP (see page 15)
- Welcome to Unified Management Portal Help (see page 20)

Getting Started with UMP

This topic tells you how to start displaying and viewing data in the Unified Management Portal (UMP). You can view the default pages that come with UMP, or you can create and save pages with a custom layout.

The Portal

The Nimsoft Unified Management Portal (UMP) is where you:

- Open and manage Service Desk tickets
- Monitor and manage computer systems
- Graph QoS data
- View and manage alarms
- Create SLAs and view SLA performance reports
- Create, view, and schedule reports
- Create and view custom dashboards
- Manage users

The following list describes the portlets available. Some portlets require an additional purchase.

- Account Admin - Allows you to manage users and user privileges, including assigning Nimsoft access control lists (ACLs) to contacts within an account. Note: The ACL must be marked as available to an account in order to assign the ACL to contacts within that account. For Account/Contact users the alarms listed are filtered by origin – users from an account see only alarms from an origin which the account has ownership of. Discovery information is handled in a similar way: a contact user sees only nodes from an origin which the account has ownership of.
- Alarm Console - Allows full viewing, filtering, and managing of alarms.
- Cloud User Experience Monitor - Allows you to monitor web sites and cloud services from around the globe. Measures the status of your transactions and services from more than 60 locations.
- Custom Dashboards - Allows you to:
  - Access your custom dashboards, which display the QoS data and alarms that are important to you in managing your network.
  - View your alarms.
  - View the Dynamic Views, which display the state (such as alarm level, performance, etc.) of the monitored computer systems on your network.
- Dashboard Designer - Allows you to design custom dashboards to display selected QoS data and alarms from some or all of your monitored computer systems.
- Discovery Status - Consists of a pie chart showing the current discovery status. Immediately after installation of the Nimsoft Server software, the Nimsoft Discovery component starts searching your network for computer systems, provided that the Discovery option was selected during the installation of the Nimsoft Server. The process runs continuously and updates the diagram to show the current status, ensuring that computer systems that are removed or newly installed are reflected in the pie chart. Clicking on the pie chart displays a table with information about the systems in the pie chart.
- Dynamic Views - Displays automatically generated dashboards for the computer systems discovered on your network. The dashboards display QoS information such as memory and CPU utilization.
- Flow Analysis - Displays network traffic flow data (NetFlow data measured and collected on router interfaces) organized into TopN reports for router interfaces, hosts, and applications.
- List Designer - Allows you to design lists to be displayed in the List Viewer application.
- List Viewer - Displays data in a table format. The data can be in the form of text, numbers, gauges, alarms, or graphs. Two kinds of lists can be created, detail or group. In detail lists, each row displays data for a single host or target. In group lists, each row displays aggregated data for a group of systems. When creating group lists, you can specify a drilldown list for each group. Typically, the drilldown list contains the data for the individual hosts or targets that make up the group.
- Maintenance Mode - Allows you to set the computer systems on your network to Maintenance Mode so they are temporarily unmonitored. The monitoring parameters for the system are retained, and when maintenance mode ends they are monitored again as before. Filtering is provided so you can more easily select the systems to designate as in Maintenance Mode.
■ My Tickets - Allows you to view basic information about your Nimsoft Service Desk tickets. Unlike the Service Desk, My Tickets can be displayed on the same page as other portlets, allowing you to view your tickets alongside other key data for your organization.

■ Nimsoft Remote Admin - Formerly named NIS Manager, provides a management console for discovery (DS) and configuration (ACE) data in NIS. It shows the state of all Configuration Items in the database. You can set the state and specify the monitoring properties for the various computer systems discovered on the network.

■ Performance Reports Designer - Formerly named QoS Chart, allows you to see a visual representation of QoS data. You select the host, QoS measurement, target, and time range, and the data is displayed as a graph. You can display multiple measurements on a single graph, and can view multiple graphs at a time. You can choose the graph format (line, area, or column graph) and can maximize the graph to view it at a larger size. You can save a set of graphs as a report to view later.

■ Relationship Viewer - Provides a facility for applications to display the status of and relationships between objects in various ways. For example, the Root Cause Analysis and Topology Manager application, if installed, uses the Relationship Viewer to display symbols that represent network devices, show the connections between those devices, and indicate the status of each device and connection.

■ Reports - Contains Quality of Service (QoS) reports and Service Level Agreement (SLA) reports. QoS reports must be manually created in the Performance Reports Designer portlet. SLA reports are created automatically after you create SLAs in the Service Level Manager (SLM) portlet.

■ Report Scheduler - Allows you to schedule reports to run at specified times. The reports are created in PDF format and can be sent via email or FTP, or stored on a server.

■ Service Desk - Provides action-based workflows based on ITIL standards that allow you to coordinate incident response and proactive IT management. Integrates data from Nimsoft Monitor to allow you to view data from operations and service management together.

■ SLA Reports - Provides SLA reports to show overall compliance, SLA details, SLOs, SLA compliance trend, and graphs on the SLO data.

■ SLM - Provides a set of tools to monitor and ensure the validity of a set of SLAs for internal and external customers. It is made up of Service Level Agreements (SLAs), Service Level Objectives (SLOs), and Quality of Service (QoS) data.

■ Unified Reports - Provides advanced reporting. You can run standard reports that are provided, or you can create your own reports in the Report Designer. This is an optional component that you must purchase. In order to use this portlet, you must set the Unified Reports permission in your Nimsoft access control lists (ACLs).

■ Unified Service Manager - Allows you to set up monitoring for groups of computer systems and to view the data collected. You can create groups of computer systems and then assign monitoring templates to them.
Create a Page

You can create custom pages where you control which portlets are displayed and the layout of the page. You can choose whether your pages are private pages, seen only by you, or public pages, which can be viewed by anyone on the Internet. When you first log in, your private pages are displayed. Public pages are accessed by choosing Go to, My Public Pages from the menu bar.

To create a page:
1. Add a page (see page 18).
2. Select a layout (see page 18).
3. Add portlets (see page 18).

Add a Page

1. Choose Add, Page from the menu bar.
2. Enter a name for the page in the text box that is displayed next to the page tabs.
3. Click the green check mark next to the text box.
4. Click on the tab for the page to view it.

Select a Layout

1. Choose Manage, Page Layout from the menu bar.
2. Select the layout you want.
3. Click Save.

Add Portlets

1. Choose Add, Portlet from the menu bar.
2. Click the + sign next to Monitoring.
3. Drag a portlet to the position on the page where you want to display it, or click Add next to the portlet.

Repeat these steps to add more portlets to your layout.

Managing Pages

You can change the settings for your pages, including permissions, by choosing Manage, Control Panel from the menu bar.
Error Console

The Unified Management Portal has an error console where you can view error messages. If errors have been generated, an icon is present on the application toolbar. The icon represents the highest severity level of messages generated:

- 🔄 = Informational warning
- 🚨 = Error message

Click the icon to display the error console:

Double-click a message to view detailed information about the error:

Click the forward or back arrows to scroll through the detailed messages. Click the down arrow to minimize the window.

Click the eraser icon under the "x" in the top right to clear either window:
Welcome to Unified Management Portal Help

This online Help system contains the how-to and reference information you need to use the Unified Management Portal (UMP) successfully. This first Help topic explains how to navigate and print the topics in this Help system.

If you are already comfortable using the online Help, you can either use the Contents, Index, or Search features in the left frame to find the Help you need now.

How to Navigate the Help Topics

The online Help is an HTML-based system that runs in standard Web browsers.

This Help system provides the following navigation features in the left frame of your browser window to help you quickly find information:

- **Contents** (see page 20)
- **Index** (see page 20)
- **Search** (see page 21)

The following subsections describe how to use each of these navigation features.

Using the Contents Feature

The Contents feature lists all the books and topics in this Help system in an expandable/collapsible tree hierarchy. This feature lets you view and navigate through the information in this Help system.

By default, the Contents list is displayed in the left frame of your browser window when the Help system first opens.

If the Contents list is not currently displayed in the left frame of your browser window, click the Contents tab at the top of the left frame.

Using the Index Feature

The Index feature lists primary and secondary keywords (UMP terms and common synonyms) used in this Help system. This feature gives you a quick way to find information on specific topics within the Help system.

**To use the Index feature**

Click the Index tab at the top of the left frame. Then, scroll to and click the keyword you want, or click on a letter at the top to jump to words beginning with that letter.
Using the Search Feature

The Search feature lets you find all topics containing a particular word or words within this Help system. This feature uses a full-text search engine that is built into the Help system and runs locally on your system.

To use the Search feature

Click the Search tab at the top of the left frame. Then, in the text box, type the word or words you want to search for and click the Search button. When the search completes, scroll to and click the Help topic you want.

How to Print Multiple Help Topics

To enable you to print multiple topics from this Help system, the content is provided in an Adobe® Acrobat® (PDF formatted) file. This file is available from the help title page.
The Account Admin application allows administrators to manage account contact users and Nimsoft Access Control Lists (ACLs). Administrators are users with the Account Administration permission in the ACL.

Administrators can add, modify, or delete accounts and account contacts (users) and set passwords for account contacts. They can also add, modify, or delete ACLs and set the permissions for the ACLs.

Changes made in the Account Admin application are reflected in the Infrastructure Manager, as both interfaces write to the same database.

If you do not have the Account Administration permission set in the ACL, you will see a "Permission Denied" message when you try to run the Account Admin application.

This section contains the following topics:

- Account Admin Pane (see page 23)
- Edit ACLs Dialog (see page 24)
- New Account/Edit Account Dialog (see page 26)
- Change Password (see page 27)

### Account Admin Pane

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account pulldown</td>
<td>Select a user account. The users for that account are displayed in the table.</td>
</tr>
<tr>
<td>Add account icon</td>
<td>Click to open the New Account Dialog (see page 26), where you can create user accounts.</td>
</tr>
<tr>
<td>Edit account icon</td>
<td>Click to open the Edit Account Dialog (see page 26), where you can edit user accounts.</td>
</tr>
<tr>
<td>Delete account icon</td>
<td>Click to delete a user account.</td>
</tr>
<tr>
<td>Help icon</td>
<td>Click to view the online help for the Account Administration application.</td>
</tr>
</tbody>
</table>
### Edit ACLs Dialog

The Edit ACLs dialog allows you to create, modify, or delete ACLs. You can choose which permissions to assign to each ACL. To access the dialog, click the Edit ACLs icon in the ACL column header of the Account Admin table.

For a list of permissions required to use UMP applications, see Setting Permissions for UMP Portlets (see page 443).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL list</td>
<td>Lists the ACLs that have been defined, using either the Account Admin application or Infrastructure Manager.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Check boxes</td>
<td>Click to select the permissions to be assigned to the ACL. Click the check box in the column header to toggle between sorting by checked and unchecked permissions.</td>
</tr>
<tr>
<td>Permission column</td>
<td>Name of the permission.</td>
</tr>
<tr>
<td>Description column</td>
<td>Description of the permission.</td>
</tr>
<tr>
<td>Type column</td>
<td>Type of permission.</td>
</tr>
<tr>
<td>Access column</td>
<td>Type of access granted for that permission:</td>
</tr>
<tr>
<td></td>
<td>■ read - Can view data only</td>
</tr>
<tr>
<td></td>
<td>■ write - Can view and modify data</td>
</tr>
<tr>
<td></td>
<td>■ admin - Can view and modify data, and make administrative changes</td>
</tr>
<tr>
<td></td>
<td>■ super - Full access</td>
</tr>
<tr>
<td>Add ACL icon</td>
<td>Click to create a new ACL, then enter a name for the ACL. Once it is created, click the check boxes to assign permissions to the ACL.</td>
</tr>
<tr>
<td>Copy ACL icon</td>
<td>Click to copy an existing ACL, then enter a name for the ACL. Once it is created, you can click the check boxes to change the permissions for the ACL.</td>
</tr>
<tr>
<td>Rename ACL icon</td>
<td>Click to change the name of the ACL.</td>
</tr>
<tr>
<td>Delete ACL icon</td>
<td>Click to delete the selected ACL.</td>
</tr>
<tr>
<td>LDAP group button</td>
<td>Click to select an LDAP group of users who will be authenticated as NMS users with the ACL currently selected.</td>
</tr>
<tr>
<td>Account link button</td>
<td>Click to select an account to associate with an LDAP group. If an account is selected, the LDAP group will be contact users in the selected account. If no account is selected, the LDAP group will not be account contact users.</td>
</tr>
<tr>
<td>OK button</td>
<td>Click to save changes and exit the dialog.</td>
</tr>
<tr>
<td>Cancel button</td>
<td>Click to exit the dialog without saving changes.</td>
</tr>
</tbody>
</table>
New Account/Edit Account Dialog

The **New Account** and **Edit Account** dialogs allow you to create or edit user accounts.

Enter the name and address information for the user. The **Ownership** is the origin assigned to the account, which determines the information visible for account and contact users. You can assign more than one origin to an account.

If you are an MSP, for example, you might designate the primary hub for each customer as the origin, thereby separating customer information. In the Alarm Console, account and contact users see only alarms from origins assigned to the account. In Nimsoft Remote Admin, account and contact users see only discovered systems from origins assigned to the account.
Chapter 3: Change Password

The Change Password application allows account contact users to change their passwords. You must be an account contact user and have the Change Password permission set in the Nimsoft Access Control List (ACL) in order to use this application.

Administrators (users with the Account Administration permission in the ACL) can use the Account Admin (see page 23) application to change an account contact user’s password or ACL permissions.

To change your password:

1. Enter your existing password in the Old Password field.
2. Enter your new password in the New Password field.
   - Passwords must be at least six characters long.
3. Enter the new password in the Confirm Password field.
   - The text in the New Password and Confirm Password fields must match exactly.
4. Click Change Password.
Chapter 4: Alarm Console

The Alarm Console is the main window for viewing and managing alarms. The window displays information about alarms in a table format, and you can use toolbar icons and menu options to view information and take action on alarms.

The Alarm Console is integrated with other Nimsoft applications, such as the Enterprise Console and Infrastructure Manager, and it can also be opened in the Service Level Manager.

This section contains the following topics:

- **Alarm Console Toolbars** (see page 29)
- **Alarm Console Table** (see page 34)
- **Popup Menus** (see page 36)
- **Dialogs** (see page 39)
- **Enabling the Alarm Console** (see page 49)
- **Troubleshooting Alarm Console** (see page 49)

Alarm Console Toolbars

The Alarm Console has a series of four toolbars you can rotate through by clicking the (Rotate) icon:

- **General Bar** (see page 29)
- **Command Bar** (see page 30)
- **Alarm Filter Bar** (see page 31)
- **History Bar** (see page 32)

General Bar

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotate icon</td>
<td>Click to display the next toolbar.</td>
</tr>
<tr>
<td>Details button</td>
<td>Opens the Details (see page 42) dialog, where you can view additional information about the alarm and manage the alarm.</td>
</tr>
<tr>
<td>Find button</td>
<td>Click to open the Find (see page 42) dialog, where you can search for alarms that contain specified text.</td>
</tr>
</tbody>
</table>
**Alarm Console Toolbars**

<table>
<thead>
<tr>
<th><strong>View pulldown</strong></th>
<th>Selects the columns to display. Click the word View to return to the Default view.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter field</strong></td>
<td>Enter text to display only alarms that contain that text.</td>
</tr>
<tr>
<td><strong>Column pulldown</strong></td>
<td>Click and select a column to apply the Filter field to that column. For example, if you want to see only alarms from a certain host, enter all or part of the host name in the Filter field and choose Host from this pulldown.</td>
</tr>
<tr>
<td><strong>Severity icons</strong></td>
<td>Click on an icon to display only alarms with that severity. The colors correspond to the following severity levels:</td>
</tr>
<tr>
<td></td>
<td>- Red = Critical</td>
</tr>
<tr>
<td></td>
<td>- Orange = Major</td>
</tr>
<tr>
<td></td>
<td>- Yellow = Minor</td>
</tr>
<tr>
<td></td>
<td>- Blue = Warning</td>
</tr>
<tr>
<td></td>
<td>- Light blue = Informational</td>
</tr>
<tr>
<td><strong>Stop updates icon</strong></td>
<td>Click to stop updates to the information in the Alarm Console. Otherwise, the alarm information is updated dynamically.</td>
</tr>
<tr>
<td><strong>Help icon</strong></td>
<td>Click to display the online help for the Alarm Console.</td>
</tr>
</tbody>
</table>

**Command Bar**

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotate icon</td>
<td>Click to rotate to the next toolbar.</td>
</tr>
<tr>
<td>Accept button</td>
<td>Click to assign the selected alarm to yourself.</td>
</tr>
<tr>
<td>Assign button</td>
<td>Click to open the Assign To (see page 41) dialog, where you can assign the selected alarm to another user.</td>
</tr>
<tr>
<td>Unassign button</td>
<td>Click to unassign the selected alarm.</td>
</tr>
<tr>
<td>Acknowledge button</td>
<td>Acknowledges the alarm. The alarm is considered closed and is removed from the Alarm Console table. The alarm is also deleted from the NimBUS Alarm Server (NAS) database, but a copy is retained in the history database.</td>
</tr>
<tr>
<td>Attach button</td>
<td>Click to open the Attach Notes (see page 41) dialog, where you can attach notes to the selected alarm.</td>
</tr>
</tbody>
</table>
Alarm Console Toolbars

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detach button</strong></td>
<td>Click to open the Detach Notes (see page 42) dialog, where you can detach notes from the selected alarm.</td>
</tr>
<tr>
<td><strong>Actions button</strong></td>
<td>Click to open the Actions (see page 39) dialog, where you can execute an action to launch a URL.</td>
</tr>
<tr>
<td><strong>Severity icons</strong></td>
<td>Click on an icon to display only alarms with that severity. The colors correspond to the following severity levels:</td>
</tr>
<tr>
<td>- Red = Critical</td>
<td></td>
</tr>
<tr>
<td>- Orange = Major</td>
<td></td>
</tr>
<tr>
<td>- Yellow = Minor</td>
<td></td>
</tr>
<tr>
<td>- Blue = Warning</td>
<td></td>
</tr>
<tr>
<td>- Light blue = Informational</td>
<td></td>
</tr>
<tr>
<td><strong>Stop updates icon</strong></td>
<td>Click to stop updates to the information in the Alarm Console. Otherwise, the alarm information is updated dynamically.</td>
</tr>
<tr>
<td><strong>Help icon</strong></td>
<td>Click to display the online help for the Alarm Console.</td>
</tr>
</tbody>
</table>

**Alarm Filter Bar**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rotate icon</strong></td>
<td>Click to rotate to the next toolbar.</td>
</tr>
<tr>
<td><strong>Alarm Filter pulldown</strong></td>
<td>Choose an alarm filter to apply. Filters display only specified alarms. Click the words Alarm Filter in the toolbar to clear all filters that have been applied.</td>
</tr>
<tr>
<td><strong>Set Alarm Filter button</strong></td>
<td>Click to create, edit, or delete a filter. Opens either the Alarm Filter Expression (see page 40) dialog, if the Default filter is selected, or the Alarm Filter (see page 40) dialog if a filter other than the Default is selected. The Alarm Filter Expression dialog allows you to specify criteria for the filter. The Alarm Filter dialog allows you to choose to add, edit, or delete a filter.</td>
</tr>
</tbody>
</table>
Alarm Console Toolbars

Filter Management button

- Click to display a popup menu:
  - Save Current Alarm Filter - Saves the current alarm filter. A dialog opens where you can enter the name for the filter. Once saved, you can choose the filter from the Alarm Filter pulldown menu.
  - Rename Current Alarm Filter - Click to rename the current filter. A dialog opens where you can edit the name of the filter.
  - Delete Current Alarm Filter - Click to delete the current filter.
  - Manage Alarm Filter ACL Associations - Opens the Manage Alarm Filter ACLs (see page 43) dialog, where you can set which ACLs the filter is accessible for.

Severity icons

- Click on an icon to display only alarms with that severity. The colors correspond to the following severity levels:
  - Red = Critical
  - Orange = Major
  - Yellow = Minor
  - Blue = Warning
  - Light blue = Informational

Stop updates icon

- Click to stop updates to the information in the Alarm Console. Otherwise, the alarm information is updated dynamically.

Help icon

- Click to display the online help for the Alarm Console.

---

History Bar

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotate icon</td>
<td>Click to rotate to the next toolbar.</td>
</tr>
</tbody>
</table>
### Alarm Console Toolbars

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alarm History button</strong></td>
<td>Click to open the <a href="#">Alarm History</a> dialog, where you can view a list of alarms for the selected time period in a separate window. The list includes acknowledged alarms, which are stored in the Nimsoft Alarm Server (NAS) history database.</td>
</tr>
<tr>
<td><strong>Query button</strong></td>
<td>Click to open the <a href="#">Query</a> dialog, where you can define a filter for the historical alarms you want to see.</td>
</tr>
<tr>
<td><strong>Run Query button</strong></td>
<td>Opens the <a href="#">Run Query</a> dialog, where you can execute a previously defined query.</td>
</tr>
<tr>
<td><strong>Transaction History button</strong></td>
<td>Click to open the <a href="#">Transaction History</a> dialog for the selected alarm. The Transaction History dialog shows the transaction log for the alarm, including the initial message, any suppressions, the closure message (when the alarm is acknowledged), and any other actions. &lt;br&gt;&lt;br&gt;Note: You can only view the transaction history for an acknowledged alarm by clicking the <strong>Transaction History</strong> button in the Alarm History dialog. See the section Alarm History Dialog.</td>
</tr>
<tr>
<td><strong>Severity icons</strong></td>
<td>Click on an icon to display only alarms with that severity. The colors correspond to the following severity levels: &lt;br&gt;&lt;br&gt;- Red = Critical &lt;br&gt;- Orange = Major &lt;br&gt;- Yellow - Minor &lt;br&gt;- Blue = Warning &lt;br&gt;- Light blue = Informational</td>
</tr>
<tr>
<td><strong>Stop updates icon</strong></td>
<td>Click to stop updates to the information in the Alarm Console. Otherwise, the alarm information is updated dynamically.</td>
</tr>
<tr>
<td><strong>Help icon</strong></td>
<td>Click to display the online help for the Alarm Console.</td>
</tr>
</tbody>
</table>
Alarm Console Table

The Alarm Console table lists information about alarms received. By default, a certain set of columns is displayed. You can change the columns displayed, or display all columns, by using the View pull-down menu on the General toolbar (see page 29). Click the text View next to the pull-down menu to return to the default view.

You can create filters to display alarms with only the specified criteria using the Filter field and the column pull-down menu, or by using the features on the Alarm Filter toolbar (see page 31). Click the word Filter or Alarm Filter to clear any filters applied.

Click on a column header to sort by that column. Clicking the column header again toggles between ascending and descending sort order.

You can change the width of the columns in the Alarm Console table. To do so, click on the column border and drag it to the width you want.

The Alarm Console table contains the following information. The columns you see depends on the setting you choose for the View pull-down menu.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Severity| Level of seriousness of the alarm. The severity levels are:  
  - Clear = Green  
  - Informational = Cyan  
  - Warning = Blue  
  - Minor = Yellow  
  - Major = Orange  
  - Critical = Red |
| Assign icons| An icon appears in this column if the alarm is assigned to a user. |
| Notes icons| An icon appears in this column if a note is attached to the alarm. |
| ID      | An automatically generated unique identification number. |
| Host    | The name of the computer hosting the probe sending the alarm.  
  Note: Occasionally the IP address of the host is displayed in this column instead of the name. You may be able to convert the IP addresses to names by changing the StripHostName setting in the Windows registry. However, this may result in timeouts.  
  To change the StripHostName setting, navigate to the setting as follows and change the value to 1: |
  ```hkey_current_user > software > nimbus software > nimbus manager > options > striphostname`` |
| Message | Description of the error condition. |
### Alarm Console Table

<table>
<thead>
<tr>
<th>Time Received</th>
<th>The last time the alarm was received by the Nimsoft Alarm Server (nas).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsystem</td>
<td>The part of the monitored computer the alarm was sent from (CPU, disk, memory, and so on).</td>
</tr>
<tr>
<td>Probe</td>
<td>Name of the probe that issued the alarm.</td>
</tr>
<tr>
<td>nas</td>
<td>Name of the Nimsoft Alarm Server (nas) storing and managing the alarm.</td>
</tr>
<tr>
<td>Origin</td>
<td>QoS data from probes is tagged with a name to identify the origin of the data. The origin name is set in the controller probe GUI. If the origin name is not set, the hub name is used.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of times the alarm was received from the probe.</td>
</tr>
<tr>
<td>Visible</td>
<td>Whether the alarm is set to Visible or Invisible.</td>
</tr>
<tr>
<td>Source</td>
<td>The IP address of the computer sending the alarm.</td>
</tr>
<tr>
<td>Subsystem ID</td>
<td>Identifier made up of one or more numbers separated by dots. This identifies which part of the monitored computer the alarm was sent from (CPU, disk, memory, and so on).</td>
</tr>
<tr>
<td>Robot</td>
<td>Name of the Nimsoft robot hosting the probe sending the alarm.</td>
</tr>
<tr>
<td>Hub</td>
<td>The hub controlling the robot hosting the probe that sent the alarm.</td>
</tr>
<tr>
<td>Domain</td>
<td>The name of the domain associated with the probe sending the alarm.</td>
</tr>
<tr>
<td>User Tag 1, User Tag 2</td>
<td>User-defined tag to be used to group or locate the source of alarms. The tag is set in the controller probe GUI, accessed via Infrastructure Manager.</td>
</tr>
<tr>
<td>Custom 1-5</td>
<td>Custom columns. You can set the value for these columns in the Set Custom Fields dialog.</td>
</tr>
<tr>
<td>Time Origin</td>
<td>The time when the alarm was sent from the probe.</td>
</tr>
<tr>
<td>Time Arrival</td>
<td>The time when the alarm was received by the nas.</td>
</tr>
<tr>
<td>Assigned To</td>
<td>User alarm is assigned to.</td>
</tr>
<tr>
<td>Assigned By</td>
<td>User who assigned the alarm.</td>
</tr>
</tbody>
</table>
There are two popup menus for the Alarm Console window. Access the popup menus by right-clicking on:

- [The toolbar](see page 36)
- [The Alarm Console table](see page 37)

### Toolbar Popup Menu

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotate Toolbars</td>
<td>Displays the next toolbar. The Alarm Console has a series of four toolbars you can rotate through. For more information, see [Alarm Console Toolbars](see page 29).</td>
</tr>
<tr>
<td>Group Alarms by Severity</td>
<td>Displays alarms of the same severity grouped together in the Alarm Console table.</td>
</tr>
<tr>
<td>Actions</td>
<td>Opens the [Actions](see page 39) dialog, where you can execute an action to launch a URL.</td>
</tr>
<tr>
<td>Manage Actions</td>
<td>Opens the [Manage Actions dialog](see page 43), where you can create, edit, or delete actions.</td>
</tr>
<tr>
<td>Set Custom Fields</td>
<td>Opens the [Set Custom Fields](see page 47) dialog, where you can set the value for the Custom columns in the Alarm Console table.</td>
</tr>
<tr>
<td>Find</td>
<td>Opens the [Find](see page 42) dialog, where you can search for alarms that contain specified text.</td>
</tr>
<tr>
<td>Select All Alarms</td>
<td>Selects all alarms in the Alarm Console table.</td>
</tr>
<tr>
<td>Deselect All</td>
<td>Deselects all alarms in the Alarm Console table.</td>
</tr>
<tr>
<td>Invert Selection</td>
<td>Reverses the selection of alarms. Alarms that were selected become deselected, and the unselected alarms become selected.</td>
</tr>
</tbody>
</table>
popup menues

chapter 4: alarm console

37

view trace log

opens the trace log (see page 48) dialog, where you can view information about each transaction for the alarm.

preferences

opens the preferences (see page 45) dialog, where you can choose settings that affect the behavior of the alarm console.

set default view

opens the set default view (see page 47) dialog, where you can set which columns are displayed in the default view.

settings

opens the adobe flash player settings (see page 40) dialog, where you can choose settings for adobe flash player.

about adobe flash player 10

opens an adobe web page with information about flash player 10.

alarm console table popup menu

<table>
<thead>
<tr>
<th>field</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>details</td>
<td>opens the details (see page 42) dialog, where you can view information about the selected alarm.</td>
</tr>
<tr>
<td>accept</td>
<td>assigns the selected alarm to yourself.</td>
</tr>
<tr>
<td>assign</td>
<td>opens the assign to (see page 41) dialog, where you can assign the selected alarm to another user.</td>
</tr>
<tr>
<td>unassign</td>
<td>unassigns the selected alarm from the user it was assigned to.</td>
</tr>
<tr>
<td>acknowledge</td>
<td>acknowledges the alarm. the alarm is considered closed and is removed from the alarm console table. the alarm is also deleted from the nimbus alarm server (nas) database, but a copy is retained in the history database.</td>
</tr>
<tr>
<td>show notes</td>
<td>opens the notes (see page 45) dialog, where you can view notes attached to the selected alarm.</td>
</tr>
<tr>
<td>attach</td>
<td>opens the attach notes (see page 41) dialog, where you can attach existing notes to the selected alarm or create new ones.</td>
</tr>
<tr>
<td>detach</td>
<td>opens the detach notes (see page 42) dialog, where you can detach notes from the selected alarm.</td>
</tr>
<tr>
<td>manage notes</td>
<td>opens the manage notes (see page 43) dialog, where you add, edit, or delete notes.</td>
</tr>
<tr>
<td>set visible</td>
<td>you can hide some alarms by marking them as invisible. to hide alarms, first select the alarms you want to hide in the alarm console table, then right-click and choose set invisible. unless the invisible alarms permission is set in the acl, the user does not see alarms that are marked invisible.</td>
</tr>
<tr>
<td>Menu Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set Invisible</td>
<td>If the Invisible Alarms permission is set in the ACL, alarms marked as invisible are displayed in the Alarm Console table in grayed out italics. To change an alarm to visible, right-click on the alarm and choose Set Visible.</td>
</tr>
</tbody>
</table>
| Transaction History    | Click to open the Transaction History (see page 48) dialog for the selected alarm. The Transaction History dialog shows the transaction log for the alarm, including the initial message, any suppressions, the closure message (when the alarm is acknowledged), and any other actions.  
**Note:** You can only view the transaction history for an acknowledged alarm by clicking the Transaction History button in the Alarm History dialog. See the section Alarm History Dialog. |
| Set Filter             | Opens the Alarm Filter Expression (see page 40) dialog, where you can create filters to display only the alarms with the properties you specify. |
| Copy to Clipboard      | Copies the selected alarm(s) to the clipboard.                                                                                                                                                     |
| Settings               | Opens the Adobe Flash Player Settings (see page 40) dialog, where you can choose settings for Adobe Flash Player.                                                                                      |
| About Adobe Flash Player 10 | Opens an Adobe web page with information about Flash Player 10.                                                                                                                                       |
Dialogs

- **Actions** (see page 39)
- **Adobe Flash Player Settings** (see page 40)
- **Alarm Filter Expression** (see page 40)
- **Alarm History** (see page 41)
- **Assign To** (see page 41)
- **Attach Notes** (see page 41)
- **Detach Notes** (see page 42)
- **Details** (see page 42)
- **Find** (see page 42)
- **Manage Actions** (see page 43)
- **Manage Alarm Filter ACLs** (see page 43)
- **Manage Notes** (see page 43)
- **New Action** (see page 44)
- **New Note** (see page 44)
- **Notes** (see page 45)
- **Preferences** (see page 45)
- **Query** (see page 46)
- **Run Query** (see page 46)
- **Set Custom Fields** (see page 47)
- **Set Default View** (see page 47)
- **Trace Log** (see page 48)
- **Transaction History** (see page 48)

### Actions Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions list</td>
<td>Click to select the action you want to execute.</td>
</tr>
<tr>
<td></td>
<td>To create, edit, or delete actions, right-click on the Alarm Console</td>
</tr>
<tr>
<td></td>
<td>toolbar and choose <strong>Manage Actions</strong> (see page 43) from the popup menu.</td>
</tr>
<tr>
<td>Execute button</td>
<td>Executes the selected action.</td>
</tr>
</tbody>
</table>
Adobe Flash Player Settings Dialog

This dialog allows you to choose settings for Adobe Flash Player. Click the (Help) button for information about these settings.

Alarm Filter Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Opens the Alarm Filter Expression (see page 40) dialog, where you can specify criteria for a filter.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the selected filter expression for editing.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected filter expression.</td>
</tr>
</tbody>
</table>

Alarm Filter Expression Dialog

The Alarm Filter Expression dialog allows you to create a filter for the alarms displayed in the Alarm Console table. You can filter on information in any of the columns in the Alarm Console table. The operator pulldown menu for most fields can be set to = or != (not equal). The Severity, Count, and Notes fields have additional choices for the operator menu. For a description of each field, see Alarm Console Table (see page 37).

Enter the information you want to filter on and then click OK. The Alarm Console table displays only the alarms that match the filter until you modify or clear the filter.

To save the filter expression in the repository click Filter Management, Save Current Alarm Filter on the Alarm Filter toolbar. Then you can choose the filter from the Alarm Filter pulldown menu.

Note: Unlike in Infrastructure Manager, the filters in the Alarm Console table in UMP use only regular expressions, not simple wildcards. For example, to filter for all hubs with a name starting with HUB, use the regular expression /HUB.*/. Entering HUB* will not work.
Alarm History Dialog

The Alarm History dialog displays information about historical alarms. To access the dialog, click Alarm History on the History toolbar (see page 32), then select a time period. For information about the columns displayed in the table, see Alarm Console Table (see page 37).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter field</td>
<td>Enter text to display only alarms that contain that text.</td>
</tr>
<tr>
<td>Transaction History button</td>
<td>Click to launch the Transaction History dialog, which shows the transaction log for the alarm, including the initial message, any suppressions, the closure message (when the alarm is acknowledged), and any other actions. Launching the Transaction History dialog from within the Alarm History dialog (rather than from the History toolbar or from the Alarm Console table pop-up menu) allows you the additional ability of viewing the transaction log for acknowledged alarms.</td>
</tr>
<tr>
<td>Show all columns check box</td>
<td>Click to show all columns of the Alarm Console. Otherwise, only the columns for the Default view are shown.</td>
</tr>
</tbody>
</table>

Assign To Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign To list</td>
<td>Lists the users you can assign the alarm to. Click a user name to select it.</td>
</tr>
<tr>
<td>Assign button</td>
<td>Assigns the alarm to the selected user.</td>
</tr>
<tr>
<td>Filter field</td>
<td>Enter text to display only user names that contain that text.</td>
</tr>
</tbody>
</table>

Attach Notes Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach Notes list</td>
<td>Lists the available notes. Click on the name of a note to select it.</td>
</tr>
<tr>
<td>OK</td>
<td>Attaches the selected note to the alarm.</td>
</tr>
</tbody>
</table>
Detach Notes dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detach Notes list</td>
<td>Lists the available notes. Click on the name of a note to select it.</td>
</tr>
<tr>
<td>OK</td>
<td>Click to detach the selected note from the alarm.</td>
</tr>
</tbody>
</table>

Details Dialog

The Details dialog provides a way to view the information in the Alarm Console table (see page 37) one alarm at a time. To access the dialog, select an alarm in the Alarm Console table and click Details on the General toolbar (see page 29); or right-click and choose Details from the popup menu (see page 37).

The information displayed is the same as in the Alarm Console table. The radio buttons on the left allow you to select which columns to view, similar to the View pulldown menu on the General toolbar. The arrows allow you to view the previous or next alarms in the Alarm Console table.

For more information about the columns or buttons in the Details dialog, see Alarm Console Table (see page 37) and Alarm Console Toolbars (see page 29).

Find Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find field</td>
<td>Enter the text you want to search for.</td>
</tr>
<tr>
<td>Column pulldown</td>
<td>Choose the column you want to search for the specified text.</td>
</tr>
<tr>
<td>Select button</td>
<td>Selects the alarms with matching text.</td>
</tr>
<tr>
<td>Find Previous button</td>
<td>Displays the previous instance of the text.</td>
</tr>
<tr>
<td>Find Next button</td>
<td>Displays the next instance of the text.</td>
</tr>
</tbody>
</table>
Manage Actions Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/URL list</td>
<td>Click to select the Name/URL of the action you want to modify.</td>
</tr>
<tr>
<td>New button</td>
<td>Click to open the <a href="#">New Action</a> (see page 44) dialog, where you can create an action.</td>
</tr>
<tr>
<td>Edit button</td>
<td>Click to modify the selected action.</td>
</tr>
<tr>
<td>Delete button</td>
<td>Deletes the selected action.</td>
</tr>
</tbody>
</table>

Manage Alarm Filter ACLs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Filter list</td>
<td>Click to select the alarm filter you want to set ACL access for.</td>
</tr>
<tr>
<td>ACL list</td>
<td>Click to select the ACLs you want to have access to the selected alarm filter.</td>
</tr>
<tr>
<td>Selected filter is accessible to all ACLs check box</td>
<td>Click to allow all ACLs to have access to the selected alarm filter.</td>
</tr>
<tr>
<td>OK button</td>
<td>Saves changes and closes the dialog.</td>
</tr>
<tr>
<td>Cancel button</td>
<td>Closes the dialog without saving changes.</td>
</tr>
</tbody>
</table>

Manage Notes Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>An automatically generated unique identification number.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the note.</td>
</tr>
<tr>
<td>Category</td>
<td>Enter the name of a category for the note.</td>
</tr>
<tr>
<td>Auto Remove</td>
<td>Whether or not Auto Remove is enabled. When enabled, the note is automatically removed from the repository when there are no active alarms that are attached to the note.</td>
</tr>
<tr>
<td>Time Modified</td>
<td>Time when the note was created or last modified.</td>
</tr>
</tbody>
</table>
New Action Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>Enter a name for the action.</td>
</tr>
<tr>
<td>URL field</td>
<td>Enter a URL for the action to launch.</td>
</tr>
<tr>
<td>Arguments button</td>
<td>Displays a list of substitution values you can use in the URL. For example, you can use $ASSIGNED_TO and the name of the user assigned to the alarm you are executing the action for is inserted in the URL.</td>
</tr>
<tr>
<td>OK button</td>
<td>Saves the action and closes the dialog.</td>
</tr>
<tr>
<td>Cancel button</td>
<td>Closes the dialog without saving changes.</td>
</tr>
</tbody>
</table>

New Note/Edit Note Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>Enter a name for the note.</td>
</tr>
<tr>
<td>Category pulldown</td>
<td>Choose a category for the note.</td>
</tr>
<tr>
<td>Text field</td>
<td>Enter text for the note.</td>
</tr>
<tr>
<td>Auto Remove checkbox</td>
<td>Check this to automatically remove this note from the repository when there are no active alarms that are attached to the note.</td>
</tr>
<tr>
<td>OK</td>
<td>Click to save the note. Your user name and the current time are automatically added to the note.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to close the dialog without saving changes.</td>
</tr>
</tbody>
</table>
### Notes Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes field</td>
<td>Text of the note.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves any changes and closes the dialog.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Closes the dialog without saving changes.</td>
</tr>
<tr>
<td>Add Comment</td>
<td>Click to add a comment to the note.</td>
</tr>
</tbody>
</table>

### Preferences Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use extended color scheme check box</td>
<td>If selected, the table cells in the Alarm Console table are colored according to severity level.</td>
</tr>
<tr>
<td>Launch on alarm image click pulldown</td>
<td>Choose a dialog to open when the icon in the severity column is clicked:</td>
</tr>
<tr>
<td></td>
<td>- [Details](see page 42)</td>
</tr>
<tr>
<td></td>
<td>- [Attach Notes](see page 41)</td>
</tr>
<tr>
<td></td>
<td>- [Actions](see page 39)</td>
</tr>
<tr>
<td>Immediate client side update of alarm lines check box</td>
<td>If selected, the Alarm Console table updates as alarms are received.</td>
</tr>
<tr>
<td>Use time zone for pulldown</td>
<td>Choose the device you want to use as the source for setting the time zone.</td>
</tr>
<tr>
<td>Set default alarm filter pulldown</td>
<td>Choose the alarm filter to be applied to the Alarm Console table by default upon opening.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves changes and closes the dialog.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Closes the dialog without saving changes.</td>
</tr>
</tbody>
</table>
Query Dialog

The Query dialog allows you to search the historical database for alarms from a specified time period. You can also specify information for each field to search for. For information about each field, see Alarm Console Table (see page 37).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Beginning of the time period you want to view alarms for.</td>
</tr>
<tr>
<td>To Date</td>
<td>End of the time period you want to view alarms for.</td>
</tr>
<tr>
<td>OK</td>
<td>Executes the query.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the query and closes the dialog.</td>
</tr>
<tr>
<td>Reset Query</td>
<td>Clears the fields in the dialog.</td>
</tr>
<tr>
<td>Save Query</td>
<td>Saves the query to a local repository. To execute a query in the repository, click the Run Query button on the History toolbar (see page 32).</td>
</tr>
</tbody>
</table>

Run Query Dialog

The Run Query dialog allows you to execute a previously defined query. To access the dialog, click the Run Query button on the History toolbar (see page 32).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query list</td>
<td>Select the query you want to run.</td>
</tr>
<tr>
<td>Run Query</td>
<td>Executes the selected query.</td>
</tr>
<tr>
<td>Delete Query</td>
<td>Deletes the selected query from the repository.</td>
</tr>
</tbody>
</table>
**Set Custom Fields Dialog**

This dialog allows you to set values for the alarm table columns My Custom 1 through My Custom 5. To access this dialog, right-click on the toolbar in the Alarm Console and choose **Set Custom Fields** from the popup menu.

You must have the appropriate permissions set in the ACL in order to access this dialog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom radio buttons</td>
<td>Select the custom field you want to set the value for. These fields are displayed as columns in the Alarm Console table.</td>
</tr>
<tr>
<td>Value field</td>
<td>Enter a value for the custom field.</td>
</tr>
<tr>
<td>Set Value button</td>
<td>Click to save changes and close the dialog.</td>
</tr>
</tbody>
</table>

**Set Default View Dialog**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Columns list</td>
<td>Lists the columns of the Alarm Console table. Click to select a column to add to or remove from the Visible Columns list.</td>
</tr>
<tr>
<td>Visible Columns list</td>
<td>Lists the columns that will be visible in the Default View for the Alarm Console table. These are the columns the user will see unless they select a different view.</td>
</tr>
<tr>
<td>Add button</td>
<td>Adds the selected column to the Visible Columns list.</td>
</tr>
<tr>
<td>Remove button</td>
<td>Removes the selected column from the Visible Columns list.</td>
</tr>
<tr>
<td>Reset button</td>
<td>Resets the Visible Columns list to the default.</td>
</tr>
<tr>
<td>Auto calculation of the alarm list width check box</td>
<td>If selected, the width of the Alarm Console table is set automatically based on the default widths of the columns displayed. If not selected, you can specify a width for the Alarm Console table in the Width spin box. You can adjust the width of individual columns by dragging the column rule in the Alarm Console table. You can also drag the columns to rearrange the order.</td>
</tr>
<tr>
<td>Width spin box</td>
<td>If the Auto calculation of the alarm list width check box is not selected, you can set the width of the Alarm Console table. You can adjust the width of individual columns by dragging the column rule in the Alarm Console table. You can also drag the columns to rearrange the order.</td>
</tr>
</tbody>
</table>
**Trace Log Dialog**

The Trace Log contains information about actions taken by the Alarm Console. It is primarily used by Nimsoft support personnel to troubleshoot problems with the Alarm Console.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of item being traced.</td>
</tr>
<tr>
<td>Token</td>
<td>Type of request, action, or incoming event being processed.</td>
</tr>
<tr>
<td>Detail</td>
<td>Additional information about the request, action, or event.</td>
</tr>
<tr>
<td>Time</td>
<td>Time the request, action, or event occurred.</td>
</tr>
</tbody>
</table>

**Transaction History Dialog**

The Transaction History dialog shows the transaction log for the alarm, including the initial message, any suppressions, the closure message (when the alarm is acknowledged), and any other actions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter field</td>
<td>Enter text to display only alarms that contain that text.</td>
</tr>
<tr>
<td>Show all columns check box</td>
<td>Click to show all columns of the Alarm Console. Otherwise, only the columns for the Default view are shown.</td>
</tr>
</tbody>
</table>
Enabling the Alarm Console

In order to access the Alarm Console application, you must enable the Alarm Details permission in the Access Control List (ACL).

1. In the Infrastructure Manager, select Security > Manage Access Control List.
2. Select the relevant ACL in the Access Control List pane.
3. In the Permissions pane, select the Alarm Details permission, then click OK.

The following permissions affect the information you can view and actions you can take in the Alarm Console:

- Accept
- Unassign
- Invisible Alarms
- Alarm History
- Acknowledge
- Alarm Management
- Assign
- Reassign

For more information about ACL permissions, see the Infrastructure Manager documentation.

Troubleshooting Alarm Console

This section tells you how to troubleshoot common issues with Alarm Console.
$PASSWORD Substitution in Alarm Console

To use $PASSWORD substitution in Alarm Console, you must enable it by adding a key to the wasp.cfg file.

Follow these steps:
1. Locate the wasp.cfg file in the following directory:
   `<UMP_installation>/probes/service/wasp/conf`
2. Open wasp.cfg in a text editor.
3. In the webapps/alarmconsole section, add the following line:
   `enable_password_arg = true`
4. Save and close the wasp.cfg file.
5. Restart wasp.

Alarm Console Loses Filters with Internet Explorer

If you launch the Alarm Console portlet from a dashboard in Internet Explorer and later reload the page, Alarm Console loses its filter state and shows all alarms.

No Data Displayed in Alarm Console

Valid for MySQL and Oracle

Symptom:
When I log into UMP as an administrative user, the Alarm Console portlet does not display any data.

Solution:
This can occur in large environments with approximately 4000 or more robots, where MySQL or Oracle is the database provider.

You may be able to fix this issue by editing the following parameters in the `<setup>` sections of the wasp.cfg and dashboard_engine.cfg files:
- In the wasp.cfg, increase nimpool_timeout from 30 to 90.
- In the dashboard_engine.cfg, increase dynamic_views from 60 to 120.
Chapter 5: Cloud User Experience Monitor

Cloud User Experience Monitor allows you to access the online service that monitors your sites, servers, and applications 24 hours a day, 7 days a week. Access to this portlet requires the NMS user to be an Account Contact User. It also requires that you have a WatchMouse account associated with this NMS Account and have obtained the required credentials associated with this WatchMouse account.

This section contains the following topics:

- Cloud User Experience Monitor Configuration (see page 51)
- WatchMouse Server Location Configuration (see page 52)
- SSO Credentials Configuration (see page 53)

Cloud User Experience Monitor Configuration

The Cloud UE Monitor portlet will NOT show up in your "Add Portlet" list. You have to log into UMP and import the lar file in order to access the portlet.

**Important:** The Cloud User Experience Monitor portlet requires the UMP user’s permissions to include the "Cloud UE Monitor" ACL permission. This ACL is included in Infrastructure Manager (IM) version 4.02 or later. Any versions of NMS previous to 5.61 will require an IM upgrade to version 4.02.

To import a lar file:

1. Navigate to http://<umpserver>/cloudmonitor/jsp/get_lar.jsp
2. Click on the CloudMonitor.lar link to download the file.
3. Login to UMP as the user that requires access to the Cloud UE Monitor portlet.
   
   **Note:** This user must be an UMP Account Contact for an account that has a WatchMouse account and associated credentials.

5. Select Private Pages > Export/Import > Import.
6. Click Browse to locate the CloudMonitor.lar file on your machine.
7. Click Import.

You should receive a message indicating the import was successful. You can now click "Back to Private Pages" to return to UMP.
WatchMouse Server Location Configuration

The server location for your WatchMouse instance must be configured via the wasp probe raw configuration.

To configure the wasp probe:

1. In Infrastructure Manager select the wasp probe on your hub.
2. Click Shift Right-click, then select Raw Configure.
3. In the webapps/cloudmonitor section, enter the value of the WatchMouse server as the value for the "url" key.
4. Click OK, then click OK to exit the configuration screen.

Example:

http://ump.cloudmonitor.nimsoft.com
SSO Credentials Configuration

There is only one Cloud User Experience login associated with all the Account Contact users for an NMS account.

**To configure single-sign-on for CUE, follow these steps:**

1. Log into your CUE account.
2. Click the **Reports** menu and select the **Access** item. The reports access page opens.
3. At the bottom of the page, look for the table labeled **Tokens can be used to provide access on your account via external applications.** If there is a token listed, you can use it. If not click the **Add token** button to create one.
   
   **Note:** Keep this page open, as you will need the **Mid** and **Token** values found here in an upcoming step.
4. Start Infrastructure Manager and log into the Nimsoft Server.
5. Click the **Security** menu and select the **Account Administration** item. Make a note of the Account name that is to be used for CUE integration.
   
   **Note:** This Account must be attached to an ACL that grants permission to **Access to Cloud User Experience Monitor portlet**. Use the **Manage Access Control List** on the **Security** menu to verify this.
6. Use a plain text editor such as Notepad or "vi" to open and edit the template SSO configuration file, which is located on the UMP server as follows:

   `<installation_directory>/Nimsoft/service/probe/wasp/webapps/cloudmonitor/ssoConfig.xml`

7. Follow the example below, and the notes in the XML syntax comment section of the file, to create an account entry using the **name**, **mid**, and **token**, information determined in previous steps. The following is an example of a finished `ssoConfig.xml` file:

   ```xml
   <?xml version="1.0" encoding="UTF-8"?>
   <ssoConfig>
     <accounts>
       <account>
         <name>Nimsoft_account_name_identified_in_step_5</name>
         <mid>53156</mid>
         <token>a3a08368cecd501871e1e29e87600d04d8aa575663d8947e5ca91af6b62c5b58</token>
       </account>
     </accounts>
   </ssoConfig>
   ```

8. Save the file when done editing.
9. Restart the **cloudmonitor** app within the **wasp** probe. Alternatively, you can restart the **wasp** probe itself.
Log into UMP as the "Contact" authorized for CUE access, and open the Cloud User Experience Monitor portlet. The display should update with your CUE data.
Chapter 6: Custom Dashboards

This application lists the custom dashboards created using the Dashboard Designer. Which dashboards you see depends on the permissions set in the ACL for your user account.

If you do not have the Custom Dashboards permission set in the ACL, you will see a "Permission Denied" message when you try to run the Custom Dashboards application.

This section contains the following topics:
- Dashboard Pane (see page 55)
- Managing Alarms in Dashboards (see page 57)

Dashboard Pane

The color of the icons in the tree structure represents the highest alarm severity for alarm objects on the dashboards. Double-click an icon and the corresponding dashboard is launched in the dashboard pane.

The dashboards can contain meters, alarm objects, gauges, charts, tables, panels, and so on.

Alarm and panel objects reflect the severity level of the alarm with the highest severity. Double-clicking an alarm object brings up the alarm list, enabling you to manage the alarms. See Managing Alarms in Dashboards (see page 57) for more information.
Mini Map Tool

The Mini Map tool zooms in on an area of a dashboard. A minimized version of the dashboard is shown in the Mini Map window. A slider lets you zoom in or out of the dashboard on the canvas.

Dragging the yellow field in the Mini Map lets you pan the dashboard.
Managing Alarms in Dashboards

If the dashboard contains alarm objects, you can display the related alarms in the Alarm Console by double-clicking an alarm icon that is not green (there are no alarms associated with green objects).
Chapter 7: Dashboard Designer

Dashboard Designer allows you to monitor computer systems on your network for QoS data and alarms using various template widgets, such as alarm objects, meter objects, charts, and tables.

- Alarm objects can be filtered to reflect the state of the computers you want to see
- Meter objects can be connected to data sources such as QoS, probes, or variables
- Panels can be used to build dashboards with several levels in a tree structure
- Table objects can be used if you want to present the output from a query to the NIS as a table in a dashboard

The layout of the dashboard components and the background canvas can be configured with a wide range of colors, fonts, sounds and data sources.

You can also import and use pre-made dashboard templates. There are four Dashboard Templates available: two for network devices and two for server systems.

You will also find several general objects, like text objects, images etc. The Dashboard Designer also contains a Preview tool, letting you see the appearance and layout of the Dashboard before publishing it.

The Dashboards will, when saved and published, be available in the Unified Management Portal. There you can see the state and QoS values of the monitored systems and also manage the alarms.

If you do not have the Dashboard Designer permission set in the ACL, you will see a "Permission Denied" message when you try to run the Dashboard Designer application. You must also have the Dashboard Publish permission set in the ACL in order to publish dashboards.

This section contains the following topics:

Designing a New Dashboard (see page 59)
The Application Window (see page 103)
Troubleshooting Dashboard Designer (see page 127)

Designing a New Dashboard

The following sections describe how to design a new dashboard.
Create Dashboard

Click the New button to create the new Dashboard.

The Create Dashboard dialog appears. Give the Dashboard a name and optionally a brief description. Click the OK button.
When creating a Dashboard, it is mandatory to specify a name, otherwise the OK button at the bottom of the dialog is disabled, and you can’t save the dashboard.

Further validation is done when you click the OK button.

First it checks for invalid characters.

**Note:** The following special characters must NOT be used in dashboard names:

| § | ! | " | # | % | & | ' | ( | ) | = | ? | \ | ] | { | } | @ | £ | $ |
If there are no invalid characters, then it checks that the Dashboard name is unique:

![Create Dashboard dialog](image)

**Note:** The Create from Xml option lets you create a Dashboard based on a XML code that you paste into a field appearing in the lower part of the dialog when clicking the Create from Xml option.

The xml code for a Dashboard opened in the Dashboard Designer will be available when clicking the XML button under the Current Dashboard tab.

![Dashboard xml code](image)

The xml code will then be opened in a separate window, enabling you to copy the code and use it as input when creating Dashboards in another environment.
Deploying Widgets

You can start deploying objects to the canvas to build your Dashboard. You can also use templates found under the Templates node.

**Note:** You may also save your own Dashboards as templates by right-clicking selecting the components on the canvas and select Save as Template.

Optionally you may prepare the canvas as described in the section Preparing the Canvas if you wish.

Expand the nodes in the Dashboard Components section in the upper left corner to locate the first object you want to use on your Dashboard. Place the cursor on the object, press and hold the left mouse button and drag and drop the object on the canvas.
The object will now appear on the canvas. The red borders indicate that the object is selected. This is important when you have multiple objects on the canvas, so that you know which object to configure.
Now you can set the properties for the object. See the section The Dashboard Components for a description of the properties for the different objects.

When finished with the first object, you may continue with additional objects until your Dashboard is finished.

**Note:** You may easily move, align and distribute objects as described below, see Managing objects on the canvas (see page 80).

When all objects are present, you must save the Dashboard. Click the Save button.

The following dialog appears. Click the OK button to finish the operation.
Finally, click the Publish button to make the Dashboard available.
Using ArrowLine and EllipseLine

ArrowLine enables you to display one or more arrows as directional markers between an alarm line that joins two widgets.

EllipseLine enables you to draw the alarm line as an elliptical curve, rather than just a straight line between the two widgets.

Create a new dashboard by clicking the New button from Dashboard List tab.

![Dashboard List](image)
Create Dashboard dialog appears. Enter a name for the dashboard. If necessary, you can also enter a description. Click OK button.

From the Dashboard Components, drag and drop the necessary components on the canvas (for example, alarm and gauge widgets).

Next, drag and drop the Alarm Line component.

From AlarmLine Properties section, click the Configure EndPoints button. A dialog appears. Select the checkboxes for the components (in this example, alarm and gauge widgets) and click Apply.
On the canvas, the alarm line links the gauge and alarm widgets.

Choose a thickness for the alarm line by selecting a value from the thickness field.

By default, ellipseX and ellipseY fields are set to 0, hence a straight line is drawn. If you wish to draw the alarm line as an ellipse, specify the necessary parameters in these fields.

Next, click the arrowDirection drop-down button to choose the direction of arrows to be displayed on alarm line. Choose the widget to which you wish to arrow to point to. (In this example, if you choose the alarm widget, the arrow will point from the gauge towards the alarm).
Next you need to specify the number of arrows to be shown on the line. By default, this value is set to 0, hence no arrows are displayed. Enter any number between 0 to 10. If you enter 1, the arrow will be placed at the midpoint of the alarm line. In case of more than one arrow, the arrows will be placed equidistant on the alarm line.

Click Publish button from Current Dashboard tab to save and publish your dashboard.
Using Line Map

Line Map component enables you to display a line that changes its color based on set of data from the external database. You can choose the color of the line when the set of values (such as QoS data) matches a particular data range.

Line Map also supports the ArrowLine (directional markers) and EllipseLine properties discussed in the previous section.

Create a new dashboard by clicking the New button from Dashboard List tab.
Create Dashboard dialog appears. Enter a name for the dashboard. If necessary, you can also enter a description. Click OK button.

From the Dashboard Components, drag and drop the necessary components on the canvas (for example, alarm and gauge widgets).

Next, drag and drop the Line Map component.

From LineMap Properties section, click the Configure Endpoints button. A dialog appears. Select the checkboxes for the components (in this example, alarm and gauge widgets) and click Apply.
On the canvas, the line map links the gauge and alarm widgets.

You can configure the line map properties by specifying the necessary parameters in thickness, ellipseX and ellipseY fields.

Next, click the arrowDirection drop-down button to choose the direction of arrows to be displayed on line map. Choose the widget to which you wish to arrow to point to. (In this example, if you choose the alarm widget, the arrow will point from the gauge towards the alarm).

Next you need to specify the number of arrows to be shown on the line. By default, this value is set to 0, hence no arrows are displayed. Enter any number between 0 to 10. If you enter 1, the arrow will be placed at the midpoint of the alarm line. In case of more than one arrow, the arrows will be placed equidistant on the alarm line.

From the lineColor, choose a color for the arrows displayed on the line map.
Next, click the arrows on the Select Datasource menu bar on the Dashboard Designer toolbar. The Select Datasource dialog appears. In the QoS tab, navigate to and select the required QoS data source. Click OK.

Next, click the Configure Ranges button. Gauge Ranges dialog appears. In the range Start field, enter the starting value for the range. In the color section, choose the color which you wish to indicate the restive range. You can add more ranges by clicking the + button. To remove a range, select it and then click the – button.

After selecting the colors for all the ranges, click apply.
Click Publish button from Current Dashboard tab to save and publish your dashboard.
Converting Data Units

The unit conversion can perform calculations on a data source value for meter and chart widgets before displaying the value.

In the Dashboard section, select the widget that you want to modify the units for.

For example, a value reported in bytes per second can be converted before display to bits per second by setting `unitMultiplier` to 8 and `unitDivisor` to 1. See the fields `unitMultiplier` and `unitDivisor` in the example below for both Gauge and Chart widgets.
Url Attribute

The widgets Text and Image offer the designer the ability to map a URL to the given widget. If the widget is clicked in player mode, the given URL will be shown in a separate window/tab.
Designing a New Dashboard

Chapter 7: Dashboard Designer

1. Select the image you want to link to a URL.

2. Click Set URL in the Image Properties section. The Set URL dialog is displayed.

3. Enter the URL in the URL text box.
Managing Objects on the Canvas

You can move an object on the canvas by placing the cursor on the object, pressing and holding the left mouse-button, and then drag the objects to a new position.

To be able to work with objects on the canvas (move, align, position, delete, align, set options etc.), the objects must be selected.

You can select multiple objects by placing the cursor on an empty space on the canvas, pressing (and holding) the left mouse button while dragging the cursor over the objects you want to select.

When multiple objects are selected, one of them will automatically be selected as a reference object for alignment of objects, marked with a red border. You can easily select another of them as a reference object for alignment by left-clicking that object.

Preparing the Canvas

It is possible to add a background image or add a background color on the canvas as a background for your Dashboard. You may also decide whether a dashboard panel should be scaled or not when launched.

Selecting the Data Source

Some of the objects used in the Dashboards (meter objects, tables, and trend graphs) display values obtained from a data source. The data can be obtained from:

- QoS data stored in the Nimsoft Information Store (NIS)
- A query to the NIS
- Values from a variable
- A probe
- A database
- An SLA

The Select Datasource dialog is accessed from the Dashboard Designer toolbar. Select the widget for which you wish to configure the data source and click the button on the Select Datasource menu bar.

The Select Datasource dialog is displayed. The dialog has these tabs: QoS, NIS, Variables, Probe, DB and SLA.
After configuring a data source, you can apply it to a widget of your choice by dragging and dropping the 🎨 icon on that widget, or by clicking **Apply**.

Not all widgets support each data source, as indicated by this 🎨 icon:

**Selecting a Data Source—QoS**

The Quality of Service (QoS) data source allows you to access data stored in the QoS database.

**Follow these steps:**

1. Click the **Tree** radio button.
2. Click the **QoS** you want, then the **Source**.
3. If there is more than one **Target**, click the **Target** you want.
   
   **Note:** Use the **QoS**, **Source**, **Target**, **Probe**, and **Origin** fields to filter for text you enter. For example, if you enter **CPU** in the QoS field you see only QoS items with **CPU** in the name.

4. Click **Apply**, or drag and drop the 🎨 icon on the object you are assigning the data source to.
Selecting a Data Source--NIS

You can also associate an object with a generic database interface. It’s important to know that the SQL statement should be constructed in such a way that a numeric value will be the result.

If a statement results in several rows of data and even multiple columns, the application will seek for the very first cell, which is the value of the first column in the first row. If using a query as data source for e.g. a table object, it is important that the query must correspond to the number of columns in the table.

Testing the NIS query

Use of long queries or badly written NIS queries can lead to degradation of the system performance. In order to avoid this, you can specify a time-period within which a query is expected to be executed. This value can be set using the sql_query_execute_time key in the dashboard_engine probe. By default, the value for this key is set to 5 seconds.

In case of Gauge widget:

Click the Test button in the Select Datasource dialog for a Gauge widget.

In case of Table widget:

Click the Test button in the Dialog window that appears when you click the Configure Columns button for a Table widget. (Please refer to section Configuring the Table widget for more details about Configure Columns).

When user clicks the Test button, the dashboard_engine executes the query and determines the elapsed time of the query. If the elapsed time of the query is greater than the value specified in the sql_query_execute_time key, the following message appears:

```
Warning

The time taken by SQL Query is 9 seconds which is more than the configured value of 6 seconds. Please change the query else it will result in degraded performance.

OK
```
Selecting a Data Source--Variables

The QoS data can also be obtained from a variable, made available from the variable_server probe. Select the variable from the list and click the OK button.

**Note:** The filter functionality is at the bottom of the dialog. Use the Name Filter field to filter the available data sources. For example, if you enter "gne" in this field, only sources containing the string "gne" in their names will be listed. To reset the filter, click the icon on the right-hand side of the filter field, and all the available data sources are again listed.

Selecting a Data Source--Probe

The Probe data source allows you to select the QoS data from a specific probe.

Start by specifying the Robot where the probe resides from the drop-down list.

Next, select the probe from the drop-down list, which displays all probes found on the specified robot.

The Request drop-down list shows all commands found for the selected probe. For some of the commands, it is possible to add further specifications. Use the Arguments section to add the necessary data.

For some of the probe requests, you can select a result token (the value you want to extract from the data returned by the probe).

**Note:** For some probe requests, the Advanced button is active, and you can use the Advanced button to further refine the result you want.

Finally, specify how often (in seconds) the request is to be executed in the Poll Interval field. The database is typically updated by probes every 5 minutes or so. Check the exact time value by viewing the configuration for the probe in question. Be careful not to specify a poll interval value for the object that queries the database unnecessarily often, as the same data will be collected if an update has not been received.
When you are done click the Test button to verify the value is as expected.

**Advanced button**

This button is active and can be used for certain probe requests. Click the Advanced button to list all the indexes (each containing a number of result tokens) available for the selected probe request.

Make your choice and click the OK button to save and return to the Select Datasource dialog. Check the result by clicking the Test button.

Click the OK button to save your data source definition.

Click the Preview button in the Dashboards to see the same value as the Test button in the meter object.

Once saved, the data source is validated again the next time you click Select Datasource button from the same dashboard,

If the selected robot is unavailable, the Robot Address value is indicated by a red border, with a tool tip “Invalid Robot”. The pre-selected probe and its parameters (such as Request, Result Token, and Poll Interval) are retained, thus enabling you to choose a different robot from the list.

In case the selected probe is unavailable, the Probe value is indicated by a red border, with a tooltip “Invalid Probe”. The pre-selected parameters (such as Request, Result Token, and Poll Interval) are retained.

When you select a different probe from the Probe drop-down menu, the pre-configured parameters are cleared.
Selecting a Data Source--DB

The DB data source allows you to execute various SQL commands to fetch any data from the selected database. You can select the database from the Databases drop down list which displays all the databases configured in dap probe. For more details please see dap probe document.

Note: The DB tab is available only for Report Template.

To execute stored procedure from dashboard designer dap, perform the following steps:

1. Add any meter, table, chart, or text widget (for e.g. "Gauge", "Table") from the Dashboard Components.
2. Select the widget.
3. Click the arrows on the Select Datasource menu bar.
4. Select the DB tab.
5. Select dap from Databases drop down list.
6. To execute stored procedure use the following syntax
7. `exec <sp_name> [<arg1> <arg2> <arg3> ... <argN>]`
    
    For example:
    ```
    exec spn_dd_GetQOSDetailsByld 1
    ```
8. Click on Test button.

Note: For meter widgets, the stored procedure will display the value of first row and first column provided the value is numeric. For text widget it will display the value of first row and first column.

Selecting a Data Source--SLA

The SLA tab shows a list of Service Level Agreements (SLAs) and their respective Service Level Objectives (SLOs).

When the dashboard is published, the widget shows the compliance percentage of the respective SLA or SLO in the dashboard player.
Configuring the Table Widget

Use the Table widget when you want to present the output as a table in a dashboard.

To select the data source for a Table widget, follow these steps:

1. Click the Table widget to select it.
2. Click the arrows on the Select Datasource menu bar.
   The Select Datasource dialog is displayed.
3. Select and configure the data source, then click OK.
   **Note:** The Table widget supports only NIS, Probe and DB data sources.
4. Click the Configure Column button to configure the table.
5. Click the +/- sign in the lower left corner to add rows to the table.
   By default the Table widget displays three rows.

**Header Label**
Replace the entries in the Header Label column with header names describing the selects.

**Data Source**
Replace the entries in the Data Source column with the appropriate data source information.

**Numeric Data**
Check the Numeric Data option for columns with data source returning numeric data.

**Align**
Select the alignment for the values in this row. Valid options are left, middle and right.

**Visualization**
Select the way the result should be presented in the different columns of the table:

- **None**
  The value will be presented as it is returned (as text or a number).
- **Bar**
  The value will be presented as a bar. Default range is 0-100.
- **Gauge**
  The value will be presented as a gauge. Default range is 0-100 Use the Range Min and Range Max to customize the range.
Map

This option lets you specify intervals for how to map numeric values to certain color and text attributes.

Color

Use this palette to select the color of the bar or gauge selected to present the values in this column.

Range Min and Range Max

Gauges and bars will by default have a range from 0 to 100. These ranges can be modified here.

Map

Select this option to enable Set Data button on the right-hand side of the dialog. Click this button to open the Set Map Data dialog.

Here, you can define how the values for the selected items should be presented in the table. You can define a number of ranges, where the values will be presented differently depending on range. Click the ‘+’ button in the lower left corner to add a range. Fill in the range (from and to value), the type (circle, square or text), color and text weight normal or bold for each of the ranges you want.

Auto

Selecting this option, the width of the column will automatically be set to fit the contents displayed in the column.

Width

De-selecting the Auto option (see above), you will be allowed to specify a specific column width in pixels.
Configuring a Widget to Use External DB Data

Some widgets (all meter widgets and the text widget) support showing data from databases other than the NIS database.

The DAP service probe is used to execute the SQL against non-NIS databases and should consequently be active in order to use this functionality.

The values available in the “Databases” drop-down box are configured using the DAP Configurator.
Using Variables for Widgets

You can use variables to assign certain properties to widgets. By using a variable, you can define the properties once and use the variable multiple times. Also, any changes to the properties can be made in a single place.

Variables are shared among all levels of a dashboard (if you use the Panel widget to create multiple levels). However, variables are not shared between dashboards.

There are four types of variables:

**QoS**

Allows you to specify a QoS measurement. You can specify source, target, probe, and origin for the QoS. This variable can be used with any widget that has a data source.

**Robot**

Allows you to specify a robot in the Probe tab of the Select Datasource dialog. You can specify the domain, hub, and robot name. This variable can be used with any widget that has a single value. It cannot be used with widgets with multiple values, such as charts (graphs).

**Host**

Allows you to use a variable for a host name for alarm objects. This variable can be used only in the Host Name field of the Set Alarm Filter dialog.

**Text**

Allows you to use a variable for text in a text widget.

The following sections describe how to create and use these variables.

**More Information:**

*Variables Pane* (see page 127)
*Customizing the Dynamic View Templates* (see page 140)
Create a Variable

You can create a variable to assign to a widget. This means you can define the properties for a variable once and use it multiple times.

To create a variable

1. Expand the Variables node in the tree of the Dashboard Components pane of the Dashboard Designer.
2. Drag-and-drop the type of variable you want onto the canvas.
   A dialog appears.
3. Enter the properties for the variable.
   Fields that are bordered with a red box are required.
   Optional fields that are left blank can be specified per widget. For example, for a QoS variable you can specify the name of the variable and the QoS, and then specify a different Source for each widget the variable is applied to. Fields that are defined for the variable (not left blank) cannot be changed for individual widgets.
   Tip: When creating a QoS variable, you can view a list of QoS measurements by selecting a meter widget on the canvas and then opening the Select Datasource dialog. This may be helpful in getting the exact QoS name.
   For Host variables, the name of the host must be the same as the name displayed in the Alarm Console.
4. Click OK.
   The variable is listed in the Variables pane.

Assigning Variables

The way that you assign a variable to a widget depends on the type of variable it is. The following sections describe how to assign each type of variable.
Assign a QoS Variable

You can assign a QoS variable to widgets that have a data source. This allows you to define the properties for a QoS and use it multiple times.

**To assign a QoS variable**

1. Click the widget on the canvas that you want to assign the variable to.
2. Click the arrows on the Select Datasource bar to display the dialog.
3. Click the QoS tab.
4. Click the Variables radio button.
5. Choose the variable from the Select Variable pull-down menu.
6. Enter information in any unpopulated fields.
   - You cannot edit fields that are defined for the variable. To change these fields, edit the variable.
7. Click Apply.
8. Drag-and-drop the data source icon onto the widget on the canvas.

Assign a Robot Variable

You can assign a robot variable to widgets that have a single data value, such as a gauge or numeric LED. This allows you to define the properties for a robot once and use it as a source for multiple widgets.

**To assign a robot variable**

1. Click the widget on the canvas that you want to assign the variable to.
2. Click the arrows on the Select Datasource bar to display the dialog.
3. Click the Probe tab.
4. Choose the robot variable from the Robot Address pull-down menu.
5. Enter information in any unpopulated fields.
6. Click Apply.
7. Drag-and-drop the data source icon onto the widget on the canvas.
Assign a Host Variable

You can assign a host variable to an alarm widget. This allows you to enter the name of the host once and use it multiple times.

To assign a host variable
1. Click the alarm widget on the canvas that you want to assign the variable to.
2. Scroll to the bottom of the Alarm Properties pane and click Select Alarm Filter. The Set Alarm Filter dialog appears.
3. Click the Value column of the Host Name field and enter $<variable name>.
   Note: You must enter $ before the variable name.
4. Enter information for other fields if wanted.
5. Click OK.

Assign a Text Variable

You can assign a text variable in a text widget. This allows you to enter text once and use it multiple times.

To assign a text variable
1. Click the text widget on the canvas that you want to assign the variable to.
2. Enter $<variable name> in the Text field of the Text Properties pane.
   Note: You must enter $ before the variable name.
   You can use the variable in a phrase, use the same variable multiple times, or use several text variables in one text widget.

Edit a Variable

You can edit a variable to change its properties.

To edit a variable
1. Click the edit icon (📝) next to the variable in the Variables pane.
2. Edit the fields as wanted, then click OK.
Delete a Variable

You can delete a variable.

To delete a variable

1. Click the delete icon (🗑️) next to the variable in the Variables pane.
   
   If the variable is assigned to an object, you see a confirmation message that lists the object(s) the variable is assigned to.
   
   Note: Deleting a variable that is assigned to objects removes the data source for those objects, and they will not function properly until you assign a new data source.
   
2. Click Yes to delete the variable, or No to cancel.

Example

This example shows how to create a simple dashboard with a text object and a gauge, showing the disk usage in % for a disk on a computer system.

Launch the Dashboard Designer.

The Dashboard Designer window contains these panes:

Dashboard Components

- Widgets that you can drag and drop on the canvas, Image object, Text object, graph object, Table object etc.
- Templates, which are customized objects you can drag and drop on the canvas.

Dashboards

- Dashboard List, listing the Dashboards and options for managing Dashboards: Create new, rename, delete etc.
- Current Dashboard, displaying the name of the Dashboard currently on the canvas and listing the objects used on the Dashboard. Tool buttons for copying, renaming, saving, deleting etc.

Canvas

- The workspace, on which you drop and configure the objects and create the Dashboards.

Properties

- Options for customizing the Dashboard and components on the Dashboard.
Create the new Dashboard by selecting New in the Dashboards section.

Give the Dashboard a name and optionally a description. See the section Dashboard Designer (see page 113) for information about invalid characters in Dashboard names. Click the OK button.
The new (and still empty) Dashboard will appear in the Current Dashboard list.

The Properties window shows the properties options for selected object or Dashboard. Left-clicking the Dashboard or object gives you the possibility to change properties for the object.

So far no objects are added to the canvas, so the properties window shows the properties for the Dashboard background.
You can add a background image or add a background color. In this example we change to a yellow background color.
Above the Properties dialog, you will find four additional properties:

**Snap-To**

If checked, objects dropped on the canvas will snap to the grid. This may be helpful for aligning components when moving them around on the canvas.

**Border**

If checked, all objects on the canvas will have a surrounding box that helps positioning, track and resize the object on the canvas. This border also makes it easier to see which object is selected.

**Grid**

Ticking this option, a grid will appear on the canvas. This makes it easier to align objects etc. The grid will only be visible in design modus.

**Note:** The selected background color, if any, will automatically be changed when selecting the grid option. This is done to make the grid more visible. This change of background color applies for the design modus only. The original background color will be used when the dashboard is stored and published.

**Help**

Selecting this option, the on-line help for the Dashboard Designer will be launched in a separate window.
To add components to the Dashboard, select and drag components from the Dashboard Components window.

The added component has focus, indicated by its red border. The properties window will show this object’s properties, where you can change colors, position, size and data etc.

**Note:** When multiple objects are added, you select an object by left-clicking it, and the object borders change to red. The Properties window will show properties for the selected object, and you can also see the selected object highlighted in the Current Dashboard list.
In this example we will add a text object and a gauge.

Example:

Drag a Text object onto the canvas and place it where you like. Left-clicking and holding the mouse button on the object, you can move the object around.
Type My first Dashboard in the text field of the properties dialog. Select text style bold and size 18.

Now, drag a Gauge object, drop it on the canvas and place it below the Text object.

Next, we select a data source for the gauge. Click the arrows on the Select Datasource menu bar to display the Select Datasource dialog. In the QoS tab we select a QoS that gives the percentage of Disk Usage on a computer.
Selecting the ranges in the properties dialog, you can add or remove ranges from the gauge.

If you want to add an additional range from 80-100, you place the cursor in the 80 range and click the + icon in the lower left corner. A new range appears. Type 80 in the Range Start field. Click in the color field and choose a color for the new range.

Click the Apply button in the lower right corner. The gauge will now look like this:
Finally save the dashboard by clicking the Save button.

Click the Preview button to see how the Dashboard appears in the window, and then the Publish button.

Go to the portal window and see that the new Dashboard now appears under the Dashboards node. Left-click it and verify that it appears in the main window.
The Application Window

The Dashboard Designer window contains the following panes:

Dashboard
This pane allows you to:
- Create a new dashboard
- Edit an existing dashboard
- Copy an existing dashboard
- Preview a dashboard
- Download dashboard templates to modify and use as your own
- Publish a dashboard
- Generate XML for a dashboard

Dashboard Components
This pane contains the building blocks, or widgets (objects), you use when designing dashboards. Drag-and-drop widgets onto the Dashboard canvas area. In addition to widgets, you can use Templates. A template is a widget that you have modified and saved for future use in other dashboards.

Dashboard History
This pane, located in the upper right corner, logs changes made to the current dashboard on the canvas. This supports an undo/redo mechanism for a number of operations; typically for adding, deleting, resizing and moving objects.

Properties
This pane, located in the lower right hand corner, contains the properties available for the selected object. When designing a dashboard, drag objects from the Dashboard Components section and drop them on the canvas. When you select an object on the canvas, the properties available for the selected object appear in the Properties section. Configure the objects by assigning the properties you want.

Note: All the panes can be resized.
Dashboard Components Pane

The following sections describe the Dashboards components available when designing your Dashboards:

- **Alarm Components** (see page 104)
- **Meters** (see page 105)
- **Panel** (see page 106)
- **Dashboard Objects Properties** (see page 109)
- **Selecting the Data Source** (see page 80)
- **Configuring the Table Widget** (see page 86)
- **Scaling Dashboards** (see page 123)
- **Undoing Operations** (see page 112)
- **The Dashboards Templates** (see page 111)
- **Example** (see page 93)

Alarm Components

Use an Alarm object to reflect the alarm state of your monitored computer systems and define what kind of action you want to take place if an alarm with this state occurs. There are two objects available:

- Alarm
- Alarm Line
Meters

Meter objects are well suited when monitoring data sources where the output is a number.

**Gauge**

The Gauge is well suited when monitoring data sources where the output is a number, but where it is not necessary to read a very exact value.

**Numeric LED**

The Numeric LED is well suited when monitoring data sources where the output is a number (free disk space from the cdm probe for example).

**Slider**

The purpose of the Slider is much the same as for the Gauge.

*Note:* Avoid using too short tick intervals when using the Slider object. Otherwise (if using too many ticks), the ticks will not be visible.

**Line Map**

Line Map component enables you to display a line that changes its color based on set of data from the external database. You can choose the color of the line when the set of values (such as QoS data) matches a particular data range.
### Panel

![Dashboard Components](image-url)

- Widgets
  - Alarm Components
  - Meters
- Panel
  - Panel
  - Link
- Chart & Table
- General
- Report
- Templates
Panels may be used to logically group elements together, emphasizing the geographical, topographical, structural or organizational placements of monitored objects.

A Panel object, when placed on the top level of a Dashboard, makes a link to a Panel, one level down in the hierarchy. The Panel object on the top level will reflect propagated alarm states from alarm objects on the level below.

**Using the Panel Object**

When creating a Dashboard, placing a panel object on the canvas and double-clicking it will bring up an empty canvas one level below. Now you can place and configure other objects on this new canvas.

Clicking the Up button in the Dashboards section brings you up to level 1 again.
The Application Window

**Link**

Using Link object on a Dashboard, you can create a link from this Dashboard to another Dashboard. To explore the actual linked dashboard, you double-click on the object, and a new window will be loaded with the Dashboard in question. The Link object will reflect propagated alarm states from alarm objects on the linked Dashboard.

**Chart & Table**

**Table**

Use this object when you want to present the output from a query to the NIS as a table in a dashboard.

**Chart**

This object displays the measured values as a graph.

**General**

**Up object**

The Up object is used in connection with Panels. Left-clicking the Up object in a Panel brings you one level up in the hierarchy.

**Image**

The Image object is used to enhance the Dashboard with images of most popular formats (.jpg, .png, .gif, .swf).

**Text**

Use the Text object for titles, headings etc. to enhance the readability of your Dashboard. Use your own choice of Font, Background and Color.

**Connector**

Use the connector to draw lines and connect objects. You can define the thickness, color etc.

**Report**

**Time Selector**

Use Time Selector to define the duration for which you want to publish the report. You can publish weekly and monthly reports, and also the last day's report.

In addition, there is a node called Templates. You may save an object as a template. If you have configured an object and want to save and use it in the future when designing other Dashboards, you right-click the object and select 'Save as Template'.

**Configuring the Objects**

To select an object on the canvas in order to edit the object properties, click the object. The object borders become red, indicating that the object is selected. The properties dialog for the object appears in the right side of the window.
Dashboard Objects Properties

Dashboard objects are associated with properties that determine the appearance and layout of the object, such as positioning on the canvas, size, text type, shadow effects, or sounds to be played when an alarm occurs.

To select an object on the canvas in order to edit its properties, click the object. The object borders turn red, indicating the object is selected. The properties dialog for the object appears in the right pane.

Some objects, such as meter objects, tables, and trend graphs, are connected to a data source.

Below is an example, describing the properties for an Alarm object.

The Alarm object reflects the alarm state for monitored computer systems. The object reflects the highest severity level of alarms.

Note: The ACL settings, defined in Infrastructure Manager, can restrict the alarms the user is allowed to see.

Object Name
Each object dropped on the canvas is assigned a unique object name of the form <object type><object number>, for example: AlarmObject-D8837BE7-409E-C6DB-2593-C970A9513B7B.

x and y
The object’s horizontal and vertical position on the canvas. Position the object by dragging it on the canvas, or by entering values in these fields.

Width and Height
The width and height of the object. Change the size of the object by clicking and pausing on one of the edges, then dragging, or by entering values in these fields.

Alpha
Transparency of the object. Enter values from 0 to 1, where 0 is most transparent.

Drop Shadow Enabled
Adds a shadow effect to the object borders.

Caption Text
Label for the object.

Caption Style
Color, style (normal or bold), and text size of the caption.

Caption Text Align
Select the alignment for the text, centered or left- or right-justified.
Configure Images

Opens the Alarm Images Configuration dialog, where you can add an image to the object. The image is displayed when an alarm occurs.

Single Image

A single image is used, regardless of alarm level.

Alarm Based Images

Allows you to specify different images for the different alarm levels.

Color Masking Image

Allows you to select an image to add as a new layer, masking the color of the object.

Configure Sounds

Opens the Alarm Sound Configuration dialog, where you can select a sound to be played when an alarm occurs.

One Sound

A single sound is used, regardless of alarm level.

Alarm Based Sounds

Allows you to specify different sounds for the different alarm levels.

Select Alarm Filter

Allows you to configure alarm objects to reflect only:

- Alarms from selected host names, source(s), subsystems, and so on
- Alarms containing specific message text
- Alarms assigned to or by specific users at specific times
- Alarms from a specific origin or tagged with user tags

Value

Enter the filter criteria in the Value row for the corresponding parameter(s), then click OK.

To enter a regular expression, place it between two forward slashes. For example: /.*/anything goes.*/.

Note: The dot, asterisk (.*), combination matches any sequence of characters in regular expressions. A character followed by the asterisk (*) matches 0 or more occurrences of the preceding character. For example, a* matches a, aa, aaa, and so on. The asterisk alone is not a valid character in regular expressions. For more information about regular expressions supported, see the ECMAScript edition 3 language specification (ECMA-262).

If the value is not surrounded by forward slashes, alarms are checked for text that matches the value.
Clear
Clears the filter.

Propagate
Allows the alarm object to propagate its highest severity up to next level in the dashboard hierarchy, if any. (You can create dashboards on multiple levels, using the Panel object.)

The Dashboards Templates

You may save an object as a template. If you have configured an object and want to save and use it in the future when designing other Dashboards, you right-click the object and select ‘Save as Template’.

The object will then be saved under the Templates node, sorted in the group the object belongs to: Alarm objects are placed in the Alarm Components group, meter objects in the Meters group etc.
Undoing Operations

The Dashboard History available when designing dashboards contains functionality for logging changes made to the current dashboard on the canvas. This supports an undo/redo mechanism for a number of operations; typically for adding, deleting, resizing and moving objects.

Clicking the Undo button will undo the operation highlighted in the Dashboard History window.
The Dashboard history will still be present, and you may redo operations removed by Undo by clicking the Redo button.

The Dashboard History will be cleared when the Dashboard is saved.

**Dashboard Designer**

The Dashboard Designer provides the following support:

**Supported report templates**

Dashboard Designer supports three templates: server, interface traffic, and connectivity with names `_rtdv_server`, `_rtdv_interface` and `_rtdv_connectivity`.

**The chart widget**

The chart objects allows for time period to not be specified and set x-axis based on time period menu choice in player.

**The TimeSelector widget**

A new dashboard widget, TimeSelector is implemented. It is a part of dashboard definition but only used by DashboardPlayer.

**Text widget**

The Text widget has two attributes:

- Datetime: true/false
- Timezone: local, db and utc (as for chart)

The flex client, if Datetime=true, modifies the time by Timezone and localize the presentation based on the browser setting.
**Dashboard Pane**

The Dashboard pane contains a top bar and two tabs, each containing a number of tool buttons.

**The top bar**

The top bar of the Dashboard pane contains four tool buttons.

![Dashboard Pane](image)

**Up button**

The leftmost button is the Up button, which is activated and can be used only when the active/visible sub panel has a parent panel.
Selecting the Up button when on a Dashboard on for example level 3 in the structure will move you to the Dashboard on level 2. Pressing the Up button again will move you to the Dashboard on level 1.

**Export button**

Click this button if you want to export a Dashboard file (a .zip file). This is convenient if you want to distribute a Dashboard to be used at another portal site. You will be asked if you want to open the file or to save it to disk. Save the file to disk. You may then copy the file to a removable storage device and bring it to the remote portal site and import the dashboard there.
Note: In Mozilla Firefox while downloading for the first time if you have clicked the check box Do this automatically for files like this from now on, then every time you click the Export button it will automatically download in the pre-defined folder.

To enable this dialog box tools > option in Mozilla and click the check box Show the Downloads window when downloading file

Note: The Flash module is not allowed to access the local file system, so therefore a browser link is invoked to complete the save operation.

**Import button**

Use this button to import existing Dashboards and Dashboard templates.

You may either import a Dashboard from the NIS or from a storage device.
Click the Import Selected Dashboard button to import a Dashboard from the NIS. When new Dashboards are created, they must be published in order to be processed by the Dashboard Engine. The dashboard will then be stored in the Nimsoft Information Store (NIS).

Click the Import Dashboard File button to import a Dashboard from a storage device. This is relevant if you have exported a Dashboard file at another portal site (see above) and want to make it available at your portal site.

**Reload button**

The rightmost button is the reload button. Clicking this button reloads the Dashboard list.

**The Dashboard List tab**

Selecting this tab, all Dashboards designed will be listed.

**Note:** These Dashboards will not be available from the portal before they are published (see the Current Dashboard section).
The following fields and tool button are available:

**Filter field**

This field lets you filter the contents of the Dashboard list. Typing e.g. NIMSOFT in this field, only Dashboards containing the phrase NIMSOFT in the name will be listed. Clear the filter by clicking the x in the right part of the field to clear the filter, and all Dashboards will be listed again.

**Sort A-Z**

Clicking this button will list the dashboards in alphabetical order from A to Z. Clicking the button again will list the Dashboards in the opposite order (from Z to A).

**New**

Click this button to create a new Dashboard. A dialog appears, asking you to specify a name and optionally a brief description of the Dashboard you are going to create.

An additional option, Create from XML, lets you create the new Dashboard based on an existing XML code by pasting the code into the dialog. For details, see the section Designing a new Dashboard (see page 59).

**Open**

Click this button to open an existing Dashboard. Selecting a Dashboard in the Dashboards list and clicking this option, a small dialog appears, asking you to confirm that you want to load the selected Dashboard.

Clicking Yes, the Dashboard will be opened on the canvas.

**Copy**

If you want to make a copy of an existing Dashboard, you select the Dashboard in the Dashboards list and click this button. The following dialog appears. Give the copy a name and click the OK button.
Click the OK button on the next dialog popping up.

On clicking Yes, the dashboard will be opened in Dashboard Designer. On clicking No, the Dashboard will be stored and appear in the Dashboards list.

**Delete**

This option lets you delete the selected Dashboard. When clicking the button, you will be asked to confirm that you really want to delete the Dashboard.

Select “Also delete published version of dashboard” option, to delete the Dashboard from the Nimsoft Information Store (NIS) if the Dashboard has been published.

**Note:** If a client has a dashboard active in the portal and you, as a designer, delete the dashboard, the client will get the following error message and see that the dashboard has been removed from the list of dashboards in the left frame in the portal:

Error in getIncrementalData

The client should accept the message and select another dashboard for viewing.

**The Current Dashboard tab**

Selecting this tab, the selected Dashboard will appear on the canvas. All objects used in the dashboard will be shown under the tab.

The following tool buttons are available:
Save

Saves the selected Dashboard. This can be either a new Dashboard or a modified existing Dashboard.

Edit

This option lets you edit the description of the selected Dashboard.

Publish

Click this button to publish the selected dashboard. When published, the dashboard will be stored in the Nimsoft Information Store (NIS) and will be processed by the Nimsoft Dashboard Engine.

Preview

Clicking this button, the current dashboard will be opened in a separate window. This is useful if you want to see how the Dashboard appears before publishing it and making it available.

View XML code

Clicking this button, the XML code for the selected Dashboard will be available in a separate window popping up. By copying this code and saving it on a storage device, you can use the code when creating Dashboards in another environment.

Properties Pane

The following sections describe background properties.

Background Color

Clicking in the Background Color field in the Properties section, a color palette will be available, letting you choose a color background for your dashboard.
Background Alpha

This option lets you set the background color more or less transparent. This option makes it easy to tune the selected background color. 0 is the maximum transparency.
Background Image URL

You may also add an image on the canvas. Clicking the Select File field, a dialog will be opened, enabling you to choose an image. Select an existing image (one of the ones already uploaded in the Dashboard Designer module). If the image you need is not uploaded, click the Upload New Image tab, browse to locate the file and upload it.

Click the Select Image button to place the selected image on the canvas. The two buttons in the lower left corner of the dialog lets you list the uploaded images either as thumbnails or as a list.
To remove an image from the canvas, you simply click the Delete button (see below).

Scaling Dashboards

The Background Properties pane for the dashboard contains an option called scaleToFit. If you select this option, the dashboard is resized to fit the browser window.

The scopeWidth and scopeHeight parameters let you define the size of the frame to be scaled. This frame appears as a grey rectangle on the canvas. Dashboard components within this frame are handled as a single image and are scaled up or down to match the size of the browser window.

If the scaleToFit option is not selected, the dashboard is displayed at its original size, regardless of the size of the browser window.
General Properties

Above the Properties dialog, you will find four properties:

**Snap-To**

If checked, objects dropped on the canvas will snap to the grid. This may be helpful for aligning components when moving them around on the canvas.

**Border**

If checked, all objects on the canvas will have a surrounding box that helps positioning, track and resize the object on the canvas. This border also makes it easier to see which object is selected.

**Grid**

Ticking this option, a grid will appear on the canvas. This makes it easier to align objects etc. The grid will only be visible in design modus.

**Note:** The selected background color, if any, will automatically be changed when selecting the grid option. This is done to make the grid more visible. This change of background color applies for the design modus only. The original background color will be used when the dashboard is stored and published.

**Help**

Selecting this option, the on-line help for the Dashboard Designer will be launched in a separate window.

**Note:** When selecting an object on the canvas, the properties dialog will be displayed on the right-hand side with the object type displayed on the top bar of the properties dialog.
Right-Clicking Objects on the Canvas

Right-clicking objects the canvas, a menu pops up with a number of properties:

- **Copy Object(s)**
- **Save as Template**
- **Delete Object(s)**
- **Bring to Front**
- **Send to Back**
- **Bring Forward**
- **Send Backward**
- **Make Size Equal to Image**
- **Make Same Size**
- **Align Horizontal**
- **Align Vertical**
- **Space Evenly Horizontal**
- **Space Evenly Vertical**
- **Settings...**
- **About Adobe Flash Player 10...**

**Copy Object(s)**

Selecting this option, you can right-click on the canvas and select Paste to paste a copy of the object(s) selected.

**Save as Template**

Selecting this option, the selected object will be saved as a template and can be used when creating other Dashboards. The following dialog appears. Give the template a name and click the OK button.

The template will appear in the Dashboard Components section in the Templates > General folder.
Delete Object(s)

Deletes the selected object(s) from the Dashboard. You will be asked to confirm that you really want to permanently delete the object(s).

Bring to Front

Use this option if you have multiple objects covering each other on the canvas, and you want to bring the selected object to front.

Bring Object Forward 1 Step

Use this option if you have multiple objects covering each other on the canvas, and you want to bring the selected object one step forward.

Bring Object Back 1 Step

Use this option if you have multiple objects covering each other on the canvas, and you want to bring the selected object one step back.

Move Object to Back

Use this option if you have multiple objects covering each other on the canvas, and you want to bring the selected object to the background.

Align Horizontal

This option is valid if more than one object is selected. The objects selected will be aligned horizontally. The reference object (the object with red borders) determines the aligned position of the objects. You may select another of the selected objects as reference object by left-clicking it.

Align Vertical

This option is valid if more than one object is selected. The objects selected will be aligned vertically. The reference object (the object with red borders) determines the aligned position of the objects. You may select another of the selected objects as reference object by left-clicking it.

Space Evenly Horizontal

This option is valid if more than two objects are selected. The objects selected will be evenly spaced horizontally.

Space Evenly Vertical

This option is valid if more than two objects are selected. The objects selected will be evenly spaced vertically.

Settings

Opens a small dialog, enabling you to modify the Adobe Flash Player settings.
Variables Pane

The Variables Pane lists the variables you have created for the current dashboard. The pane contains the following fields:

**Name**
- Name of the variable.

**Type**
- Type of variable.

**Edit icon (Editor)**
- Opens a dialog where you can edit the properties for the variable.

**Delete icon (Trash)**
- Deletes the selected variable.

More Information:

Using Variables for Widgets (see page 89)

Troubleshooting Dashboard Designer

This section tells you how to troubleshoot common issues with Dashboard Designer.
Dashboard API on Windows Does Not Work on Linux

**Symptom:**

When I run the API commands "dashboard.addWidget" or "widget.create" on a Linux robot they do not work correctly.

**Solution:**

Run these commands on a Windows platform.
Chapter 8: Discovery Status

This section contains the following topics:

- Viewing Discovery Status (see page 129)
- Discovery Status Pie Chart (see page 129)
- Pie Chart Detailed View (see page 130)
- Discovery Status Table (see page 132)

Viewing Discovery Status

The Discovery Status application provides a way to quickly view the types of systems discovered on your network and view information about each system.

If you do not have the Discovery Pie permission set in the ACL, you will see a "Permission Denied" message when you try to run the Discovery Status application.

Discovery Status Pie Chart

This pie chart shows the current discovery status. Immediately after the installation of the Nimsoft Server, the Nimsoft Discovery component starts searching your network for computer systems. The process runs continuously and updates the pie-chart to reflect computer systems that are removed or added.
Pie Chart Detailed View

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pie sections</td>
<td>The pie-chart divides the discovered systems into three groups:</td>
</tr>
<tr>
<td></td>
<td>■ UNIX</td>
</tr>
<tr>
<td></td>
<td>■ Windows</td>
</tr>
<tr>
<td></td>
<td>■ Other (routers, printers, and so on)</td>
</tr>
<tr>
<td></td>
<td>Each section of the pie-chart represents the percent of total for that group. Place the cursor over the section to see the number and percentage of discovered computer systems for that section displayed.</td>
</tr>
<tr>
<td></td>
<td>Click in one of the sections to display the [Discovery Status Table](see page 132), where information about discovered computer systems is listed, and to change the pie chart to the [Pie Chart Detailed View](see page 130).</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pie sections</td>
<td>Displays a pie chart according to OS version. For example, if you clicked the Windows section in the <a href="#">Discovery Status Pie Chart</a> (see page 129), this pie chart is divided into sections for XP Professional, Vista, 2003 Server, and so on. Each section of the pie-chart represents the percent of total for that group. Place the cursor over the section to see the number and percentage of discovered computer systems for that section displayed. Click in one of the sections to display only computer systems in that section in the <a href="#">Discovery Status Table</a> (see page 132). Click in the center of the pie chart to return to the Discovery Status Pie Chart.</td>
</tr>
</tbody>
</table>
## Discovery Status Table

The filter fields located above most columns allow you to enter text to display only items containing that text.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>M (Manage State)</td>
<td>Managed state of the computer:</td>
</tr>
<tr>
<td></td>
<td>■ = None. All systems are initially in this state when discovered. For each system assign one of the states below.</td>
</tr>
<tr>
<td></td>
<td>■ = Ignored. The system is ignored by the NIS Manager and is not monitored.</td>
</tr>
<tr>
<td></td>
<td>■ = Managed. The system will be monitored according to the default monitoring properties.</td>
</tr>
<tr>
<td></td>
<td>■ = Maintenance. Set the system to Maintenance mode to temporarily stop monitoring the system. The system retains its monitoring parameters and will be monitored as before when set back to Managed mode.</td>
</tr>
<tr>
<td></td>
<td>■ = Unauthenticated. The system was discovered but not authenticated. For example, if during installation you did not select device type Linux/Unix servers to be monitored, these systems are discovered but not authenticated. Unauthenticated systems are grayed out and cannot be managed.</td>
</tr>
<tr>
<td>A (Alarm Status)</td>
<td>Alarm status for the computer system. The highest severity of alarms from the computer system is shown:</td>
</tr>
<tr>
<td></td>
<td>■ Green = clear</td>
</tr>
<tr>
<td></td>
<td>■ Light blue = informational</td>
</tr>
<tr>
<td></td>
<td>■ Blue = warning</td>
</tr>
<tr>
<td></td>
<td>■ Yellow = minor</td>
</tr>
<tr>
<td></td>
<td>■ Orange = major</td>
</tr>
<tr>
<td></td>
<td>■ Red = critical</td>
</tr>
</tbody>
</table>
## Discovery Status Table

<table>
<thead>
<tr>
<th>Connect Status</th>
<th>Connect status, indicating the state of the computer system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>■✅</td>
<td>= Status information was gathered from the computer system within the last 15 minutes.</td>
</tr>
<tr>
<td>■⚠</td>
<td>= Between 30 and 60 minutes has passed since the last time status information was gathered from the computer system.</td>
</tr>
<tr>
<td>■⛔</td>
<td>= More than 60 minutes has passed since the last time status information was gathered from the computer system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of the computer system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Domain of the computer system.</td>
</tr>
<tr>
<td>DNS Name</td>
<td>DNS name of the computer system.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the computer system.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>Media Access Control (MAC) address of the computer system.</td>
</tr>
<tr>
<td>OUI Organization</td>
<td>Organizationally unique identifier.</td>
</tr>
<tr>
<td>OS Type</td>
<td>Type of operating system (OS) installed on the system.</td>
</tr>
<tr>
<td>OS Name</td>
<td>Name of the OS installed on the system.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Version of the OS installed on the system.</td>
</tr>
<tr>
<td>OS Description</td>
<td>Description of the OS installed on the system.</td>
</tr>
<tr>
<td>Dedicated</td>
<td>The dedicated function of the system.</td>
</tr>
</tbody>
</table>
Chapter 9: Dynamic Views

The Dynamic Views portlet displays automatically generated dashboards for the monitored computer systems and devices on your network. The dashboards display QoS information such as memory, CPU utilization, etc. The data in the dashboards updates at regular intervals, configured in the dashboard_engine probe.

This section tells you how to view the Dynamic View dashboards, how to view Performance Reports of the dashboard data, how to customize the Dynamic View templates, and how to troubleshoot Dynamic Views.

This section contains the following topics:
- View a Dynamic View (see page 135)
- Understanding the Dynamic Views Tree (see page 136)
- Data Sources for Dynamic Views (see page 137)
- View System Information in USM (see page 139)
- MiniMap Tool (see page 139)
- Viewing the Data as a Performance Report (see page 140)
- Customizing the Dynamic View Templates (see page 140)
- Troubleshooting Dynamic Views (see page 144)

View a Dynamic View

To view a Dynamic View dashboard, double-click a computer system or device in the tree structure. The dashboard is displayed in the Dashboard pane with data for the last 24 hours.

If the dashboard contains alarm objects, you can display the related alarms in the Alarm Console by double-clicking an alarm icon that is not green (there are no alarms associated with green objects).
Understanding the Dynamic Views Tree

The tree structure displays discovered devices in two main groups:

**Network**

Network-related systems, such as network interfaces, routers, and so on. These systems are grouped into two subgroups, **Connectivity** and **Interface Traffic**.

**Server**

Server-related systems. By default these systems are grouped into subgroups based on the OS, such as **Unix** and **Windows**. Additional groups created in the Unified Service Manager portlet (USM) are also displayed.

The colored icons of the tree nodes represent the highest severity of alarms for the computer systems under that node of the tree. The highest severity level is propagated up the tree structure. For example, if a Windows system sends a critical alarm (red), the icon representing that computer system is red, and the **Windows** and **Server** nodes are also red.

To filter the systems you see in the tree, click the Search icon (🔍) and enter text in the text field. Only the items with text that matches are displayed. The filter is applied only to items currently displayed in the tree. For example, if you want to see only Windows servers named with the prefix "Customer1", expand the **Server** and **Windows** nodes of the tree so that all Windows servers are displayed. Click the Search icon and enter **Customer1** in the text field. Only servers with names that contain "Customer1" are displayed.

When you add or modify groups in USM, the changes are reflected in the Dynamic Views tree; however, it may take several minutes for the Dynamic Views tree to reflect the changes.

Empty groups are not shown in the Dynamic Views tree. There must be at least one system collecting QoS data in the group in order for the group to appear in the tree.

If there are systems that are being monitored that have not been assigned to a group, you see a special group named **(Not Grouped)**. You may want to assign these systems to a group in USM to more easily manage monitoring templates for them.

You can expect to see more systems listed in USM groups than you see in the groups in the Dynamic Views tree. In USM, all discovered systems are listed in the group. The Dynamic Views tree displays only those that are monitored; if they are not monitored, there is no QoS data to generate a Dynamic View.
Data Sources for Dynamic Views

The Dynamic Views tree displays systems that are being monitored. A system is monitored if a probe is collecting QoS data for the system.

The following probes must be collecting data in order for systems to appear in the Dynamic Views tree:

- **Network > Interface Traffic** node: interface_traffic probe
- **Network > Connectivity** node: net_connect probe
- **Server** node: cdm (local) or rsp (remote) probe

These probes all support service-oriented configuration (SOC). With SOC probes, if you selected the Discovery module during Nimsoft Monitor installation the computer systems detected on the network will send QoS data as soon as their state is set to Managed. This state can be set in the Unified Service Manager (USM) portlet.

If the Discovery module was not selected during Nimsoft Monitor installation, the cdm probe must be distributed to each computer system to be monitored and then configured to send QoS data. Also, the interface_traffic and net_connect probes on the computer running the Nimsoft Monitor software must be configured with profiles for each of the systems to be monitored.

Customize Data Sources for Systems

By default the colors of the icons in the Server section of the Dynamic Views tree reflect the status of alarms from the cdm and rsp probes only. However, the icons in the Alarms pane of the Dynamic View dashboard reflect alarms from other probes. For example, the Windows node in the tree may be green, indicating no alarms, but the Availability icon in the Alarms pane of a server dashboard may be red, indicating a critical alarm. This is because the status of the Availability icon reflects alarms from the hub probe.

If you want the alarm status of the tree node icons and the Alarms icons to match, you can add probes as alarm sources for the tree node icons.

To add probes to the alarm status icons, you add a key to the configuration for the dashboard_engine probe. Alarms from each probe listed in the key are reflected in the alarm status of the tree icons.

The following table lists the probes whose alarms are reflected in the Alarms icons.
Note: The icons displayed in the Alarms pane of a Dynamic View dashboard vary depending on which probes are monitoring the system. For example, systems monitored by the rsp probe have fewer Alarms icons than those monitored by the cdm probe.

<table>
<thead>
<tr>
<th>Alarm icon</th>
<th>Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>hub</td>
</tr>
<tr>
<td>CPU</td>
<td>cdm or rsp</td>
</tr>
<tr>
<td>Memory</td>
<td>cdm or rsp</td>
</tr>
<tr>
<td>Processes</td>
<td>processes</td>
</tr>
<tr>
<td>Services</td>
<td>ntservices</td>
</tr>
<tr>
<td>Storage</td>
<td>cdm or rsp</td>
</tr>
<tr>
<td>Log Files/Event Logs</td>
<td>logmon, ntevl (Windows)</td>
</tr>
<tr>
<td>All</td>
<td>All probes</td>
</tr>
</tbody>
</table>

Follow these steps:

1. Use Infrastructure Manager to open the Raw Configure window for the dashboard_engine probe:
   a. Select the dashboard_engine probe.
   b. Press the Ctrl key and right-click on the dashboard_engine probe.
   c. Choose Raw Configure.
2. Select the data folder.
3. Click New Key.
   The New Key dialog is displayed.
4. Enter the following values:
   - Key = server_alarm_probes
   - Value = rsp, cdm, <probes you want to add>
   The entries for the key value must be a comma-separated list. Make sure to include the rsp and cdm probes.
5. Click OK, then click OK again to close the Raw Configure window.
   The dashboard_engine probe is automatically restarted if it was running when you opened the Raw Configure dialog. If the probe was not running, you must restart it manually.
View System Information in USM

To view performance and other information in the Unified Service Manager (USM) portlet, click **USM**.

**Note:** If the **USM** button is not activated (is grayed out), click the **Rebuild from template** icon (⚙️).

If you linked to USM from a Dynamic View for a group, the **Members** table for the group is displayed in a new window. The **Members** table displays information about systems in the group. From here you can also access the **Alarms** tab, where you can view summary information about alarms for the group and manage alarms.

If you linked to USM from a Dynamic View for a device (a computer system, interface, or connectivity node), the **System** tab for that device is displayed in a new window. Depending on which probes are monitoring the system, the **System** tab displays information about system properties, alarms, disk usage, interface traffic, and performance. From here you can access other tabs where you can manage alarms or view metrics, group assignments, monitor assignments, and reports.

**MiniMap Tool**

The Mini Map tool allows you to adjust the zoom level and to pan around the dashboard. A small version of the dashboard is shown in the Mini Map window. Move the slider to adjust the zoom level. Drag the yellow field in the Mini Map to pan around the dashboard.
Viewing the Data as a Performance Report

You can view Dynamic View dashboard data in the format of a Performance Report.


The tables below the graphs contain the following information for the interval shown in the graph:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The computer hosting the probe sending the QoS data.</td>
</tr>
<tr>
<td>Target</td>
<td>The device/target being monitored, supplying the probe with QoS data.</td>
</tr>
<tr>
<td>Maximum</td>
<td>The maximum value for the interval shown.</td>
</tr>
<tr>
<td>Minimum</td>
<td>The minimum value for the interval shown.</td>
</tr>
<tr>
<td>Average</td>
<td>Average of the samples within the report period.</td>
</tr>
<tr>
<td>Stdev</td>
<td>Standard deviation of the samples within the report period.</td>
</tr>
</tbody>
</table>

As with any Performance Report, you can change the time interval for the report. Use the time selection buttons on the toolbar at the bottom of the report. Click the back (←) or forward (→) icons to toggle between start/end date fields and quick view buttons.

Customizing the Dynamic View Templates

You can customize the Dynamic View report templates by editing them in the Dashboard Designer. The following sections contain information on template names, supported variables, and how to edit the templates.

Template Names

The following table lists the templates and which nodes in the Dynamic Views tree they are displayed for. In other words, in the Dynamic Views tree, when you click on a server that is monitored by the cdm probe, for example, the Dynamic View you see uses the _dtdv_server template.

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Nodes Displayed For</th>
</tr>
</thead>
<tbody>
<tr>
<td>_dtdv_server</td>
<td>Server subnodes monitored by the cdm probe</td>
</tr>
<tr>
<td>Template Name</td>
<td>Nodes Displayed For</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>_dtdv_server_rsp</td>
<td>Server subnodes monitored by the rsp probe</td>
</tr>
<tr>
<td>_dtdv_connectivity</td>
<td>Connectivity subnodes monitored by the net_connect probe</td>
</tr>
<tr>
<td>_dtdv_interface</td>
<td>Interface subnodes monitored by the interface_traffic probe</td>
</tr>
</tbody>
</table>
Supported Variables

When editing the Dynamic View templates, you can use a limited set of variables. Variables can be used in the following fields:

**Alarm widgets**

In the Set Alarm Filter dialog, accessed by clicking Select Alarm Filter at the bottom of the Alarm Properties pane, in the following fields:
- Host Name
- Subsystem
- Subsystem ID
- Domain
- Robot
- Probe
- Origin
- NAS

**Widgets that can connect to the QoS or NIS data sources**

- In the Target Index/Token field of the QoS tab of the Select Datasource dialog (not supported for connectivity templates)
- In the Query field of the NIS tab of the Select Datasource dialog (not supported for interface or connectivity templates)

**Text widgets**

The following lists the variables supported for each template.

**Server (_dtdv_server and dtdv_server_rsp templates)**

- \$nimbus_address (not available for the dtdv_server_rsp template)
- \$hubname (not available for the dtdv_server_rsp template)
- \$has_qos
- \$alarm_status
- \$source_override
- \$source
- \$origin
- \$domain
- \$robotname
- \$robotip
- \$os_major
$os_minor
$os_version
$os_description
$os_user1
$os_user2
$cpu_usage
$memory_usage
$memory_paging

**Connectivity** (_dtdev_connectivity template)_

$host
$origin
$alarm_status
$icmp_response

**Interface Traffic** (_dtdev_interface template)_

$origin
$alarm_status
$device
$interface
$traffic
$errors
$discards
$in_utilization
$in_speed
$out_utilization
$out_speed

**More Information:**

*Using Variables for Widgets* (see page 89)
Edit a Dynamic View Template

You can edit the templates for Dynamic Views to customize them.

Follow these steps:
1. Open the Dashboard Designer.
2. Click the **Import a dashboard from NimBUS or file** icon in the Dashboard pane.
   The **Import Dashboard From NimBUS** dialog appears.
3. Click the name of the template to select it, then click **Import Selected Dashboard**.
   A notification dialog appears.
4. Click **OK**.
5. Double-click the template name in the Dashboard pane to open it.
   You can edit the template as any dashboard, except only certain variables are supported for alarm widgets.

Troubleshooting Dynamic Views

This section tells you how to troubleshoot common issues with Dynamic Views.

Dynamic Views May Display Redundant Tree Nodes

If you run the net_connect probe on two different robots to monitor the same systems, redundant tree nodes may appear in the left-hand navigation pane of the Dynamic Views portlet.

**Note:** Avoid running the net_connect probe from two different robots against the same systems.
**Duplicate Data Series are generated**

**Symptom 1:**

While using the CDM probe, dynamic views displays the updated data series when I switch from using "Short name for QoS Source" to "Long name QoS Source" or vice-versa only for the first time. When I switch from generating long or short names again, dynamic views does not display the updated data series.

Similarly, duplicate entries for the same node is available for selection while setting up a data source of the widget in dashboard designer.

**Solution:**

While using the CDM probe, if you switch between using Short name for QoS Source and Long name for QoS Source, two data series will be generated for the same QoS.

To see the updated data series in Dynamic Views as per the latest selection for generating QoS names, remove the latest entry manually from S_QOS_DATA table for the duplicated data series.

**Symptom 2:**

When CDM and RSP probes are simultaneously monitoring the same system, two data series for the same QoS are generated and only latest is shown in the dynamic views dashboard.

**Solution:**

Do not monitor any single system with both the CDM probe and the RSP probe simultaneously. Use either one of them.

**Dynamic View is not Displayed**

**Symptom:**

When I double-click on a server in the tree view of Dynamic Views, nothing happens and no dashboard is displayed in the right pane.

**Solution:**

This can be resolved by increasing the value for a timeout setting in the wasp probe.

1. In Infrastructure Manager, select the server in the tree view and double-click the wasp probe.
2. In the Raw Configure dialog, select the setup folder.
3. Double-click the nimpool_timeout key and change the value to 120.
4. Click OK.
5. Click Apply, and then close the window.
No Access Error

Symptom:
The Dynamic View dashboards do not load and I see an error that says "DashboardService SRV_ERR_NO_ACCESS".

Solution:
This may happen if you use the group_server probe to create groups and the Name and Caption fields have different values. To resolve this, enter the same values for the Name and Caption fields in the group_server probe. You can open the configuration GUI for group_server in Infrastructure Manager.

Note: Newer implementations of UMP use the nis_server probe instead of the group_server probe. To determine whether you are using group_server, check the use_nis_server setting in the dashboard_engine.cfg file. If it is set to 0, you are using group_server.

No Existing Interfaces Error

Symptom:
The Dynamic View dashboards do not load and I see a "none existing interfaces" error message in Dynamic Views.

Solution:
This may happen if all of these are true:

- You use the group_server probe. Newer implementations of UMP use the nis_server probe instead of the group_server probe. To determine whether you are using group_server, check the use_nis_server setting in the dashboard_engine.cfg file. If it is set to 0, you are using group_server.
- You have interfaces monitored by the interface_traffic probe that have a hyphen (-) in their names.
- You have enabled aggregated QoS measurements of interface traffic.

This occurs because the interface name is not recognized by the group_server probe. To resolve this, rename the interfaces (with no hyphens in the name) in the interface_traffic probe. You can open the configuration GUI for the interface_traffic probe in Infrastructure Manager.
Chapter 10: Flow Analysis

Chapter 11: List Designer

The List Designer allows administrators to design lists to be displayed in the List Viewer. The List Viewer displays information in a table format. The information can be in the form of text, numbers, gauges, alarms, or line graphs.

You can create two kinds of lists, detail or group. In detail lists, each row displays information for a single host or target. In group lists, each row displays aggregated information for a group of systems.

For group lists, you can specify a Drilldown Template (another list). Typically, the drilldown list contains data for the individual hosts or targets that make up the group. When viewing the group list in the List Viewer, you can click the name of a group to display the Drilldown Template.

For detail lists, you can click the name of a system to see a Drilldown Report with data for the system you clicked. The Drilldown Report is a Performance Report chart, created in Performance Reports Designer and specified in the Drilldown Report setting in the List Designer.

When you create a new list, by default it is a detail list. To create a group list, add groups to the list.

If you do not have the List Designer permission set in the Access Control List (ACL), you will see a "Permission Denied" message when you try to run the List Designer.

This section contains the following topics:

- Design a List (see page 150)
- User Tags (see page 152)
- List Designer Window (see page 153)
- Troubleshooting List Designer (see page 167)
Design a List

You can create a list to be displayed in the List Viewer application.

Follow these steps:

1. Click the New View icon.

2. From the Row Source pull down menu, select Hosts or Targets, then click Apply.

   Choose Hosts to display data for the systems doing the monitoring or Targets to display data for the endpoints of a test.

   For example, for disk usage choose Hosts to see information about the systems where Nimsoft Monitor (NM) is installed. For a URL test choose Targets to see information about the destination of the URL test.

3. Enter information in the remaining fields in the table definition area:

   Column Header

   Allows you to give the source column a name other than Host or Target.

   Hide Repeating Entries

   Displays host or target names only once in the source column in the List Viewer, making groups of entries easier to see.

   Drilldown Report/Drilldown Template

   Specifies the item to display when you click the name of a group or host in the List Viewer to drill down for more information:

   ■ A list to be displayed when you click on the name of a group. The Drilldown Report can be any list, but typically it contains data for the individual systems that make up the group. This field name changes to Drilldown Template if the list has more than one group. The specified list is used as a template, displaying data for the members of whichever group is drilled down from.

   ■ A Performance Reports Designer chart to be displayed when you click on the name of a host or source. If no Performance Reports Designer chart is designated, the standalone USM is launched instead.

   Click the Find view icon next to the Drilldown Report field to browse to a list or chart to designate as the Drilldown Report or Drilldown Template.

   Row Limit

   This sets the number of rows displayed in the list. For example, if you set this to 10, the top 10 rows for the sorting you have selected in the table are displayed.

   If you leave it set to 0, the List Viewer displays the number of rows that fit on a single page.
4. Add a group to the list if wanted:
   a. Enter information in the filter fields of the New Group pane.
   b. Click Apply.

5. Add more groups if wanted by clicking the Add group icon ( ) and then entering information in the fields in the group pane. The following fields are not self-explanatory:

   **Override Template**
   Allows you to drill down to a list other than the one specified for the Drilldown Template.

   **Static**
   Allows you to display data for the systems defined in the Override Template report instead of for the members of the group. This is most often used when working with virtual hosts.

   **Group name**
   Highlight the name of a group and enter a new name to rename it.

6. Add a column to the list by clicking Add Column.

7. Do the following:
   a. Select a QoS.
   b. If you are in Hosts mode (you selected Hosts from the Row Source pull down menu), select a target.
      
      The list of targets is populated once you select a QoS. If you are in Target mode the list of targets is not displayed since data will be displayed for all targets listed in the table. To restrict the targets listed in the table, add a group and use the filters in the New Group pane.
   c. If you are in Targets mode (you selected Targets from the Row Source pull down menu), click the Select All QoS check box if you want to display all QoS reported for the target in a single column. If you select this it is recommended that you also add a column with the Info data format (choose Info from the Display as pull down menu) and select QoS from the Info Type pull down menu. This allows you to see what each QoS is.

8. In the data format (right) pane, select the data format for the column from the Display as pull down menu.

9. Enter information for the column type you selected. For information about specific fields, see Add Column Panes (see page 157).

10. Click Apply.

11. Continue adding as many columns as you want.

   To change the order of the columns drag the column headers. To return to the group view, click the header of the source (host or target) column.
12. Click the Save icon.
   
a. Select the directory location where you want to save the list and enter a name for the list. To save the list in a subdirectory, enter a directory structure such as servers/disk_usage/latest_list. This creates the subdirectories servers and disk_usage and the list named latest_list.

b. Select public, account, or private from the drop-down list to the right of the name field.

c. Click Save.

User Tags

You can filter on two user-defined criteria, called User Tags, in portlets that have filters. You can also automatically create groups according to User Tag.

User Tag 1 and User Tag 2 are text fields that are defined on the robot. You can enter any text in these fields. (Use Infrastructure Manager to open the configuration window for the robot.) Once you have done so, you can filter for these values in the Unified Service Manager, Performance Reports Designer, and List Designer portlets.

For example, you could use User Tag 1 for geographic location and User Tag 2 for type of server. For some systems you enter Europe for User Tag 1 in the robot configuration, and for some systems you enter Asia. For User Tag 2, you enter either production server or web server.

You can then create reports for your regional systems by filtering on User Tag 1 in the Performance Reports Designer (in the Filters tab) or List Designer (in the filter fields of the New Group pane). To do so, you would set the filter to User Tag 1 is Europe or User Tag 1 is Asia.
In the Unified Service Manager portlet, you can create separate groups for your production and web servers and apply different monitoring templates to them. To create the groups, in the Filters section of the Edit Group dialog you would set the filter to **User Tag 2 is production server** for one group, and **User Tag 2 is web server** for the other group.

**User Tag 1** and **User Tag 2** can be used to filter for any system that has a Nimsoft Monitor robot running on it. You cannot use **User Tag 1** and **User Tag 2** to filter for network devices that do not have a Nimsoft Monitor robot.

For information about automatically creating groups according to User Tag, see **Automatic Groups** (see page 390).

### List Designer Window

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Column button</td>
<td>Displays the [Add Column panes](see page 157), where you can define a column for a list.</td>
</tr>
<tr>
<td>Remove Column button</td>
<td>Removes the selected column from the table.</td>
</tr>
<tr>
<td>View as PDF icon</td>
<td>Opens the [PDF Preferences Dialog](see page 166), where you can choose settings for a PDF version of the list.</td>
</tr>
<tr>
<td>Refresh icon</td>
<td>Updates the data displayed in the table.</td>
</tr>
<tr>
<td>New view</td>
<td>Clears all fields or resets them to the defaults. Edit the settings to create a new list, then click the Save view (保存) or Save view as (保存为) icon.</td>
</tr>
<tr>
<td>Open view icon</td>
<td>Opens the [Open View](see page 165) dialog, where you can select an existing list.</td>
</tr>
<tr>
<td>Save view as icon</td>
<td>Saves the list.</td>
</tr>
</tbody>
</table>
### List Designer Window

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save view icon</strong></td>
<td>Opens the Save View (see page 166) dialog, where you can name the list and save it as either a public or private list. Public lists can be viewed by all users. Private lists can be viewed only by you. You can also use the Save View dialog to delete lists.</td>
</tr>
<tr>
<td><strong>Help icon</strong></td>
<td>Displays the online help for the List Designer.</td>
</tr>
<tr>
<td><strong>Table</strong></td>
<td>Displays the columns defined for the list. Drag the column headers to change the order of the columns. Enter text in a field next to a column header to filter for that text.</td>
</tr>
<tr>
<td><strong>Column Header field</strong></td>
<td>Enter a name for the column you are defining.</td>
</tr>
<tr>
<td><strong>Rows Source pull down menu</strong></td>
<td>Select whether the data is to be displayed for the hosts (the systems doing the monitoring) or the targets (the endpoints of a test). For example, for disk usage choose Hosts to see information about the systems where Nimsoft Monitor (NM) is installed. For a URL test choose Targets to see information about the destination of the URL test.</td>
</tr>
<tr>
<td><strong>Hide Repeating Entries check box</strong></td>
<td>Select this so that repeating names of hosts or targets are not displayed. For example, if there are multiple rows for the same host (source), the host is listed only once and that column is blank for subsequent rows for the same host. This makes it easier to see groups of entries.</td>
</tr>
<tr>
<td><strong>Apply button</strong></td>
<td>Updates the table with your changes.</td>
</tr>
</tbody>
</table>
**Drilldown Report/Template**

Specifies a list to use to drill down and view more information about the list.

The name of this field changes from Drilldown Report to Drilldown Template for lists with more than one group.

For a list that has only a single group, you can click the name of a system in the group in the List Viewer and drill down to a Performance Report for the system. The report is displayed with metrics for the system you clicked on.

For a list with multiple groups, you can click the name of a group in the List Viewer to display the specified Drilldown Template. The Drilldown Template can be any list, but typically it contains data for the individual systems that make up the group.

For example, you have groups named Data Center 1 and Data Center 2 made up of the systems at each data center. Your top-level list displays aggregated data for each data center. However, you want to drill down and see data for each system. To do this, you create a list named Data Center System Metrics with measurements for individual systems. You set the Data Center System Metrics template as the Drilldown Template. Now when you drill down from Data Center 1 or Data Center 2 aggregated data, you see the Data Center System Metrics report with data for the systems in that group.

Enter the name of a list, or click the Find view icon (🔍) to the right of this field to select the list from a menu.

The list specified as the Drilldown Template is used by default for all groups. To use a different drilldown template for a group, click the Override Template check box.

**Edit button**

(Displayed when a Drilldown Template is specified)

Allows you to edit the list specified as a Drilldown Template. You must save the current list in order to edit the Drilldown Template.

This button is not available for lists with only a single group. In this case, the Drilldown Report is a Performance Report, which cannot be edited in the List Designer.
| **Row Limit** | Limits the number of rows displayed. This makes loading the report in the List Viewer faster, especially if you have a large number of systems in the list.  
For example, if you set this to 10, the top 10 rows for the sorting you have selected in the table are displayed. If you sort the table by a CPU Usage column, the systems with the 10 largest CPU Usage values are displayed.  
If the Row Limit is set to 0, the report displays the number of reports that fit onto one screen.  
To see data for more systems, increase the Row Limit.  
**Note:** Setting the Row Limit to a very large number may make loading the list slow or cause the List Viewer to time out, depending on your environment. By default the List Viewer times out after 10 minutes. |
| **Add group icon** | Adds a New Group accordion, where you can create a group to display in the list. A group displays aggregated data for a set of hosts or targets, rather than data for each individual host or target. |
| **Remove group icon** | Deletes the current group. |
| **Override Template check box** | Select to specify a drilldown template for this group other than the one specified in the Drilldown Template field.  
Enter the name of a list, or click the Find view icon (🔍) to the right of this field to select the list from a menu. |
| **Static check box** | Select to display data for the systems defined in the Override Template report instead of for the members of the group.  
For example, if you have a group made up of VMware hosts you may want to see data not for the group members (hosts), but for the VMware instances on those hosts. To do so, use a report with the VMware instances defined as the data source as the Override Template and select the static check box. |
List Designer Window

Chapter 11: List Designer

Edit button

Allows you to edit the list specified as the Override Template. You must save the current list in order to edit the Override Template. This button is not available for lists with only a single group. In this case, the Drilldown Report is a Performance Report, which cannot be edited in the List Designer.

Filter fields

- Use these fields to display only specified hosts or targets in the list. For example, you can filter for only hosts monitoring a certain QoS measurement, or for all hosts or targets on a specified hub.
- not button - Click to display all items except the specified items.
- Source pull down menu - Select the item you want to filter for.
- Operator pull down menu - Select the operator (starts with, ends with, contains, or is) you want to use for the filter
- Text box - Enter the text you want to filter on.

Add filter icon

Click to add another row of filter options.

Remove filter icon

Click to remove the row of filter options. This icon is visible if you have more than one row of filter options.

Add Column Panes

The Add Column panes are displayed when you click the Add Column button. The fields vary depending on whether you selected Hosts or Targets in the Row Source pull down menu.

Hosts mode:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS panel</td>
<td>Select the QoS measurement you want to display in the column.</td>
</tr>
</tbody>
</table>
### Target panel
Select a target for the QoS measurement. This list is populated once you select a QoS measurement. If for the QoS measurement you selected the host name is part of the target, you see $HOST at the top of the host list. This variable allows you to create a single column for the data. Otherwise, because the host name is part of the target, you would have to create a new column for each system. Usually if the $HOST option is present you will want to use it.

### Data Format pane
Use the fields in this pane to define the data to be displayed in the column. The fields and buttons in this pane change depending on the data format selected from the Display as pull down menu. For information on each field or button see the description for each data format:

- **Numeric** (see page 159)
- **Spark** (see page 159) (mini-graph)
- **Gauge** (see page 160)
- **Time Slice** (see page 161)
- **Alarm** (see page 163)
- **Status** (see page 164)
- **Info** (see page 165)

### Targets Mode:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select All QoS check box</strong></td>
<td>Check to display all QoS reported for the target in a single column. If you select this it is recommended that you also add a column with the Info data format (choose Info from the Display as pull down menu) and select QoS from the Info Type pull down menu. This allows you to see what each QoS is. You can also use the filter fields in the New Group pane to restrict which QoS or targets are displayed (see List Designer Window for a description of these filter fields).</td>
</tr>
<tr>
<td><strong>QoS panel</strong></td>
<td>Select the QoS measurement you want to display in the column.</td>
</tr>
</tbody>
</table>
Use the fields in this pane to define the data to be displayed in the column. The fields and buttons in this pane change depending on the data format selected from the Display as pull down menu. For information on each field or button see the description for each data format:

- **Numeric** (see page 159)
- **Spark** (see page 159) (mini-graph)
- **Gauge** (see page 160)
- **Time Slice** (see page 161)
- **Alarm** (see page 163)
- **Status** (see page 164)
- **Info** (see page 165)

### Numeric Data Format Pane

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display as pull down menu</td>
<td>Select the data format for the column.</td>
</tr>
<tr>
<td>Apply button</td>
<td>Updates the table display with the changes you made.</td>
</tr>
<tr>
<td>Column Header field</td>
<td>Enter a name for the column.</td>
</tr>
<tr>
<td>Aggregation pull down menu</td>
<td>Choose the method you want to use to aggregate the data.</td>
</tr>
<tr>
<td>Time Period combo box and pull down menu</td>
<td>Select the number and units for the interval you want to see data for.</td>
</tr>
<tr>
<td>Show Units check box</td>
<td>Click to display the unit of the measurement, such as percent or second, in the column.</td>
</tr>
</tbody>
</table>

### Spark Data Format Pane

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display as pull down menu</td>
<td>Select the data format for the column.</td>
</tr>
<tr>
<td>Apply button</td>
<td>Updates the table display with the changes you made.</td>
</tr>
<tr>
<td>Column Header field</td>
<td>Enter a name for the column.</td>
</tr>
</tbody>
</table>
List Designer Window

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display as pull down menu</td>
<td>Select the data format for the column.</td>
</tr>
<tr>
<td>Field or Button</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Apply button</td>
<td>Updates the table display with the changes you made.</td>
</tr>
<tr>
<td>Column Header field</td>
<td>Enter a name for the column.</td>
</tr>
<tr>
<td>Aggregation pull down menu</td>
<td>Choose the method you want to use to aggregate the data.</td>
</tr>
<tr>
<td>Time Period combo box and pull down menu</td>
<td>Select the number and units for the interval you want to see data for.</td>
</tr>
<tr>
<td>Show Value, Show Units</td>
<td>Whether to display numeric values on the gauge. If Show Value is selected, you can choose whether to display the units.</td>
</tr>
<tr>
<td>Max</td>
<td>Enter the maximum value to display.</td>
</tr>
<tr>
<td>Find Max Value icon</td>
<td>Finds the maximum value to date for the selected QoS measurement. Click the icon, then click Apply.</td>
</tr>
<tr>
<td>Thresholds fields</td>
<td>Enter threshold values for the color display in the gauge:</td>
</tr>
<tr>
<td></td>
<td>■ All values up to Warn are green</td>
</tr>
<tr>
<td></td>
<td>■ All values between Warn and Critical are yellow</td>
</tr>
<tr>
<td></td>
<td>■ All values between Critical and Max are red</td>
</tr>
</tbody>
</table>

**Time Slice Data Format Pane**

The time slice data format is a bar graph where each bar represents aggregated data for an interval, or slice of time. You can define how long each time slice is. For example, if you want to see hourly data for a 24-hour period, set the Time Period to 24 Hours and the Slice Period to 1 Hour. You will see a bar graph with 24 bars, or time slices, where each slice represents an hour’s worth of data. You can set thresholds so that the color of each slice indicates the aggregated value of the data. You can also set a threshold so that if a specified number of null values is included in the data, the color of the slice indicates that.
<table>
<thead>
<tr>
<th>Time Period spinner box and pull down menu</th>
<th>Select the number and units for the interval you want to see data for.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slice Period spinner box and pull down menu</td>
<td>Select the number and units for the length of each time slice (interval).</td>
</tr>
<tr>
<td>Slice Aggregation pull down menu</td>
<td>Choose the method you want to use to aggregate the data for each time slice.</td>
</tr>
<tr>
<td>Detect Null Values check box</td>
<td>Select if you want time slices with null values to be a different color. Some types of monitors return null values if no data is obtained. For example, when application response time is monitored, a null value is returned if the probe cannot contact the target web site. To see a visual indication that null values were returned, use this check box together with the Null Color selector and the Null Count Threshold. <strong>Note:</strong> In List Viewer you can double-click on a time slice to see a Performance Report chart of the data for that slice. Null values are represented in line graphs by a dotted line.</td>
</tr>
<tr>
<td>Null Color selector (Displayed only if Detect Null Values check box is checked)</td>
<td>Select the color for slices with null values. If the Null Count Threshold is reached, this color is displayed instead of the color defined in the Thresholds fields.</td>
</tr>
<tr>
<td>Null Count Threshold (Displayed only if Detect Null Values check box is checked)</td>
<td>Enter the number of null values that you want to trigger the change in color for a slice. For example, if you set the Null Color selector to blue and only want to see a slice be blue if it contains 3 or more null values, set the Null Count Threshold to 3. If a slice contains 2 null values it will be the color set in the Thresholds fields. If it contains 3 or more null values it will be blue. <strong>Note:</strong> This threshold is a count of the number of null values returned. This is different than the The Thresholds fields below, which reflect the aggregated value of the data.</td>
</tr>
</tbody>
</table>
Thresholds fields

Use these fields to assign a color for a specified range of values. These thresholds determine the color of each slice.

In the From and To fields, enter a range of values for the color. Or, leave the From field blank to include all values up to the value in the To field. In the Color pull down menu, choose a color icon for the slice.

To add or delete rows, click the add row (➕) or remove row (➖) icons to the right of the Color pull down menu. You can also reorder the rows by clicking the Move up (↑) and Move down icons (↓).

**Alarm Data Format Pane**

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display as pull down menu</td>
<td>Select the data format for the column.</td>
</tr>
<tr>
<td>Apply button</td>
<td>Updates the table display with the changes you made.</td>
</tr>
<tr>
<td>Status/Summary pull down menu</td>
<td>Whether to display alarm Status or Summary.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Status</strong> - Displays the highest severity of alarms. For example, if a</td>
</tr>
<tr>
<td></td>
<td>system has three major alarms and one critical, critical is displayed as</td>
</tr>
<tr>
<td></td>
<td>the status.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Summary</strong> - Displays a colored bar indicating the distribution of</td>
</tr>
<tr>
<td></td>
<td>alarms. For example, if a system has three major alarms and one critical,</td>
</tr>
<tr>
<td></td>
<td>the bar is 75 percent orange and 25 percent red.</td>
</tr>
<tr>
<td>Column Header field</td>
<td>Enter a name for the column.</td>
</tr>
<tr>
<td>Source Override field</td>
<td>Enter the name of a source (host or target) to see only alarms for that</td>
</tr>
<tr>
<td>Subsystem field</td>
<td>Enter the name of a subsystem to see only alarms for that subsystem.</td>
</tr>
<tr>
<td>Probe field</td>
<td>Enter the name of a probe to see only alarms for that probe.</td>
</tr>
<tr>
<td>User Tag field</td>
<td>Enter a User Tag to see only alarms with that User Tag.</td>
</tr>
</tbody>
</table>
### Status Data Format Pane

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display as pull down menu</td>
<td>Select the data format for the column.</td>
</tr>
<tr>
<td>Apply button</td>
<td>Updates the table display with the changes you made.</td>
</tr>
<tr>
<td>Column Header field</td>
<td>Enter a name for the column.</td>
</tr>
<tr>
<td>Aggregation pull down menu</td>
<td>Choose the method you want to use to aggregate the data. If you choose Last, the last measurement is used and the time period is not relevant. If you choose a method other than Last, the Time Period fields are activated.</td>
</tr>
<tr>
<td>Time Period combo box and pull down menu</td>
<td>Select the number and units for the interval you want to see data for.</td>
</tr>
<tr>
<td>Thresholds fields</td>
<td>Use these fields to assign a status to a specified range of values. You can add more rows to create a series of status levels.</td>
</tr>
</tbody>
</table>

In the From and To fields, enter a range of values for the status. Or, leave the From field blank to include all values up to the value in the To field. In the status icon pull down menu, choose a color icon for the status. In the Text field, enter the text to be displayed for data that falls in the specified range. For example, you could create a series of statuses that display the words low, medium, high, severe, and critical. To add more rows, click the add row icon (➕) to the right of the Text field.
Source Data Format Pane

The Info data format displays information about the system associated with the source, origin, or QoS.

**Source column**

This can be useful if you are viewing QoS measurements by target. For example, if the target you are monitoring is disk space on the C drive, the Source column tells you which system the C drive is on.

**Origin column**

Displays the origin for the source (host or target) for the row. Origins are a way of grouping data. For example, origins can represent data centers or MSP customers.

**QoS column**

The category of the data. This can be a useful column to display in target-based lists. Target names can be ambiguous and the QoS helps clarify this.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display as pull down menu</td>
<td>Select the data format for the column.</td>
</tr>
<tr>
<td>Apply button</td>
<td>Updates the table display with the changes you made.</td>
</tr>
<tr>
<td>Column Header field</td>
<td>Enter a name for the column.</td>
</tr>
<tr>
<td>Info Type</td>
<td>Type of data to display: Source, Origin, or QoS.</td>
</tr>
<tr>
<td>Hide Repeating Entries</td>
<td>Hides the name of repeating hosts or targets. For example, if there are multiple rows for the same host (source), the host is listed only once and that column is blank for subsequent rows for the same host. This makes it easier to see groups of entries.</td>
</tr>
</tbody>
</table>

Open View Dialog

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open button</td>
<td>Displays the selected list in the List Designer.</td>
</tr>
<tr>
<td>Cancel button</td>
<td>Closes the dialog without displaying a list in the List Designer.</td>
</tr>
</tbody>
</table>
**PDF Preferences Dialog**

The PDF Preferences dialog allows you to choose settings for viewing a report as a PDF. The PDF can be printed or saved.

The PDF Preferences dialog has the following fields or buttons:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Report icon (Not available from List Designer)</td>
<td>Opens the Create New Job dialog in the Report Scheduler portlet, where you can schedule the report to be run and delivered.</td>
</tr>
<tr>
<td>Orientation pull-down menu</td>
<td>Choose the page orientation for the PDF, Portrait or Landscape.</td>
</tr>
<tr>
<td>Size pull-down menu</td>
<td>Choose the page size for the PDF.</td>
</tr>
<tr>
<td>Quality pull-down menu</td>
<td>Choose the level of quality for the PDF.</td>
</tr>
<tr>
<td>OK button</td>
<td>Closes the dialog and displays the PDF.</td>
</tr>
<tr>
<td>Cancel button</td>
<td>Click to exit the dialog without creating a PDF.</td>
</tr>
</tbody>
</table>

**Save Dialog**

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory tree</td>
<td>Select a directory to save the list in.</td>
</tr>
<tr>
<td>Text field</td>
<td>Enter a name for the list. Enter a directory structure before the list name to create subdirectories. For example, servers/disk_usage/latest_list creates the subdirectories servers and disk_usage and the list named latest_list.</td>
</tr>
</tbody>
</table>
| Access type pull down menu | Choose the type of access for the list:  
  ■ public - Can be viewed by all users.  
  ■ account - Can be viewed only by users of the account you are logged in as.  
  ■ private - Can be viewed only by you.  
  **Note:** Saving to an account requires the Portal Administrator ACL. |
| Delete button         | Deletes the list that is selected in the directory tree.                    |
| Save button           | Saves the list.                                                             |
Cancel button | Closes the dialog without saving the list.

**Disable Public Reports**

You can block users from saving Performance Reports and List Reports as public reports. You may want to do this if, for example, you are an MSP and you do not want your customers to be able to see reports from other UMP customers.

If saving public reports is disabled, users can save reports as either private or account reports. Users can still open public reports for viewing; they are only blocked from saving new reports as public reports.

**Follow these steps:**

1. Open Infrastructure Manager.
2. Click on the robot for the primary hub in the tree view.
3. Click the wasp probe to select it in the top right pane.
4. Press CTRL and right-click, then choose Raw Configure from the popup menu.
5. Click the ump_common folder in the tree view of the Raw Configure window.
6. Double-click allow_public_reports and change the value to false.
7. Click OK, then click OK again to close the Raw Configure window.
8. Restart the wasp probe.

**Troubleshooting List Designer**

This section tells you how to troubleshoot common issues with List Designer.
Time Slice Column Does Not Display Any Data

Symptom:
When I define a Time Slice column in List Designer, or look at a Time Slice column in List Viewer, the Time Slice column does not display any data.

Solution:
This occurs if the Time Slice column is too narrow for the slices to be at least one pixel wide.

Time slices may be narrower than a pixel if you enter a value in the Time Period field that is very long relative to the value you enter in the Slice Period field. For example, if you set the Time Period to 1000 Hours and the Slice Period to 1 Minute with the default column width, the slices are narrower than a pixel and are not displayed. Try decreasing the Time Period, increasing the Slice Period, or increasing the column width.

Time Slice Column Is Missing Data

Symptom:
When I define a Time Slice column in List Designer, or look at a Time Slice column in List Viewer, the Time Slice column is missing intervals of data in between time slices.

Solution:
The Time Slice column may appear to be missing data if the QoS sampling interval is longer than the Slice Period you selected. For example, if QoS sampling occurs every five minutes, and you select 1 Minute for the Slice Period field, the Time Slice column will display four minutes of blank space between each slice. To avoid this, use slice periods that are as long as or longer than the QoS sampling interval.
Chapter 12: List Viewer

The List Viewer displays information in a table format. The information can be in the form of text, numbers, gauges, alarms, or graphs.

Lists are configured in the List Designer application, or you can display predefined lists. The lists that you can view depend on your permissions.

If you do not have the List Viewer permission set in the Access Control List (ACL), you will see a "Permission Denied" message when you try to run the List Viewer application.

This section contains the following topics:

- Drilling Down in List Viewer (see page 169)
- List Viewer Window (see page 170)

Drilling Down in List Viewer

You can click in some cells in the List Viewer to drill down and see more information. The information displayed depends on the type of cell you click in.

**Group name**

Click on a group name in the source column to see a list with information about the members of the group. The list that is displayed is set in the List Designer, in the Drilldown Template or Override Template settings.

**Host or Source name**

Click on the name of a system in the Host or Source column to see a Performance Reports Designer chart with data for the system you clicked on. The report that is displayed is specified in the List Designer, in the Drilldown Report setting. If no Performance Reports Designer chart was specified as the Drilldown Report, the standalone USM is launched instead.

**Data cell**

Double-click on any data cell to see a Performance Reports Designer chart of that data.

**Note:** For a Time Slice column, double-clicking on a slice displays a Performance Reports Designer chart for the time slice, rather than the entire time period. However, when you hover your mouse over the column, a tool tip displays data for the entire time period.
**List Viewer Window**

The List Viewer window contains the List Viewer table and a toolbar.

When working in the table, you can click on a column header to sort by that column. Click the header again to toggle the sort between ascending and descending order. Enter text in a field next to a column header to display only items containing that text. To change the order of the columns, drag the column headers.

You can also double-click in some cells in the table to drill down to more information. The information displayed depends on the type of cell you click in.

**Note:** For a Time Slice column, double-clicking on a slice displays a Performance Reports Designer chart for the time slice, rather than the entire time period. However, when you hover your mouse over the column, a tool tip displays data for the entire time period.

The List Viewer toolbar has these fields or buttons:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View as PDF icon</td>
<td>Displays the PDF Preferences dialog (see page 166), where you can choose settings for viewing the report as a PDF. The PDF can be printed or saved.</td>
</tr>
<tr>
<td>Refresh icon</td>
<td>Updates the data displayed in the List Viewer.</td>
</tr>
<tr>
<td>Open view icon</td>
<td>Opens the Open View (see page 171) dialog, where you can select a list for display in the List Viewer.</td>
</tr>
<tr>
<td>Help icon</td>
<td>Displays the online help for the List Viewer.</td>
</tr>
</tbody>
</table>
Preferences Dialog

Access the Preferences dialog by clicking the Settings icon ( ), then clicking Preferences.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List/Report/SLA Name field</td>
<td>Choose the name of the report you want to open by default in this instance of the portlet. If no report name is selected here, the portlet window contains no data when opened. After choosing a report and saving your preferences, log out and log back into UMP to see the specified report displayed by default.</td>
</tr>
<tr>
<td>Period field</td>
<td>Choose the time interval to display for the default report.</td>
</tr>
<tr>
<td>Height field</td>
<td>Enter the height, in pixels, for this instance of the portlet to open to.</td>
</tr>
<tr>
<td>Maximized Height field</td>
<td>Enter the height, in pixels, for this instance of the portlet to display at when the maximize icon ( ) is clicked.</td>
</tr>
<tr>
<td>Save button</td>
<td>Click to save your changes.</td>
</tr>
</tbody>
</table>

Open View Dialog

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open button</td>
<td>Displays the selected list in the List Viewer.</td>
</tr>
<tr>
<td>Cancel button</td>
<td>Closes the dialog without displaying a list in the List Viewer.</td>
</tr>
</tbody>
</table>
Chapter 13: Maintenance Mode

This section contains the following topics:
Using Maintenance Mode (see page 173)

Using Maintenance Mode

The Maintenance Mode application allows you to set the computer systems on your network to Maintenance Mode so they are temporarily unmonitored. The monitoring parameters for the system are retained, and when maintenance mode ends they are monitored again as before.

If you do not have the Maintenance Mode permission set in the ACL, you will see a "Permission Denied" message when you try to run the Maintenance Mode application.
The Maintenance Mode application has these fields and buttons:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Mode icon</td>
<td>Click to display only systems in maintenance mode in the Host list.</td>
</tr>
<tr>
<td>Host filter field</td>
<td>Enter text to list only hosts with names that contain that text.</td>
</tr>
<tr>
<td>Status icons</td>
<td>Indicates the status of the host:</td>
</tr>
<tr>
<td></td>
<td>□ = System is up</td>
</tr>
<tr>
<td></td>
<td>■ = System is down</td>
</tr>
<tr>
<td></td>
<td>□ (white) = System is in maintenance mode</td>
</tr>
<tr>
<td>Host list</td>
<td>Click a host name to select that host. You can Shift + click or Ctrl + click to select multiple hosts.</td>
</tr>
<tr>
<td>Set button</td>
<td>Click to set the selected host(s) to maintenance mode. A calendar dialog opens, where you can set the time for maintenance mode to end.</td>
</tr>
<tr>
<td>End button</td>
<td>Click to end maintenance mode for the selected host(s). A confirmation dialog opens. If you end maintenance mode, the host is monitored again as it was before it was set to maintenance mode.</td>
</tr>
</tbody>
</table>
Chapter 14: My Tickets

My Tickets offers a flexible display where you can view basic information about your Nimsoft Service Desk tickets. My Tickets displays a subset of the data available in the Service Desk and has a subset of the functionality. Unlike the Service Desk, My Tickets can be displayed on the same page as other portlets, allowing you to view your tickets alongside other key data for your organization.

The main view displays the Requests List, a table listing information about your tickets. From the Requests List you can click on a ticket to open it and view information about the ticket, add Work Log notes, or add attachments to the ticket.

This section contains the following topics:

- **User Types** (see page 175)
- **Requests List** (see page 176)
- **Viewing Tickets** (see page 176)
- **Add a Note to a Ticket (Self Service Users)** (see page 176)
- **Add an Attachment to a Ticket** (see page 177)
- **Add A Work Log Item to a Ticket (Agent or Admin Users)** (see page 177)

User Types

There are three types of users of Service Desk and My Tickets:

**Self Service Users**

Self service users are the end users who request IT support services. A self service user has limited interaction with Service Desk and My Tickets, using them mainly to submit requests and monitor the progress of their requests.

**Service Desk Agents**

Service Desk agents are the providers of IT support services. Service Desk agents, supervisors, and managers use Service Desk extensively to submit requests on behalf of end users across the organization and to track and monitor resolution and closure of requests.

**Service Desk Application Administrators**

Service Desk administrators are responsible for establishing the IT support process flow and setting up Service Desk to deliver IT support according to their organization's requirements. Administrators set up Service Desk records and workflows and use Service Desk to ensure that IT support standards are met.
Requests List

The Requests List contains a table that displays information about tickets. The information displayed varies depending on the type of user you are. Self service users can toggle between viewing only the tickets they submitted and viewing all tickets for their organization. Agent and administrator users see tickets they submitted, tickets assigned to them, or tickets assigned to a group they are a member of.

Also, agent and administrator users see more columns in the Requests List table than self service users.

Click a column header to sort the table by that column.

Click on any row to open the ticket.

Viewing Tickets

You can open a ticket to view more information. Agent and administrator users see more information in the ticket than self service users.

From the ticket you can add a Work Log note or an attachment. To perform other actions, such as submitting new requests, performing searches, exporting data, printing tickets, or relating configuration items to the request, use the Service Desk.

To view a ticket

Click on any row in the Requests List to open a ticket.

Note: You can open only one ticket at a time. If you click on a row and the ticket is not displayed, check to see whether you already have a ticket window open.

Add a Note to a Ticket (Self Service Users)

Self service users can add a note to the Work Log for a ticket. Notes can be used to provide additional information about the issue or to communicate with the person who is working on the ticket.

To add a note to a ticket

1. Click on the ticket in the Requests list that you want to add the note to.
   The Modify Request window opens.

2. Scroll to the Work Log Information section.

3. Enter the note in the Description field.
4. Click Update.

The note is added to the ticket and is listed in the table in the Work Log Information section as a Client Note. Depending upon how Service Desk is configured at your company, the person assigned to work on your request may be notified that you have updated the request.

**Add an Attachment to a Ticket**

You can add an attachment to a ticket. This can be used to include images of error messages, data files, and so on. The maximum size for attachments is 3 MB. Once you add an attachment you cannot delete it.

**To add an attachment to a ticket**

1. Click on the ticket in the Requests list that you want to add the attachment to.
   The Modify Request window opens.
2. Scroll to the Attachments section.
3. Enter information in the Name and Description fields.
4. Click Browse and select the file you want to attach.
5. Click Upload.
   The attachment is added to the ticket and is listed in the table in the Attachments section. You can view any attachments in the table by clicking on the row in the table.

**Add A Work Log Item to a Ticket (Agent or Admin Users)**

Agent or administrator users can add a work log item to a ticket.

**To add a work log item to a ticket**

1. Click on the ticket in the Requests list that you want to add the note to.
   The Modify Request window opens.
2. Scroll to the Activity Information section.
3. Enter information about the item in the Description field.
4. Select a Worklog Type from the drop-down menu.
5. Select Yes or No for the Client Viewable field depending on whether you want the client to be able to see the item.
6. Enter the number of minutes in the Time Spent field that you spent doing the item.
7. Click Update.

The item is added to the ticket and is listed in the table in the Activity Information section. If you selected Yes for the Client Viewable field, self service users will see the item in the Work Log Information table of the ticket.
Chapter 15: Nimsoft Remote Admin

The Nimsoft Remote Admin application provides a management console for discovery and configuration data in the Nimsoft Monitor database, Nimsoft Information Store (NIS).

The Nimsoft Remote Admin portlet displays information about the computers in the network in a table format. It shows the state of all Configuration Items in the database. You can set the state for the computer systems discovered on the network.

Nimsoft Remote Admin supports multi-tenancy. Account and contact users see only discovered systems from the origin(s) assigned to the account they belong to. Accounts are created, and origins assigned, in the Account Admin portlet.

In order to access the Nimsoft Remote Admin application, you must have the Basic Management permission enabled in the Access Control List (ACL).

This section contains the following topics:

Migration for Legacy Users (see page 180)
Troubleshooting Nimsoft Remote Admin (see page 180)
Migration for Legacy Users

Unlike earlier versions of the Nimsoft Remote Admin product, formerly known as NIS Manager, the Nimsoft Remote Admin portlet does not manage monitoring. The Service Catalog functionality has been removed, and monitoring is now performed using the Unified Service Manager (USM) portlet.

If you previously used Nimsoft Remote Admin, your Service Catalogs are automatically migrated to USM in the following manner:

- USM groups are created for each Service Catalog under a container named Service Catalogs.
- USM monitoring templates are created and assigned to each Service Catalog.
- Service Elements are converted to USM monitors for the appropriate monitoring template. Monitors have the same name as the Service Elements.

Which devices are monitored depends on a setting you can choose while installing Nimsoft Monitor. If you select the unmanaged systems should be treated as managed option, all devices that have been discovered will be monitored.

**Note:** For implementations where discovery is already running, it is recommended that you do NOT select the unmanaged systems should be treated as managed option. Typically it is not desirable to monitor all previously discovered systems.

If this option is not selected, you must do the following in USM for devices that you want to monitor:

1. Set the device state to Managed. This can also be set in the Nimsoft Remote Admin portlet.
2. Make sure the devices are assigned to a USM group.
3. Make sure there is a monitoring template assigned to the USM group.

**Note:** For implementations where discovery has not run, it is recommended that you select the unmanaged systems should be treated as managed option. In this case you do not need to do step 1 above. All devices in a USM group that has a monitoring template assigned to it will be monitored.

Troubleshooting Nimsoft Remote Admin

This section tells you how to troubleshoot common issues with Nimsoft Remote Admin.
USM Templates Do Not Deploy

Symptom:

When I deploy USM templates in the Nimsoft Remote Admin portlet, I see the error message **Computer System State Error** in the **Status** column, and the templates do not deploy.

Solution:

This occurs if the **State** of the device is not set to **Managed**.

Do the following:

1. In Remote Admin, right-click the device in the tree pane and select **Set State**.
2. Under the **State** drop-down menu, select **Managed**.
Chapter 16: Performance Reports Designer

The Performance Reports Designer allows you to see a visual representation of QoS data. You select the host, QoS measurement, target, and time range, and the data is displayed as a chart. You can display multiple measurements on a single chart, and can view multiple charts at a time. You can drag charts between rows or drag a data series from one chart to another. You can choose the chart format (line, area, or column chart), and the Filters tab allows you to plot only the data that matches specified filters on the chart. You can easily change the source (host or target) of the data by using the Choose Source menu. You can save a set of charts as a report to print or to view later. The import and export features allow you to share charts with other users.

If you do not have the QoS Access permission set in the ACL, you will see a "Permission Denied" message when you try to run the Performance Reports Designer application.

This section contains the following topics:
- Understanding Performance Data (see page 183)
- Viewing Raw Performance Data (see page 184)
- QoS Selection Tabs (see page 185)
- Filters Tab (see page 186)
- User Tags (see page 187)
- Charts Pane (see page 188)
- Automatic Replacement of Fields in PRD Templates (see page 193)
- Toolbar (see page 194)
- Defining Reports with a URL (see page 198)
- Troubleshooting PRD (see page 204)

Understanding Performance Data

Performance Reports Designer uses intervalized data. The software selects a data interval based on the scale of the chart you are viewing. The scale is affected by the timeframe you are viewing data for and the resolution of your screen. Performance Reports Designer selects the smallest interval so that there is only one data point per pixel. Possible intervals range from one minute to one day.

If there are multiple data samples for an interval, the values are averaged. For example, if the data is sampled every 5 minutes but the Performance Reports Designer chart is displaying 15-minute intervals, there are three data samples per interval. In this case, the average of the three data samples is displayed in the chart.
Conversely, if there are fewer data samples than intervals, Performance Reports Designer displays interpolated data. For example, if the data is sampled every 15 minutes but Performance Reports Designer is displaying 5-minute intervals, two of the three data points for each interval are interpolated. If the data is interpolated, when you mouse over the data point in the chart the data tip labels the number as Estimate rather than Value.

Performance Reports Designer also interpolates data for periods where data is missing. Missing data is indicated by a dotted line in a line or area chart. In a bar chart, missing data is interpolated but there is no visual indication. However, if you stack multiple data series on a bar chart and one data series has fewer data samples, you see shadow columns for interpolated data. This allows you to stack a denser data series on top of a sparser one.

For bar charts, each column displays data for five times the interval for the chart. For example, if the chart is using 1-minute intervals, each column represents 5 minutes.

If you export the Performance Reports data to a CSV file, only the actual data samples are included; interpolated data is not included in the CSV file.

**Viewing Raw Performance Data**

You can view the raw data collected for a chart, rather than the intervalized data. You may want to do this if you want to see the actual maximum and minimum values, or if you want to see details such as spikes in the data. However, because it may require retrieving and displaying a large amount of data, performance of the portlet may be slower.

To view raw data for a chart, click the Configure icon and choose **Raw Data** from the menu. Raw data is displayed in the chart, and the aggregates listed below the chart (**Min**, **Max**, and **Standard Deviation**) also reflect the raw data.

The raw data setting is saved as a property of the chart. If you refresh your browser or reopen the chart, it continues to display raw data. If you add a data series, it will also display raw data.

To return to viewing intervalized data, click the Configure icon and choose **Raw Data** again to de-select it.

You cannot display raw data for stacked charts, and you cannot stack raw data charts. Due to performance issues, it is not recommended to display raw data in column style charts.
QoS Selection Tabs

The QoS Selection tabs are where you can select the host, QoS measurement, and target you want to view data for. There are two QoS Selection tabs, the QoS Selection by Host tab and the QoS Selection by Target tab. The two tabs function the same way, but the order in which you select hosts and targets is different.

- QoS Selection by Host - Use this to easily find multiple measurements from the same host
- QoS Selection by Target - Use this to easily find measurements of the same type on multiple hosts

The selection panes have the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Host name of the computer you want to chart measurements for.</td>
</tr>
<tr>
<td>QoS</td>
<td>Type of QoS measurement you want to chart.</td>
</tr>
<tr>
<td>Target</td>
<td>Which measurement, if more than one measurement for the selected QoS type is taken. For example, for CPU usage you can choose Idle, System, User, Wait, or &lt;host name&gt;.</td>
</tr>
</tbody>
</table>

Work from left to right in the selection panes. Enter text in the filter field at the top of each selection pane to display only items that contain that text.

To select a measurement for charting in the QoS Selection by Host tab, for example:

1. In the Host pane, select the host name of the computer you want to chart measurements for.

   Once you select the host, the QoS measurements for tests you have running on that host are listed in the QoS pane.

2. In the QoS pane, select a QoS measurement.

   Once you select a QoS measurement, the available targets are listed in the Target pane.

3. In the Target pane, select a target, then drag it to a chart pane to display it.

   You can drag multiple targets to each chart. If the targets are measured in different units, a second y-axis is added on the right side of the chart. You can add as many targets with the units on the two y-axes as you want, but you cannot add a target with different measurement units. For example, if the left y-axis represents percent and the right y-axis represents seconds, you can add an unlimited number of targets measured in percent or seconds, but you cannot add a target that is measured in megabytes.
The Filters tab is where you can create filters to narrow down the data to be charted. Once you enter your filter options, check the results with the Check Filters button to make sure the results are not too broad, then drag the drag bars to a chart. Charts update dynamically at a regular interval to reflect changes in the search results.

The Filters tab has the following fields:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>Enter a name for the filter.</td>
</tr>
<tr>
<td>Check Filters button</td>
<td>Displays the items that match the filter in the pane to the right. Use this to make sure the filter is narrow enough that you do not bog down your system charting a huge amount of data.</td>
</tr>
<tr>
<td>Apply button</td>
<td>Applies changes to the filter to the currently displayed charts.</td>
</tr>
<tr>
<td>Drag bars</td>
<td>Drag these bars to a chart to graph the results for the filter.</td>
</tr>
<tr>
<td>Add filter icon</td>
<td>Click to create a new filter.</td>
</tr>
<tr>
<td>Remove filter icon</td>
<td>Deletes the current filter. Visible when you have multiple filters.</td>
</tr>
<tr>
<td>Filter options</td>
<td>Use these fields to display only data from specified hosts or targets in the chart. For example, you can filter for only hosts monitoring a certain QoS measurement, or for all hosts or targets on a specified hub.</td>
</tr>
<tr>
<td></td>
<td>(blank)/not button - Click to display all items except the specified items.</td>
</tr>
<tr>
<td></td>
<td>Criterion pull-down menu - Select the item you want to filter for, such as Source, Probe, QoS, and so on.</td>
</tr>
<tr>
<td></td>
<td>Operator pull-down menu - Choose the appropriate operator, such as is, contains, starts with, and so on.</td>
</tr>
<tr>
<td></td>
<td>Text field - Enter the appropriate text for the criterion you chose.</td>
</tr>
<tr>
<td>Add filter row icon</td>
<td>Click to add another row of filter options.</td>
</tr>
<tr>
<td>Remove filter row icon</td>
<td>Click to remove the row of filter options. This icon is visible if you have more than one row of filter options.</td>
</tr>
</tbody>
</table>
Up/down icons

<table>
<thead>
<tr>
<th>Character</th>
<th>MySQL</th>
<th>Oracle</th>
<th>MS SQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>\</td>
<td>Not applicable</td>
<td>\ (No escape character required)</td>
</tr>
<tr>
<td>%</td>
<td>%</td>
<td>Not applicable</td>
<td>[%]</td>
</tr>
<tr>
<td>_ (underscore)</td>
<td>_</td>
<td>Not applicable</td>
<td>[_]</td>
</tr>
</tbody>
</table>

Note: The special characters \, %, and _ must be preceded with an escape character when using basic search, advanced search, or filters in Unified Service Manager or filters in Performance Reports Designer. In the case of advanced search and filters, this applies when the contains, starts with, or ends with operator is selected.

The escape character required depends on the type of database you use. For MySQL, the backslash (\) is the escape character; for MS SQL, special characters are enclosed in square brackets ([ ]). Searching for special characters is not supported for Oracle.

The table shows how to enter special characters for each database type.

User Tags

You can filter on two user-defined criteria, called User Tags, in portlets that have filters. You can also automatically create groups according to User Tag.

User Tag 1 and User Tag 2 are text fields that are defined on the robot. You can enter any text in these fields. (Use Infrastructure Manager to open the configuration window for the robot.) Once you have done so, you can filter for these values in the Unified Service Manager, Performance Reports Designer, and List Designer portlets.

For example, you could use User Tag 1 for geographic location and User Tag 2 for type of server. For some systems you enter Europe for User Tag 1 in the robot configuration, and for some systems you enter Asia. For User Tag 2, you enter either production server or web server.
You can then create reports for your regional systems by filtering on **User Tag 1** in the Performance Reports Designer (in the **Filters** tab) or List Designer (in the filter fields of the **New Group** pane). To do so, you would set the filter to **User Tag 1 is Europe** or **User Tag 1 is Asia**.

In the Unified Service Manager portlet, you can create separate groups for your production and web servers and apply different monitoring templates to them. To create the groups, in the **Filters** section of the Edit Group dialog you would set the filter to **User Tag 2 is production server** for one group, and **User Tag 2 is web server** for the other group.

**User Tag 1** and **User Tag 2** can be used to filter for any system that has a Nimsoft Monitor robot running on it. You cannot use **User Tag 1** and **User Tag 2** to filter for network devices that do not have a Nimsoft Monitor robot.

For information about automatically creating groups according to User Tag, see **Automatic Groups** (see page 390).

## Charts Pane

The charts pane is where you can view the data for the selected host, QoS, and target. You can select the chart format, maximize the display, or adjust the data range for the y-axis. Hover over a data point to display information about the data in a pop-up window. You can drag charted data to move it from one chart to another. For a line chart, for example, click on a line and drag it to another chart.

To zoom in on an area of a chart, drag the cursor to select that area. Repeat to zoom in again. Click the graph to zoom all the way out. Drag the cursor to select a portion of an axis to zoom in on the selected range.
The charts have the following fields:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title bar</td>
<td>Double-click on Title to enter a title for the report.</td>
</tr>
<tr>
<td>Style icon</td>
<td>Click on a data series in the chart, and then click the <strong>Style</strong> icon to apply one of the following styles, or to remove a data series from the chart:</td>
</tr>
<tr>
<td></td>
<td>■ = Line chart</td>
</tr>
<tr>
<td></td>
<td>■ = Area chart</td>
</tr>
<tr>
<td></td>
<td>■ = Column chart</td>
</tr>
<tr>
<td></td>
<td>■ = Removes the selected data series from the chart</td>
</tr>
<tr>
<td>Choose Source combo box</td>
<td>Click to chart the same set of data series for another host or target.</td>
</tr>
<tr>
<td></td>
<td>If you have selected multiple targets for a single host (QoS Selection by Host), clicking this displays a list of hosts with the same QoS measurements and targets. This allows you to easily view the same set of measurements for different hosts.</td>
</tr>
<tr>
<td></td>
<td>If you have selected a single target for multiple hosts (QoS Selection by Target), clicking this displays a list of targets for the selected QoS measurement. This allows you to easily view different measurements for the same hosts.</td>
</tr>
<tr>
<td></td>
<td>The menu bar displays the name of the current host or target. If there are no other corresponding hosts or targets, the combo box is not displayed.</td>
</tr>
</tbody>
</table>
| **Configure icon** | Click to display a pop-up menu with the options below. Once you choose a menu option, a check box is displayed to the right of the Configure icon. Click the check box to enable the chosen function. For the Scale option, instead of a check box there is a text box where you can enter a number for the scale factor you want.  
- Stacked - Stacks the data series on top of each other.  
- Legend - Toggles the display of the legend on and off. The legend, which appears at the bottom left of the chart, displays the host/QoS/target for each data series in the chart.  
- Raw Data - Displays all data collected, rather than intervalized data. This allows a detailed view of the data and displays the actual minimums and maximums, but does result in slower performance.  
- Title - Adds a title to the chart. Double-click the word Title at the top of the chart, then enter your text.  
- Info text - Adds descriptive information to the bottom of the chart. Double-click the words Info text, then enter your text.  
- Percentile - Adds a line marking a specified percentile to the chart. Enter the percentile in the spinner box.  
- Scale - Adds a scale factor to the selected data series. For example, a scale of 2 doubles the values of the series. |
<p>| <strong>Maximize icon</strong> | Maximizes the display of the chart within the portlet window. |
| <strong>View CSV data</strong> | Click to export the data displayed on the chart to a CSV file. The Chart CSV Preview dialog displays the first 10 records so you can preview the data. From the dialog you can save the data to a file or copy it to the clipboard. Only actual data samples are included; interpolated data (for intervals that are missing data) is not included in the CSV file. |</p>
<table>
<thead>
<tr>
<th>Generate chart URL</th>
<th>Click to generate a URL that can be used to display the chart from a browser without being logged into UMP. This displays the Chart URL dialog. Click the Copy to clipboard icon to save the URL to the clipboard.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear icon</td>
<td>Clears chart of data.</td>
</tr>
<tr>
<td>Remove chart icon</td>
<td>Deletes the chart.</td>
</tr>
<tr>
<td>Data range buttons</td>
<td>By default, the y-axis displays the range of data values for the measurement(s) plus or minus 5 percent. For example, if the data values range from 40 to 80, the y-axis displays a range of 38 to 84. However, for some data units, such as percentages, you may prefer to see the data displayed at a different scale. Clicking the button sets the baseline of the y-axis to zero, and clicking the button sets the top of the y-axis to 100 percent. The buttons appear next to the left or right y-axes if appropriate for the data units. If the data unit is percent, for example, the top and bottom buttons are displayed. If the data unit is megabytes, however, only the bottom data range button is present.</td>
</tr>
<tr>
<td>Page up icon</td>
<td>Displays the previous page.</td>
</tr>
<tr>
<td>Move row up/Move row to previous page icon</td>
<td>Moves the row up. If the row is the top row, it moves to the previous page.</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add row icon</td>
<td>Adds a row of charts.</td>
</tr>
<tr>
<td>Add chart icon</td>
<td>Adds a chart to the row.</td>
</tr>
<tr>
<td>Move row down/Move row to next page icon</td>
<td>Moves the row down. If the row is the bottom row, it moves to the next page.</td>
</tr>
<tr>
<td>Page down icon</td>
<td>Displays the next page.</td>
</tr>
</tbody>
</table>
Automatic Replacement of Fields in PRD Templates

A new capability available in UMP 6.0 is the automatic replacement of fields in PRD templates. This feature allows you to enter parameterized syntax, or variables in a PRD template. After saving the template, you can launch it from USM or Dynamic Views, and the parameterized values are automatically replaced with actual values for the system.

You can use variables in the title bar, chart title, or in the chart info text of a PRD template. When you view the report for a system, the values for that system are displayed.

For example, if you enter $name: $ip in the title bar of a template, when you view the report for a system the system name and IP address are displayed as the title of the report.

You can use the following variables:

- $caption
- $description
- $name
- $domain
- $origin
- $ip
- $dns_name
- $mac
- $oui_organization
- $os_type
- $os_name
- $os_version
- $os_description
- $dedicated
- $ad_name
- $ad_domain
- $nb_name
- $nb_domain
- $user_tag_1
- $user_tag_2
The toolbar allows you to select the time range to display data for, view or print a report as a PDF, save a report, or view previously saved reports.

The toolbar has the following fields and buttons:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undo/Redo icons</td>
<td>Click to undo a change you made, or to redo it after undoing it.</td>
</tr>
</tbody>
</table>

Time selection fields:
Click the back (逆行) or forward (前进) icons to scroll through the time selection options:

- **Start/end date fields** - Useful for charting a specific time period. Click to display a calendar, where you can select the start or end time for the data you want to chart. If the end time is the current time or is in the future, the word Now is displayed in the date box and the charts are updated at 1-minute intervals.

- **Date and time sliders** - Useful for browsing the same time period on different days. To use the sliders, work from left to right. The lefthand slider lets you select the level of granularity you want (year, month, day, or hour). Once you select that, the middle slider lets you select which year, month, day, or hour you want to chart. Once that is selected, the righthand slider lets you select a period within that year, month, day, or hour.
  For example, if you are viewing data for 3 to 5 p.m. for the current day and want to view data for the same time the previous day, move the middle slider to the left one increment. (If you are viewing data for a specific day, the lefthand slider is already set to Day.)
  You cannot move the sliders beyond the increment for the current time.

- **Quick View buttons** - Useful for viewing data for common time intervals:
  - = Previous hour
  - = Previous day
  - = Previous week
  - = Previous month
  The interval is a sliding window so that as time passes new values are appended and old values are dropped.
Toolbar

<table>
<thead>
<tr>
<th>Toolbar buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>= Displays the PDF Preferences dialog (see page 166), where you can choose settings for viewing the report as a PDF. The PDF can be printed or saved.</td>
<td></td>
</tr>
<tr>
<td>= Clears all charts of data.</td>
<td></td>
</tr>
<tr>
<td>= Opens the Manage Reports dialog (see page 196), where you can save a report, or open or delete previously saved reports.</td>
<td></td>
</tr>
<tr>
<td>= Launches the online help.</td>
<td></td>
</tr>
</tbody>
</table>

PDF Preferences Dialog

The PDF Preferences dialog allows you to choose settings for viewing a report as a PDF. The PDF can be printed or saved.

The PDF Preferences dialog has the following fields or buttons:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Report icon (Not available from List Designer)</td>
<td>Opens the Create New Job dialog in the Report Scheduler portlet, where you can schedule the report to be run and delivered.</td>
</tr>
<tr>
<td>Orientation pull-down menu</td>
<td>Choose the page orientation for the PDF, Portrait or Landscape.</td>
</tr>
<tr>
<td>Size pull-down menu</td>
<td>Choose the page size for the PDF.</td>
</tr>
<tr>
<td>Quality pull-down menu</td>
<td>Choose the level of quality for the PDF.</td>
</tr>
<tr>
<td>OK button</td>
<td>Closes the dialog and displays the PDF.</td>
</tr>
<tr>
<td>Cancel button</td>
<td>Click to exit the dialog without creating a PDF.</td>
</tr>
</tbody>
</table>

Save Dialog

The Manage Reports dialog allows you to save a set of charts as a report, open or delete previously saved reports, and import or export reports.

The Manage Reports dialog has the following fields and buttons:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports tree</td>
<td>Click the name of a previously saved report to select it.</td>
</tr>
<tr>
<td>Reports text box</td>
<td>Displays the name of a report selected in the Reports tree. Or, enter the name of a new report.</td>
</tr>
</tbody>
</table>
Account type pull-down menu | Choose the type of account access for the report. If you are an administrator, you can assign the report to a specific account.
- public - Users from all accounts can view the report.
- account - Can be viewed only by users of the account you are logged in as.
Note: Saving to an account requires the Portal Administrator ACL.
- private - Only you can view the report.

Delete button | Deletes the selected report.
Import button | Imports a previously exported report.
Export button | Exports the selected report to an XML file.
Open button | Opens the selected report.
Save button | Saves the report named in the Reports text box.
Cancel button | Closes the dialog without taking further action.

Disable Public Reports

You can block users from saving Performance Reports and List Reports as public reports. You may want to do this if, for example, you are an MSP and you do not want your customers to be able to see reports from other UMP customers.

If saving public reports is disabled, users can save reports as either private or account reports. Users can still open public reports for viewing; they are only blocked from saving new reports as public reports.

Follow these steps:
1. Open Infrastructure Manager.
2. Click on the robot for the primary hub in the tree view.
3. Click the wasp probe to select it in the top right pane.
4. Press CTRL and right-click, then choose Raw Configure from the popup menu.
5. Click the ump_common folder in the tree view of the Raw Configure window.
6. Double-click allow_public_reports and change the value to false.
7. Click OK, then click OK again to close the Raw Configure window.
8. Restart the wasp probe.
Defining Reports with a URL

Preferences Dialog

Access the Preferences dialog by clicking the Settings icon (🔧), then clicking Preferences.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List/Report/SLA Name field</td>
<td>Choose the name of the report you want to open by default in this instance of the portlet. If no report name is selected here, the portlet window contains no data when opened. After choosing a report and saving your preferences, log out and log back into UMP to see the specified report displayed by default.</td>
</tr>
<tr>
<td>Period field</td>
<td>Choose the time interval to display for the default report.</td>
</tr>
<tr>
<td>Height field</td>
<td>Enter the height, in pixels, for this instance of the portlet to open to.</td>
</tr>
<tr>
<td>Maximized Height field</td>
<td>Enter the height, in pixels, for this instance of the portlet to display at when the maximize icon (🗹) is clicked.</td>
</tr>
<tr>
<td>Save button</td>
<td>Click to save your changes.</td>
</tr>
</tbody>
</table>

Defining Reports with a URL

You can use URLs with parameters to define reports from a browser without being logged into UMP. You may want to do this if you want to share reports with people who do not have UMP accounts, or to link to reports from a third-party application.

You can not only view reports as defined, but you can change parameters such as the source, QoS, target, or time period by specifying one in the URL. For example, if you have a report named CPU that displays a series of CPU measurements, you can view the same measurements for a different computer system by specifying a different source in the URL.

You can define one or more data series for each chart, and you can have multiple charts in a row and multiple rows.

The syntax for the URL is:

http://<umpserver>/qoschart/jsp/standalone.jsp?user=<user>&password=<pass>&def=<def>
If you omit the user and password you will be prompted for credentials.

The def parameter

The def parameter uses the JSON syntax using single quotes rather than double quotes. The full specification can be viewed at http://www.json.org/.

The JSON syntax is a set of key value pairs specified as {'key':value, 'key2':value2}.

All of the options except time specifications are listed in an array to define set of charts. Each set of charts is listed in an array to define a set of rows.
Example - Multiple Rows

Note: Normally the URL is specified in a single line. However, to make it easier to read our examples are broken into multiple lines.

def=
{'time': '-1hour', 'rows': [
    {'charts': [
        {'parms': "...", 'series': [
            {'sqt': 'myserver|QOS_CPU_USAGE|Total', 'scale': '1', 'color': '8000', 'style': 'line'},
            {'sqt': 'myserver|QOS_CPU_USAGE|User', 'scale': '1', 'color': '800000', 'style': 'line'}
        ]},
        {'parms': "...", 'series': [
            {'sqt': 'myserver|QOS_CPU_USAGE|Total', 'scale': '1', 'color': '8000', 'style': 'line'},
            {'sqt': 'myserver|QOS_CPU_USAGE|User', 'scale': '1', 'color': '800000', 'style': 'line'}
        ]}
    ]}
]

Example - Single Row

To define a single row you can omit the 'row' option.

def=
{'time': '-1hour', {'charts': [
    {'parms': "...", 'series': [
        {'sqt': 'myserver|QOS_CPU_USAGE|Total', 'scale': '1', 'color': '8000', 'style': 'line'},
        {'sqt': 'myserver|QOS_CPU_USAGE|User', 'scale': '1', 'color': '800000', 'style': 'line'}
    ]}
]
Similarly, you can omit the charts parameter if you only have one chart.

Syntax

Strings are enclosed in single quotes.

Because this is a URL, certain characters, including single quotes, must be properly escaped:

- Single quotes are written as `\` or `\`
- The ampersand (&) is written as `_amp_`
- The backslash is written as `\\`

Numbers are written as numbers.

An array is a set of JSON objects enclosed in brackets.

For `<boolean>` 'y', 'yes', 1, 't', 'true', true, or 'on' can be used for true. For false you can use 'n', 'no', 0, 'f', 'false', false, or 'off'.

The top level fields for the `def` parameter are:

- title
  - Title of the report. If omitted there is no title.

- info
  - Informational text displayed at the bottom of the chart.

- time
  - Time parameters for the report.
    - `<epoch>` is a specific time in seconds since epoch
    - `<period>` is a time period supporting the units "sec", "min", "hour", "day", "month", "year". For example, "60min" or "2hour"
Time can be specified as follows:

'\langle epoch\rangle-\langle epoch\rangle' - start time to end time

'\langle epoch\rangle-' - start time to now

'\langle epoch\rangle-\langle period\rangle' - the \langle period\rangle leading up to \langle epoch\rangle

'\langle epoch\rangle+\langle period\rangle' - the \langle period\rangle after \langle epoch\rangle

'\langle period\rangle' - the last \langle period\rangle. For example, '\langle period\rangle' shows the last 60 minutes.

'tref'

Time reference. If a time is specified you can highlight a time or a time period.

'\langle epoch\rangle+\langle period\rangle,[\langle epoch\rangle+\langle period\rangle]' - Start and stop of the highlighted period (stop is optional).

"S" for epoch is the chart start time. "E" is the end time.

Example: 'tref': 'S+10min,E-1hour' will highlight the area from 10 minutes after the chart starts to 1 hour before it ends.

'stacked'

<boolean> Stack the series for the chart

'lmax'

Set the maximum value for the left axis

'lmin'

Set the minimum value for the left axis

'rmax'

Set the maximum value for the right axis

'rmin'

Set the minimum value for the right axis
'legend'
  <boolean> to turn it off. Use an empty string to only show labels. Specific legend
  annotations can be specified and ordered.

  'M' - maximum value
  'm' - minimum value
  'l' - last value
  't' - total of all values
  'a' - average value
  'p' - show the percentile if it's turned on for the series
  Example: 'legend':'Mpla' would show the max, percentile, last value, then
  average.

'rows'
  An array of row definitions. A row contains one or more charts.

'charts'
  An array of chart definitions. A chart contains one or more series.

'series'
  An array of series definitions.
  Series are defined as follows:

  'sqt'
    Specify the data for the series as '<source>[assign the value for qos in your
    book]]<target>'. An asterisk (*) can be used as a wild card for a full or partial
    word.

  'scale'
    Scale the series by this factor

  'ptile'
    Show the specified percentile, for example 'ptile':95 shows the 95th percentile
    for the series

  'style'
    Series style, must be one of 'line', 'area', 'col'

  'color'
    Color of the series specified in RGB in hex. For example, FF0000 is red.

  'rawData'
    Use with a value of true to see the data in CSV format instead of a graph or chart.
Troubleshooting PRD

Performance Reports May Convert Incorrectly to PDF

Symptom:

When I convert a PRD report containing many charts to a PDF, the PDF version does not display correctly.

Solution:

When you convert a PRD report with a large number of charts to a PDF, the system tries to place the entire report, regardless of the number of charts it contains, on one page of PDF output.

For PRD reports to display correctly in PDF format, it is recommended that you include no more than four or five charts per PRD report. If your PRD report contains more than four or five charts, remove charts as needed until the PDF output displays correctly. Depending on the number of charts in your report, you may be able to correct this issue in printed PDF output by selecting a larger paper size.
Chapter 17: Relationship Viewer

This section contains the following topics:

Overview (see page 205)
Using the Relationship Viewer (see page 207)
Launching the Relationship Viewer using the WebContent Portlet (see page 217)

Overview

This section provides conceptual information about the Relationship Viewer.

About the Relationship Viewer

The Relationship Viewer portlet provides a graphical view of managed elements and their relationships to one another. Managed elements appear as icons, connected by lines that represent the relationships between them.

The Relationship Viewer displays information that is created by various applications—you might have any number of them. With this flexibility, the Relationship Viewer can depict almost any kind of objects and their relationships:

- Computers and network device icons, with the relationship line indicating a network connection between two of them.
- User and service icons, with the relationship line indicating a user’s subscription to a service.
- Physical locations, with the relationship line indicating perhaps a direct transportation route or some other link between locations.

Remember, the underlying applications determine what objects and relationships are available for presentation in the Relationship Viewer.

In addition, the icons and lines may each have visual attributes that depict the state of the element or relationship. For example, if the underlying data provides it, the operational status of a router may be shown as in a "Normal" state, "Failure" state, or other states.

Controls in the Relationship Viewer let you navigate the view in various ways, such as zooming, panning, altering the layout, and so on.
Clicking the mouse on an icon or connecting line causes a descriptive panel to pop-up. For example, clicking on a router icon will display a panel that includes key information about the router including its name, state, address, and so on. Some descriptive panels may offer buttons or links to further detail about the object.

More information:

Accessing the Relationship Viewer (see page 206)
Using the Relationship Viewer (see page 207)

Accessing the Relationship Viewer

There are three ways to access the Relationship Viewer:

Portal access via the USM Actions menu

The most common way to access the Relationship Viewer is by choosing Launch Relationship Viewer from the Actions menu in the Unified Service Manager (USM) portlet.

Note: The Launch Relationship Viewer menu option is present only if the relationship_services probe is running and the optional Relationship Viewer portlet in UMP is licensed.

If you first select a group or specific managed element, the Relationship Viewer opens with the selected element(s) centered and with the radius slider visible. If you do not make such a selection first, the Relationship Viewer opens with all managed elements visible at the lowest zoom level.

If multiple relationships are available, a sub-menu of your choices is displayed when you click Launch Relationship Viewer; click your preference to open the Relationship Viewer using that relationship.

Adding the Relationship Viewer to a Portal page

You can add the Relationship Viewer to any page in your portal in the same way you add any other application. See Adding a Page (see page 18).

Adding a Web Content application to a Portal page

Using the UMP WebContent portlet, you can create a URL that opens the Relationship Viewer. This lets you place multiple Relationship Viewers on a single portal page, which can be useful if you want to have separate views for different contexts (say, Building-1 and Building-2). See Launching the Relationship Viewer using the WebContent Portlet (see page 217) for details.
More information:

Launching the Relationship Viewer using the WebContent Portlet (see page 217)

Using the Relationship Viewer

This section shows you how to use the controls and functionality provided in the Relationship Viewer. When using the Relationship Viewer, you have two primary kinds of actions:

- Changing what you see; that is, what is visible and how it appears.
- Finding objects and seeing details about them.

Changing What You See

There are several ways to change what you see in the Relationship Viewer:

**Navigate within the picture**

You navigate within the view by zooming in on a part of it, or by panning the view port to various areas when the entire view is too large to fit within the boundaries of the window.

- To zoom in or out, you can do any of the following actions:
  - Drag the Zoom slider right or left to zoom in and out, respectively.
  - Drag the handle of the view port indicator in the Radar View.
  - Use the mouse wheel (providing you have one).

- To pan across a view that exceeds the size of the view port, you can either drag the view port indicator in the Radar View or use the scroll bars along the edges of the view port.

There is also a "magnifier" tool that simulates a circular magnifying glass that follows your mouse over the view. This can be helpful when a region of the view is especially detailed.
Using the Relationship Viewer

Change the Layout Style

There are several kinds of layouts available:

- Circular
- Organic
- Orthogonal
- Hierarchic

Each one displays the same managed elements and relationships, but different layouts are more natural for different situations.

Change the Relationship

If the underlying applications model more than one type of relationship, you can select which type of relationship you want to view for the current managed elements.

Change the Radius

If the Relationship Viewer is launched with the context of specified elements (including groups of elements), it includes the "Radius" slider. Such context is most frequently seen when launching the Relationship Viewer from the Unified Service Manager (USM) portlet. The Radius slider lets you adjust the radius of relationships shown from those elements.

All of these are accomplished with controls in the Relationship Viewer control bar.

More information:

- Radar View Button (see page 210)
- Change Layout Style Selector (see page 210)
- Magnify Button (see page 212)
- Zoom Slider (see page 212)
- Radius Slider (see page 213)
- Relationship Selector (see page 213)
- Search and Clear Search Controls (see page 213)

Relationship Viewer Control Bar

The controls for the Relationship Viewer are all located at the top of the screen.

Show/Hide Radar View (button)

Toggles the radar view (an overlay with a small representation of the whole) on or off.

Layout Style (selection list)

Lets you select which style of layout you prefer.
Magnify (button)
Toggles the magnifier (a simulated magnifying glass that follows the mouse) on or off.

Zoom (slider)
Dragging the indicator right zooms in on the view; dragging it left zooms out.

Radius (slider)
Visible only when the Relationship Viewer is launched with a context (system, or group), dragging this slider changes the radius of visible relationships.

Relationship (selection list)
Lets you select which kind of relationship you want displayed, providing that the underlying applications support multiple types of relationships.

Search (button)
Activates a search for the entity in the text field.

Search entry (field)
Enter an identifier for the managed element you want to locate, and click the "Search" button.

Clear
Clears the search field, removes the "matched element" glow, and resets the zoom to show everything.

Get Link URL (icon: 🌐)
Opens a small window that displays the URL of the current view. You can copy this and use it as the basis for a building a URL to use in the WebContent portlet, or to launch the Relationship Viewer from an arbitrary browser. See Launching the Relationship Viewer using the WebContent Portlet (see page 217) for details.

More information:
Radar View Button (see page 210)  
Change Layout Style Selector (see page 210)  
Magnify Button (see page 212)  
Zoom Slider (see page 212)  
Radius Slider (see page 213)  
Relationship Selector (see page 213)  
Search and Clear Search Controls (see page 213)  
Get Link URL Button (see page 216)  
Search and Clear Search Controls (see page 213)
Radar View Button

The Radar View, a small representation of the whole view, is the key to easy navigation within the Relationship Viewer. It is an overlay in the top left corner of the main window, as shown below.

Use the "Show/Hide Radar View" button to alternately show or hide the Radar View.

Note the shaded rectangle within the boundary of the Radar View. It shows the dimensions and location of the current view port with respect to the main view.

You can click anywhere within the shaded rectangle and drag it to a new region of the main view. The view port reflects the change as you drag.

Also note the small black square, or handle, at the lower right corner of the view port locator. You can drag that handle to resize the view port indicator, which at the same time zooms the view in the main window accordingly.

Change Layout Style Selector

This selector looks like a labeled button, with a drop-down arrow on the right-hand end:  

The label indicates the current layout style.

Click the drop-down arrow to open a list of available layouts. Each layout style displays the same managed elements and relationships, but different layouts are more natural for different situations.
About Layout Styles

This section describes the various available layouts and their uses.

Circular Layout

A circular layout emphasizes group and tree structures among related elements, arranging significant groups as separate circles. These separate circles are presented in as a radial tree, with connections between them.

This layout emphasizes group and tree structures within the relationships.

Hierarchical Layout

A hierarchical layout is primarily used when the relationships being modeled are directed. The elements are placed a hierarchy, and most relationship lines are similarly oriented. For example, the lines may generally run from top-to-bottom.

The hierarchical layout style is good for showing dependency relations between elements, particularly any chain of dependencies between the elements. It is not a particularly good layout for symmetric relationships, such as network connections.

Organic Layout

An organic layout is a general purpose layout for symmetric relationships. It can be used with complex networks, including enterprise networking or system management.

In essence, elements are treated as physical objects with a repulsive force, while connections are treated as springs attached to each pair of elements. The springs produce repulsive or attractive forces between their end points depending on their degree of stretch or compression. In the end, this layout arranges the elements in a way that balances all these pseudo-forces.

Depending on the relationships involved, this layout can help you visualize inherent symmetries and clusters within the data, and show a well-balanced distribution of elements with a minimum of edge crossings.

Orthogonal Layout

An orthogonal layout produces a "bus-oriented" layout. Common connection lines are shown in parallel. This layout can be used to visualize commonalities across relationships.
Magnify Button

The Magnifier simulates a circular magnifying glass on the view port, as shown below. You can click on an element or relationship to view its details panel even when using the magnifier.

Use the "Magnify" button to turn the Magnifier on or off.

Zoom Slider

Drag the Zoom control—illustrated here—to zoom in or out of the main view.
Using the Relationship Viewer

Chapter 17: Relationship Viewer

Drag the indicator left zooms out; dragging it right zooms in.

Radius Slider

Drag the Radius control — illustrated here — to set the maximum radius visible from selected elements in your view.

Note: Because radius is based on hops from specific managed elements, this control is only available if you select a specific managed element or group of elements when opening the Relationship Viewer.

Example:

Providing you have the Nimsoft topology application installed, one useful application of this control is to launch the Relationship Viewer with a context such as, say, "Servers". Setting the radius to zero places all the servers in the view. By incrementally increasing the radius, you can observe how and where their connections are related.

Relationship Selector

This selector looks like a labeled button, with a drop-down arrow on the right-hand end: Network Connectivity. The label indicates the current relationship being depicted. For example, Nimsoft offers the Root Cause Analysis and Topology Manager, which models network topology; in this case, the label is Network Connectivity.

If NSM applications that create elements and relationships model multiple different relationships, click the drop-down arrow of the Relationship Selector to choose which type of relationship you want to view.

The availability of different relationships depends on what additional applications are present in your installation.

Search and Clear Search Controls

You can easily locate any managed element and center it in the view by performing a search on its name. The Search button, search entry field, and Clear button appear in that order near the right-hand end of the Relationship Viewer Control bar:
To search for specific managed elements

1. Enter an identifier for the managed element in the text entry field beside the "Search" button. Valid identifiers include the following:
   - Name
   - Class
   - State
   - IP address
   - MAC address.

You can use a wildcard character (*) at the beginning, end, or both ends of the search text. The following are all valid search parameters:

   - **MySwitch** — finds the element with the name "MySwitch", if it exists.
   - **Switch** — finds any and all elements that end with the string "Switch".
   - **building1** — finds any and all elements that contain the string "building1"
   - **My** — finds any and all elements that begin with the string "My".
   - **10.0.4.6** — finds the element with the address "10.0.4.6", if it exists.
   - **10.0.4.** — finds any and all elements whose addresses begin with "10.0.4".
   - **.6** — finds any and all elements whose addresses end with "6".
   - **.4.** — finds any and all elements that include a field in their address with the value "4"

**Note:** You can only use a wildcard character at the beginning or end of a search term (or both ends). You can not embed one within a search term. For example, the following is an invalid search term: **10.*.4.***
2. Click the **Search** button. If a managed element by that name exists, the Relationship Viewer zooms in to it. If more than one element matches the search, the Relationship Viewer zooms in to a point where all elements are visible in the view port. All elements that match the search are highlighted with a green glow. For example, entering `*.4.6` in the search entry field and then pressing the **Search** button would yield the following:

![Diagram showing multiple highlighted elements]

If no managed element matches the search criteria, the search entry box turns red: 10.0.4.125. No objects are highlighted as a result of the search.

3. Subsequent searches after the first add new elements to the set of highlighted elements; that is, existing highlights remain. To remove the highlights, press the **Clear** button to the right of the search entry field.

**Note:** The search function examines all relevant identifiers in the database to find a match. This means it may find a match on a subordinate identifier, not the one used to label the object in the view. This is, of course, a valid match but may not appear so at first.
Get Link URL Button

At the extreme right edge of the Relationship Viewer, you will notice the Get Link URL button:

Click this button to open a small window that contains a template URL to the current view. You can use the Copy to Clipboard button ( ), if applicable in your environment, to capture the URL. You can use the template URL as the basis for building a functional URL to use in the WebContent portlet, or to launch the Relationship Viewer from an arbitrary browser.

The template URL does not include authentication information. See Launching the Relationship Viewer using the WebContent Portlet (see page 217) for information on how to add authentication information to the template, so that it becomes a usable URL.

Viewing Object Details

By clicking on a managed element or relationship line in the Relationship Viewer, you can get further details about the element or relationship. The specific details depend on the underlying application, and will vary accordingly.

Managed Element details

Click on any managed element to display a panel of information about that element.

This panel includes the following information:

- The primary name of the element.
- A symbol for the element, chosen to represent its type.
- A block of information about the element, including its class, manufacturer, and type.
- A logo that quickly identifies the manufacturer of the element.
- A button that lets you quickly access any alarm information about the element.
- A state indicator, which shows you the current state of the element at a glance.

At the bottom of the panel there is an arrow: 🔻. Click this arrow to display a table of the elements properties and values according to data stored for it.

Relationship details

Click on any relationship line that connects managed elements to display a panel of information about that relationship.
Launching the Relationship Viewer using the WebContent Portlet

This panel includes the following information:

- The type of the relationship.
- A symbol representing the status and type of relationship.

- This symbol indicates a symmetric relationship:
- This symbol indicates a directional relationship:

- For each of the related elements, the panel includes the following:
  - A symbol chosen to represent the element's type.
  - The primary name of the element.
  - The class of the element.
  - Port information for each element with respect to the relationship. In this instance, the word "port" should be taken to be generic. That is "port information" is information about the means by which the element is related to the other.

More information:

Changing What You See (see page 207)
Relationship Viewer Control Bar (see page 208)

Launching the Relationship Viewer using the WebContent Portlet

This section shows you how to form a URL that will launch the Relationship Viewer using the WebContent portlet.

Note: A URL constructed according to the information in this section can be used to open the Relationship Viewer in any browser at any location. For example, you could use such a URL from your computer at home. To accomplish this, simply prefix the Source URL as defined below with http://<host>[<port>]. You can use the link icon in the Relationship Viewer to obtain most of the URL; remember that the username and userspass parameters are mandatory. You will have to add them after copying the URL. See the Relationship Viewer Control Bar (see page 208) topic for further information.

First, add a Web Content application to your target page. Once the Web Content application is added, a link prompts you to configure it. Click the link to open the the WebContent editor, where you will enter the URL information.
The format of a full Source URL is as follows:

/relationshipviewer/jsp/standalone.jsp?type=type&relationship=relationship_name&elements=id&radiu
s=integer&user=username&password=userpass

**Note:** All URL parameters except *username* and *userpass* are optional. The parameters can be in an arbitrary order. Also note that you should use URL encodings for certain characters of the values. See, for example, the [W3schools web-site](https://www.w3schools.com) (not affiliated with Nimsoft).

As shown in the above example, the parameters for the URL are separated by an ampersand character—&. They are defined as follows:

- **type**
  - The type of managed element or elements to display.
  - Options: *computer*, *group*, or *configuration_item*
  - Default: *computer*

**Example:**

```
...&type=group&...
```

- **relationship**
  - The relationship type, e.g., *physical_connection*, which is the relation type for Root Cause Analysis and Topology Manager.
  - Other options depend on what other relationships are available with your installed applications
  - Default: *physical_connection*

**Example:**

```
...&relationship_name=physical%5Fconnection&...
```

Note that the underscore character is encoded in the value.
elements=Id

id

Obtaining group IDs and/or device IDs to use in the elements parameter(s) requires that you inspect your database to find the necessary identifiers. You will need to look for identifiers of these types:

- **csId**: the unique id of a computer system. csIds constitute a column in the CM_COMPUTER_SYSTEM table.
- **ciId**: the unique id of a configuration item. ciIds constitute a column in the CM.Configuration_ITEM table.
- **grp_id**: the unique ID of a group. grp_ids constitute a column in the CM_GROUP table.

There can be any number of elements parameters, separated by ampersands. That is, you can have multiple elements parameters, but each can specify only one id.

**Example:**

...&elements=256&elements=257&elements=4572&...

user=username

**username**

The user’s login identification in clear text. This is a required parameter, with no default value.

**Example:**

...&user=TimA&...

password=userpass

**userpass**

The user’s login password in clear text. This is a required parameter, with no default value.

**Example:**

...&password=pi AlaMode4me
radius=integer

integer

The desired radius (number of hops from specified systems or group members) to show in the view.

Options: any integer value.

Default: unconstrained radius.

Example:

...&radius=1&...
Chapter 18: Reports

This section contains the following topics:

- Reports Overview (see page 221)
- Quality of Service Reports (see page 221)
- Service Level Agreement Reports (see page 224)

Reports Overview

There are two kinds of web reports that you can view in the Reports portlet:

- Quality of Service reports, which must be created manually in the Performance Reports Designer (PRD) portlet.
- Service Level Agreement (SLA) reports, which are created automatically after you create SLAs in the Service Level Manager (SLM) portlet.

The Reports application uses a folder structure that groups web reports into the following three sets:

- Custom - The Custom folder contains custom QoS reports from the PRD portlet. Access to the Custom reports requires the Custom Reports ACL permission.
- SLA - The SLA folder contains SLA reports from the SLM portlet. Access to the SLA reports requires the SLM View ACL permission.

You can browse the Custom, Dynamic, or SLA folders and double-click any report to display that report in a separate window.

Quality of Service Reports

This section describes the QoS reports that open when you double-click a report in the Custom or Dynamic folder.

The following items describe how the graph and its features respond to mouse movements:

- When you move the cursor within a graph, two bisecting guidelines appear and follow the cursor. The date and time that the cursor points to in the graph is shown at the top or bottom of the vertical guideline.
■ If you click and hold, you can drag the guidelines and select an area in the graph. The graph updates and displays the area you selected over the entire area of the graph.

■ When you move the cursor within the graph, buttons appear, some of which remain grayed out until you hover the cursor over them.

The graphs contain the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Style icon</td>
<td>Click to choose the style of the chart or to remove a data series from the chart:</td>
</tr>
<tr>
<td></td>
<td>■ = Line chart</td>
</tr>
<tr>
<td></td>
<td>■ = Area chart</td>
</tr>
<tr>
<td></td>
<td>■ = Column chart</td>
</tr>
<tr>
<td></td>
<td>■ = Removes the selected data series from the chart</td>
</tr>
<tr>
<td>Choose Source combo box</td>
<td>Click to chart the same set of data series for another host or target.</td>
</tr>
<tr>
<td></td>
<td>If you have selected multiple targets for a single host (QoS Selection by Host), clicking this displays a list of hosts with the same QoS measurements and targets. This allows you to easily view the same set of measurements for different hosts.</td>
</tr>
<tr>
<td></td>
<td>If you have selected a single target for multiple hosts (QoS Selection by Target), clicking this displays a list of targets for the selected QoS measurement. This allows you to easily view different measurements for the same hosts.</td>
</tr>
<tr>
<td></td>
<td>The menu bar displays the name of the current host or target. If there are no other corresponding hosts or targets, the combo box is not displayed.</td>
</tr>
<tr>
<td>Maximize icon</td>
<td>Maximizes the display of the chart within the portlet window.</td>
</tr>
<tr>
<td>View CSV data</td>
<td>Click to export the data displayed in the chart as a CSV file. The Chart CSV Preview dialog displays the first 10 records so you can preview the data. From the dialog you can save the data to a file or copy it to the clipboard.</td>
</tr>
</tbody>
</table>
Generate chart URL

Click to generate a URL that can be used to display the chart from a browser without being logged into UMP. This displays the Chart URL dialog. Click the Copy to clipboard icon to save the URL to the clipboard.

Data range buttons

By default, the y-axis displays the range of data values for the measurement(s) plus or minus 5 percent. For example, if the data values range from 40 to 80, the y-axis displays a range of 38 to 84. However, for some data units, such as percentages, you may prefer to see the data displayed at a different scale. Clicking the button sets the baseline of the y-axis to zero, and clicking the button sets the top of the y-axis to 100 percent. The buttons appear next to the left or right y-axes if appropriate for the data units. If the data unit is percent, for example, the top and bottom buttons are displayed. If the data unit is megabytes, however, only the bottom data range button is present.

Reports opened from the Dynamic folder have a table below each graph, which contains the following fields and information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The computer hosting the probe sending the QoS data.</td>
</tr>
<tr>
<td>Target</td>
<td>The device/target being monitored, supplying the probe with QoS data.</td>
</tr>
<tr>
<td>Min</td>
<td>The minimum value for the QoS, if applicable.</td>
</tr>
<tr>
<td>Max</td>
<td>The maximum value for the QoS, if applicable.</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>Standard deviation of the samples within the report period (using the STDEV() function in SQL Server).</td>
</tr>
</tbody>
</table>
Service Level Agreement Reports

This section describes the Service Level Agreement (SLA) reports that open when you double-click a report in the SLA folder. SLA reports display information about compliance with SLAs and Service Level Objectives (SLOs). SLA reports are created automatically after you create SLAs in the Service Level Manager (SLM) portlet.

The initial page provides the Service Level Objectives (Summary), which lists the SLOs defined in the SLA, and status information, weight information, and an achieved/expected compliance percentage.

Select an SLO from the Objective column to view the QoS constraints within the SLO. The Quality of Service (Summary) lists the QoS constraints defined in the SLO, and status information, source/target, weight information, and an achieved/expected compliance percentage.

Select a QoS constraint from the Object column to see a graph of the current compliance period for the selected QoS constraint.

The Unavailability Report

Below the graph is a report summarizing the periods with threshold breaches or when the service was unavailable.

The table contains the following information:
- State (why the data was unavailable)
- Period start
- Period end
- Minutes (how long the data was unavailable)

The following icons indicate the status:

= breach

= unavailable service
Chapter 19: Report Scheduler

The Report Scheduler portlet allows you to schedule reports to run at specified times. Reports can be either Performance Reports or SLA Reports. The reports can be delivered as a PDF via email or FTP, or can be stored on a server.

This section contains the following topics:

Working with Report Scheduler (see page 225)
Administering Report Scheduler (see page 234)
Troubleshooting Report Scheduler (see page 239)

Working with Report Scheduler

This section tells you how to work with jobs in Report Scheduler. It tells you how to create, edit, delete, preview, copy, and run jobs. It also tells you how to view the history for a job and how to view the log file for each job run. The jobs table of the Report Scheduler is also described.

Create a Job

In order to schedule reports, you create a job.

To create a job

1. Click the Create New Job icon (CreateInfo) in Report Scheduler.
   The Create New Job dialog opens with the Job Info accordion displayed.
2. Specify Job Information (see page 225).
3. Schedule a Job (see page 226).
4. Choose a Job Delivery Method (see page 227).

Specify Job Information

To create or edit a job for Report Scheduler, enter information in the Job Information accordion. To access the Job Information accordion, click the Create New Job or Edit Job icon in Report Scheduler, then click Job Information.

To specify Job Information

Enter information as appropriate in the following fields of the Job Info accordion. Fields marked with an asterisk (*) are required.
*Name

Name for the job.

Enabled

Whether or not the job is enabled. You can disable a job so that it does not run.

Account

Assigns the job to a customer account. Account contact users can only see jobs assigned to their account. Nimsoft Monitor users can see all jobs.

Description

Text description for the job.

Type

Whether the report is a Performance Report or an SLA Report.

*Report

The report to run. Click the folder icon to browse to the report.

Time Frame

Choose the time interval that you want to see data for. Time intervals beginning with Last Full are for the most recent interval that was completed. Time intervals beginning with Previous are up to the current time. For example, if you choose Last Full Month and you run the report on June 3, the report shows data for the month of May. If you choose Previous 30 Days and run the report at 10 a.m. on June 3, the report shows data from 10 a.m. on May 4 through 10 a.m. on June 3.

PDF Page Orientation

Whether the PDF of the report should be oriented in Landscape or Portrait page layout.

PDF Page Size

Page size for the PDF of the report.

Schedule a Job

You can schedule a job to run once or on a regular basis at specified times.

Scheduling has these requirements:

- If you specify an end date, it must be later than the start date.
- If you select a weekly schedule, you must select at least one day.
- If you select a monthly schedule, you must select at least one month.

To schedule a job

Enter information as appropriate in the following fields of the Schedule accordion.
Scheduling

How often to run the report. You can select Once only, Hourly, Daily, Weekly, or Monthly.

Run this job

Specify the time and date to run the report. Your selection in the Scheduling field affects the options that appear under Run this job. Click the link next to Starting or Ending to open a calendar where you can edit the date and time. The job will run at the first specified time after the Starting time you set.

Use the With Time Zone drop-down menu to select the time zone for the report. The time zone you select determines when the job is executed, and which time zone is displayed in the report. If you do not select a time zone, by default the local time zone is used.

Use the Scheduling and Run this job fields together to specify a schedule. For example, to run a report on Mondays, Wednesdays, and Fridays, click Weekly under Scheduling and under Run this job click Mon, Wed, and Fri. To run a job a set number of days apart, click Daily under Scheduling, and under Run this job, set the Every field to 1, 2, 3, 5, 9, 14, 21, etc. days. The maximum value you can set under Daily is Every 31 days.

Choose a Job Delivery Method

Reports can be sent via email or FTP, or stored in a predefined location on the server. You must choose at least one delivery method for each job in Report Scheduler.

To Choose a Job Delivery Method

Note: In order to send reports via email, you must set up email for UMP.

Do at least one of the following. Fields marked with an asterisk (*) are required.

- Click Email using this template and enter information in the following fields:
  - *To
    Email address(es) to send the report to. Separate multiple email addresses with a comma.
  - *Subject
    Subject for the report.
  - Message
    Text message.

- Click FTP with these settings and enter information in the following fields:
  - *FTP server
    Host name (<host>,<domain>) or IP address of the FTP server.
*Username

User name to use to access the FTP server.

Password

Password. May or may not be required for your FTP server.

*Port

Port number to use to access the FTP server. The default value is 21.

Location

Subdirectory to save the report in. For example, enter reports/monthly to save the report in a subdirectory named monthly.

Passive

Whether to use passive or active FTP mode. Passive mode is recommended if the UMP server and FTP server are separated by a firewall.

Test Connection

Attempts to connect to the FTP server to validate the connection information specified.

- Click Store on server.

Stores the report in a predefined location on a server. The location is set in the wasp probe configuration settings using Infrastructure Manager.

More information:

Set up Email for UMP (see page 446)
Set Where Reports are Stored on a Server (see page 234)

Edit a Job

You can edit any of the settings for existing jobs, including disabling the job so that it does not run.

To edit a job

1. Click the Edit Selected Job icon ( ) in Report Scheduler.

   The Edit Job dialog opens with the Job Info accordion displayed.

2. Specify Job Information (see page 225).

3. Schedule a Job (see page 226).
4. **Choose a Job Delivery Method** (see page 227).

### Specify Job Information

To create or edit a job for Report Scheduler, enter information in the Job Information accordion. To access the Job Information accordion, click the Create New Job or Edit Job icon in Report Scheduler, then click Job Information.

**To specify Job Information**

Enter information as appropriate in the following fields of the Job Info accordion. Fields marked with an asterisk (*) are required.

**Name**

Name for the job.

**Enabled**

Whether or not the job is enabled. You can disable a job so that it does not run.

**Account**

Assigns the job to a customer account. Account contact users can only see jobs assigned to their account. Nimsoft Monitor users can see all jobs.

**Description**

Text description for the job.

**Type**

Whether the report is a Performance Report or an SLA Report.

**Report**

The report to run. Click the folder icon to browse to the report.

**Time Frame**

Choose the time interval that you want to see data for. Time intervals beginning with Last Full are for the most recent interval that was completed. Time intervals beginning with Previous are up to the current time. For example, if you choose Last Full Month and you run the report on June 3, the report shows data for the month of May. If you choose Previous 30 Days and run the report at 10 a.m. on June 3, the report shows data from 10 a.m. on May 4 through 10 a.m. on June 3.

**PDF Page Orientation**

Whether the PDF of the report should be oriented in Landscape or Portrait page layout.

**PDF Page Size**

Page size for the PDF of the report.
Schedule a Job

You can schedule a job to run once or on a regular basis at specified times.

Scheduling has these requirements:

- If you specify an end date, it must be later than the start date.
- If you select a weekly schedule, you must select at least one day.
- If you select a monthly schedule, you must select at least one month.

To schedule a job

Enter information as appropriate in the following fields of the Schedule accordion.

Scheduling

How often to run the report. You can select Once only, Hourly, Daily, Weekly, or Monthly.

Run this job

Specify the time and date to run the report. Your selection in the Scheduling field affects the options that appear under Run this job. Click the link next to Starting or Ending to open a calendar where you can edit the date and time. The job will run at the first specified time after the Starting time you set.

Use the With Time Zone drop-down menu to select the time zone for the report. The time zone you select determines when the job is executed, and which time zone is displayed in the report. If you do not select a time zone, by default the local time zone is used.

Use the Scheduling and Run this job fields together to specify a schedule. For example, to run a report on Mondays, Wednesdays, and Fridays, click Weekly under Scheduling and under Run this job click Mon, Wed, and Fri. To run a job a set number of days apart, click Daily under Scheduling, and under Run this job, set the Every field to 1, 2, 3, 5, 9, 14, 21, etc. days. The maximum value you can set under Daily is Every 31 days.

Choose a Job Delivery Method

Reports can be sent via email or FTP, or stored in a predefined location on the server. You must choose at least one delivery method for each job in Report Scheduler.

To Choose a Job Delivery Method

Note: In order to send reports via email, you must set up email for UMP.

Do at least one of the following. Fields marked with an asterisk (*) are required.
- Click Email using this template and enter information in the following fields:
  
  *To
  Email address(es) to send the report to. Separate multiple email addresses with a comma.
  
  *Subject
  Subject for the report.
  
  Message
  Text message.

- Click FTP with these settings and enter information in the following fields:

  *FTP server
  Host name (<host>.<domain>) or IP address of the FTP server.

  *Username
  User name to use to access the FTP server.

  Password
  Password. May or may not be required for your FTP server.

  *Port
  Port number to use to access the FTP server. The default value is 21.

  Location
  Subdirectory to save the report in. For example, enter reports/monthly to save the report in a subdirectory named monthly.

  Passive
  Whether to use passive or active FTP mode. Passive mode is recommended if the UMP server and FTP server are separated by a firewall.

  Test Connection
  Attempts to connect to the FTP server to validate the connection information specified.

- Click Store on server.
  Stores the report in a predefined location on a server. The location is set in the wasp probe configuration settings using Infrastructure Manager.

More information:

Set up Email for UMP (see page 446)
Set Where Reports are Stored on a Server (see page 234)
**Preview a Job**

You can view a PDF of a report without sending it to the selected delivery methods by previewing it. This also provides an easy way to save the report on your computer.

**To preview a report**

1. Click the job you want to preview in the Report Scheduler table to select it.
2. Click the Preview Report of Selected Job icon (ビュー).

   A PDF of the report is displayed in your browser.

**Run a Job**

You can run a job at any time. The report is sent to the specified delivery method(s). Running a job does not affect the regular schedule for the job.

**To run a job**

1. Click the job you want to run in the Report Scheduler table to select it.
2. Click the Run Selected Job Now icon (実行).

   The job runs and the report is sent to the specified delivery method(s). The report is named `<job_name>_<yearmonthdate>_<hoursminutesseconds>.pdf`. Any invalid symbols or characters in the job name are removed.

**Copy a Job**

You can make a copy of an existing job. This is useful if you want to create another job with similar settings.

**To copy a job**

1. Click the job you want to copy in the Report Scheduler table to select it.
2. Click the Copy Selected Job icon (コピー).

   The Set Name of Copy dialog is displayed.
3. Enter a name for the copy of the job.
   
   If you do not enter a name, the new job is named Copy of `<job name>`.
4. Click OK.

   The copy of the job is created. You can edit the settings of the copy.
More information:

Edit a Job (see page 228)

Delete a Job

You can delete jobs that you no longer want. When you delete a job all runs of the job and the job history are also deleted.

To delete a job

1. Click the job you want to delete in the Report Scheduler table to select it.
   
   You can press Ctrl + click to select multiple jobs, or Shift + click to select contiguous rows of jobs.

2. Click the Delete Selected icon ( Trash Can ), then click Yes.
   
   The job is deleted.

View Job History

You can view the run history of a job. The history displays the time(s) the job ran and the status of each run. You can also access the log for each job run.

To view job history

1. Click the job you want to view the history of in the Report Scheduler table to select it.
   
   The <Job Name> History dialog is displayed.

2. To view the log for a job run, click the run to select it and click View Log.

View the Job Log File

You can view the log file for each run of a job. The log file includes information such as actions taken, times, status, and errors.

To view the job log file

1. Click the job in the Report Scheduler table to select it.
   
   The <Job Name> History dialog is displayed.
2. Click the run you want to view the log for and click View Log.

The log is displayed.

You can also access the log file from an error message if a job is unsuccessful. The Job Run dialog displays the error message and a link for viewing the log file.

**Report Scheduler Jobs Table**

The Report Scheduler jobs table lists the jobs you have created. To take action on a job, first click on the job in the table to select it.

Click a column heading to sort the list of jobs by that column, and click again to toggle between ascending and descending order. Enter text in the field next to a column header to filter for that text.

The far left column contains icons indicating the status of the job definition:

- ■ ✔ = Enabled.
- ■ ▼ = Disabled.
- ■ 🛠️ = Invalid schedule. This may mean the date specified for running the job does not exist (for example, Feb. 30) or that the date is in the past.

**Administering Report Scheduler**

This section tells you how to perform administrative tasks for Report Scheduler.

**Set Where Reports are Stored on a Server**

One of the delivery options in Report Scheduler is to store reports on a server. By default the reports are stored under the root directory webapps/reportscheduler/archive, but you can define the root directory for storing reports. If the report is associated with an account, the report is stored in a directory with that account name under the specified root directory.

**To set where reports are stored on a server**

1. Open Infrastructure Manager.
2. Click on the robot for the primary hub in the tree view.
3. Click the wasp probe to select it in the top right pane.
4. Press CTRL and right-click, then choose Raw Configure from the popup menu.
5. Expand the webapps folder in the tree view of the Raw Configure window.
6. Click reportscheduler in the tree view.
   The Report Scheduler keys are displayed in the right pane.

7. Click New Key.
   The New Key dialog is displayed.

8. Enter file_store_root in the Enter key name field.

9. Enter the directory path you want to use as the root directory for storing reports in the Enter value field.

10. Click OK, then click OK again to close the Raw Configure window.

11. Restart the wasp probe.

More information:

Choose a Job Delivery Method (see page 227)
Default Fonts for Reports

This section provides information about the default fonts you can use for generating reports with Report Scheduler. The default fonts, which are listed below, vary by language and platform. In addition, note that Report Scheduler generates reports using the language in which the report was originally created, which may or may not be the language of subsequent users.

In general, the default fonts below are installed with the corresponding operating system software. However, if you are having trouble with hash signs appearing in your reports, you may not have a default font installed for your language and platform. Use the information below and the troubleshooting topic Unexpected Characters Appear in Reports (see page 241) to determine if you are missing a default font.

If you are missing a default font, simply install one from the list below in the default fonts directory for the operating system. When you restart wasp, the default font is automatically found. You can also use a custom font, although doing so requires further manual steps after installing the font. See the section Set a Custom Font for Reports (see page 238).

For Windows, the default fonts directory is C:\Windows\Fonts. Fonts can also be installed under the Nimsoft installation directory \jre\jre1.6.0_24\lib\fonts.

For reports generated in English, Spanish, or Portuguese, Report Scheduler by default uses a Sans Serif font.

For reports generated in Japanese, Report Scheduler uses one of the following default fonts, provided the font is installed in the default fonts directory for the operating system:

- Windows
  - MS Gothic
  - MS Mincho
- Linux
  - IPA Mincho
  - IPA Gothic
  - VL Gothic
- Ubuntu
  - Sazanami Gothic
  - Sazanami Mincho
  - Kochi Mincho
  - Kochi Gothic
  - Solaris TrueType
- ricoh hg gothic b
- ricoh hg mincho l
- ricoh hg gothicb sun
- ricoh hg minchol sun
- ricoh heiseimin
- ricoh mincho
- ricoh gothic

**Note:** If none of the default fonts above is installed, Report Scheduler will use a Sans Serif font instead.

For reports generated in Chinese, Report Scheduler uses one of the following fonts, provided the font is installed in the default fonts directory for the operating system:

- **Windows**
  - SimSun
  - SimHei
  - MingLiU
  - FangSong
  - KaiTi
  - MS Gothic - supports *some* Chinese characters.

- **Linux**
  - WenQuanYi Micro Hei
  - WenQuanYi Zen Hei

- **Solaris TrueType**
  - Hei
  - Kai
  - Ming

**Note:** If none of the default fonts above is installed, Report Scheduler will use a Sans Serif font instead.
Set a Custom Font for Reports

Most users will want to generate reports using an available default font for their operating system. However, you can manually set a custom font.

Follow these steps:

1. Start Infrastructure Manager.
2. Expand the appropriate hub and select **Service** to verify that the wasp probe is running.
   
   **Note:** If the wasp probe is not running, right-click **wasp** and select **Activate**. When wasp starts, continue to the next step.
3. Right-click **wasp** and select **Configure**.
   
   The **wasp** dialog opens.
4. Under the **Webapps** tab, right-click **reportscheduler**, and select **Stop Webapp**.
5. Open Windows Explorer and browse to `probes\service\wasp\webapps\reportscheduler\WEB-INF\lib` in the Nimsoft installation directory.
   
   **Note:** On Windows, the default fonts directory is `C:\Windows\Fonts`. Fonts can also be installed under the Nimsoft installation directory `\jre\jre1.6.0_24\lib\fonts`.
6. Copy the file `umpreportexport.jar` to a temporary folder.
7. Change the file extension of `umpreportexport.jar` to `.zip`, and extract its contents to the temporary folder you created.
8. In the files you extracted, open the transforms folder and locate the file `prd2fo.xsl`.
9. Open `prd2fo.xsl` in a text editor and do the following:
   
   a. Locate the line near the top of the file containing `<xsl:param name="font-family-param"> </xsl:param>`.
   b. Edit the line to specify your custom font between the characters `> <`, as in `<xsl:param name="font-family-param">custom_font</xsl:param>`.
   c. Save and close the `prd2fo.xsl` file.
10. In the files you extracted, open the transforms folder and locate the file `sla2fo.xsl`.
11. Open `sla2fo.xsl` in a text editor and do the following:
   
   a. Locate the line near the top of the file containing `<xsl:param name="font-family-param"> </xsl:param>`.
   b. Edit the line as follows to specify your custom font: `<xsl:param name="font-family-param">custom_font</xsl:param>`.
   c. Save and close the `sla2fo.xsl` file.
12. In the temporary folder you created:
a. Create a .zip file with the folders com, META-INF, and transforms, ensuring that these folders are at the top level of the .zip file.
b. Rename the .zip as umpreportexport.jar.

13. Overwrite the old umpreportexport.jar by copying the one you created to probes\service\wasp\webapps\reportscheduler\WEB-INF\lib in the Nimsoft installation directory.

14. Restart the reportscheduler webapp.

15. Restart the wasp probe.

Troubleshooting Report Scheduler

This section tells you how to troubleshoot common issues with Report Scheduler.

Report Scheduler: Removing an Account User's Access

In the Reports Scheduler portlet, an account user can still run an SLA report that was moved from their account to an account they do not have access to. In this case, the account user cannot edit the SLA report, but can view and run the SLA report.

To completely remove an account user's access to an SLA report you must:

- Move the SLA report to an account the account user cannot access
- Move the job to an account the account user cannot access

After an administrator moves the SLA report and the job, the account user can still see and run the SLA report until the page is refreshed.
Report Scheduler Shifts Time Axis in PDF Format

In the Performance Reports portlet, you can create a report and then view it as a PDF. You can create the same report with Report Scheduler and view it as a PDF, but the two versions of the same report may appear different. The actual data displayed in each report is the same, but the x-axis of the Report Scheduler report may appear slightly shifted. This occurs because different technology is used to produce PRD and Report Scheduler reports.

In addition, depending on the time scale of the report, the x-axis shift in the Report Scheduler report may be more or less noticeable. For example, if the time scale is in minutes, any x-axis shift in the Report Scheduler report may not even be visible. However, if the time scale is in days, the x-axis shift in the Report Scheduler report may be more noticeable.

Report Scheduler Does Not Display Estimated Values

When you generate a report with Performance Reports, the chart uses bars to display estimated values for periods without data. However, if you use Report Scheduler to email or print the same chart, the chart does not appear the same. This is because charts created with Report Scheduler do not use bars to display estimated values for periods without data.

Java Exception Displayed When Scheduling Reports

Symptom:
When I try to run a job it fails, and when I view the log file a java exception error is displayed.

Solution:
There may be a problem delivering the report. This could be due to an invalid delivery setting, such as FTP server information, email address, or server path. Check the log file for more information. If you see "UNABLE TO EMAIL REPORT!" before the java exception message, you may need to configure UMP for email or the email address may not be valid.

If you see "FTP Reply: 550 550 can't access file." in the java exception message, one of the following problems may be occurring:

- The disk on the FTP server is full.
- The specified FTP user does not have permission to write to the directory.
- The file name contains characters that cannot be saved on the FTP server. Make sure the job name contains only alphanumeric characters.
More information:

Set up Email for UMP (see page 446)
Choose a Job Delivery Method (see page 227)

Some Scheduled Jobs are Not Running

Symptom:
Some scheduled jobs are not running.

Solution:
If you have multiple large jobs running at the same time some jobs may time out. By default, jobs try to execute for 5 minutes. If the job fails to execute within 5 minutes, that job is skipped until the next scheduled run. If this occurs, you can increase the timeout interval. To do so, change the value of the org.quartz.jobStore.misfireThreshold setting the in the WEB-INF/classes/quartz.properties file.

You can also try increasing the number of threads that are allowed to execute jobs.

Note: Increasing the number of threads used to execute jobs increases the resources used by UMP and could cause performance problems.

To increase the number of threads used to execute jobs, edit the org.quartz.threadPool.threadCount setting in the WEB-INF/classes/quartz.properties file. The default value is 6.

Unexpected Character Appears in Reports

Symptom:
When I generate a report with ReportScheduler, the pound, or hash sign (#) appears in place of normal characters.

Solution:
This occurs if your operating system does not have a default font installed for your locale. If this is the case, glyphs that are missing are replaced with hash signs, and the log file provides a message similar to Glyph "?" (0x4e2d) not available in font "Times-Roman."

Verify that you are using one of the default fonts for your locale described in Default Fonts for Reports (see page 236). If necessary, install a default font and then restart wasp so that the new font is located.
Note Icon Does Not Display in Report Scheduler Reports

In the SLM portlet, you can define SLAs and SLOs, and optionally attach notes to them. When you view an SLA or SLO with an attached note in the SLA Reports portlet, a note icon appears on the same line, indicating an attached note.

However, if you use Report Scheduler to run a report that includes an SLA or SLO with an attached note, the note icon does not appear in the report.
Chapter 20: Service Desk

Nimsoft Service Desk is a full-featured service management solution. Service Desk provides action-based workflows in accordance with ITIL standards that allow you to coordinate incident response and proactive IT management.

Service Desk integrates data from Nimsoft Monitor to allow you to unify service management processes with operational monitoring. The Unified Console, for example, displays the My Tickets view of Service Desk tickets and the NM Alarm Console on a single page.

NM and Service Desk data are also integrated in the areas of:
- Incident creation from events (alarms)
- Alarm closure when tickets are closed
- CMDB data
- Reporting

To access detailed information about how to use Service Desk, click the Product Documentation link under Home in the navigation pane.

**Note:** Unlike other UMP portlets, Service Desk must be displayed on a page by itself. It cannot be displayed on a page with other portlets. The My Tickets portlet, however, can be displayed on the same page with other portlets.

This section contains the following topics:
- [Create Tickets from Alarms](#) (see page 244)
- [CMDB Integration](#) (see page 245)
- [Reports with Integrated Data](#) (see page 245)
- [Users in Service Desk](#) (see page 246)
Create Tickets from Alarms

Service Desk incidents can be created manually or automatically from alarms generated by NM.

If a Service Desk ticket that is associated with an alarm is closed, the related alarm is also closed.

You can see the relationship between alarms and tickets by using the ID numbers in each. NM alarms contain the SD Ticket number in the Details window (double-click on an alarm in the Alarm Console to open the Details window). Service Desk tickets contain the Alarm ID in the Additional Information tab.

Automatically Create Tickets from Alarms

Typically when Service Desk is configured it is set up to automatically create incidents from NM alarms.

For information on how to do so, see the section Install and Configure the Service Desk Gateway.

Manually Create an Incident from an Alarm

You can manually create a Service Desk incident from an alarm (event) in the Alarm Console. This allows you to easily assign the alarm to the appropriate workflow in Service Desk.

To manually create an incident from an alarm

1. Right-click on the alarm in the Alarm Console and choose Assign from the popup menu.
2. Click nimsoft_service_desk in the Assign To dialog.
3. Click Assign.
CMDB Integration

The Nimsoft CMDB Gateway probe and Service Desk Adapter automatically discover and record the attributes and relationships of devices monitored by NM into the Service Desk CMDB. This allows Service Desk tickets to provide additional information about relationships and processes, including incidents, problems, known errors, changes, and releases, and to apply automatic workflow rules.

The information in the Service Desk CMDB is synchronized with NM data; when information about a device is updated in NM or a new monitored device is discovered, the Service Desk CMDB is automatically updated.

For information on configuring the CMDB Gateway probe and the Service Desk Adapter, see the Service Desk Integration Guide.

Reports with Integrated Data

Service Desk comes with preconfigured Unified Reports that combine data from NM and Service Desk. The following reports can be found in the Service Desk folder of Unified Reports:

- **Top 10 Applications by Events and Incidents** - Displays the top 10 applications defined in NM with the most events (alarms) and incidents for the specified time period.
- **Top 10 Servers by Events and Incidents** - Displays the top 10 servers defined in NM with the most events and incidents for the specified time period.
- **Top 10 Network Devices by Events and Incidents** - Displays the top 10 network devices defined in NM with the most events and incidents for the specified time period.
- **Top 10 Devices by Mean Time to Repair vs. Service Quality** - Displays the top 10 devices defined in NM with the highest mean time to repair (the time between the start and close of the event) and service quality (the time between when incidents related to the event were created and resolved) for the specified time period.
- **Top 10 Accounts by Service Desk Incidents** - Displays the top 10 accounts defined in Service Desk with the most incidents for the specified time period.
- **Top 10 Accounts by NM Events** - Displays the top 10 accounts defined in NM with the most events for the specified time period.
Users in Service Desk

In order to use Service Desk, you must log in with a user name that matches the name of a user in NM. In addition, the NM user must have the Service Desk ACL assigned to it.

The following sections tell you how to create users in NM and Service Desk.

Create NM Users

This section explains how to create NM users. The user names must match the names of the Service Desk users you will create in the next section.

**Note:** The NM users must have the Service Desk ACL assigned to them.

**To create NM users**

1. Click Security, User Administration in Infrastructure Manager.
2. Right-click in the User Administration window and click New User.
3. Enter information in the User, Full Name, and Description fields.
   **Note:** Avoid creating Nimsoft users and LDAP users with identical user names.
4. Choose the appropriate items from the Access Control List and Default Profile pull-down menus.
   Be sure to assign the Service Desk ACL to the user. You can create a new profile for the user if needed. For more information on creating profiles, see the Infrastructure Manager online help.
5. Click Set Password, enter a password for the user, and click OK.
6. Click OK in the New User dialog.
   The user is created.

Create Service Desk Users

This section explains how to create a self-service user for Service Desk. The user name must match the name of an NM user created in the previous section.

**To configure a Service Desk user account**

1. Click the Manage Contacts link in the Application Setup Section of the Service Desk Navigation Panel.
   The Manage Contact form is displayed.
2. Enter information in the First Name and Last Name fields.
   This will be the Display Name for the client. Both fields are required.
   **Note:** The user name must match the name of an NM user created in the previous section.

3. Enter additional information if desired, or leave the rest of the contact record form blank.

4. Click Apply Changes.
   The new contact record is created.
   The Contact Details, Location, Open Items, and other tabs are now displayed on the form. The Enable Login check box, Out of Office check box, and other related fields are enabled.

5. Click the Enable Login check box in the contact record section.

6. Relate the user to an organization in the Location tab of the contact record.
   This will be the primary organization of the user. You can relate multiple organizations, but only one organization can be marked as primary.

7. Do the following in the Application tab of the contact record:
   - Assign System User ID for the End User
   - Assign License type as Self-Service
   - Check the Disable Service Feedback check box as this contact is not needed to participate in the Service Feedback process.

8. Click Apply Changes. The user account is automatically associated with the Self-Service group and can access the Service Desk modules allocated to such users.
Chapter 21: SLA Reports

This section contains the following topics:

- Introduction to SLA Reports (see page 249)
- SLOs (see page 252)
- QoS Objects (see page 252)
- Preferences Dialog (see page 253)
- Saving Information as a PDF (see page 253)

Introduction to SLA Reports

The SLA Reports portlet application displays performance information for service level agreements (SLAs) defined in the SLM portlet application.

An SLA is an agreement between a client and a service provider that specifies the service to be provided, times, priorities, responsibilities, guarantees, and warranties. SLAs consist of one or more service level objectives (SLOs), which are specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or quality.

SLOs are composed of one or more QoS objects that are combined to produce the SLO achievement value. For example, an availability SLO may depend on multiple components, each of which has a quality of service (QoS) availability measurement.

QoS objects specify the source, target, threshold, and operating period settings for the QoS measurement.

SLA Reports displays performance information for all three levels of the SLA. When you first open an SLA report, you see information about the SLA as a whole, including compliance levels for each SLO. Click the name of an SLO to view the QoS objects defined for the SLO and compliance information for each QoS object. Click the name of a QoS object to see a graph of the data collected for that QoS object during the current operating period.

You can also view historical information for the SLA. Information in any of the windows can be viewed as a PDF, which can be saved or printed.

If you do not have the SLM View permission set in the Access Control List (ACL), you will see a "Permission Denied" message when you try to run the SLA Reports portlet application.
Viewing SLA History

The SLA History chart shows historical information about the SLA and provides an easy way to view the same SLA report for different periods.

1. Click the History icon.

The SLA History chart is displayed.

Compliance periods where the SLA objectives were met are shown as green columns, while compliance periods where SLA objectives were not met are shown as red columns. Hover over a column to see a pop-up window with the dates of the compliance period and the compliance percentage. The trend line for the data is shown in blue, and the compliance objective is shown as a red line. Click the Maximize icon to enlarge the SLA History chart to the size of the portlet window.

2. Click a column in the history chart to view the SLA report for that compliance period.
Understanding SLA Reports

SLA reports display information about compliance with service level agreements (SLAs) that are created in the SLM portlet.

The report tells you the compliance period, the goal, and the compliance percentage for the current period. It also lists the service level objectives (SLOs) that are part of the SLA and the percentage of fulfillment for each SLO.

To view information about an SLO, click the name of the SLO.

Viewing SLA Reports

1. Open the SLA Reports portlet. Or, if the portlet is already running, click the Open SLA icon.

You see the SLAs dialog.

**Note:** If you do not have the SLM View permission set in the Access Control List (ACL), you will see a "Permission Denied" message when you try to run the SLA Reports portlet application.

2. Click the name of the SLA you want to view a report for.

3. Click OK.

The SLA report is displayed.
SLOs

An SLO is a service level objective, which is a specific measurable characteristic of the service being monitored. SLOs are composed of one or more QoS objects. One or more SLOs makes up an SLA.

To view information about an SLO, in an SLA report click the name of the SLO. You see the SLO window.

The SLO window provides compliance information about the SLO. It also provides information about each QoS object defined in the SLO and fulfillment information for each QoS object.

To view a graph of data collected for the QoS object, click the name of the QoS object.

QoS Objects

QoS objects are the smallest component of an SLA. QoS objects specify the source, target, threshold, and operating period settings for the QoS measurement. One or more QoS objects make up an SLO, which in turn make up an SLA.

To view a graph of data collected for a QoS object, in an SLO window click the name of the QoS object. You see the QoS object window.

If there was a compliance breach for the SLA, or if the probe was unable to collect data, you see an Unavailability Report below the graph.

The Unavailability Report lists the periods for the breach or lack of data. The State column indicates the cause for the unavailability:

gages = breach
x = unavailable service
Preferences Dialog

Access the Preferences dialog by clicking the Settings icon ( ), then clicking Preferences.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List/Report/SLA Name field</td>
<td>Choose the name of the report you want to open by default in this instance of the portlet. If no report name is selected here, the portlet window contains no data when opened. After choosing a report and saving your preferences, log out and log back into UMP to see the specified report displayed by default.</td>
</tr>
<tr>
<td>Period field</td>
<td>Choose the time interval to display for the default report.</td>
</tr>
<tr>
<td>(Only for Performance Reports)</td>
<td></td>
</tr>
<tr>
<td>Height field</td>
<td>Enter the height, in pixels, for this instance of the portlet to open to.</td>
</tr>
<tr>
<td>Maximized Height field</td>
<td>Enter the height, in pixels, for this instance of the portlet to display at when the maximize icon ( ) is clicked.</td>
</tr>
<tr>
<td>Save button</td>
<td>Click to save your changes.</td>
</tr>
</tbody>
</table>

Saving Information as a PDF

The information displayed in the SLA Reports portlet can be viewed in PDF format. The PDF can then be saved or printed.

To view information as a PDF:
1. Click the View as PDF icon.
2. Choose the page layout and quality options you want for the PDF, then click OK.

The information is displayed as a PDF.
More information:

PDF Preferences Dialog (see page 166)
Chapter 22: SLM

This section contains the following topics:

SLM Overview (see page 255)
Setting Up a Probe to Deliver Quality of Service Data (see page 265)
Setting Permissions to Use SLM (see page 265)
Compliance Calculation (see page 266)
Using SLM (see page 277)
SLM Interface Reference (see page 338)
SLM Terms and Definitions (see page 349)
Troubleshooting SLM (see page 354)

SLM Overview

Introduction to SLM

The SLM portlet application allows you to define service level agreements (SLAs).

An SLA is an agreement between a client and a service provider that specifies the service to be provided, times, priorities, responsibilities, guarantees, and warranties. SLAs consist of one or more service level objectives (SLOs), which are specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or quality.

SLOs are composed of one or more QoS objects that are combined to produce the SLO achievement value. For example, an availability SLO may depend on multiple components, each of which has a quality of service (QoS) availability measurement.

QoS objects specify the source, target, threshold, and operating period settings for the QoS measurement.

The SLM portlet application allows administrators to quickly define and deploy SLAs based on objectives stated in the agreements between the client and service provider. Once the SLA is defined and activated, data is recorded and computed automatically. You can view reports about SLA compliance in the SLA Reports portlet application.
What is Service Level Management?

Service-level management is the set of people and systems that allows the organization to ensure that SLAs are being met and that the necessary resources are being provided efficiently.

A service level agreement (SLA) is an agreement between a client and a provider of the service. It is vital to the contract and the relationship between the client and the service provider that both parties identify and document their service needs.

In short, Service Level Management embraces a set of tools to monitor and ensure the validity of a set of SLAs for internal customers (e.g. an IT-department providing services for a user-department) and external customers. We like to visualize the Service Level Management task as the following hierarchy:

- Service Level Management (SLM)
  - Service Level Agreement (SLA)
    - Service Level Objective (SLO)
      - Quality of Service (QoS)
SLM Overview

Chapter 22: SLM

Probes
Collecting data from different parts of the NimBUS Infrastructure.

QoS data

Service Level Manager

data_engine
Receives QoS data from the probes and inserts data into the database.

SLA

SLO
QoS
QoS
...

sla_engine
Handles the data inserted into the database by the data_engine. Performs calculations, based on the settings and conditions for the different SLAs and writes the result back into the database.

report_engine
Provides SLA reports, based on calculations performed by the sla_engine.

SLA Reports

SLSs consist of one or more SLOs, each with one or more QoS constraints. These components are configured with a set of terms and conditions. Each SLA is assigned a structure in the database.
This section explains basic concepts of Service Level Management (SLM) as they relate to the SLM portlet.

Service level management oversees the delivery of network and application services as defined in service level agreements (SLAs). The following illustration shows the various components that may comprise an SLA.

The above SLA contains three service level objectives (SLOs) that contain one or more constrained Quality of Service (QoS) objects. A QoS object is the smallest measurable entity within an SLA, typically a checkpoint value (e.g., CPU usage, network usage) provided by a QoS-enabled probe.

The SLM portlet is designed to help you break down SLAs into SLOs and QoS objects, allowing you to build powerful, extensible, and measurable agreements with clients. This is achieved through a highly modularized architecture that allows you to deploy only the components you require, and distributes the workload across multiple network nodes.

Key to building a successful SLM environment is understanding the following areas:

- Data collection
- Data transport
- Data repository
Data Collection

Data collection is normally performed by task-oriented software (probes) dedicated to monitor and report changes and threshold breaches. A QoS enabled probe, such as the cdm (the CPU, Disk and Memory monitoring probe) will generate a Quality of Service message each time it checks its objective, hence giving us the opportunity to gather the collected data and perform various processing techniques on the data.

You may browse the QoS data-series in the Service Level Manager and utilize the same data in your Service Level Objectives.

Note: When computers hosting QoS enabled probes are renamed or when moving the monitoring from one machine to another or renaming a machine, the QoS objects will be stored in new tables in the QoS database. To keep your existing data you can merge the existing data with the new data, giving you one table with the full data series (see the description of Merge Objects in the section on The Active Objects Tab in Viewing the Actual Database Usage (see page 326)).

Data Transport

The underlying infrastructure of the transport mechanism is the message-bus. This message-bus is based on high-availability architecture in a multi-platform environment.

Data Repository

One of the key elements of the SLM is the Data Engine. This engine subscribes to QoS messages and processes the messages into the database. Currently we support Microsoft SQL Server, over the ActiveX Data Objects (ADO) layer. The Data Engine will timely process the recorded QoS data into the Service Level Objectives and Service Level Agreements according to its configurations.
SLM Database Structure

The tables in the SLM database have prefixes indicating the type of data they contain.

The naming convention for the tables is of the form:

- S_ for tables used to store system data
- D_ for data tables
- H_ for tables containing historic data
- HN_ for data tables containing historic/compressed data
- RN_ for data tables containing unprocessed (raw) data directly from the probes

To view the SLA database schema:

1. Open the SQL Server Enterprise Manager.
2. Select the SLA database node.
3. Select the Diagrams child node and right-click on it.
4. Select New Database Diagram.
   The Create Database Diagram Wizard is started.
5. Follow the instructions in the wizard and select all the tables starting with S_ and D_.
   Finishing the wizard gives you the complete database schema for SLAs.

QoS Data Tables

The QoS data structure is dynamically created by the data_engine on the first startup, and when the first unique QoS_DEFINITION or QoS_MESSAGE message is received from a probe.

The S_QOS_DEFINITION table contains the definitions of known QoS types (e.g. QOS_CPU_USAGE), and is updated when a probe sends a QoS_DEFINITION describing a new QoS type.

The S_QOS_DATA table contains an index of all data tables for the QoS objects. When a probe sends a QoS_MESSAGE containing a QoS object that is not already defined in the S_QOS_TABLE, a new entry is added to the table and the data is inserted into the table referenced in column r_table (typically RN_QOS_DATA_nnnn) with the table_id that the new row is given when inserted into the S_QOS_DATA table.

Note: Do not drop the data tables manually. Instead delete the entry from the S_QOS_DATA table, and the tables will be dropped by a trigger. You must restart the data_engine afterwards.
SLA Configuration Tables

The Service Level Manager is used to describe the SLAs and the descriptions are stored in the following key tables:

- S_SLA_DEFINITION
- S_SLO_DEFINITION
- S_QOS_CONSTRAINTS

There are also other tables, containing data about exclude periods, operating periods, and so on. Here is a list of some of these tables.

- S_SLA_EXCLUDE_PERIODS
- S_SLO_EXCLUDE_PERIODS
- S_SLA_NOTES
- S_SLO_NOTES
- S_SLA_CALCULATION
- S_SLO_CALCULATION
- S_QOS_CALCULATION
- S_OPERATING_PERIOD
- S_TIME_SPECIFICATION

SLA Calculation Tables

The first step for a SLA to be calculated is that a job is added to the D_SLA_JOBS table manually by a user or automatically by the sla_engine. The sla_engine detects that there is a new calculation job and performs the calculations. The results are stored in these tables:

- D_SLA_COMPLIANCE
- D_SLO_COMPLIANCE
- D_QOS_COMPLIANCE

When the last job for a SLA in the compliance period is calculated, the result will be added to the historic tables:

- H_SLA_COMPLIANCE
- H_SLO_COMPLIANCE
- H_QOS_COMPLIANCE
Account Tables

The following tables support the Account views and data ownership functionality.

- Accounts Table (CM_ACCOUNT)
- Contacts Table (CM_CONTACT)
- Account-SLA reference Table (CM_ACCOUNT_SLA)
- Origins Table (CM_ACCOUNT_OWNERSHIP)
- Roles Table (CM_ROLE)
- Access Control Lists Table (CM_ACCOUNT_ACLS)
- Dashboard Table (CM_ACCOUNT_DASHBOARD)
- Group Table (CM_ACCOUNT_GROUP)
- Properties Table (CM_ACCOUNT_PROPERTIES)

SLA Engine

The primary task of the SLA Engine is to compute Service Level Agreement compliance for the SLAs, based on the settings for the SLAs entered in the Service Level Manager.

Calculation jobs are automatically started and run on a schedule specified in the sla_engine user interface. For more details, see the SLM Probes > sla_engine > sla_engine Configuration section in the Probes online help.

Calculation jobs may also be started manually (see Exporting the QoS Data Series (see page 325)).
Data Engine

The Data Engine has two primary focus areas:

- Subscribes to Quality of Service messages
- Inserts QoS data into the database

The Data Engine should ideally be installed as close to the database server as possible, preferably on the same server to reduce the network traffic. A subscriber channel is opened to the primary Hub, and this hub will be referred to as the SLM Hub. QoS messages are fed to the Data Engine using this channel. The incoming messages will be reacted upon, and database operations will be performed accordingly.

Quality of Service Messages

The Quality of Service requires a valid license (SLM-QOS) in the Data Engine. For more details, please refer to SLM Probes > data_engine > data_engine Configuration section in the Probes online help.
Defining the Quality of Service Object

Any QoS enabled probe will initiate itself (during startup) by sending a QOS_DEFINITION message. This is picked up by the Data Engine and decoded for information. The content of this message refers to a Quality of Service object in the database. The object will automatically be created in the database with the provided information. You may, however, also create the QOS object manually, by adding the definition using the SLM application.

This is done by selecting New > Quality of Service in the menu bar.

The following table describes the various fields in the dialog form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The actual object name.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the QoS object.</td>
</tr>
<tr>
<td>Group</td>
<td>The group the object belongs to (drop-down list).</td>
</tr>
<tr>
<td>Unit</td>
<td>A string stating the unit (e.g. Milliseconds, Centimeter, etc.).</td>
</tr>
<tr>
<td>Unit abbreviation</td>
<td>Used by reports and views (e.g. ms, cm, % etc).</td>
</tr>
<tr>
<td>Has maximum value</td>
<td>Defines the object with a maximum value.</td>
</tr>
<tr>
<td>Is of type Boolean</td>
<td>Sets the type of the object to be Boolean (True/False).</td>
</tr>
</tbody>
</table>
Populating the Quality of Service Tables

The QoS enabled probe will issue a QOS_MESSAGE on each run. This message refers to an object that should be defined in the database and contains sample data (such as time, value, source, target, etc.).

You can display the database usage (which objects occupy the most space) by selecting Tools/Database status on the SLM menu-bar.

Setting Up a Probe to Deliver Quality of Service Data

Let's configure a probe to generate QoS data while monitoring your system. In this example, we use the cdm probe.

Launch the property window of the cdm probe of your choice (assuming that you have Nimsoft administrative rights) from the Infrastructure Manager.

The cdm probe supports QoS for each disk, CPU, Memory, Paging activity and Processor Queue length. All QoS definitions, except for the disk properties, are located under the Advanced tab. Check the ones you are interested in.

The QoS definitions for the disk properties are located under the Status tab. Double-click the disk you are interested in and check the Disk Usage QoS Message (in Mb and/or %) option in the dialog.

Reply Yes when prompted for a restart.

The probe will initially send a QOS_DEFINITION message to the data_engine causing the SLM system to recognize the new QoS Object.

This procedure differs from probe to probe.

Setting Permissions to Use SLM

If you do not have the SLM Admin permission set in the Access Control List (ACL), you will see a "Permission Denied" message when you try to run the SLM portlet application.
Compliance Calculation

The primary task of the SLA Engine is to compute SLA compliance based on the settings entered in the SLM portlet application.

Calculation jobs are automatically started and run on a schedule specified in the sla_engine user interface. For more information, see the SLM Probes > sla_engine > sla_engine Configuration section in the Probes online help.

Calculation jobs may also be started manually (see Watching SLA Calculations (see page 334)).

Definition of Compliance Percentage

The compliance percentage is the percentage of time that the QoS, constrained by e.g. operating period and thresholds, is compliant within the compliance period.

Each sample is checked within the compliance period by the data_engine and summarized as failed or successful. The result is compared against the expected compliance percentage (defined by the user).
Consider the data represented by the illustration. The red line represents the threshold value, the green line represents the average value and the blue line represents the actual sample values.

How many samples within the operating period are above the threshold settings?

Zero samples breach the threshold line within the operating periods, thus fulfilling 100% of our compliance requirements. The 5 samples that breach the threshold are outside the compliance period, which was e.g. Monday to Monday, with operating periods, every weekday from 08:00 to 17:00.

Let's assume that the total number of samples within the operating period is 129, with 9 samples breaching the threshold. This implies that 6.98% of the samples are accounted for as out of compliance (9 * 100/129).

If our Service Level Agreement requires a compliance of 98.50% (or better) and the only data defined in this SLA is the above data, then our requirements to the SLA is breached due to a current compliance percentage of 100% - 6.98% = 93.02%.

**Defining the Calculation Terms and Conditions**

An SLA consists of one or more SLOs, each with one or more QoS constraints.

- The compliance is calculated on each QoS and forwarded to the SLO.
- The SLO handles the received compliance data from the underlying QoS’s, makes its calculations and forwards the result to the SLA.
- The SLA handles the received compliance data from the underlying SLOs and calculates the total compliance percentage.
The high level process is:

1. Each of the QoS constraints compares the collected data values from the probes with the defined threshold value and calculates the compliance percentage.

2. The SLO collects the compliance values from the QoS constraints and computes the compliance percentage based on a selected calculation method (selects the best value, the worst value, the average value, etc.).

3. The SLA collects the compliance value from the SLOs and calculates the total compliance value, also based on a selected calculation method.

**Calculation Terms and Conditions for the QoS**

The QoS reflects the data series measured by the probes. The compliance percentage is calculated for each QoS, and the results are presented to the SLO.

The compliance percentage for a QoS is calculated, based on the following parameter settings:

- **Threshold value** - You define a threshold value for each QoS, against which each sample in the data series received from the probe is compared. 972 sample values of 1000 equal to, or better than the specified threshold value, means 97.2% compliance for that QoS.

- **Operating period** - Defines in which time period the compliance percentage should be measured (e.g. Monday to Friday from 08:00 – 17:00). Data series outside this period does not influence the compliance percentage.

- **Calculation method** - Here you can select between different calculation methods, determining the way the compliance percentage is calculated for the QoS:
  - Default - Calculation based on all received samples in the operating period. Missing samples are excluded.
  - A set of configurable custom defined formulas. The following formulas are currently available:
    - Average of all samples
    - Number of samples that meets the constraints
    - The median value of all samples
Calculation Terms and Conditions for the SLO

The SLO receives the compliance calculations from the associated QoS’s. The compliance percentage is calculated on each SLO, and the result is presented to the SLA.

The compliance percentage on the SLO is calculated, based on three different parameters:

- **Excluded period** - You can specify periods, which will not count when the compliance is calculated for the SLO. This may e.g. be periods when the monitored system is planned to be shut down due to maintenance etc. Note that the compliance data received from the QoS’s within this excluded period will not count when the compliance is calculated.

- **Calculation method** - Here you can select between different calculation methods determining the way the compliance percentage is calculated for the SLO.

- **You may select between two different types of calculation methods, Formula or Profile:**
  
  **Formula**
  
  Here you can select a mathematical formula to calculate the compliance percentage, based on the input from the QoS’s:
  
  - **Average** - Calculates the average value of the input from the QoS’s
  - **Best** - Looks for the QoS with the best result and selects this result.
  - **Sequential** - The difference between 100% and the achieved compliance for each QoS is summarized and then extracted from 100%.
    
    Example: The SLO receives the compliance calculations from two QoS’s with compliance of 70% and 90%.
    
    Calculated compliance: 100% - ((100% - 70%) + (100% - 90%)): 60%.
  - **Weight** - The possibility to weigh the importance of the different QoS.
  - **Worst** - Looks for the QoS with the worst result and selects this result.
  
  **Profile**
  
  A set of configurable custom defined formulas, currently available are:
  
  - **AND**. The values of all samples in all QoS’s are AND-ed, resulting in one compliance value. AND means that all sample values from all QoS’s simultaneously must equal or be better than the threshold value to be compliant.
    
    See also the section [Definition of Multi-Series Calculation](#) (see page 272).
  - **OR**. The values of all samples in all QoS’s are OR-ed, resulting in one compliance value. OR means that at least one of the sample values must equal or be better than the threshold value to be compliant.
    
    See also the section [Definition of Multi-Series Calculation](#) (see page 272).
Calculation Terms and Conditions for the SLA

The SLA receives the compliance calculations from the associated SLOs and calculates the total compliance percentage, based on three different parameters:

- **Operating period** - Defines in which time period the compliance percentage should be measured (e.g. Monday to Friday from 08:00 – 17:00). Data series outside this period does not influence the compliance percentage.

- **Weight** - Possibility to weigh the importance of the different SLOs.

- **Calculation method** - Here you can select a mathematical formula to calculate the compliance percentage, based on the input from the SLOs:
  
  - **Average** - Calculates the average value of the input from the SLOs.
  
  - **Best** - Looks for the SLO with the best result and selects this result.
  
  - **Sequential** - The difference between 100% and achieved compliance for each SLO is summarized and extracted from 100%.

  **Example:** The SLA receives the compliance calculations from two SLOs with compliance of 70% and 80%.

  Calculated compliance: 100% - ((100% - 70%) + (100% - 80%)) = 50%.

- **Weight** - Enables the possibility to weigh the importance of the different SLOs.

- **Worst** - Looks for the QoS with the worst result and selects this result.
Summary

Service Level Agreement

A Service Level Agreement (SLA) monitors and calculates the compliance from one or more Service Level Objectives(s) (SLO).

The compliance values are calculated according to the selected Calculation method:

- **Average**
  Calculates the average compliance from the SLOs.
- **Best**
  Selects the SLO with the best compliance value.
- **Sequential**
  The difference between 100% compliance and actual achieved compliance for each SLO are summarized. The sum is then extracted from a compliance of 100%.
- **Weight**
  Calculates the compliance according to the weighted value applied for each SLO.
- **Worst**
  Selects the SLO with the worst compliance value.

SLOs monitor the computed values from one or more QoS constraints.

The values from the QoS constraints are calculated according to the selected Calculation method:

- **Average**
  Calculates the average compliance from the QoSes.
- **Best**
  Selects the QoS with the best compliance value.
- **Sequential**
  The difference between 100% compliance and actual achieved compliance for each QoS are summarized. The sum is then extracted from a compliance of 100%.
- **Weight**
  Calculates the compliance according to the weighted value applied for each QoS.
- **Worst**
  Selects the QoS with the worst compliance value.

User defined Calculation Profiles:

- **And**
  Calculates the compliance value for the different QoS measurements within the same time period. The AND operator makes sure that all the QoS constraints are valid only when the samples are within the threshold at the same time period.
- **Or**
  Calculates the compliance value for the different QoS measurements within a time period. The OR operator makes sure that all the QoS constraints are valid when one or more of the QoS constraints are within the threshold in the given time period.

One or more QoS Constraints are attached to a SLO.

A QoS Constraint is a QoS sample value, following a set of calculation rules:

- **Default**
  Calculates the percentage achieved according to the valid number of samples within the time period.

User defined Calculation Profiles:

- **Average of all samples**
  Calculates the average value for all the samples. Parameters that can be modified are:
  - Availability in percentage en breuk
  - Values used to replace NULL values
  - Availability when samples are missing
  - Adjust parameter on how missing samples should be calculated.
  - **Median**
    Calculate the availability from the median of the QoS samples
    Parameters that can be applied are:
    - Ignore values above
    - Ignore values below
Definition of Multi-Series Calculation

When defining the calculation settings for a SLO, you have the option to select a multi-series calculation profile.

(These profiles are custom-defined - see the section Creating a Calculation Profile (see page 299)).

Currently supported profiles are:

- **OR** - Compliant if one of the QoS constraints equals or is better than the threshold value.
- **AND** - Compliant when all of the QoS constraints equals or are better than the threshold value.

**Example OR:**

[Graph showing OR condition with two data series]

OR - At least one of the data series must equal to or be better (in this example lower) than the expected value:

In the graph above, this is achieved, except for the period marked red.

**Example AND:**

[Graph showing AND condition with two data series]

AND – Both data series must be equal to or better (in this example lower) than the expected value:

In the graph above, this is achieved, except for the period marked red.
**Calculation Examples**

The high level process for calculating SLA compliance is:

1. Each of the QoS constraints compares the collected data values from the probes with the defined threshold value and calculates the compliance percentage.
2. The SLO collects the compliance values from the QoS constraints and computes the compliance percentage based on a selected calculation method (selects the best value, the worst value, the average value, etc.).
3. The SLA collects the compliance value from the SLOs and calculates the total compliance value, also based on a selected calculation method.

**Example 1: One QoS and One SLO**

If using calculation method other than Default for the QoS, see the section *Creating a Calculation Profile* (see page 299).
Example 2: Two QoSs and One SLO

If using calculation method other than Default for the QoS, see the section Creating a Calculation Profile (see page 299).

Example 3: Two QoSs and One SLO, Using Calculation Method AND or OR

If using calculation method other than Default for the QoS, see the section Creating a Calculation Profile (see page 299).
Example 4: Two SLOs, Each with Three QoS

If using calculation method other than Default for the QoS, see the section Creating a Calculation Profile (see page 299).

The figure at the bottom of this page shows a SLA with two SLOs, each with three QoS constraints.

Example assumptions:

On the figure below:

- SLO 1: Calculating the compliance percentage from QoS 1, 2 and 3, using calculation method Worst makes a compliance percentage of 70%.
- SLO 2: Calculating the compliance percentage from QoS 4, 5 and 6, using calculation method Average makes a compliance percentage of 90%.
The table below the figure shows the total SLA compliance percentage, using different calculation methods for the SLA.

<table>
<thead>
<tr>
<th>QoS 1</th>
<th>Computed value: 100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS 2</td>
<td>Computed value: 100%</td>
</tr>
<tr>
<td>QoS 3</td>
<td>Computed value: 70%</td>
</tr>
<tr>
<td>QoS 4</td>
<td>Computed value: 100%</td>
</tr>
<tr>
<td>QoS 5</td>
<td>Computed value: 90%</td>
</tr>
<tr>
<td>QoS 6</td>
<td>Computed value: 80%</td>
</tr>
</tbody>
</table>

Calculation method: Default

SLO 1: Calculation method: Worst
Selects the compliance from the QoS Constraints with the worst values.

Achieved Compliance (worst of QoS1, QoS2 and QoS3): 70%

SLO 2: Calculation method: Average
Calculates the average compliance from the QoS constraints.

Achieved Compliance: Average of (100% + 90% + 80%)/3 = 90%

Service Level Agreement:
Calculation method: Best
Selects the compliance from the SLO with the best values.

Achieved compliance (best of SLO1 and SLO2): 90%
The table shows the SLA compliance percentage for the example above, selecting different calculation methods for the SLA:

<table>
<thead>
<tr>
<th>Calculation method</th>
<th>Achieved compliance</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>80 %</td>
<td>The average value of the two SLOs (70% + 90%)/2: 80 %</td>
</tr>
<tr>
<td>Best</td>
<td>90 %</td>
<td>The best value of the two SLOs (70% and 90%): 90 %</td>
</tr>
<tr>
<td>Worst</td>
<td>70 %</td>
<td>The worst value of the two SLOs (70% and 90%): 70 %</td>
</tr>
<tr>
<td>Sequential</td>
<td>60 %</td>
<td>The difference between 100% and achieved compliance for each SLO is summarized and extracted from 100%: 100% - ((100% - 70%) + (100% - 90%)) = 60 %</td>
</tr>
<tr>
<td>Weight</td>
<td>82 %</td>
<td>Assuming that the weight distribution between SLO 1 and SLO 2 is set to 40/60 for the SLA: (70% * 40/100) + (90% * 60/100) = 82 %</td>
</tr>
</tbody>
</table>

Using SLM

This section describes how to create and work with Service Level Agreements (SLAs).
Overview of Creating Service Level Agreements

The process of creating SLAs consists of the following tasks:

1. Create a new SLA and define the:
   - Compliance requirement
   - Compliance period
   - Calculation method
   - Excluded periods
   - SLA account to attach to (optional)

2. Create SLOs and define the:
   - Calculation method
   - Excluded periods

3. Define QoS constraints with:
   - QoS object and source
   - Expected QoS value
   - Operating period
   - Calculation method

Creating an SLA

You can create a new SLA in the following ways:

- In the top of the left-hand navigation pane, select New > Service Level Agreement.

- In the top of the left-hand navigation pane, click the icon next to Service Level Agreement and select New Service Level Agreement.

To create a new SLA group, click the icon next to that group in the navigation pane and select New Group.
Service Level Agreement Form

The following section describes the fields in the SLA form:

Name

Use this field to provide a short name for the SLA.

Account

Use the Account drop-down list to assign an SLA to an account.

An account typically defines a customer or organization and its associated privileges. Administrators can create and manage accounts through the Security menu in Infrastructure Manager.

ID

Each SLA you create is automatically assigned an ID number.

Description

Use this field for descriptive text, such as the purpose of the SLA.

Calculation Methods

This drop-down menu allows you to determine how compliance input from SLOs is used. You can define periods to exclude from the compliance period, such as maintenance windows, or company holidays. The sample values are calculated based on the option you choose from the following drop-down menu options:

Average

Calculates the average compliance from the SLOs.

Best

Selects the best compliance values for the SLOs.

Sequential

Summarizes the periods when the expected value is not met for all SLOs and calculates the compliance, which is the difference between 100 percent and achieved compliance for each SLO.

Weight

Selecting this option opens the Weight Properties dialog, where you can weight the importance of the different SLOs, either manually or automatically.

Note: If you select Weight, the Weight icon to the right of the Calculation Methods field is enabled.

Worst

Selects the compliance from the SLO with the worst values.

Compliance Period
Click the button to the right of the **Compliance Period** field to open the Compliance Period dialog. This dialog allows you to define the start date and time period for an SLA (including its underlying SLOs and QoS). The system uses your selections to compute the SLA compliance percentage. When a compliance period ends, the system measures its compliance and records it in the database.

SLA compliance periods are often one month, but the following three options are available:

- Day
- Week(s)
- Month(s)

By default, weekly and monthly compliance periods have a fixed start date. For example, if you select **Month(s)**, the **Starting** day is the first day of the month. However, you can change the day the report starts to meet your requirements.

**Timezone setting**

This option within the Compliance Period dialog allows you to set the time zone for your location. By default, the system selects the time zone where the data_engine is located. If the user’s location is the same as that of the date_engine, the default setting is normally appropriate. However, you can adjust the timezone setting if you collect data from a location in another time zone.

**Percentage**

This field allows you to set the compliance percentage of the SLA.

**Status**

This message provides the current date and time.

**The current period**

Shows the current period defined in the Compliance Period settings.

**Time used in the compliance period**

A status bar indicating the current point in the compliance period.

**Achieved compliance**

Shows the current compliance percentage values.

**Expected compliance**

Shows the expected compliance percentage values.

**Trend analysis**

Indicates if and when the SLA is breaching the defined compliance percentage. The status bar indicates in red how much of the allowed unavailability has been used. If the status bar is almost completely red, the compliance percentage is close to being breached.
Note: As soon as you enter text or change any selections in the SLA form, the ability to save is enabled in the following buttons:

- The Save icon in the upper right-hand corner
- The Save button in the bottom right-hand corner
- When clicked, the small x that closes the form prompts you to save any changes before the form closes.

Objectives (SLO) Tab in SLA Form

The service level objective list shows the status of the objectives within the SLA. The following section describes the fields and buttons under the Objectives (SLO) tab.

Name
Use this field to provide a short name for the SLO.

Description
Use this field for descriptive text, such as the purpose of the SLO.

Weight
This field allows you to weight the importance of the SLO in relation to the other SLOs within the same SLA. The possible values are auto or a percentage value.

Fulfilled
Shows the percentage of fulfillment of the objective. 100% means completely fulfilled.

New [Button]
Opens a dialog where you can create a new objective within the current SLA.

Edit [Button]
Edit the selected objective.

Delete [Button]
Removes the selected objective from the current SLA.

Save [Button]
Save is enabled as soon as you enter text or change any selections in an SLO.

Legend

- The SLO is compliant with the requirements stated by the SLA and with the QoS constraints defined within the SLO.
- The SLO is not compliant.
- No compliance values are currently available.
Alarm Notification Tab in SLA Form

SLM is capable of generating alarms whenever an SLO breaches the defined compliance settings. Like others, these alarms may be forwarded to email, paging, etc.

**Alarm when compliance is breached**

Check this option to be notified of an SLA breach. A standard alarm is issued when the compliance breaches the value you specify in the **Expected** field.

**Severity Level**

Select the appropriate severity level.

**Alarm Message**

Enter the message to be generated when compliance is breached.

**Subsystem**

Select the subsystem in which alarms will appear in the Alarm Console of Infrastructure Manager.

**Alarm when warning threshold is breached**

Check this option to be notified prior to an SLO breach.

**Severity Level**

Select the appropriate severity level.

**Alarm Message**

Enter the message to be generated when the warning threshold is breached.

**Save [Button]**

Save is enabled as soon as you enter text or change any selections in the Alarm Notification tab.
Notes Tab in SLA Form

The Notes tab lets you record relevant information pertaining to an SLA. For example, a system administrator can leave a note about an event that affected SLA compliance while he or she was working.

Date
Ties the note to a specific date and time.

Title
Descriptive text explaining the circumstances for the note.

Official
Use this check box to include the note in reports.

Text
The actual body of the note.

New [Button]
Create a note within the current SLA. The Note editor appears for you to type your note.

Edit [Button]
Edit the selected note.

Delete [Button]
Removes the selected note from the current SLA.

Save [Button]
Save is enabled as soon as you add a new note or make changes to an existing note.
Calculations Tab in SLA Form

A compliance calculation is automatically performed on schedules as specified in the sla_engine. However, you can use the Calculations tab to recalculate compliance for specific jobs.

The list shows all available compliance jobs related to the current SLA.

**Job Id**

The identification number assigned to a new job.

**Period Begin**

Defines the starting date and time of the compliance calculation period.

**Period End**

Defines the end date and time of the compliance calculation period.

**Owner**

The name of the operator that requested the calculation job.

**Job Start**

Defines the date and time for the compliance calculation job to start.

**Job Expire**

Defines the date and time to automatically remove the job from the SLM system.

**History**

Indicates that compliance data should recorded and saved for historic reports.

**New [Button]**

Opens a dialog where you can initiate a new compliance calculation using the current SLA.

**Edit [Button]**

Edit the selected job. This is enabled only when the job is queued.

**Delete [Button]**

Deletes the selected job from the system.

**View [Button]**

View the result of the compliance calculation for the selected job.

**Save [Button]**

Save is enabled as soon as you add or make changes to calculations.

Also see the section Exporting the QoS Data Series (see page 325).
Excluded Periods

The Excluded Periods tab allows you to exclude designated maintenance periods, or other provisioned down time, so that availability data isn't affected. Clicking the New button launches the Exclude Periods dialog where you can specify excluded periods. After you define an excluded period, it will appear in the list that displays when the Excluded Periods tab is selected.

**From date**
Defines the starting date and time for when to exclude data.

**To date**
Defines the ending date and time for when to exclude data.

**Note**
Use this field to add notes about the excluded period.

**Official**
Select this check box to include the Note in reports.

**New [Button]**
Opens the Exclude period dialog, where you can define an excluded period for the SLA selected.

**Edit [Button]**
Allows you to edit the selected excluded period.

**Delete [Button]**
Deletes the selected excluded period.

**Save [Button]**
Save is enabled as soon as you add a new excluded period or make changes to an existing excluded period.

See also the section Excluding Quality of Service Data (see page 303).
Create a New Service Level Objective (SLO)

You can create a new SLO as follows:

1. Double-click an SLA in the left-hand navigation pane to add the SLO to.
2. With the Objectives (SLO) tab selected, click the **New** button in the Service Level Agreement form.

The Service Level Objective [example_SLA/New SLO] form appears.

An SLO is built around one or more constrained Quality of Service (QoS) objects. The combination you select of source, target, threshold and operating period settings constrains each QoS object. As with SLAs, you can set alarms for SLO breaches. If necessary, you can exclude an SLO from certain periods, such as scheduled down-time for maintenance.
Service Level Objective Form

The following are fields or messages in the main SLO form:

**Name**

Use this field to provide a short name for the SLO.

**Description**

Use this field for descriptive text, such as the purpose of the SLO.

**Status**

This message provides the current date and time.

**The current period**

Shows the current period defined in the Compliance Period settings.

**Achieved compliance**

Shows the current compliance percentage values.

**Expected compliance**

Shows the expected compliance percentage values.

**Note:** As soon as you enter text or change any selections in the SLO form, the ability to save is enabled in the following buttons:

- The Save icon in the upper right-hand corner
- The Save button in the bottom right-hand corner
- When clicked, the small x that closes the form prompts you to save any changes before the form closes.
The Quality of Service Tab

The following items appear under the Quality of Service tab.

QoS Name
The name of the Quality of Service object.

Source
Shows the source device of the QoS data.

Target
Shows the target device of the QoS data.

Weight
Shows the assigned weight of the QoS constraint in relation to the other QoS objects within the selected SLO. The possible values are **Auto** or a percentage value.

Fulfilled
Shows the percentage of fulfillment of the QoS constraint. **100%** means completely fulfilled.

Operator
The operator code for the value comparison.

Threshold
Shows the value set as the expected QoS value.

Op. Period
Shows the defined operating period for the QoS constraint.

Total
Defines the data samples used for calculations.

New [Button]
Create a new QoS constraint within the current SLO.

Edit [Button]
Edit the selected QoS constraint.

Delete [Button]
Removes the selected QoS constraint from the current SLO.

Browse [Button]
Browses the QoS samples related to the current compliance period. You can select to view a graph or table of the QoS samples.

Save [Button]
Save is enabled as soon as you enter text or change any selections to QoS definitions.
Using SLM

Chapter 22: SLM

Move Up, Move Down [Icons 🕹️, 🕷️]

Allow you to change the order of the QoS constraints in the list.

The Quality of Service constraints for the selected SLO show a current state based on the last computations of the SLA Engine. A green indicator shows a positive direction, for example, the QoS is above the SLA compliance percentage. A red indicator means that the QoS is not in compliance with the expected SLA fulfillment. However, this does not necessarily mean that the objective is breached. For the SLO to be breached depends on the weight of the QoS constraint in relation to the other constraints. The legend is as follows:

🔍-The QoS is compliant within the defined constraints (source, target, threshold and period).

⚠️-The QoS is not compliant.

ℹ️-No compliance values are currently available.
Alarm Notification Tab in SLA Form

SLM is capable of generating alarms whenever an SLO breaches the defined compliance settings. Like others, these alarms may be forwarded to email, paging, etc.

**Alarm when compliance is breached**
Check this option to be notified of an SLA breach. A standard alarm is issued when the compliance breaches the value you specify in the *Expected* field.

**Severity Level**
Select the appropriate severity level.

**Alarm Message**
Enter the message to be generated when compliance is breached.

**Subsystem**
Select the subsystem in which alarms will appear in the Alarm Console of Infrastructure Manager.

**Alarm when warning threshold is breached**
Check this option to be notified prior to an SLO breach.

**Severity Level**
Select the appropriate severity level.

**Alarm Message**
Enter the message to be generated when the warning threshold is breached.

**Save [Button]**
Save is enabled as soon as you enter text or change any selections in the Alarm Notification tab.
Notes (SLO Form)

The Notes tab lets you record relevant information pertaining to an SLA. For example, a system administrator can leave a note about an event that affected SLA compliance while he or she was working.

**Date**

Ties the note to a specific date and time.

**Title**

Descriptive text explaining the circumstances for the note.

**Official**

Indicates the note is official.

**Text**

The actual body of the note.

**New [Button]**

Create a note within the current SLO. The Note editor appears for you to type your note.

**Edit [Button]**

Edit the selected note.

**Delete [Button]**

Removes the selected note from the current SLA.

**Save [Button]**

Save is enabled as soon as you add a new note or make changes to an existing note.
The Excluded Periods Tab

The service level objective list shows the status of the objectives within the current SLA. The following describes the fields and the action buttons related to SLOs.

**From date**
Start of the exclusion period.

**To date**
End of the exclusion period.

**Note**
The actual text of the note.

**Official**
Defines the note to be official.

**New [Button]**
Create a new period within the current SLO.

**Edit [Button]**
Edit the selected period.

**Delete [Button]**
Removes the selected period from the current SLO.

**Save [Button]**
Save is enabled as soon as you make any changes.
The Calculation Settings Tab

The Calculation Settings tab allows you to select how the compliance for an SLO is computed (see the section Compliance Calculation (see page 266)).

The following are fields under the Calculation Settings tab of the SLO form:

Calculation Type

Use the radio buttons to select Formula or Profile. This selection affects the selections available in the Calculation Method drop-down menu.

Calculation Method

The options in the Calculation Method drop-down menu depend on the Calculation Type you select - Formula or Profile.

If you select Formula, you can select one of the following methods from the drop-down menu:

Average

Calculates the average compliance percentage from the QoS constraints.

Best

Selects and uses the compliance percentage from the QoS constraint with the best compliance.

Sequential

Summarizes the periods when the expected value is not met for all QoS constraints and calculates the compliance.

The difference between 100 % and achieved compliance for each QoS is summarized and extracted from 100%.

Weight

Weights the compliance from the different QoS constraints according to importance. When Weight is selected, the Weight Properties dialog opens, enabling you to set the importance of the different QoS constraints.

Worst

Selects and uses the compliance percentage from the QoS constraint with the worst compliance.

If you select Profile, you can select one (if any) of the defined profiles in the drop-down menu under Calculation Method. Note that these are listed under the Calculation Profiles node in the left-hand navigation pane.

Save [Button]

Save is enabled as soon as you make any changes.
Defining a Quality of Service Object

Any QoS enabled probe will initiate itself (during startup) by sending a QOS_DEFINITION message. This is picked up by the Data Engine and decoded for information. The content of this message refers to a Quality of Service object in the database. The object will automatically be created in the database with the provided information. You may, however, also create the QOS object manually, by adding the definition using the Service Level Manager. Select File > New > Quality of Service from the menu bar.

The following table describes the various fields in the dialog form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The actual object name on the form QoS_xxx.</td>
</tr>
<tr>
<td>Description</td>
<td>A short descriptive text.</td>
</tr>
<tr>
<td>Group</td>
<td>The group the object belongs to.</td>
</tr>
<tr>
<td>Unit</td>
<td>A string stating the unit (e.g. Milliseconds, Centimeter, etc.)</td>
</tr>
<tr>
<td>Unit abbreviation</td>
<td>Used by reports and views (e.g. ms, cm)</td>
</tr>
<tr>
<td>Has maximum value</td>
<td>Defines the object with a maximum value.</td>
</tr>
<tr>
<td>Is of type Boolean</td>
<td>Sets the type of the object to be Boolean (True/False).</td>
</tr>
</tbody>
</table>

Defining QoS Constraints

The Quality of Service data itself has no value to the service objective unless it is constrained to a specific time-period, specific source/target information and rules to check the actual sample values.

Pressing the New button in the SLO form displays the QoS constraint dialog.

The following table describes the various fields in the dialog-box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A short descriptive text.</td>
</tr>
<tr>
<td>Object</td>
<td>The Quality of Service object.</td>
</tr>
<tr>
<td>Source</td>
<td>From where the sample-value originates.</td>
</tr>
<tr>
<td>Target</td>
<td>The target name of the sample, e.g. a disk, URL etc.</td>
</tr>
<tr>
<td>Value (Expect Quality of Service to be)</td>
<td>The threshold value, used in conjunction with the rules (greater than, less than etc.</td>
</tr>
</tbody>
</table>
A QoS definition describes a unit for the QoS value (e.g. kilo, % mS etc). This will be the default unit. For some QoS objects you can select other units. This drop-down list lets you select another unit, if available. Note that the value will automatically be converted to match the new value.

**Example:**
If the value initially is 1 second, and you change the unit to milliseconds, the value will automatically change to 1000.

For the selected period the constraint is valid. You can select one of the defined operating periods or select Always (means 24 hours a day, 7 days a week).

Here you can select Default or one of the custom-made Calculation Profiles (if any) for QoS calculations. See the sections Compliance Calculation (see page 266), and Creating a Calculation Profile (see page 299). These settings describe the way the SLO will calculate the compliance input from the QoS constraints.

The value dropdown list will (if available) reveal the following values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Smallest value in sample range (last 24 hours)</td>
</tr>
<tr>
<td>Average</td>
<td>Average value the last 24 hours.</td>
</tr>
<tr>
<td>High</td>
<td>Highest value in the sample range.</td>
</tr>
<tr>
<td>Maximum</td>
<td>The QoS definition states that a maximum value exists for this QoS object, such as a disk sample.</td>
</tr>
</tbody>
</table>

**Viewing the Current Sample Values**

Use the QoS sample browser (see Viewing the Quality of Service Data (see page 323)) to determine the best possible values for your QoS threshold settings.
Distributing Importance (Weight)

When setting up service level agreements and objectives, we recognize the fact that some objectives are more important than others. The same fact applies to QoS constraints. The weight distribution feature will help the user to either automatically or manually set up importance (measured in percent) for SLO or QoS constraints.

In Calculations Settings Tab, select Calculation Method as Weight and click the Modify button. Clicking the Modify button opens the weight dialog, showing a pie chart representing the importance (%).

Automatic Weight Distribution

Click button for automatic distribution of weight. The weight will automatically be computed based on the number of objects available (objectives or constraints). This is the default method.

Manual Weight Distribution

This mode enables you to manually distribute weight using the selected object (from the list) and the slider. You can also use the buttons for manual weight distribution. Please note that all of the 100% needs to be distributed. The defined weight will then be displayed in the Weight % column in QoS tab.
Creating a Compliance Period

The compliance period will constrain the SLA (with its underlying SLO and QoS constraints) to a user-defined timeframe, complying with an agreement between two parties. A typical period for SLA monitoring is on a monthly basis. You may, however, create daily and weekly periods as you wish.

The compliance period will, depending on its type (weekly and monthly) have fixed starting dates. If weekly is selected then the starting day is Mondays, and if monthly is selected then the starting day is the first day of the month. However, it is possible to modify the starting day according to your specific needs. E.g. let’s say you want starting day from the 15th; then you adjust the starting date accordingly.

Click the Compliance Period button on the SLA dialog to open the Compliance Period dialog.

See below for a description of the difference in the interpretation of the starting date (at the bottom of the dialog) for the compliance period types.

Day
- The starting date is irrelevant.

Week(s)
- The starting date defines the starting day in every week.

Month(s)
- The starting date defines starting day of every month.

Timezone Setting
This option enables you to set the time zone for your location. By default, the time zone of the location where the data engine is located is selected. As long as the SLM and the data engine are located in the same time zone, this setting should normally be used. If you collect data from another time zone, you can select this time zone here.
Creating an Operating Period

Operating periods are used to constrain the measured values (Quality of Service) to specific hours of any day.

The operating period is defined to be a collection of time periods, and is used when we define new SLAs. We use the Operating Periods when defining the QoS constraints.

Samples falling outside these time specifications will not influence the SLO/SLA compliance requirements.

The Operating Period dialog is opened by clicking icon beside the Operating Period Node in the Navigation Pane and selecting the New Operating Period option.

Give the operating period a name and an optional description. Click the New button in the dialog to add days and time specifications.

To edit an entry in the list, simply double-click the entry to open the time specification dialog for the selected entry.

For example, let’s create an operating period we can call Company Hours. First let’s define our work-hours. Normally, they are Monday-Friday, from 0700 to 1700. The scheduled downtime is every Tuesday at 1500-2000 (*)

The "Company Hours" profile will contain a list of time-specifications (days and time) like the one below:

<table>
<thead>
<tr>
<th>Day</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday</td>
<td>07:00</td>
<td>17:00</td>
</tr>
<tr>
<td>Tuesday</td>
<td>07:00</td>
<td>15:00 *</td>
</tr>
<tr>
<td>Wednesday</td>
<td>07:00</td>
<td>17:00</td>
</tr>
<tr>
<td>Thursday</td>
<td>07:00</td>
<td>17:00</td>
</tr>
<tr>
<td>Friday</td>
<td>07:00</td>
<td>17:00</td>
</tr>
</tbody>
</table>

* We simply ignore the scheduled downtime because it is outside our "work hours".

The format of the operating period and the time-specifications is so flexible that we can create complex operating periods.
Creating a Calculation Profile

Users are allowed to define their own calculation profiles. This is done by clicking the icon beside any of the Calculation Profiles sub-nodes in the Navigation Pane and selecting New.

- Click the icon beside the SLO Calculation sub-node (or one of the defined SLO calculation profiles), selecting New, opens an empty dialog enabling you to define a new SLO Calculation profile.
- Click the icon beside the QoS Calculation sub-node (or one of the defined QoS calculation profiles), selecting New, opens an empty dialog enabling you to define a new QoS Calculation profile.

These Calculation Profiles can be selected when defining the calculation properties for Service Level Objects (SLOs) and Quality of Service Constraints.

The profiles are based on built-in plug-ins distributed with the Service Level Manager application.

Name
Give the new Calculation profile a name in this field.

Description
Give a short description of the Calculation profile in this field.

Calculation
You can select one of the available calculation plug-ins from the drop-down list. Available plug-ins in the list depends on if you have opened the dialog for a SLO calculation profile (multi-series calculations) or the list for a QoS calculation (single-series calculations).

We currently have four plug-ins:

For QoS calculations:
- Calculate availability from the average of all samples.

  Finds the average value of all samples and compares this value against the defined threshold value.

  If the average value of all samples meets the constraints, the availability for that QoS is 100%.

  If the average value of all samples does not meet the constraints, the availability for that QoS is by default set to 0%. Note: Setting the Breach value to another value, using Variable configuration (see below), and the percentage (on breach) can be set to another value than 0%.

  Also note that you can define the way NULL values are handled.

  (NULL value, typically if a probe does not measure a value from the target due to a timeout, e.g. no answer to a ping).
Example:
Threshold: 5
Samples: 5, 4, 8, 6, 2 and one NULL sample.
Define NULL sample as ignored and Breach Value as 35%, using the Variables Configuration.
Availability: The NULL sample is ignored, giving an average value of 
\[(5 + 4 + 8 + 6 + 2)/5 = 4.6.\]
This is below the threshold (5), and therefore a breach condition (which we have set to 35%).

- **Calculate availability from number of samples that meets the constraints.**
  This profile calculates the availability by finding the percentage of samples that meets the constraints.
  Note that you may, using the Variables Configuration, define how missing samples should be treated: either ignored (and not influencing the availability) or treated as samples not meeting the constraints.
  Example:
  Threshold: 5
  Samples: 5, 4, 8, 6, 2 and one sample missing.
  Define missing samples as ignored, using the Variables Configuration.
  Availability: One sample missing (ignored), 3 of four samples meets the constraints, giving an availability of 75%.

- **Calculate availability from the median.**
The median of a number of values is found by sorting the values in a row in descending order. The value found in the middle of the row is the median value.
  Example:
  Threshold: 5
  Samples: 5, 4, 8, 6, 2.
  Sorted in descending order:
  2, 4, 5, 6, 8 The value in the middle of the row is 5, which means that the median value is 5.
  Availability: The median value 5 means that the threshold value is not breached. This means 100% availability.
  **Note:** Using the Variables Configuration, you are allowed to define a floor level and a ceiling level. Values below the floor level and above the ceiling level will be ignored and not count when calculating the median value.

- **For SLO calculations:**
Calculate availability by AND-ing or OR-ing the data series.

Calculate availability by logical expression

For creating a new Multi Expression in SLM, create a new Calculation Profile under SLO Calculations. For setting the logical expression in the profile, set the value of the “Expression” field.

**Data Series**

**Automatic**

QoS Data is recorded at intervals as specified in the probe configuration.

**Asynchronous**

QoS Data is recorded each time the measured value changes.

**Variable Configuration**

This field enables you to modify the selected plug-in.

Example 1:

If using the plug-in “Calculate availability from the average of all samples”, you double-click the lines in this field to define how to handle Null values samples and Breach values.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach Value</td>
<td>Availability in percentage on breach</td>
<td></td>
</tr>
<tr>
<td>NULL Value</td>
<td>Value used to replace NULL samples</td>
<td></td>
</tr>
</tbody>
</table>

**Breach value**

When the average value breaches the defined threshold for the QoS, the average value is by default set to 0 % availability for that QoS. This can be overridden by clicking the Breach value entry and set the Breach value to another percentage, e.g. 54 % as in this example.
Null value

In the case of Null value samples in the data series, you have the following options on how these samples should be treated:

If none of the options described below are selected, a NULL sample will be treated as a not compliant value.

Ignore

The samples will be ignored and will not influence on the compliance percentage. The value “0” will be entered in the Value column.

Min

The samples will be set to the same value as the minimum sample value found in the dataseries. The value “1” will be entered in the Value column.

Max

The samples will be set to the same value as the maximum sample value found in the dataseries. The value “2” will be entered in the Value column.

Note: Click the icon beside the NULL value entry and select Clear Parameter to reset the current parameter value

Type:

If using the plug-in with AND or OR calculation, you double-click the line in this field to select if the series should be AND-ed or OR-ed.
Expression

If using the plug-in with logical expression, you double-click the line in this field to define the logical expression.

For setting the expression use following guideline otherwise the expression parser error will occur:

- Use AND, OR and NOT operators either in upper and lower case.
- The QOS are represented by integer number.
- Each expression must be enclosed in bracket.
- Each token in the expression must be separated by a space.

Some valid samples of the logical expression are

- ( 1 or 2 )
- ( 1 AND 2 )
- ( 1 and ( NOT 2 ) )
- ( 1 AND 2 ) OR ( 3 AND ( not 4 ) )

Excluding Quality of Service Data

Backup, hardware/software upgrades etc. are normal system administrative tasks that make the systems unavailable for shorter or longer periods of time. Normally these procedures are placed to off-hours, such as evenings and weekends. Scheduled maintenance is covered by the agreement between the service provider and the customer. SLM allows you to exclude data for the period in question prior to the event, or after the event (this requires a recalculation of the SLA compliance).

Excluded periods may be created in two different ways:

- You may create an excluded period for a specific SLA by or SLO.

You may create an excluded period for multiple SLAs by running the Add Exclude Period wizard (see the section Creating an Exclude Period using Add Exclude Period Wizard).
Creating an Exclude Period

You may create an excluded period for a specific SLA or SLO by selecting the Excluded Periods tab in the SLA/SLO dialog and clicking the New button. This opens the Exclude Period dialog. Ticking the Add Note option expands the dialog to display the Note section, which otherwise is hidden.

**From**

- Defines the start date/time for the exclude period.

**To**

- Defines the end date/time for the exclude period.

**Add Note**

- Checking this option expands the dialog to display the Note section, which otherwise is hidden.
- The textual note related to this exclude period.

**Official note**

- If this option is checked, the excluded period and the note will appear on the reports.

**Title and text**

- A title and a short text, describing the reason for the excluded period.

You may exclude data for the entire SLA or per SLO. The excluded data will not influence the SLA compliance calculations, and should therefore also be present in the report as a note.
Creating an Exclude Period, using the Add Exclude Period Wizard

You may create an exclude period for multiple SLAs by running the Add Exclude Period wizard. Launch this wizard by selecting Tools > Wizards > Add Exclude Period from the menu bar.

This wizard will add an exclude period with an optional note to one or more SLA/SLO definitions.

The first dialog lets you define when the period starts and stops.

Ticking the Add Note option lets you add an optional title and description of the period. Ticking the Official Note option, the excluded period and the note will appear on the reports.
Click the Next button to continue.

In the next dialog appearing, all SLAs are listed.

If ticking the Show Service Level Objectives (SLO) option, also SLOs will be listed below the SLA they are associated with. Select the components to which you want to add the exclude period.

Click the Next button to continue.

The final dialog appears. Click the Finish button to finish and exit the wizard.
Example - Defining a Simple Service Level Agreement

Important prerequisite:
To be able to measure the service level, you must ensure that the probes monitoring your system are configured to generate QoS (see description in the section Setting Up a Probe to Deliver QoS Data (see page 265)).

The steps involved when defining a simple SLA are as follows:
1. Define your operating periods.
2. Create a new SLA and define your compliance requirement and measure period.
3. Define the Service Level Objectives that make up your agreement.
4. Exclude periods.

Step 1 – Define an Operating Period

The first step is to define an operating period. You will need it in step 3.

The Operating Period dialog is opened by clicking icon beside the Operating Period Node in the Navigation Pane and selecting the New Operating Period option.

Defining no period will default to a 24 hours x 7 days per week service availability, but most organizations have a little more complexity than that. E.g. there may be a regularly scheduled maintenance window when services do not have to be available, or some services may only need to be available during business hours. In the example below, we have chosen to define a “business hours” period.

You can define multiple periods for multiple different services as appropriate.

See also the section Creating an Operating Period (see page 298) for more information.

Defined operating periods will appear in the Operating Periods node in the Navigation Pane, available when defining new SLAs.
Step 2 – Create a new SLA and Define the Service Level Compliance Requirement

Select New > SLA or click icon beside the SLA Node in the Navigation Pane and selecting the New SLA option.

Give the new SLA a name and a description, and set the compliance percentage to 99.9%.

Click the Set period button.

Select Compliance Period

- Day
- Week(s)
- Month(s)

Choose one of the period intervals as your compliance period.

Timezone setting

Ok Cancel
This is the period over which the service level will be measured and your committed compliance amount (measured as a percentage) i.e. if you are going to define a service level of say 99.9% availability; over which period will this be measured? You could define this as a daily service level, in which case your SLA compliance will be measured on a day-to-day basis, or it could be measured weekly or monthly. You also define when you want the measurement period to start.

In this case, we have selected a weekly service level that starts on a Monday and ends on Sunday and we are committed to 99.9% compliance.

Leave the Time zone field empty if your SLM is located in the same time zone as the data engine.

Also, see the section Compliance Calculation (see page 266) for selecting a Calculation method different from Average, which is default.

**Step 3 – Define the Individual Service Level Objectives**

Each Service Level Agreement is comprised of one or more Service Level Objectives. Each objective is a data point that we can measure and calculate into the report – the available data points are automatically prompted to the user by using the pull-down tabs.

Make sure the Objectives (SLO) tab is selected and click the New button.

The Service Level Objective window appears. (Note that the section Creating a Service Level Objective (see page 286) contains additional information).

Give the new Service Level Objective a name and a description. Select the Quality of Service tab and click the New button.

Now the Quality of Service Constraints dialog appears.

In this case we have selected Network Connectivity Response to be less than or equal to 100 seconds and we have selected that this objective should be measured in the “business hours” period that we defined in step 1. We also have the ability to manually “weight” each objective – so that if there are several objectives for us to meet, we can tell the product either to apply equal weightings (automatically selected) or to weight one objective more heavily than others. In this case, we will just select a single objective. See also the section Distributing Importance (Weight) (see page 296) for more information.

The definition of the Service Level Agreement is now complete.
Step 4 – Excluding Periods

Now the SLA setup is complete. But what happens if there is an event outside our control that we want to “exclude” from the SLA calculation? Some examples of this could be that you have agreed with your customers that there will be a one-off maintenance window required for applying some much needed Service Packs. Or, maybe there was a complete power outage to your building that you agree should not count towards the SLA calculation or perhaps a company holiday.

We simply enter the period that we wish to exclude, and add a “note” to that exclusion. Again, by selecting the “official note” box, this note will appear on the reports that everyone gets to see. This feature is extremely useful, because it means that we no longer have to go back and manually recalculate data.

In this case, we have agreed with our web-hosting provider that there was critical maintenance to be performed on our SQL Server database to protect it from the latest Internet worm. We have agreed to take a 2-hour outage that will not count towards the SLA Measurement.

For more information, see the section Creating Service Level Agreements (see page 278).

Creating an SLA Using the SLA Wizard

The SLA Wizard can be launched by selecting the Tools > Wizards Option in the Service Level Manager Toolbar.

Two different SLA wizards are available:
- Creating a SLA based on a service
- Creating a SLA based on an existing SLA

Example – Creating an SLA Based on a Service

This wizard will create a SLA group containing one or more SLAs, based on your selections through this wizard (one SLA for each selected source computer). Each SLA will consist of one SLO with one or more QoS constraints, according to your selections.

1. Launch the wizard by selecting Tools > Wizards > Create SLA By Service.
2. First you have to select the type of SLA you want to create. You have two options:
   - Server SLA - Creating SLAs computing data from server related probes.
3. Make your selection and click the Next button to continue.

When selecting source in the wizard, it means:

- The robot hosting the probe for the net_connect probe.
- The device (e.g. a router) for the interface_traffic probe.

In this example we describe a Server SLA.

4. Click the Next button to continue.
Step 1 prompts you for the following information:

**Group Name**
This will be the name of the created SLA group.

**Description**
This is a short informative description of the SLA. This information will be displayed in the Description field of each of the SLAs created through this wizard.

**Account**
Select the Account under which the SLA Group is to be created.

Select Compliance percentage, Compliance period, QoS calculation method and QoS Operating Period as described in the chapter Creating Service Level Agreement.

Optionally attach the SLA to an account.
5. Click the Next button to continue.

Step 2 enables you select the cdm properties for the SLAs. You can select:

- If you want to include CPU usage, Memory usage and Disk usage.
- Which disks to include
- If you want to completely skip the cdm part (selecting Do not include).
6. Click the Next button to continue.

Step 3 enables you select the ntservices properties for the SLAs. You can select:

- One or more of the services listed.
- If you want to completely skip the services part.
7. Click the Next button to continue.

Step 4 enables you to select the processes properties for the SLAs. You can select:

- One or more of the processes listed.
- If you want to completely skip the processes part.
8. Click the Next button to continue.

Finally you can select one or more QoS Source. One SLA will be created for each of the selected QoS sources, and the SLAs will be placed in the SLA group created with the name specified in step 1.

9. Click the Next button to continue.

The wizard is now finished. When you click the Finish button, the SLA group will be created with one or more SLAs, depending on your selections.

Each of the SLAs contains one SLO with one or more QoS objects according to your selections.
Example – Creating a SLA Based on the Selected SLA

This wizard will create a SLA, based on a SLA selected in the Navigation Pane. The underlying SLO(s) and QoS definitions for the selected SLA will be used as a template.

1. Launch the wizard by selecting Tools > Wizards > Create SLA Based On The Selected SLA.
2. Give the new SLA a name and an optional short description.
   - The SLA Description field will initially contain the description of the SLA that we use as basis for the new SLA.
   - The Based on field will contain the name of the SLA you have selected to use as a template.
3. Select an account from the drop-down list at the bottom of the dialog if you want to attach the new SLA to an account, otherwise leave the field empty.
4. Click the Next button to continue.
   - The next dialogs ask you to choose a source and a target for all of the QoS definitions defined for the template SLA.
5. Select your definitions (you may skip one or more QoS objects for the new SLA by checking the Skip this QoS object option).
6. Click the Next button to continue.
   - When all QoS objects are defined, the following dialog appears:
7. Click the Finish button, and the newly defined SLA will appear in the Navigation Pane.

If the new SLA is based on a SLA in a SLA group, the new SLA will be placed in the same group.

Creating a QoS Monitoring Profile

You can create monitoring profiles that are based on QoS data instead of live information from a system.

The feature will be activated and visible, provided that the qos_engine probe is installed. For each QoS Object you will be allowed to create one or more monitoring profiles of same or different types.

A dedicated probe (the qos_engine) will subscribe to QoS messages, each QoS message will be checked to see if it fits a monitoring profile (a QoS can match to more than one profile). If one or more profiles match the incoming QoS message, the values are evaluated and alarms issued if a threshold violation is detected.

Creating and configuring monitoring profiles can be done by clicking icon beside a QoS object and selecting Create Monitor option under the QoS node in the Navigation pane.

The QoS Monitor dialog pops up, enabling you to set the monitoring properties.

Baseline Value Definition

The baseline value is a central element for the threshold when creating monitors of type Dynamic.

The baseline is calculated from measurements collected at a specific time each day for the last N days, or a specific time for the same weekday the last N weeks.

The samples within all the time spans are used to calculate the average and standard deviation of those values. This gives some fundamental values that can be used for further calculations.

For example, a weekly baseline definition is set to 4 weeks and a time span of 1 hour. The QoS arrives at a Friday 13:00:00. This will, with a sample rate at 5 minutes, give 12 samples for each of the previous 4 Fridays between 12:30 and 13:30. These 48 samples are the basis for the baseline calculation.
QoS Monitors List

Selecting Tools > QoS Monitors in the SLM Menu bar, the QoS Monitors window will be launched. This window lists the QoS Monitors defined (if any).

QoS monitors are created as described in the section Creating a QoS Monitoring Profile (see page 317).

See also the section QoS Monitor Properties (see page 319) for details.

Click icon in the list which gives you the possibility to:

- Edit the properties for the selected QoS monitor (see QoS Monitor Properties (see page 319)).
- Delete QoS monitors.
- View the baseline values for the selected monitor (see Baseline Value Definition (see page 317)).
**QoS Monitor Properties**

**Monitor Name**

The monitor name is automatically filled in, based on the QoS name, source and target. This name may be overruled by a name of your own choice.

**Monitor Subsystem**

This field is automatically filled in with the sub-system ID for the device, identifying from which part which part of the system the QoS and alarms come. The sub-system IDs are maintained by the Nimsoft Alarm Server (nas).

**Monitor Types**

Select a monitor type to be used as a basis for the threshold calculation. Your choice here depends on what you want to achieve:

**Static**

Use Static if you want alarms to be issued if the QoS value exceeds the threshold specified.

You may specify the threshold as an absolute value or as a percentage of the maximum value (maximum value is only available for QoS types with maximum size, otherwise grayed out). You may also select that at least n consecutive breaches must occur before an alarm will be issued.

**Dynamic**

Use Dynamic if you for example want to consider that the QoS values have a regular fluctuation, such as high during the work hours and low at night.

Alarms will be issued if the QoS value exceeds the threshold, calculated from the baseline value.

You must specify Period Type, Periods and Timespan to find the baseline value, which will be used to calculate the error threshold.

- Period Type is day or week.
- Periods are numbers, defining how many days or weeks to be used to calculate the Baseline.
- Timespan is the time window within each period, from which samples should be used to calculate the Baseline value.

The baseline is calculated from measurements collected at a specific time each day for the last N days or a specific time for the same weekday the last N weeks.

The threshold is defined as an expression that is calculated in a Lua script. The expression can contain the following variables that are calculated based on the baseline settings:

- AVG
- STDEV
Example:
Period Type: Day
Periods: 4
Timespan 1 hour

A sample collected at for example 12.15 o’clock, will be compared with the threshold, which is calculated from the Baseline value. The Baseline value will be calculated based on the average value of the samples collected within the timespan (1 hour) for the four past days.
The threshold can be by either selecting one of the formulas in the drop-down list, such as 20% Above Baseline.

Selecting Custom, you may specify a threshold manually.

Percentile

As for Dynamic (see above), you may use Percentile if you for example want to consider that the QoS values have regular fluctuations.

Alarms will be issued if the QoS value exceeds the threshold, which is a percentile of the values of the samples collected within the time spans for the periods specified.

The threshold can be specified as for example greater than the 95 percentile of the calculated value.

**Alarm thresholds:**

Error thresholds must be defined for the QoS monitors in order to have alarm messages issued on threshold breaches.

For monitors configured to use monitor type Static and Dynamic, it is also possible to define a warning threshold, and you may also select to monitor for unavailable data.

The operands available to be used to set the error- and warning thresholds are:

- Less Than
- Less Than Or Equals To
- Equals to
- Greater Than
- Greater Than Or Equals To

**Threshold values**

- Custom - Selecting Custom, you can compose your own threshold value. If first selecting one of the predefined threshold values, and then selecting Custom
- Baseline - The baseline is calculated from measurements collected at a specific time each day for the last N days or a specific time for the same weekday the last N weeks.
- 10 % Above Baseline
- 20 % Above Baseline
- Baseline + Standard Deviation
- Baseline + 20 % of Stdev
- Baseline Period Minimum
- Baseline Period Maximum
The alarm message text can contain some variables that will be expanded before the alarm is sent. The following variables are supported:

- NAME
- MONID
- VALUE
- OPERATOR
- THRESHOLD
- AVG  (dynamic)
- STDEV (dynamic)
- MIN   (dynamic)
- MAX   (dynamic)
- COUNT (dynamic)

A typical alarm message example would be: $NAME has breached the threshold value ($THRESHOLD)
Viewing the Quality of Service (QoS) Data

The navigation window contains the Quality of Service node. All registered QoS objects are listed under this node using the description field in the QoS object. This view enables the user to quickly browse the database for particular data-series.

The structure is organized like illustrated below:

- Quality of Service
  - Quality of Service object name
    - Source
    - Target

Note: This is the structure if the QoS objects are ordered on the QoS name. Clicking the icon beside QoS node in the Navigation Pane lets you select another sorting key, such as order by QoS group, where the QoS objects will be grouped into logical groups.

Let's explain the structure using "real" data. The cdm probe provides the QoS data registers the QoS objects it will use during the startup sequence. These messages are collected by the Data Engine and transformed into database tables and definitions. The cdm probe will, on a timed interval, send its QoS data, based on its findings and calculations to the Data Engine as messages (subject: QOS_MESSAGE).

This will populate the database tables matching the cdm QoS configuration. Let's say we configured the cdm to send QoS on CPU usage and Disk usage (C:) data. You are now able to browse the data using the Service Level Manager. Find the Quality of Service node and double-click to expand it. This brings up the QoS descriptions registered by the Data Engine. Find the Disk Usage node and double-click to expand it. The children nodes will reflect the sources (Robots) that are generating the QoS data. The target node holds the last piece of information needed to pinpoint the recorded data in the database, in this case e.g. C:. We can address each QoS using the QoS-Name, Source and Target.
Generating a Graph

The Service Level Manager generates a graph when double-clicking a QoS objects target node in the Navigation Pane.

![Graph](image)

Select Period

- Last month
- Last day
- Last week
- Last month
- Specify period
You may select the period from the drop down list (last day, last week etc.).

Using the field Max Value, you may also set the maximum value of the vertical axis in the graph to a proper value to compress the graph in cases where you have "peaks".

**Exporting the QoS Data Series**

You may export QoS data to a file, using the following method.

Using the Export QoS Data wizard, accessible from clicking the icon beside the respective QoS in the Database Status dialog and selecting Export Data option from the menu (see *Viewing the Actual Database Usage* (see page 326)).

Note that this wizard may also be started, clicking the icon beside QoS constraint under the QoS node in the Navigation pane and selecting Export data.
Exporting QoS Data Using Export QoS Data Wizard

1. Select Tools > Wizards > Export QoS Data from the menu-bar to launch the wizard.
2. Click the Next button to continue.
   The next dialog lets you configure the QoS source and targets.
   (Note that the fields in this dialog are already filled in if the wizard was started from
   the Database Status window).
3. Click the Next button to continue.
   The next dialog lets you select which period to export.
4. Configure the period to select data from and click the Next button to continue.
5. In next dialogue box, modify the column and or row separators if wanted, and
   include or exclude column headers in the formatted file.
6. Click the Next button to continue to the last dialog.
7. Click the Finish button to finish and exit the wizard.

Two other ways to launch the Export Data wizard:

You may also launch the wizard by selecting Tools > Database Status from the menu-bar.

This will open the Database Status window, showing you various information related to
the QoS data stored in your database.
Click the icon beside the respective QoS in the list which opens a small menu.
Selecting the Export Data option will launch the wizard.

Also clicking the icon beside the respective QoS object under the Quality of Service
node in the Navigation pane and selecting Export Data will launch the Export wizard.

Data Management

All Quality of Service data is received by the data_engine and inserted into the
database. The data_engine may be configured to perform automatic clean-up
procedures by defining configuring the data management section of the data_engine.

You may, however, perform manual data-management by using the Service Level
Manager.

Viewing the Actual Database Usage

Select Tools > Database Status from the menu bar to bring up the Database Status
window. This will show you various information related to the QoS data stored in your
database. The tabs represent various ways of getting information regarding the
database usage.
The Active Objects Tab

Shows all available QoS objects registered within the database structure. Bring up the action menu by issuing a right-mouse button-click. View the QoS data by double-clicking the list element, or perform a selective data-management by selecting delete.

- F5 - Refresh list
- F6 - Update/view sample period for the selected QoS objects.

The Sub menu

On clicking icon beside any of the QoS objects in the list opens a small menu with the following options:

Update

Updates the selected row with data from the current compliance period.

Get Statistics

Finds the details statistics like Historic Row, First Sample, Last Sample, S./Min etc. within the current compliance period.
This information will then be found in the respective columns in the window.

Delete Object(s)

Deletes the selected QoS object(s) (not only the data series) from the database. The deleted QoS object will disappear from the database and will not be re-created before the probe is restarted.

Merge Objects

Allows you to merge two QoS objects of the same type. Left-click the first object and <ctrl>+left-click the next object. Click icon and select the merge object option.

Note that you can toggle the direction of the merge operation by clicking the arrow in the middle of the dialog.
The newly merged QoS objects will take the “destination” QoS object’s name.
You also have the option to delete the “source” QoS after the merge operation.
The deleted QoS object will disappear from the database and will not be re-created before the probe is restarted.

View Data

Opens the graph, displaying the data for the current compliance period.

Delete Data

Opens the Data Management dialog for the selected QoS constraint, allowing you to delete the complete QoS data series, or just for a selected period. The QoS object is not deleted selecting this option, and data for the selected QoS constraint will continue to be stored in the database table.

Export Data
Opens the Export QoS Data wizard, enabling you to export the data series for the selected QoS constraint dialog to a file. See the section Exporting the QoS Data Series (see page 325).

Filter by QoS

Selecting one entry in the list and selecting Filter by QoS, all entries with the same QoS as the selected one will be listed, all others will be removed from the list. In the example below, all entries with QOS_CPU_USAGE will be collected in a list; all others will be removed from the list.

Click the icon beside the respective QoS and select Update to return to the original list.

Filter by Source

Same as Filter by QoS, but in this case, entries with identical source will be collected in the list.

Filter by Target

Same as Filter by QoS, but in this case, entries with identical target will be collected in the list.

Filter by Host

Same as Filter by QoS, but in this case, entries with identical host will be collected in the list.

Filter by Robot

Same as Filter by QoS, but in this case, entries with identical robot will be collected in the list.

Filter by Probe

Same as Filter by QoS, but in this case, entries with identical probe will be collected in the list.

Filter by Origin

Same as Filter by QoS, but in this case, entries with identical origin will be collected in the list.

All messages received by a given hub are stamped with an origin element. The default origin name will be the HUB name.

Change origin

Selecting one or more entries in the list, clicking the icon and selecting Change Origin lets you change origin for the selected entries (all messages received by a given hub is stamped with an origin element. The default origin name will be the HUB name). Available origins will be listed in the dialog popping up. You can also create a new origin by clicking the Add button.

The columns in the window

The followings columns appear in the window when the Active Objects tab is selected:
Quality of Service

The name of the QoS object.

Source

From where the sample originates.

Target

The target of the sample.

Rows

The number of rows in the database table containing data for the QoS Object.

Note that this information is made available after clicking the icon beside the entry and selecting Get Statistics option.

Historic rows

The number of rows in the historic database table containing data for the QoS Object.

Note that this information is made available after clicking the icon beside the entry and selecting Get Statistics option.

First sample

The time and date of the first sample within the current compliance period.

Note that this information is made available after clicking the icon beside the entry and selecting Get Statistics option.

Last sample

The time and date of the last sample within the current compliance period.

Note that this information is made available after clicking the icon beside the entry and selecting Get Statistics option.

Table id

An ID number assigned to each of the QoS objects registered within the database structure.

S./min.

The number of samples per minute.

Note that this information is made available after clicking the icon beside the entry and selecting Get Statistics option.

Originator

The address of the computer running the probe.

Host

The IP-address of the host hosting the probe from which the sample originates.

Robot
Using SLM

The name of the robot from which the sample originates.

**Probe**

The name of the probe from which the sample originates.

**Origin**

This is the origin of the QoS sample. All messages received by a given hub are stamped with an origin element. The default origin name will be the HUB name.
### QoS Definition Tab

Shows a list of QoS definitions and their properties. Allows you to create new QoS definitions, or edit or delete existing QoS definitions.

**Name**

Name of the QoS.

Click the icon next to the name to display a popup menu with these choices:

- **New**
  
  Opens the QoS Definition dialog, where you can define a new QoS.

- **Properties**
  
  Opens the QoS Definition dialog for that QoS, where you can view its properties.

- **Delete**
  
  Deletes the QoS.

- **Update**
  
  Updates the QoS definition table.

**Group**

Group the QoS belongs to. This determines how QoS are grouped in the tree in navigation pane.

**Unit**

Unit of measurement for the QoS.

**Abbreviation**

Abbreviation for the unit of measurement for the QoS. For example, if the unit is **Bytes/sec** the abbreviation is **B/s**. You can use either the **Unit** or the **Abbreviation** when creating reports.

**Is Boolean**

Whether or not the value for the QoS is Boolean.

**Has Max**

Whether or not there is a maximum value for the QoS.

**Type**

Data type of the QoS.

**Objects**

Number of objects this QoS definition is assigned to.

**Rows**

Number of rows in the database with entries for the QoS.
**Size (KB)**

Size, in kilobytes, of the rows with entries for the QoS.

**Historic**

Number of measurements in the historic database for the QoS.

**Size (KB)**

Size, in kilobytes, of the historic measurements for the QoS.

**The QoS Probes Tab**

Shows the QoS objects registered per probe. Delete the selected data-series by clicking icon and selecting Delete Data option. This operation deletes all objects matching the "host" field and the "QoS" field.

The followings columns appear in the window when the QoS Probes tab is selected:

**Registered**

The time the QoS object was registered in the database,

**Host**

The IP address of the host where the probe sending the QoS data is installed.

**Probe**

The name of the probe sending the QoS data.

**Quality of Service**

The name of the QoS object.

**Information Tab**

Shows information related to the database, such as:

- Database server name
- Database name
- SLM version
- Database owner
- When the database was created
- Database usage
- Database location
Managing your QoS Data

Select Tools > Data Management from the menu-bar to bring up the Data Management Dialog, where you can change the period settings and delete historic data for the selected QoS constraint. The various fields in the dialog are described below:

**Quality of Service Object**

**Description**

The QoS description string.

**Object**

The QoS object name.

**Source**

The source of the QoS data. E.g. computer, device etc.

**Target**

The target of the QoS data. E.g. the disk, network service, CPU, etc.

**Operation**

**Delete Data**

Select this option to delete the QoS data related to the source and target settings.

**Invalidate Data**

Select this option to invalidate the QoS data related to the source and target settings.

**Delete Historic data**

Select this check box to delete the historic data for this QoS constraint.

**Period settings**

You can select a period, or you can select Ignore, which means that the measurement is not restricted to specific periods.
Watching SLA Calculations

Selecting Tools > SLA Calculations in the Menu bar opens the Service Level Calculations window, listing the current calculations for the SLAs.

A service level agreement (SLA) will automatically get recalculated for the current period by the sla_engine (on a schedule as specified in the sla_engine user interface), but you can manually recalculate a SLA by clicking icon beside desired SLA and selecting New option (see below), or clicking icon beside the SLA in the Navigation Pane and selecting Recalculate.

New Job
Using this option, you may manually recalculate the SLAs.

The Job properties dialog is opened, allowing you to select a SLA to be recalculated.

The time period for the report can be specified, either as a Fixed report, where you can select one or more fixed periods, or as a Custom report, where you can select a time range.

The Job start time specifies when the job calculation job should be started; the Job expiration time specifies when the job is removed from the database.

The Create historic data option lets you select the compliance data to be recorded/saved for historic reports, and the Delete report when expired will delete the report from the database when the report has expired.

SLAs are also automatically recalculated on a schedule as specified in the sla_engine user interface.

Delete
Deletes the calculations for the selected SLA from the list in the window.

Update
Updates the selected row with data from the current compliance period.

View
This option opens the compliance job description window for the selected SLA.

The columns in the window

The Service Level Calculations window contains the following columns:

Job Id
The job identification number assigned to a new job.

SLA
Shows the name of the SLA being calculated.

Description
Indicates if the calculation job runs automatically as scheduled, or if it was manually started by the administrator.

**Period Begin**

Displays the starting date/time of the compliance calculation period.

**Period End**

Displays the end date/time of the compliance calculation period.

**Owner**

The name of the operator that requested the calculation job.

**Job Start**

Defines the date/time for when the compliance calculation job should start.

**Job Expire**

Defines the date/time for when the job is automatically removed from the SLM system.

**History**

Indicates that compliance data should be recorded/saved for historic reports.

Double-clicking one of the SLAs in the window opens the Calculated SLA Compliance job window for that SLA.

The window displays:

- The selected Compliance period
- The name and description of the SLA
- The Status, with the expected and the achieved value
- The SLOs, listed in the lower left corner
- The QoS constraints, listed in the lower right corner, supplying the following information:
  - The name of the QoS object
  - The name of the source computer
  - The name of the target computer
  - The achieved compliance
  - The expected compliance
  - The total number of samples

Double-clicking one of the QoS constraints brings up the QoS graph (also see the section [Generating a Graph](#) (see page 324)).

**SLA ID**

The identification number assigned to the SLA.
Sending SQL Queries to the Database

The SLM portlet includes a SQL Query tool you can use to enter custom SQL queries. From the SLM portlet, select the **Tools** tab > **SQL Query** to access this tool. This function can be used to query the database directly, and is useful for testing and verification purposes.

**Important!** The SQL Query tool in SLM is intended for experienced users only.

Here you can select a query from the combo box, and send the query to the database by clicking the **Start Query** button.

You can do the following with the SQL Query tool:

- Use any SQL command.
- Enter carriage returns.
- Enter queries that consist of multiple statements.
  
  **Note:** To use multiple statements, you must separate each statement with a semicolon.
- Run queries of multiple statements *and* a query selected from the combo box simultaneously.
- Enter multiple statements, then highlight one or more of the statements to run just the highlighted statements.
- Stop a query that is running by clicking the **Stop Query** button.

The result of a query will appear in a table under the **Recordset** tab. When you run a query that consists of multiple statements, a separate **Recordset** tab appears for each statement. The number of rows found is also displayed on the tab header.
Size Limits for SQL Queries

In environments with extensive monitoring, database tables may contain a considerable number of rows. In this situation with a previous UMP version, a SQL query in SLM could cause UMP to become unresponsive. For this reason, SLM SQL queries in UMP 6.0 are now limited to a maximum size of 1000 rows; columns are now limited to a maximum of 1024 bytes.

Although it is not recommended, you can override these limits. To do so, edit the <webapp/slm> section of the wasp.cfg file, and add the parameters max_rows and max_field. See the following example.

Example

```xml
<slm>
    reloadable = true
    cross_context = true
    load_on_startup = true
    unpack_war = true
    path = /slm
    max_rows = 10
    max_field = 2048
</slm>
```
SLM Interface Reference

The Service Level Management application window consists of the following main parts:

- The Menu Bar
- The Navigation Pane
- The Main Window Pane
The Menu Bar

This section gives a short description of the different functions and tools found in the menu line. Note that some of the menus are partly restricted, depending if your user is classified as operator or super user.

New

This option can be used when defining a new:

**Service Level Agreement**

Opens the Service Level Agreement dialog, where you can create new SLAs. See description in the section [Creating Service Level Agreements](#) (see page 278).

**Operating Period**

Opens the Operating Period dialog; see description in the section Creating an Operating Period.

**Quality of Service**

Opens the QoS Definition dialog; see description in the section Defining a Quality of Service object.

Tools

This option can be used when defining a new:

**Database Status**

Opens the Database Status window. The window contains relevant database information, such as:

- Database information, such as server name and database name, size and location.
- Listing QoS objects and probes enabled for sending QoS messages to the database.
- See description in the section [Viewing the Actual Database Usage](#) (see page 326).

**Data Management**

Opens the Data Management dialog. The data_engine may be configured to perform automatic clean-up procedures, but using the Data Management dialog, you may perform manual data-management.

**SLA Calculations**

Opens the Service Level Calculations window, listing the last calculations for currently running SLAs. Double-clicking the entries in the list, you can observe the calculated SLA Compliance for each of the SLAs in separate windows.
QoS Monitors
Selecting this option, the QoS Monitors window will be launched, listing the QoS Monitors defined (if any).

QoS Monitors can be defined by clicking icon beside a QoS object in the Navigation pane, selecting Create Monitor.

This feature will be activated and visible, if the qos_engine probe is installed.

View SLM Alarms
Displays alarms related to Service Level Management in the Alarm Console portlet in a new window.

Wizards
Lets you start a wizard for creating one or more SLAs, based on your selections through the wizard. A group will be created with one or more SLAs in the group. There are different types of wizards:

- Creating SLAs from scratch, based on a selected service, see Example – Creating a SLA based on a service (see page 310).
- Creating SLAs based on an existing SLA. Selecting a SLA in the Navigation Pane, the wizard will create a new SLA, based on the properties for the selected SLA.
- Exporting QoS data. For more details, see Exporting QoS Data Using Export QoS Data Wizard (see page 326).
- Adding an Excluded period. Normally this is done individually for SLAs/SLOs in the respective dialogs. Using this wizard, you can add an Excluded period and attach the period to some or all of your existing SLAs/SLOs.

SQL Query
Opens the SQL Query dialog, allowing you to send SQL queries to the database. This is useful if you want to test and view database contents. Also, see Sending SQL Queries to the Database (see page 336).

Window
Open Windows
Shows the list of currently open windows. At any given time, you can open any number of windows.

Maximized
If this option is selected, by default the window opens in its maximized state.
Save

Lets you save new definitions, or any modifications to existing definitions.

Help

Provides version information and shortcuts to online documentation.

Preferences Dialog

Access the Preferences dialog by clicking the Settings icon (⚙️), then Preferences.

The following options and properties are available:

Height

Enter the height, in pixels, for this instance of the portlet to open to.

Maximized Height

Enter the height, in pixels, for this instance of the portlet to display at when the maximize icon (✦) is clicked.

Edit QoS Constraint on double-click

When this option is checked, double-clicking a QoS constraint in an SLO dialog opens the properties dialog for the QoS constraint. When this option is not checked, double-clicking a QoS constraint in an SLO dialog opens the QoS constraint graph.

QoS Data Folders

This option lets you organize the QoS objects located under the QoS node in the Navigation Pane into folders.

Minimum number of objects to create a folder

Lets you define the minimum number of objects that must be present for objects to be automatically organized into folders.

Create folders for network addresses

Checking this option enables automatic folder creation, based on network address, if the minimum number of objects you defined is reached.

Create folders for host names

Checking this option enables automatic folder creation, based on host name, if the minimum number of objects you defined is reached.

Order by QoS Group, Order by QoS Name, Order by Probe

Choose up to six data selectors under each heading to change the hierarchy of the tree in the navigation pane. The available data selectors are ACCOUNT, ORIGIN, HOST, ROBOT, PROBES, SOURCE, QOSNAME, QOSGROUP, TARGET, and NONE.

Note: The data selectors are not combined in any way.
Save
Allows you to save any modifications to your preferences.

The Navigation Pane
The Navigation Pane is present to the left-hand side of the application. It can be collapsed by clicking the icon and can be opened again by clicking the icon. It contains a tree-like structure, showing the various elements/nodes in the Nimsoft Service Level Management product suite.
Service Level Agreements

This node lists all defined SLAs. The SLAs may appear as:

- Single SLAs
- Grouped SLAs - The SLAs may be placed in one group, or in sub-groups on multiple levels under the main group. SLAs can be moved between groups, using drag-and-drop.
- SLAs attached to Accounts - Under the Accounts node, you will find all Accounts available. When creating SLAs, these can be attached to one of these Accounts. Under these Accounts, you may again create groups where you place the SLAs.

Click icon to define new SLAs or SLA groups.

**New SLA**

Opens an empty SLA dialog, where you can define a new SLA (see the section Creating Service Level Agreements (see page 278)).

**New Group**

Opens a New Group dialog, where you can define a new SLA group. Give the new group a name and optionally a description.

**Refresh**

Updates the Service Level Manager to reflect the latest modifications.

An SLA group or an Account is selected:
View

Opens the current group in edit mode. You can view or edit the desired group details and save it.

New Group

Opens a New Group dialog, where you can define a new SLA group. Give the new group a name and optionally a description.

New SLA

Opens an empty SLA dialog, where you can define a new SLA (see the section Creating Service Level Agreements (see page 278)).

Delete

Deletes the selected SLA group, including all SLAs in that group.

Recalculate

Starts a new calculation job for all SLAs in the selected group.

Note: Clicking Recalculate option of a SLA group will not open the Job Properties dialogue. To see the Job Properties dialogue, select the Recalculate option of individual SLA within the group.

Refresh

Updates the Service Level Manager to reflect the latest modifications.

An SLA is selected:
View

Opens the current SLA in edit mode. You can view or edit the desired SLA details and save it.

New

Opens an empty SLA dialog, where you can define a new SLA (see the section Creating Service Level Agreements (see page 278)).

New Clone

Makes a copy of the selected SLA, and appends the name of the clone with the text (COPY X). Note that if you clone an SLA that has a name that is longer than 57 characters, the name of the clone is truncated.

New Based On

Starts the SLA wizard, enabling you to create a new SLA, based on the selected one. Note that some input fields are not editable.

Delete

Deletes the selected SLA.

Recalculate

Starts a new calculation job for the selected SLA. The Job Properties dialog is opened, allowing you to edit the job parameters.

Refresh

Updates the Service Level Manager to reflect the latest modifications.
Operating Periods

This node lists the defined operating periods. Operating Periods are used to constrain the measured QoS values to specific hours of any day (the period the QoS constraint is valid.)

The operating period is defined to be a collection of time periods, and is used when we define new SLAs. We use the Operating Periods while defining the QoS constraints (see the section Creating an Operating Period)

This means that samples falling outside these time specifications will not influence the SLO/SLA compliance requirements.

Click icon and select New Operating Period which opens an empty dialog, enabling you to define a new Operating Period (see the section Create an Operating Period).

Click icon that is beside one of the defined Operating Periods listed under the node, which opens a small menu containing four options:

**View**

Opens the existing Operating Period in edit mode. You can view or edit the existing Operating Period and save it.

**New**

Opens an empty dialog, enabling you to define a new Operating Period.

**Refresh**

Updates the Service Level Manager to reflect the latest modifications.

**Delete**

Deletes the selected Operating Period.
Calculation Profiles

This option allows you to define your own calculation profiles.

These calculation profiles are used when defining the calculation properties for Service Level Objects and Quality of Service Constraints.

When defining calculation profiles, the profiles will be grouped either as SLO calculations or as QoS calculations, depending on if the selected plug-in supports single-data or multi-data series. See the section Creating a Calculation Profile (see page 299) and Compliance Calculation (see page 266).

Click the icon beside the SLO Calculation sub-node (or one of the defined SLO calculation profiles), selecting New, opens an empty dialog enabling you to define a new SLO Calculation profile.

Click the icon beside the QoS Calculation sub-node (or one of the defined QoS calculation profiles), selecting New, opens an empty dialog enabling you to define a new QoS Calculation profile.

Clicking icon offers four other options, common for both sub-nodes.

View

Opens the existing Operating Period in edit mode. You can view or edit the existing Operating Period and save it.

New

Opens an empty dialog, enabling you to define a new Operating Period.

Refresh

Updates the Service Level Manager to reflect the latest modifications.

Delete

Deletes the selected Operating Period.
Quality of Service

Under this node, you will find the available registered QoS objects, grouped into logical groups based on the description field in the QoS object. This view enables the user to quickly browse the database for particular data-series.

Click the icon beside QoS node that opens a small menu containing four options:

**Browse Menu Editor**

Launches the Browse Menu Editor, enabling you to define your own ways to group and sort the QoS objects listed under the QoS Node.

Choosing **New**, a new sorting view will be added to the list. The new entry will by default be given the name New Menu Item. Rename it, giving it a descriptive name.

Select your sorting criteria, one or more, from the Data Selector drop-down menus and select descending or ascending sorting order.

Click the OK button, and you will be asked if you want to save the view.

Choosing **Delete**, the selected view will be deleted.

When saved, the entries in the list will appear as menu items in the menu available when you click the icon beside the QoS node in the Navigation Pane.

They will be presented in the order they appear in the list in the Browse Menu Editor.

When saved, the new views will appear as menu items when you click the icon beside the QoS node in the Navigation Pane.

**Order by QoS group**

All QoS objects will be presented in their logical groups.
In addition, see the section Properties for information on sorting and organizing QoS objects in folders.

**Order by QoS**

All QoS objects will be listed alphabetically (and not grouped).
In addition, see the section Properties for information on sorting and organizing QoS objects in folders.

**Order by Probes**

All the QoS objects will be listed as per the Probes.

Main Window Pane

This is the application frame. All child windows are contained within the frame of the main-window.
SLM Terms and Definitions

This section contains definitions of terms related to the SLM portlet.

**Automatic (Interval) data type**

QoS Data is recorded at intervals, individually specified in the probe configuration for each of the probes.

**Asynchronous data type**

QoS Data is recorded each time the measured value changes.

**Calculation method**

Calculation method is the set of rules and conditions determining the way the SLA compliance is calculated.
**Compliance period**

The compliance period defines the period of time that the SLA should meet the requirements stated by the compliance percentage, typically a day, a week or a month.

The illustration shows the relationship between the operating period and the compliance period.

The gray area illustrates the compliance period, and the blue area illustrates an operating period with 5 time-specifications.

Example:

Let’s say that the compliance period (gray area) is defined to be one week (Monday to Monday). Our requirements for the SLA are defined to be between 08:00 and 17:00 every weekday (operating period). Notice that the data (blue plot) within the operating periods (blue area) are included in the SLA computations.
Compliance percentage

The compliance percentage is defined to be the percentage of time that the QoS, constrained by e.g. operating period and thresholds, should be considered compliant within the compliance period.

Each sample is checked within the compliance period by the data_engine and summarized as failed or successful. The result is compared against the expected compliance percentage (defined by the user).

Consider the data represented by the illustration. The red line represents the threshold value, the green line represents the average value and the blue line represents the actual sample values.

How many samples within the operating period are above the threshold settings?

Zero samples breach the threshold line within the operating periods, thus fulfilling 100% of our compliance requirements. The 5 samples that breach the threshold are outside the compliance period which was e.g. Monday to Monday, with operating periods every weekday from 08:00 to 17:00.

Let’s assume that the total number of samples within the operating period is 129, with 9 samples breaching the threshold. This implies that 6.98% of the samples are accounted for as out of compliance (9 * 100/129).

If our Service Level Agreement requires a compliance of 98.50% (or better) and the only data defined in this SLA is the above data, then our requirements to the SLA is breached due to a current compliance percentage of 100% - 6.98% = 93.02%.
Data Types

We use the following different data types when calculating the compliance:

Automatic (Interval)
QoS Data is recorded at intervals, individually specified in the probe configuration for each of the probes.

Asynchronous
QoS Data is recorded each time the measured value changes.

Domain

The Domain is the top-level node in the hierarchy, and a site is normally set up with one Domain. It is used to group one or more Hubs in a logical set such as a company or enterprise.

Hub

The Hub is a message concentrator and re-distributor. It is the collection point for all messages coming from the various installed Robots. Many other Nimsoft components can connect to the Hub to receive dedicated messages and perform other specific activities. One such component is the Alarm server.

NULL value

A NULL value will be recorded into the database typically if a probe does not measure a value from the target due to a timeout, e.g. no answer to a ping). In the QoS Calculation Profiles, available under the Calculation Profiles Node in the Navigation Pane of the SLM, you may define how these NULL values are handled in a compliance calculation.

Operating period

The operating period constrains the QoS samples to one or more time-specifications within the compliance period. This means that samples falling outside these time specifications will not influence the SLO/SLA compliance requirements. Each operating period is defined as a union of one or more time-specifications.
Probes

Probes are small dedicated pieces of software that monitor specific resources or events. Each probe can be easily configured for your own specific monitoring requirements.

Robot

The Robot is the first line of management for the Probes. The Robot starts and stops the probes at the required times, collects, queues and forwards messages from the probes onto the specified Hub.

Service Level Agreement (SLA)

A Service Level Agreement (SLA) is an agreement to deliver a service within a specified/fixed time-period to an extent where both parties agree on a measurable service levels. The parties may be an IT department delivering services to another department within the company, or by a company and an external service provider.

The services included in the SLA may be a collection of monitored objectives we call Service Level Objectives (SLO). These objectives (or group of objectives) are monitored by dedicated programs (often standard probes) that monitor e.g. network connectivity, application (Oracle, Exchange, e-mail) availability and service (DNS, DHCP) availability.

SLO

A Service Level Objective (SLO) is a combination of one or more component measurements (Quality of Service) to which constraints are applied. A SLO is said to be in compliance if the underlying measurement values are within the specified constraints. SLO’s may have operating periods during which the SLO has to be compliant.

SLM

The Service Level Manager (SLM) is the application where service level configuration and monitoring is performed. The application needs a valid license to operate.
The Quality of Service (QoS) is the atom of the Service Level Management. The QoS is the actual value (sample) collected and used centrally to determine the state of the service level objective. This value is normally collected by a probe like cdm, net_connect, url_response etc. The value is first used for alarm purposes, but if the probe is configured to deliver Quality of Service, then a QoS message is issued.

A QoS constrained by threshold, source, target and operating period settings is used as the building blocks for SLO's.

The QoS object is defined by its QoS name, source and target. All sample-data with this unique combination form data-series that may be used as part of any Service Level Objective.

A constrained QoS object is defined by its QoS name, source, target, threshold and operating period. This constrained object is the building block of the Service Level Objective.

To use logical expressions for calculation profiles in the SLM portlet, you must enclose the expressions in parenthesis to be valid. If you don't enclose a logical expression in parenthesis, SLM will allow you to save it without displaying a warning message that the expression is invalid.
The SLM Portlet Does Not Record a QoS Object

**Symptom**
The probe has been configured, but the QoS object does not appear in SLM.

**Solution**
This may occur if you configure a probe to deliver QoS before you install the data_engine. In this case, the QOS_DEFINITION message is ignored, and the QoS object does not appear in SLM.

Restart the probe (deactivate/activate) or restart the robot if you have modified the configuration of more than one probe.

If you restart the probe or robot and the QoS object still does not appear under the QoS node, wait a moment, and then select **Update** from the action menu.

SLM Portlet Displays Incorrect Data Set

Depending on factors such as the user’s time zone, the time zone of the database, and whether or not SLAs have been assigned a time zone, users may see the wrong data set in the SLM portlet. If this occurs, switch to the SLA Reports portlet to view SLA data.
Chapter 23: Unified Reports

This section contains the following topics:

Running Unified Reports (see page 357)
Preconfigured Reports (see page 357)

Running Unified Reports

The Unified Reports application provides advanced reporting. You can run standard reports that are provided, or you can create your own reports in the Reports Designer.

If you do not have the Unified Reports permission set in the ACL, you will see a "Permission Denied" message when you try to run the Unified Reports application.

To Run Unified Reports

The reports available to you are listed in a tree structure in the Unified Reports application. Double-click a report in the tree structure to open the report in a new window.

You can also create and run ad hoc reports in the Reports Designer, accessed by clicking the Create tab in the report window.

For information about designing reports, see the documentation for Unified Reports.

Preconfigured Reports

The following table lists the preconfigured reports that come with the Unified Reporter product. The table lists the probe that must be activated and the QoS measurement(s) that must be enabled on the probe in order to obtain data for each report.

You can also design custom reports using the Reports Designer.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Probe</th>
<th>QoS Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD Average Replication Age, Last 24 Hours</td>
<td>ad_response</td>
<td>QOS_AD_REPLICATION_AGE</td>
</tr>
<tr>
<td>Apache Top 10 HTTP Response Time, Last 24 Hours</td>
<td>apache</td>
<td>QOS_APACHE_HTTPRESPONSETIME</td>
</tr>
<tr>
<td>Report Name</td>
<td>Probe</td>
<td>QoS Required</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Apache Requests Per Second, Last 24 Hours</td>
<td>apache</td>
<td>QOS_APACHE_REQPERSEC</td>
</tr>
<tr>
<td>Apache Top 10 Busy Workers, Last 24 Hours</td>
<td>apache</td>
<td>QOS_APACHE_BUSYWORKERS</td>
</tr>
<tr>
<td>Apache Top 10 Bytes per Request, Last 24 Hours</td>
<td>apache</td>
<td>QOS_APACHE_BYTESPERREQ</td>
</tr>
<tr>
<td>Apache Top 10 Idle Workers, Last 24 Hours</td>
<td>apache</td>
<td>QOS_APACHE_IDLEWORKERS</td>
</tr>
<tr>
<td>Apache Top 10 Requests Average Time, Last 24 Hours</td>
<td>apache</td>
<td>QOS_APACHE_REQAVETIME</td>
</tr>
<tr>
<td>Cisco Call Manager Top 10 CPU Last 24 Hours</td>
<td>ccm_monitor</td>
<td>QOS_CPU_USAGE</td>
</tr>
<tr>
<td>Cisco Call Manager Top 10 Memory, Last 24 Hours</td>
<td>ccm_monitor</td>
<td>QOS_CCM_PERFORMANCE</td>
</tr>
<tr>
<td>Cisco QoS Top 10 Drop Bitrate, Last 24 Hours</td>
<td>cisco_qos</td>
<td>QOS_CISCO_DROP_BITRATE</td>
</tr>
<tr>
<td>Cisco QoS Top 10 Post Policy Bitrate, Last 24 Hours</td>
<td>cisco_qos</td>
<td>QOS_CISCO_POST_POLICY_BITRATE</td>
</tr>
<tr>
<td>Cisco QoS Top 10 Post Policy Bytes, Last 24 Hours</td>
<td>cisco_qos</td>
<td>QOS_CISCO_POST_POLICY_BYTE</td>
</tr>
<tr>
<td>Cisco QoS Top 10 Pre Policy Bitrate, Last 24 Hours</td>
<td>cisco_qos</td>
<td>QOS_CISCO_PRE_POLICY_BITRATE</td>
</tr>
<tr>
<td>Cisco Top CPU, Last 1 Minute</td>
<td>cisco_monitor</td>
<td>QOS_CPU_USAGE</td>
</tr>
<tr>
<td>Cisco Top 10 Memory Free, Last 24 Hours</td>
<td>cisco_monitor</td>
<td>QOS_MEMORY_USAGE</td>
</tr>
<tr>
<td>Cisco Top 10 by Memory Used, Last 24 Hours</td>
<td>cisco_monitor</td>
<td>QOS_MEMORY_USAGE</td>
</tr>
<tr>
<td>End to End Top 10 Transactions, Last 24 Hours</td>
<td>e2e_appmon</td>
<td>QOS_E2E EXECUTION</td>
</tr>
<tr>
<td>Report Name</td>
<td>Probe</td>
<td>QoS Required</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>MySQL % of Maximum Allowed Connections, Last 24 Hours</td>
<td>mysql</td>
<td>QOS_MYSQL_CONNECTION_USAGE_RATE</td>
</tr>
<tr>
<td>Oracle SGA Memory Free, Last 24 Hours</td>
<td>oracle</td>
<td>QOS_ORACLE_SGA_MEMORY_FREE</td>
</tr>
<tr>
<td>Oracle Top 10 Databases by Size, Last 24 Hours</td>
<td>oracle</td>
<td>QOS_ORACLE_DATABASE_SIZE</td>
</tr>
<tr>
<td>Oracle Top 10 Tables Space Allocated Free, Last 24 Hours</td>
<td>oracle</td>
<td>QOS_ORACLE_TABLESPACE_ALLOC_FREE</td>
</tr>
<tr>
<td>Oracle Top 10 Tables Space Free, Last 24 Hours</td>
<td>oracle</td>
<td>QOS_ORACLE_TABLESPACE_FREE</td>
</tr>
<tr>
<td>Top 10 DHCP Response Time, Last 24 Hours</td>
<td>url_response</td>
<td>QOS_DHCP_RESPONSE</td>
</tr>
<tr>
<td>Top 10 DNS Response Time, Last 24 Hours</td>
<td>url_response</td>
<td>QOS_DNS_RESPONSE</td>
</tr>
<tr>
<td>Top 10 Exchange Mail Roundtrip Time, Last 24 Hours</td>
<td>exchange_response</td>
<td>QOS_EXCHANGE_MAIL_ROUNDTRIP</td>
</tr>
<tr>
<td>Top 10 Hosts by Response Time, Last 24 Hours</td>
<td>net_connect</td>
<td>QOS_NET_CONNECT</td>
</tr>
<tr>
<td>Top 10 Interfaces by Discards, Last 24 Hours</td>
<td>interface_traffic</td>
<td>QOS_INTERFACE_DISCARDS</td>
</tr>
<tr>
<td>Top 10 Interfaces by Errors, Last 24 Hours</td>
<td>interface_traffic</td>
<td>QOS_INTERFACE_ERRORS</td>
</tr>
<tr>
<td>Top 10 Interfaces by Queue Length, Last 24 Hours</td>
<td>interface_traffic</td>
<td>QOS_INTERFACE_QLEN</td>
</tr>
<tr>
<td>Top 10 LDAP Response Time, Last 24 Hours</td>
<td>ldap_response</td>
<td>QOS_LDAP_RESPONSE_TIME</td>
</tr>
<tr>
<td>Top 10 MS SQL Server Free Allocated Space, Last 24 Hours</td>
<td>sql_server</td>
<td>QOS_SQLSERVER_ALLOC_SPACE</td>
</tr>
<tr>
<td>Top 10 MS SQL Server Users, Last 24 Hours</td>
<td>sql_server</td>
<td>QOS_SQLSERVER_ACTIVE_USERS</td>
</tr>
<tr>
<td>Top 10 MS SQL Server Transactions, Last 24 Hours</td>
<td>sql_server</td>
<td>QOS_SQLSERVER_TRANSACTIONS</td>
</tr>
</tbody>
</table>
### Preconfigured Reports

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Probe</th>
<th>QoS Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 NTP Response Time, Last 24 Hours</td>
<td>ntp_response</td>
<td>QOS_NTP_RESPONSE_TIME</td>
</tr>
<tr>
<td>Top 10 Processes by CPU Usage, Last 24 Hours</td>
<td>processes</td>
<td>QOS_PROCESS_CPU</td>
</tr>
<tr>
<td>Top 10 Processes by Memory Usage, Last 24 Hours</td>
<td>processes</td>
<td>QOS_PROCESS_MEMORY</td>
</tr>
<tr>
<td>Top 10 Processes by Thread Count, Last 24 Hours</td>
<td>processes</td>
<td>QOS_PROCESS_THREADS</td>
</tr>
<tr>
<td>Top 10 Processes by Queue Length, Last 24 Hours</td>
<td>processes</td>
<td>QOS_PROC_QUEUE_LEN</td>
</tr>
<tr>
<td>Top 10 Remedy Response, Last 24 Hours</td>
<td>remedy_response</td>
<td>QOS_REMEDY_RESPONSE</td>
</tr>
<tr>
<td>Top 10 RUM Completed Transaction Rate, Last 24 Hours</td>
<td>nim-rumapp</td>
<td>QOS_RUM_COMPLETED_TRANSACTION_RATE</td>
</tr>
<tr>
<td>Top RUM Network Time, Last 24 Hours</td>
<td>nim-rumapp</td>
<td>QOS_RUM_AVG_NETWORK_TIME</td>
</tr>
<tr>
<td>Top 10 RUM Page Time, Last 24 Hours</td>
<td>nim-rumapp</td>
<td>QOS_RUM_AVG_PAGE_TIME</td>
</tr>
<tr>
<td>Top 10 RUM Server Time, Last 24 Hours</td>
<td>nim-rumapp</td>
<td>QOS_RUM_AVG_SERVER_TIME</td>
</tr>
<tr>
<td>Top 10 SQL Response Time, Last 24 Hours</td>
<td>sql_response</td>
<td>QOS_SQL_RESPONSE</td>
</tr>
<tr>
<td>Top 10 URLs by Response Time, Last 24 Hours</td>
<td>url_response</td>
<td>QOS_URL_RESPONSE</td>
</tr>
<tr>
<td>Top 10 VMware Guests by CPU, Last 24 Hours</td>
<td>vmware</td>
<td>QOS_CPU_USAGE</td>
</tr>
<tr>
<td>Top 20 Hosts by Response Time, Last 24 Hours</td>
<td>net_connect</td>
<td>QOS_NET_CONNECT</td>
</tr>
<tr>
<td>Top 20 Interfaces by Bandwidth, Ordered by Inbound</td>
<td>interface_traffic</td>
<td>QOS_INTERFACE_TRAFFIC_PERC</td>
</tr>
<tr>
<td>Top 20 Interfaces by Bandwidth, Ordered</td>
<td>interface_traffic</td>
<td>QOS_INTERFACE_TRAFFIC_PERC</td>
</tr>
<tr>
<td>Report Name</td>
<td>Probe</td>
<td>QoS Required</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Top 20 Interfaces by Errors, Last 24 Hours</td>
<td>interface_traffic</td>
<td>QOS_INTERFACE_ERRORS</td>
</tr>
<tr>
<td>Top 20 Server Disk Space</td>
<td>cdm (local) or rsp (remote)</td>
<td>QOS_DISK_USAGE_PERC</td>
</tr>
<tr>
<td>Top 20 Servers by CPU Usage, Last 24 Hours</td>
<td>cdm (local) or rsp (remote)</td>
<td>QOS_CPU_USAGE</td>
</tr>
<tr>
<td>Top 20 Servers By Physical Memory Usage, Last 24 Hours</td>
<td>cdm (local) or rsp (remote)</td>
<td>QOS_MEMORY_PHYSICAL_PERC</td>
</tr>
<tr>
<td>Top 20 URLs by Response Time, Last 24 Hours</td>
<td>url_response</td>
<td>QOS_URL_RESPONSE</td>
</tr>
<tr>
<td>Top 20 VMware Guests by CPU Usage, Last 24 Hours</td>
<td>vmware</td>
<td>QOS_CPU_USAGE</td>
</tr>
<tr>
<td>Top 20 VMware Guests by CPU Usage MHz, Last 24 Hours</td>
<td>vmware</td>
<td>QOS_CPU_USAGE</td>
</tr>
<tr>
<td>Top 20 VMware Hosts by Disk Free, Last 24 Hours</td>
<td>vmware</td>
<td>QOS_DISK_FREE</td>
</tr>
<tr>
<td>Top 20 VMware Hosts by VM Count, Last 24 Hours</td>
<td>vmware</td>
<td>QOS_VMWARE_VARIABLE</td>
</tr>
<tr>
<td>Top 20 VMware Hosts by Memory Used, Last 24 Hours</td>
<td>vmware</td>
<td>QOS_VMWARE_VARIABLE</td>
</tr>
<tr>
<td>DCIE, Last 24 Hours</td>
<td>power</td>
<td>QOS_DCIE</td>
</tr>
<tr>
<td>PUE, Last 24 Hours</td>
<td>power</td>
<td>QOS_PUE</td>
</tr>
<tr>
<td>CO2 Emissions Rate, Last 24 Hours</td>
<td>power</td>
<td>QOS_CO2_EMISSIONS_RATE</td>
</tr>
</tbody>
</table>
Chapter 24: Unified Service Manager

The Unified Service Manager (USM) portlet offers an easy way for you to visualize and organize your infrastructure and to configure monitoring in Nimsoft Monitor.

USM’s dynamic and flexible grouping features allow you to organize your infrastructure into an unlimited hierarchy of groups and subgroups. You can organize groups according to concepts such as service, customer, geography, organization, technology, etc. Membership in groups is managed automatically based on rules, defined by you, that filter on device attributes. Servers and network devices are automatically added to groups whose attributes they match. Once your rules are defined, USM manages and updates group membership with newly discovered devices.

Groups allow you to apply a set of monitoring parameters to multiple systems from a service-oriented perspective. This is called service-oriented configuration (SOC). SOC provides simplified configuration of monitoring through the use of policies, called monitoring templates, that hide the underlying traditional Nimsoft Monitor individual probe configuration and deployment. You create monitoring templates by assigning one or more monitors. Monitors are metrics such as CPU usage, ping response time, or URL monitoring. Monitoring templates allow you to configure a monitor once and use it multiple times across your environment. You can configure monitor settings such as thresholds and data collection intervals. When a monitor is assigned to a group, probes are automatically pushed to robots and configured with the appropriate settings for each monitor.
USM also has these features:

**Enforcement of monitoring policies**

Monitoring policies are enforced through the inheritance of monitoring templates. All members of a group, including subgroup members, inherit monitoring templates. This allows you to enforce a minimum standard set of monitors for all existing and future devices in any subgroup. Group priorities can be configured to override lower level templates to enforce top-level monitoring policies. Or, you can set lower level groups with a higher priority to override the inherited policy.

**Multi-tenancy support**

Portal administrators can define which accounts have access to groups so that each account is able to view only its own groups.

**Display of your IT asset inventory**

USM provides a device details view for keeping track of inventory. You can view a detailed inventory including device count per group and device details such as IP, host name, MAC address, OS, OS version, vendor and more.

**Customizable report templates per group**

Create custom reports using the Performance Reports Designer and use the reports as templates for groups. Multiple report templates can be assigned to groups so that you have multiple report choices when viewing device details. Select a report type to view real-time performance reports for a device.

**Device views**

Out-of-the-box views provide dynamic information about the device, including performance graphs and a high-level view of alarms, disk usage, and interface status. You can drill down to view alarm details or performance graphs for disk usage and interface traffic.

**Metrics**

Performance data is displayed for each device. The metrics displayed vary according to the type of device and the probes monitoring the device, and can include, for example, metrics related to system uptime, database server performance, or memory usage on virtual machine hosts. Alarms related to a metric are indicated on the graph.

**Executive views**

Out-of-the-box executive-level views, or badges, show the overall status of critical services and customers. You can drill down into each badge to view detailed availability, performance, and alarm data for groups and devices, and can switch in context between three levels of badge views and a hierarchical tree view.

**Integrated alarm view**
An integrated alarm console allows you to view alarms for each group or device. You can move between summary and detailed views, and can view alarm details and history in-line in the console. Also available in-line in the console are performance graphs for the metric that triggered the alarm, with the alarm occurrence indicated on the graph.

Auto agent deployment

The auto agent deployment feature allows you to distribute agents (robots) to systems in bulk. You can specify the target systems in USM or import a list of systems from an XML file. USM automatically installs, configures, and launches robots on the target systems.

Out-of-the-box device reports

Out-of-the-box device dashboards and reports provide consolidated views of QoS, availability, and monitoring, and continue the move away from legacy components such as the dashboard_engine probe and the Dynamic Views portlet.

Automatic grouping

Dynamic groups can be created according to several criteria. The groups are created under a parent group that you can name. For example, an MSP can automatically create groups by Origin under a parent group named Customers. This automatically creates a dynamic group in USM for each MSP customer.

Standalone USM

A standalone version of USM (outside of UMP) can be launched using a URL or an HTML file. This allows you to link to USM from other applications, or to integrate data for a group or system in USM into a web page. For example, if you are concerned about a particular service or group of customers, you can display a view of their availability, performance, or alarm data in a frame on your home page.

This section contains the following topics:

Permissions in USM (see page 366)
Navigating in USM (see page 366)
Automatic Agent Deployment (see page 373)
Getting Started with Service-Oriented Configuration (see page 386)
Working with Groups (see page 388)
Working with Monitors (see page 400)
Working with Alarms (see page 414)
Viewing System Information (see page 424)
Working with Reports (see page 432)
Launching a Standalone USM (see page 433)
Permissions in USM

To view USM you must have the USM Basic permission set in the Access Control List (ACL). Otherwise, you will see a "Permission Denied" message when you try to run USM.

Additional permissions control whether a user can modify groups, monitors, and monitoring templates; deploy agents automatically; and take actions on alarms. For a complete list of permissions for USM, see Set Permissions for UMP Portlets (see page 443).

Navigating in USM

USM provides several tools to display and find information. You can view your groups and systems in different types of views, the tree view or several badge views, and you can search for systems using either a basic or advanced search. If Relationship Viewer is running, you can launch Relationship Viewer in context, displaying relationships for the group or system selected in USM.

Views

USM provides several ways to view the systems in your environment. You can choose the tree view or one of three badge views. The tree view allows you to access detailed information, while the badge views provide high-level information at a glance.

Choose the view by clicking one of the icons in the toolbar.

Tree View

The tree view displays your groups in a hierarchical tree in a navigation pane on the left. A status icon indicates the highest severity alarm for each node in the tree, and the number of systems in each group is indicated in parentheses after the group name. As you hover over a group name, icons appear that allow you to add, edit, or delete groups.

The pane on the right displays detailed information about groups, alarms, or systems.

Click on a group name in the tree to see a table listing information about group members. Click a column header in the table to sort by that column. Click the Alarms tab to see information about alarms for the group.
Navigating in USM

Chapter 24: Unified Service Manager

367

Click the name of a system in the tree to view system properties and performance data for the past 24 hours. Click an alarm icon to view alarm data for the system. If the system reports disk usage information, click the usage bar graph to view a Performance Report of disk usage data.

**Badge View**

The badge views display groups or systems as icons. There are three different badge views at different "zoom" levels. The functionality is the same in all three views, but the amount of information displayed on the badges varies.

All of the badges have icons that indicate alarm status and OS type, and the color of the badge indicates alarm status. The Badge 2 (medium badges) view also displays the system name. The Badge 1 (large badges) view also displays the number of alarms and, for groups, the number of elements in the group and all its subgroups. In the Badge 2 and Badge 3 views (medium and small badges), hover over a badge to see all the information for that badge.

In all three badge views, you can drill down to the next level by clicking on a badge. Click on a badge for a system to view detailed information about the system. This is the same system information displayed when you click on the name of a system in the tree. To move back up a level in a badge view, click the bread crumb link.

**Paging**

If there are more than 100 items in a group, the first 100 are shown and you can page through the remaining items.

To page through items, click the View Next or View Previous icons. These icons are displayed only if there are more than 100 subgroups or systems in the selected group. The View Previous icon is displayed once you page past the first page.

In the badge views, the paging icons are under the toolbar in the top left of the window.
In the tree view, the paging icons are displayed next to the name of the group when you mouse over the group name.

You can also page through items in the Members table in the tree view.

**Sorting**

You can sort groups or computer systems in the badge or tree views according to:

- Name
- Severity
- Alarm Count
- Element Count

To sort items, choose the sorting criterion you want from the *Sort by* pull-down menu.
USM Alarm and Device Icons

Icons indicate alarm severity and device type in USM. These icons appear in the badge views, tree view, and device view.

The following icons indicate the highest severity alarm for the system:

- Critical
- Major
- Minor
- Warning
- Informational
- Clear

The following icons indicate the type of device:

- Group container
- Group
- Hub
- Linux
- Robot
- Router
- Server
- Solaris
- Switch
- Unix
- Unknown device type
Search for Computer Systems

You can search for computer systems according to various criteria. For example, you can search for all systems with a certain OS Type or with a certain Origin.

There are two types of search, Basic Search and Advanced Search.

**Basic Search**

Use to do a full-text search for any of the fields in the Members table, except for Nimsoft Type and State.

**Advanced Search**

Use to search for Nimsoft Type or State, to search for multiple criteria, or to filter out certain criteria.

Both Basic and Advanced Search search through all of your systems, regardless of whether you have selected a group in the tree or badge views.

**Basic Search**

You can use Basic Search to do a full-text search for any of the fields in the Members table, except for Nimsoft Type and State.

*Note:* You cannot search for Nimsoft Type (robot, hub, etc.) or State (managed, unmanaged, etc.) using Basic Search. To search for these attributes, use Advanced Search.
**Note:** The special characters `\`, `%`, and `_` must be preceded with an escape character when using basic search, advanced search, or filters in Unified Service Manager or filters in Performance Reports Designer. In the case of advanced search and filters, this applies when the **contains**, **starts with**, or **ends with** operator is selected.

The escape character required depends on the type of database you use. For MySQL, the backslash (`\`) is the escape character; for MS SQL, special characters are enclosed in square brackets (`[]`). Searching for special characters is not supported for Oracle.

The table shows how to enter special characters for each database type.

<table>
<thead>
<tr>
<th>Character</th>
<th>MySQL</th>
<th>Oracle</th>
<th>MS SQL</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\</code></td>
<td><code>\\</code></td>
<td>Not applicable</td>
<td><code>\</code> (No escape character required)</td>
</tr>
<tr>
<td><code>%</code></td>
<td><code>\%</code></td>
<td>Not applicable</td>
<td>[%]</td>
</tr>
<tr>
<td><code>_</code> (underscore)</td>
<td><code>_</code></td>
<td>Not applicable</td>
<td><code>[]</code></td>
</tr>
</tbody>
</table>

**Follow these steps:**

1. Enter text in the **Search** field, then press **Enter**.
   
   The text field is not case-sensitive.
   
   In the badge views, the search results are displayed as a list of badges. In the tree view, the search results are displayed in the **Search Results Members** table, and under the **Search Results** node of the tree.

2. To drill down to view information about a system in the search results, click the name of the system (the badge, the node in the tree, or the row in the **Search Results Members** table).

3. To return to the search results, click the **Search Results** node in the tree (tree view) or the **Search Results** bread crumb link (badge view).
Advanced Search

You can use Advanced Search to search for any field in the Members table (including Nimsoft Type or State), to search for multiple criteria, or to filter out certain criteria.

**Note:** For Oracle, systems with null database values for a search criterion are not included in the results unless explicitly specified. For example, if you search for not OS Type is windows, systems that have null values for OS Type are not included in the search results. To include these, add or OS Type is null as a second search criterion.

**Note:** The special characters \, %, and _ must be preceded with an escape character when using basic search, advanced search, or filters in Unified Service Manager or filters in Performance Reports Designer. In the case of advanced search and filters, this applies when the contains, starts with, or ends with operator is selected.

The escape character required depends on the type of database you use. For MySQL, the backslash (\) is the escape character; for MS SQL, special characters are enclosed in square brackets ([ ]). Searching for special characters is not supported for Oracle.

The table shows how to enter special characters for each database type.

<table>
<thead>
<tr>
<th>Character</th>
<th>MySQL</th>
<th>Oracle</th>
<th>MS SQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>\ \</td>
<td>Not applicable</td>
<td>\ (No escape character required)</td>
</tr>
<tr>
<td>%</td>
<td>%</td>
<td>Not applicable</td>
<td>[%]</td>
</tr>
<tr>
<td>_ (underscore)</td>
<td>_</td>
<td>Not applicable</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

Follow these steps:

1. Choose **Advanced Search** from the **Actions** menu.

   The search filters are displayed in the tree view.

   **Note:** If you choose Advanced Search while in a badge view, the display switches to the tree view, where you can perform the search.

2. Choose items from the pull-down menus and enter text in the text field as appropriate.

   The text fields are not case-sensitive.

   The search filter fields work the same way as the filter fields for creating groups. For an example of how to use the filter fields to create a group, see Filter Example. (see page 394)

3. Click the **Add Filter** icon (○) to add additional rows to the filter if wanted.

4. Click **Search**.

   The search results are displayed in the **Search Results Members** table.
5. (Optional) To drill down to view information about a system in the search results, click the name of the system in the tree or click the row in the **Search Results Members** table.

6. (Optional) To return to the search results, click the **Search Results** node in the tree.

7. (Optional) To view the search results in a badge view, click one of the badge view icons.

**Pop Out Graphs**

Data graphs are displayed in a number of places in USM. Click the Pop out icon (_graphics_) in the upper right corner of a graph, visible when you mouse over the area, to display the graph in Performance Reports Designer in a new window. From here you can use the full functionality of Performance Reports Designer, such as changing the time interval, changing the style of the graph, or exporting the data to a .csv file.

**Launch Relationship Viewer**

If the Relationship Viewer portlet is available, you can launch the Relationship Viewer in context from USM by choosing **Launch Relationship Viewer** from the **Actions** menu.

**Note:** The **Launch Relationship Viewer** menu option is present only if the relationship_services probe is running and the optional Relationship Viewer portlet in UMP is licensed.

The Relationship Viewer opens in a new browser window. If you first select a group or specific managed element, the Relationship Viewer opens with the selected element(s) centered and with the radius slider visible. If you do not make such a selection first, the Relationship Viewer opens with all managed elements visible at the lowest zoom level.

If multiple relationships are available, a sub-menu of your choices is displayed when you click **Launch Relationship Viewer**; click your preference to open the Relationship Viewer using that relationship.

**Automatic Agent Deployment**

Nimsoft Monitor administrators can use USM to deploy agents (robots) automatically to a group of systems or to an individual system. You can:

- Deploy agents to all, or selected, members of a group
- Deploy an agent to a specific system
- Do a Basic or Advanced Search for systems to deploy agents to
- Import an XML file listing systems to deploy agents to
Once you select the systems and start a deployment job, agents are automatically installed on the selected systems.

In order to select in the USM UI systems to deploy agents to, the system must have known credentials. Credential information is entered in the Nimsoft Remote Admin portlet and associated with systems during discovery. Systems that do not have known credentials cannot be selected in the UI for automatic agent deployment. When importing a list of systems from an XML file, however, the credentials are specified in the XML file and the systems do not need to have known credentials through the discovery process.

You must have the USM Automatic Robot Installation ACL permission in order to deploy agents automatically. Account contact users cannot deploy agents automatically. Also, the automated_deployment_engine probe version 1.10 or later must be running in your environment.

Administrators can also use either the GUI or the command-line interface for the automated_deployment_engine probe to automatically deploy agents. For more information on these methods, see the Nimsoft Monitor Server Installation Guide.

For a list of platforms that support automatic agent deployment, see the Nimsoft Compatibility Support Matrix (http://support.nimsoft.com/downloads/doc/Compatibility_SupportMatrix_current.pdf).

Note: Agents are called robots in some areas of Nimsoft Monitor; the terms are interchangeable. For example, the agents you deploy automatically through USM are called robots when you view them in Infrastructure Manager.

**Deploy Agents Automatically**

Nimsoft Monitor administrators can deploy agents (robots) automatically to a group of systems or to an individual system. You must have the USM Automatic Robot Installation ACL permission in order to deploy agents automatically. Also, the automated_deployment_engine probe version 1.10 or later must be running in your environment.

Note: If you do not have the USM Automatic Robot Installation ACL permission, or if you are an account contact user, the Deploy Agents tab is not displayed.
Follow these steps:

1. Do one of the following:
   - In the tree view, click the group or system you want to deploy agents to.
   - In a badge view, drill down to the group or system you want to deploy agents to.
   - After doing a Basic or Advanced Search for systems you want to deploy agents to, click on the Search Results node in the tree view (to deploy agents to all the systems found) or click on a system under the Search Results node (to deploy agents to that system only).

2. Choose Deploy Agents from the Actions menu.
   The Administration dialog opens with the Deploy Agents tab selected and the group members or system(s) listed in the table.

3. Select the systems you want to deploy agents to.
   **Note:** The systems must have been discovered with known credentials in order to select them to automatically deploy agents to. If the system does not have known credentials, you cannot select the check box. If you import a list of systems from an XML file you can specify the credentials in the XML file.

   To select all systems that have credentials, click the check box in the column header. To find specific systems in the list, enter part or all of the system name in the Find field. This highlights the first occurrence of the name in the table.

4. Choose a Hub for the agents to report to.

5. Enter an Origin for the agents.
   If you do not enter an origin, the name of the hub is assigned as the origin.

6. (Optional) Edit the Job Description for this agent deployment.

7. Click Deploy.
   Deployment begins and the Agent Deployment Status dialog opens. The table on the right displays messages about the current deployment job. The status is updated every 10 seconds.

8. Click Close when the deployment is complete.

**Deploy Agents to Systems Listed in a File**

Nimsoft Monitor administrators can import a list of systems to deploy agents (robots) to automatically. To do so, first define the list of systems in an XML file, then import the list into the Deploy Agents tab.
Define the XML File

The XML file must list each computer system where an agent is to be installed, along with required agent attributes. Optional agent attributes may also be specified (see the table below).

**Note:** Windows host names must specify the domain as well as the host name (domain\host name).

The following is an example of XML that lists the required attributes.

```xml
<hosts>
  <host>
    <profile>Linux</profile>
    <arch>64</arch>
    <hostname>server1</hostname>
    <username>root</username>
    <password>nimsoft</password>
    <domain>customer1</domain>
    <hubip>101.101.101.101</hubip>
    <hub>primaryhub</hub>
    <hubrobotname>robot1</hubrobotname>
    <hubport>48002</hubport>
  </host>
  <host>
    <profile>Windows</profile>
    <arch>64</arch>
    <hostname>customer1\server2</hostname>
    <username>root</username>
    <password>nimsoft</password>
    <domain>customer1</domain>
    <hubip>10.10.10.10</hubip>
    <hub>primaryhub</hub>
    <hubrobotname>robot1</hubrobotname>
    <hubport>48002</hubport>
  </host>
</hosts>
```

The following table describes the agent attributes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile</td>
<td>Yes</td>
<td>Operating system (OS) of the host. Enter either <strong>Linux</strong> or <strong>Windows</strong>. This value is case-sensitive.</td>
</tr>
<tr>
<td>arch</td>
<td>Yes</td>
<td>Whether the host OS is 32-bit or 64-bit. Enter either <strong>32</strong> or <strong>64</strong>.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hostname</td>
<td>Yes</td>
<td>Name or IP address of the computer system where the agent is to be installed. For Windows systems, you must include the domain name: domain\host.</td>
</tr>
<tr>
<td>username</td>
<td>Yes</td>
<td>User name for logging onto the system. The user must be an administrative user (Windows) or a root user (Linux) for the host where the agent is to be installed.</td>
</tr>
<tr>
<td>password</td>
<td>Yes</td>
<td>Password for logging onto the system.</td>
</tr>
<tr>
<td>domain</td>
<td>Yes</td>
<td>Domain the robot will belong to.</td>
</tr>
<tr>
<td>hubip</td>
<td>Yes</td>
<td>IP address of the Nimsoft Monitor primary hub.</td>
</tr>
<tr>
<td>hub</td>
<td>Yes</td>
<td>Name of the Nimsoft Monitor primary hub. This is automatically updated if the hub name changes.</td>
</tr>
<tr>
<td>hubrobotname</td>
<td>Yes</td>
<td>Name of the agent (robot) on the Nimsoft Monitor primary hub. This is automatically updated by the controller if the hub robot name changes.</td>
</tr>
<tr>
<td>hubport</td>
<td>Yes</td>
<td>Port number of the hub. The default is 48002.</td>
</tr>
<tr>
<td>tempdir</td>
<td>No</td>
<td>Path on remote system where the Automatic Deployment Engine (ADE) places temporary resources for installation.</td>
</tr>
<tr>
<td>rsakeyfile</td>
<td>No</td>
<td>Local path to RSA public key file used to connect via SSH to certain remote targets.</td>
</tr>
<tr>
<td>first_probe_port</td>
<td>No</td>
<td>If specified, the controller gives probes port numbers to use. Otherwise random unused ports are taken.</td>
</tr>
<tr>
<td>secondary_domain</td>
<td>No</td>
<td>Domain of the secondary hub. Typically this is the same as the domain of the primary hub.</td>
</tr>
<tr>
<td>secondary_hub</td>
<td>No</td>
<td>Name of the secondary hub. This is automatically updated if the hub name changes.</td>
</tr>
<tr>
<td>secondary_hubrobotname</td>
<td>No</td>
<td>Name of the robot on the secondary hub. This is automatically updated by the controller if the hub robot name changes.</td>
</tr>
<tr>
<td>secondary_hubip</td>
<td>No</td>
<td>IP address of the secondary hub.</td>
</tr>
<tr>
<td>secondary_hubport</td>
<td>No</td>
<td>Hub port of the secondary hub. The default is 48002.</td>
</tr>
<tr>
<td>secondary_hub_dns_name</td>
<td>No</td>
<td>Fully qualified DNS name of the system the hub runs on. If this value is specified it overrides the secondary_hubip, which is then used only as a cached value if the DNS lookup fails.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>secondary_robotip_alias</td>
<td>No</td>
<td>NAT address the robot should use when connected to the secondary hub. Valid values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ same = the NAT address for the primary hub. This is the default value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ An IP address</td>
</tr>
<tr>
<td>robot_mode</td>
<td>No</td>
<td>Whether the robot initiates or accepts communication with its hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ normal - The robot can accept communication from, and initiate communication with, its hub</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ passive - The robot cannot initiate communication with its hub. All contact must be initiated by the hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ offline - The robot does not initiate or expect communications from its hub.</td>
</tr>
<tr>
<td>robotname</td>
<td>No</td>
<td>Name for the agent (robot) to be installed. The default is the host name.</td>
</tr>
<tr>
<td>robotip</td>
<td>No</td>
<td>Local IP address of the robot. The robot will send using this interface only. This value is propagated to its probes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default no value is specified, in which case the robot automatically finds its IP address. In some cases where the machine has multiple interfaces it is unpredictable which interface the robot will use to communicate with its hub. Enter a value if you want to set which interface is used.</td>
</tr>
<tr>
<td>robotip_alias</td>
<td>No</td>
<td>In a NAT environment, the robot uses this IP address to identify itself to its hub.</td>
</tr>
<tr>
<td>controller_port</td>
<td>No</td>
<td>Specify a value to override the default controller port, which is 48000.</td>
</tr>
<tr>
<td>spooler_port</td>
<td>No</td>
<td>Specify a value to override the default spooler port, which is 48001.</td>
</tr>
<tr>
<td>hub_dns_name</td>
<td>No</td>
<td>Name of the DNS server for the hub.</td>
</tr>
<tr>
<td>hubdomain</td>
<td>No</td>
<td>Domain of the hub.</td>
</tr>
<tr>
<td>os_user1</td>
<td>No</td>
<td>User tag to be sent with messages generated from the robot. Used by the controller when sending internal messages directly to the hub and by the spooler when any message is spooled.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>os_user2</td>
<td>No</td>
<td>User tag to be sent with messages generated from the robot. Used by the controller when sending internal messages directly to the hub and by the spooler when any message is spooled.</td>
</tr>
<tr>
<td>set_qos_source</td>
<td>No</td>
<td>Whether the probe should use the robot name as the qos source instead of the host name. Valid values are yes and no. The default is no.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This does not work for older probes.</td>
</tr>
<tr>
<td>system_uptime_qos</td>
<td>No</td>
<td>Whether to send asynchronous QoS when the robot is up or down. Valid values are yes or no. The default is no.</td>
</tr>
<tr>
<td>autoremove</td>
<td>No</td>
<td>Whether the agent should unregister itself from the hub after it terminates. Valid values are yes and no. The default value is no.</td>
</tr>
<tr>
<td>default_priority_level</td>
<td>No</td>
<td>Default priority level for probes. Probes with lower priority levels are started first, with a delay between each priority level. This functionality is made redundant by the new start_after property of the probes.</td>
</tr>
<tr>
<td>proxy_mode</td>
<td>No</td>
<td>If set to 1, the controller acts as a proxy for all its probes so that all callback functions to the robot or its probes can be performed through the controller port. Valid values are 0 (off) and 1 (on). The default is 0.</td>
</tr>
<tr>
<td>proxy_log</td>
<td>No</td>
<td>Logging level for proxy functions in the controller.log file. Valid values are 0-8; the default value is 4. Typically values 1-5 are used. The controller.log file is located in the installation directory for the target robot.</td>
</tr>
<tr>
<td>hub_update_interval</td>
<td>No</td>
<td>Interval, in seconds, at which the controller should send alive or probelist information to the hub. The default is 900.</td>
</tr>
<tr>
<td>loglevel</td>
<td>No</td>
<td>Level of logging, 0-8, for messages from the agent. The default is 0.</td>
</tr>
<tr>
<td>logsize</td>
<td>No</td>
<td>Size, in kilobytes, for the controller.log file to reach before it is copied and truncated. The default is 100. The controller.log file is located in the installation directory for the target robot.</td>
</tr>
<tr>
<td>logfile</td>
<td>No</td>
<td>Name for the log file. The default is controller.log.</td>
</tr>
<tr>
<td>config_lock_timeout</td>
<td>No</td>
<td>Timeout, in seconds, for the configuration file lock. The default is 360.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>port_alive_check</td>
<td>No</td>
<td>Interval, in seconds, for port alive checking. The default is 330.</td>
</tr>
<tr>
<td>port_alive_include_local</td>
<td>No</td>
<td>Whether to include ports registered from local probes when performing the port check. Valid values are yes or no. The default is yes.</td>
</tr>
<tr>
<td>startup_timeout</td>
<td>No</td>
<td>When there is a hub on the robot, this is the time, in seconds, the controller will wait for the local hub to start until other probes are started. If this timeout is reached, the robot does a failover. The default value is 900.</td>
</tr>
<tr>
<td>suspend_on_loopback_only</td>
<td>No</td>
<td>Suspend all probes if loopback is the only network. Valid values are yes or no. The default is yes.</td>
</tr>
<tr>
<td>temporary_hub_broadcast</td>
<td>No</td>
<td>If set to yes, only failover to the secondary hub is allowed; no broadcast occurs if the secondary is not available. Valid values are yes or no. The default is no.</td>
</tr>
<tr>
<td>do_not_broadcast</td>
<td>No</td>
<td>Same as temporary_hub_broadcast except broadcast is also disallowed for finding a primary hub. Valid values are yes or no. The default is no.</td>
</tr>
<tr>
<td>unmanaged_security</td>
<td>No</td>
<td>When broadcasting for a hub, this setting determines which hubs are candidates for establishing contact. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>not_locked</strong> - The controller can broadcast to any hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>none</strong> - The controller can broadcast to any hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>open</strong> - The controller can broadcast to any hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>domain_locked</strong> - The controller can broadcast only to hubs in its current domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>domain</strong> - The controller can broadcast only to hubs in its current domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>hub_locked</strong> - No broadcast is allowed. The controller can only contact its hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>hub</strong> - No broadcast is allowed. The controller can only contact its hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is <strong>domain_locked</strong>.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>send_alive</td>
<td>No</td>
<td>Whether or not to send alive messages to the hub. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1 - Send alive message to hub at each hubupdate interval.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 0 - Do not send alive messages. Use this, for example, when running in an offline mode where you want contact between the robot and hub to be established only when needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ -1 - Use this if the alive message format is not understood by the (very old) hub. This sends the complete probe list instead.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 1.</td>
</tr>
<tr>
<td>alarm_level_comfail_restart</td>
<td>No</td>
<td>Whether to send an alarm, and at which severity level, when the controller is unable to communicate with a probe (that has a registered port). After the fourth attempt this alarm is sent and the probe is restarted. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ no alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ minor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ major</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is no alarm.</td>
</tr>
<tr>
<td>alarm_level_dispatch_error</td>
<td>No</td>
<td>Severity level for an internal alarm indicating a socket system failure. This alarm is sent only if the loglevel setting is set to a number greater than 0. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ minor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ major</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is major.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>alarm_level_max_restarts</td>
<td>No</td>
<td>Severity level for an alarm issued when a probe is restarted 10 times and quickly terminated each time. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- minor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- major</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is major.</td>
</tr>
<tr>
<td>alarm_level_start_error</td>
<td>No</td>
<td>Whether to send an alarm, and at which severity level, when unable to start a probe. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- no alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- minor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- major</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is major.</td>
</tr>
<tr>
<td>alarm_level_suspended</td>
<td>No</td>
<td>Whether to send an alarm, and at which severity level, when aborting the start of a probe because the robot state is suspended. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- no alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- minor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- major</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is no alarm.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| alarm_level_timed_not_finished| No        | Severity level of an alarm issued when a timed probe is not completed at the next scheduled start time. The timed probe is restarted when this occurs. Possible values are:  
- clear  
- informational  
- warning  
- minor  
- major  
- critical  
The default is **warning**. |
| alarm_level_timed_error_return| No        | Whether to send an alarm, and at which severity level, when a timed probe does not return 0 on termination. Possible values are:  
- no alarm  
- informational  
- warning  
- minor  
- major  
- critical  
The default is **warning**. |
| alarm_level_unregister        | No        | Severity level of alarm issued when a probe unregisters its port but does not terminate. Possible values are:  
- clear  
- informational  
- warning  
- minor  
- major  
- critical  
The default is **major**. |
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm_level_request_error</td>
<td>No</td>
<td>Whether to send an alarm, and at which severity level, when unable to issue a request to distsrv. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ no alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ minor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ major</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is <strong>major</strong>.</td>
</tr>
<tr>
<td>alarm_level_postinstall</td>
<td>No</td>
<td>Whether to send an alarm, and at which severity level, when unable to start a post-install script on completing a package distribution and when the post-install script does not return the OK (0) status. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ no alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ minor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ major</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is <strong>no alarm</strong>.</td>
</tr>
<tr>
<td>audit</td>
<td>No</td>
<td>When and where to send audit messages. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ post – Send audit message on controller events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ yes – Log controller events to local file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ post_detail – Send audit event on controller events and configuration file changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ file_detail – Log controller events and file change events to local file</td>
</tr>
<tr>
<td>audit_max_config_size</td>
<td>No</td>
<td>Maximum size, in bytes, of configuration file for content comparison.</td>
</tr>
<tr>
<td>audit_checkpoint_count</td>
<td>No</td>
<td>Number of versions of configuration files to retain.</td>
</tr>
</tbody>
</table>
### Attribute Table

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm_timeout</td>
<td>No</td>
<td>Interval, in minutes, at which alarms for probes in the <strong>error</strong> state are repeated.</td>
</tr>
<tr>
<td>wait_after_unregister</td>
<td>No</td>
<td>Wait time, in seconds, after a probe unregisters a port. If the process is still running the unregister alarm is issued and the probe is set to the <strong>error</strong> state.</td>
</tr>
<tr>
<td>tz_offset</td>
<td>No</td>
<td>Timezone offset override in seconds, positive or negative.</td>
</tr>
<tr>
<td>config_locking</td>
<td>No</td>
<td>Signals the configuration tools that they should acquire a lock when starting relinquish it on termination. Possible values are <strong>yes</strong> or <strong>no</strong>. The default is <strong>no</strong>.</td>
</tr>
<tr>
<td>capture_output</td>
<td>No</td>
<td>Creates pipes for each started probe to capture any output they send to stdout or stderr. This output is appended to the probes log file. Enabling this functionality introduces an extra overhead in the probe. On Windows systems the probes must inherit resources from the controller and in some situations this may cause the controller to not terminate properly. Possible values are <strong>yes</strong> or <strong>no</strong>. The default is <strong>no</strong>.</td>
</tr>
<tr>
<td>default_fail_window</td>
<td>No</td>
<td>Number of seconds when a probe is started that it needs to run before the restart counter is reset for the probe. The default is 15. The default_fail_window set for the robot applies to all probes managed by the robot. If you want a different setting for a certain probe, you can set the fail_window setting in the configuration window for the probe.</td>
</tr>
<tr>
<td>max_restarts</td>
<td>No</td>
<td>Number of starts allowed before a probe is set to the <strong>error</strong> state. The restart counter is reset for a probe if it runs longer than its fail_window.</td>
</tr>
</tbody>
</table>

### Import the File

Nimsoft Monitor administrators can import a list of systems to deploy agents (robots) to automatically. You must have the **USM Automatic Robot Installation** ACL permission in order to deploy agents automatically. Also, the automated_deployment_engine probe version 1.10 or later must be running in your environment.

**Note:** If you do not have the **USM Automatic Robot Installation** ACL permission, or if you are an account contact user, the **Deploy Agents** tab is not displayed.
Follow these steps:

1. Click the Administration icon (iß).
   The Administration dialog opens.
2. Click the Deploy Agents tab.
3. Click Import.
4. Browse to an appropriate XML file and click Open.
   The systems listed in the file are listed in the Deploy Agents table.
5. (Optional) Edit the Job Description for this agent deployment.
6. Click Deploy.
   Deployment begins and the Agent Deployment Status dialog opens. The table on the right displays messages about the current deployment job. The status is updated every 10 seconds.
7. Click Close when the deployment is complete.

View the Status of Agent Deployment

You can view status messages for automatic agent deployment jobs, including jobs that have completed.

Follow these steps:

1. Click the Administration icon (iß).
2. Click the Deploy Agents tab.
3. Click Deployment Status.
   The Agent Deployment Status window opens.
4. In the table on the left, click the job you want to see messages for.
   Status messages for the job are displayed in the table on the right.

Getting Started with Service-Oriented Configuration

Service-oriented configuration allows you to define what you want to monitor in a monitoring template and then apply the template to a group of devices. The USM portlet automatically deploys the probes that support the monitors in the template and configures the appropriate probe settings. This eliminates the need to manually deploy and configure probes.
Not all probes support service-oriented configuration. For a list of probes that do, see SOC-Supported Probes.

Probes can also be configured through a configuration interface, accessed using Infrastructure Manager.

**Important:** Service-oriented configuration of the probes is not compatible with standard configuration through the probe's configuration interface. Do not mix or interchange configuration methods. If you do, the result will be unpredictable monitoring of your devices.

The above notice has these implications:

- If you use service-oriented configuration to configure a probe, thereafter you must not make any changes whatsoever to the configuration through the probe's native configuration interface!
- If you want to revert a probe from service-oriented configuration to standard configuration, contact Nimsoft support for assistance.

### Set Up Service-Oriented Configuration

**Follow these high-level steps:**

1. Download the service-oriented configuration probes you want to use from the Nimsoft web archive to your local archive on your Nimsoft Monitor server.
   
   The probes must be in your local archive in order to see the monitors for the probes in the list of available monitors when creating monitoring templates in USM.
   
   **Note:** Service-oriented configuration can be used only with probes that support it. For a list of probes that support service-oriented configuration, see the SOC-Supported Probes topic in the SOC Probes Configuration Reference (SOC-probes/index.htm).


3. USM portlet – For existing implementations, set the device state to Managed for systems you want to monitor.
   
   This is not necessary for new implementations where discovery has not run (assuming you select the "unmanaged systems should be treated as managed" option during NM installation). For more information, see Migration for Legacy Users (see page 180).

4. USM portlet – Create groups.

5. USM portlet – Create monitoring templates.

6. USM portlet – Assign monitoring templates to groups.
SOC Probes Configuration Reference

This document describes configuration settings for probes configured using service-oriented configuration. To view this documentation, see the SOC Probes Configuration Reference (http://docs.nimsoft.com/prodhelp/en_US/UMP/6.0/SOC-probes/index.htm).

Not all probes support service-oriented configuration, but more and more do. For a current list of probes that do, see the SOC-Supported Probes topic at the top of the document.

Probes can also be configured through a configuration interface, accessed using Infrastructure Manager. For configuration information using the native configuration interfaces, see the Nimsoft Probe Library (http://docs.nimsoft.com/prodhelp/en_US/Probes/Catalog/index.htm).

Important: Service-oriented configuration of the probes is not compatible with standard configuration through the probe’s configuration interface. Do not mix or interchange configuration methods. If you do, the result will be unpredictable monitoring of your devices.

The above notice has these implications:

- If you use service-oriented configuration to configure a probe, thereafter you must not make any changes whatsoever to the configuration through the probe’s native configuration interface!
- If you want to revert a probe from service-oriented configuration to standard configuration, contact Nimsoft support for assistance.

Working with Groups

Groups are lists of computer systems. Administrators can create groups to assign the same monitoring template or report template to multiple computer systems.

There are three types of groups:

Container

A parent to other groups.

Dynamic

Contains the computer systems that meet a specified set of criteria. The membership of dynamic groups is updated automatically every 15 minutes. You can change the update interval in the nis_server probe configuration in Infrastructure Manager. Dynamic groups can be created manually, or UMP can automatically create groups based on OS Type, OS Name, Origin, User Tag 1 or User Tag 2.
Static

Contains a specified list of computer systems. Once you specify the list of systems that are members of the group, the membership does not change unless you manually add or remove systems.

You can use groups to organize your infrastructure by location, technology, or even a service. For example, you could create a container group named e-Commerce, a business service. The e-Commerce group could contain three groups named Web Servers, Application Servers, and Database Servers. These could be either dynamic or static groups and would contain servers to support each aspect of the e-Commerce service.

Note: A discovery agent must be running in your environment to discover the devices that can be added to groups. You can use the UMP Remote Admin portlet to deploy and configure remote discovery agents.

Note: You must have the USM Group Modification permission set in the Access Control List (ACL) in order to create, edit, and delete groups.

Create a Group

You can create a group so that you can apply the same monitoring settings or report templates to all devices in the group.

Follow these steps:

1. In a badge or tree view, click on a container group and choose Add Group from the Actions menu. Or, in the tree view mouse over the name of a container group and click the Add Group icon ( ).
   
   Note: The Add Group option is available only for container groups.

   The Edit Group <Group Name> dialog is displayed.

2. In the Properties tab, edit the settings as needed:
   Type
   
   Choose Container, Dynamic, or Static.

   Name
   
   Enter a name for the group.

   Description
   
   Enter a description of the group.

   Priority
   
   Assign a priority. For more information, see Priority (see page 402).
Monitoring Template State

Choose whether or not monitoring templates assigned to the group are active. When templates are **Active**, all templates assigned to the group are applied to all members of the group. When templates are **Inactive**, none of the templates are applied to members of the group. However, the same monitoring templates remain active for other groups.

Account

Choose **No Account** if you do not want account contact users to see the group. Or, choose an account so that only account contact users assigned to that account or regular Nimsoft users can see the group (account contact users from other accounts cannot see the group).

**Note:** You cannot set **Priority** or **Monitoring Template State** for container groups.

3. For dynamic or static groups, you can create a filter.

For a static group, create a filter to help find the systems to be assigned to the group. Once the **Members** table is populated, select the systems to include in the group in the **Included** column.

For a dynamic group, create a filter that defines the systems to be in the group.

For information on filters, see [Filters](#) (see page 392).

4. Click **OK**.

5. Click the **Monitoring Templates** tab to assign monitoring templates to the group. For more information, see [Working with Monitors](#) (see page 400).

6. Click the **Report Templates** tab to assign report templates to the group. For more information, see [Reports](#) (see page 432).

**Automatic Groups**

Unified Service Manager (USM) can create certain dynamic groups automatically. You can create dynamic groups automatically according to:

**OS Type**

Creates groups according to type of OS, such as Windows, Unix, and so on.

**OS Name**

Creates groups according to name of operating system. For Unix systems, for example, creates groups such as Linux, Solaris, AIX, or HP-UX. For Windows systems, creates groups such as Windows 7, Windows XP, and so on.
Origin

Creates groups according to origin. The origin is a name assigned to QoS data from probes to identify the origin of the data. If you are an MSP, for example, typically the origin is the name of each customer. For enterprise customers, typically the hub name is used. The origin name can be set in the Origin field under Advanced Settings in the hub configuration interface in Infrastructure Manager. If no origin is assigned, the hub name is used.

User Tag 1, User Tag 2

Creates groups according to user tags. User tags are text fields that you define on the robot. For example, user tags could be used for geographic location or type of server.

If you create groups automatically by origin, for example, USM creates one dynamic group for each origin you have specified. As with other dynamic groups, membership is updated automatically, every 15 minutes by default.

It is recommended that you enter a name in the Parent Group field. This creates a container group for the automatic groups. If you leave the Parent Group field blank, the automatic groups are created under the root Groups node.

For example, if you are an MSP and are creating automatic groups by origin, you might name the parent group Customers.

You cannot create multiple levels of child groups for automatic groups; only one level of parent-child relationship is supported. If you enter the name of an existing group in the Parent Group field, the automatic groups are added to that parent group.

Note: When entering the name of an existing group in the Parent Group field, it is recommended that the group be a container group.

UMP comes with automatic groups created by OS Type under the parent group Servers.

Choosing more than one type of automatic group does not combine the types; each property you select creates groups for that property. For example, if you retain the OS Type with Parent Group Servers and also select Origin, with Parent Group Customers, groups for OS Type are created under the Servers group and groups for Origin are created under the Customers group.

You can view settings for automatic groups by clicking on an automatic group in the tree or badge view and choosing Edit Group from the Actions menu. However, settings for automatic groups cannot be modified.

Note: You cannot assign automatic groups to accounts. The Priority for automatic groups is 0 (highest priority) and the Monitoring Template State is Active.
Create Groups Automatically

USM can automatically create dynamic groups according to certain criteria.

In order to create groups automatically, you must not be an account contact user. For account contact users, the Configure Automatic Groups tab is not active.

Follow these steps:

1. Click the Administration icon () in Unified Service Manager.
   The Administration dialog opens.
2. Click the Configure Automatic Groups tab.
3. Select the type of automatic groups to create.
   Note: Choosing more than one type of automatic group does not combine the types; each property you select creates groups for that property.
4. If you want to create a group to be a parent of the automatic groups, enter a name in the Parent Group field.
   For example, if you are an MSP and are creating automatic groups by origin, you could name the parent group Customers. If you leave the Parent Group field blank, the automatic groups are created under the root node.
5. Click OK.

Filters

Filters are used to find systems to include in static groups or to define the members of dynamic groups. For static groups, create the filter and then choose which of the listed systems to include in the group. For dynamic groups, create a filter to specify which systems are in the group. The list of members in the group is automatically updated every 15 minutes.

Create a Filter

Create a filter to define the members of a group. For dynamic groups, the filter defines which devices are in the group. For static groups, the filter helps you find which devices to include in the group.
Note: The special characters \, %, and _ must be preceded with an escape character when using basic search, advanced search, or filters in Unified Service Manager or filters in Performance Reports Designer. In the case of advanced search and filters, this applies when the contains, starts with, or ends with operator is selected.

The escape character required depends on the type of database you use. For MySQL, the backslash (\) is the escape character; for MS SQL, special characters are enclosed in square brackets ([ ]). Searching for special characters is not supported for Oracle.

The table shows how to enter special characters for each database type.

<table>
<thead>
<tr>
<th>Character</th>
<th>MySQL</th>
<th>Oracle</th>
<th>MS SQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>\</td>
<td>Not applicable</td>
<td>\ (No escape character required)</td>
</tr>
<tr>
<td>%</td>
<td>%</td>
<td>Not applicable</td>
<td>[%]</td>
</tr>
<tr>
<td>_ (underscore)</td>
<td>_</td>
<td>Not applicable</td>
<td>[]</td>
</tr>
</tbody>
</table>

Follow these steps:

1. Do one of the following:
   - In a badge view, display a group and choose Edit Group from the Actions menu.
   - In tree view, click on a group and choose Edit Group from the Actions menu, or click the Edit Group icon ( ) next to the group name in the tree.

   The Edit Group dialog is displayed.

2. In the Filters section of the Properties tab, choose items from the pull-down menus and enter text in the text field as appropriate.

3. Click the Add Filter icon ( ) to add additional rows to the filter if wanted.
4. Once you have defined the rows for the filter, click the Apply Filters icon (✔️) to confirm the results in the Members table.

Systems that have not yet been added to the group are shaded in gray. Not all systems that match the filter criteria may be displayed; up to 100 systems that match the filter are displayed.

For dynamic groups, all systems that match the filter are included in the group, even if they are not displayed in the Members table when you click Apply Filters. To view all members in the group, save the group and click on the group in a badge or tree view. All members are displayed. If there are more than 100 members click the arrow icon (.paginator) to page through the list.

For static groups, existing group members are displayed in addition to the filter results. For example, you select 50 systems as members of a static group and save the group. Then you edit the group, creating a filter to add members to the group. Up to 100 systems that match the filter plus the 50 existing members are displayed in the Members table when you click Apply Filters. If more than 100 systems match the filter and you do not see those you want to add to the group, you may need to refine the filter criteria so the systems you want to add are displayed in the Members table.

5. If the filter is for a static group, click the check boxes in the Included column to choose the systems you want to add to the group.

6. Click OK.

The filter is saved and the systems added to the group are no longer shaded in gray in the Members table.

Example

We have a client, called Client A, who has both Windows and UNIX systems. Client A wants a group containing only Windows systems that are web servers or SQL servers.
First we narrow down the list using a unique attribute. Client A's system names all start with `clienta` so we select the `Name` field, the `contains` operator, and enter `clienta` in the text field. Then we click the **Apply Filters** icon to see the results. Now we see only Client A's systems.

Next we narrow down the group to only Windows systems. We click the **Add Filter** icon to add a row of filter options. We select the `and` operator, the `OS Type` field, and the `is` operator. We enter `windows` in the text field, then click the **Apply Filters** icon. Now we see only Client A's Windows systems.

Next we narrow down the group to include only web servers and SQL servers. We click the **Add Filter** icon to add a row of filter options. We select the `and` operator, the `Name` field, and the `ends with` operator and enter `websrvr` in the text field.

We click the **Add Filter** icon to add another row of filter options. We select the `or` operator, the `Name` field, and the `ends with` operator, and enter `sqlsrvr` in the text field.
We click the **Apply Filters** icon and the list now contains only Client A’s Windows systems that are web servers or SQL servers.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>OS Type</th>
<th>OS Name</th>
<th>OS Version</th>
<th>Build Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>clients-sq1</td>
<td>192.168.129.108</td>
<td>Windows</td>
<td>Windows XP Pro</td>
<td>3.1.2600</td>
<td>Service</td>
</tr>
<tr>
<td>clients-web1</td>
<td>192.168.129.109</td>
<td>Windows</td>
<td>Windows XP Pro</td>
<td>5.1.2600</td>
<td>Service</td>
</tr>
</tbody>
</table>

**User Tags**

You can filter on two user-defined criteria, called User Tags, in portlets that have filters. You can also automatically create groups according to User Tag.

**User Tag 1** and **User Tag 2** are text fields that are defined on the robot. You can enter any text in these fields. (Use Infrastructure Manager to open the configuration window for the robot.) Once you have done so, you can filter for these values in the Unified Service Manager, Performance Reports Designer, and List Designer portlets.

For example, you could use **User Tag 1** for geographic location and **User Tag 2** for type of server. For some systems you enter **Europe** for **User Tag 1** in the robot configuration, and for some systems you enter **Asia**. For **User Tag 2**, you enter either **production server** or **web server**.
You can then create reports for your regional systems by filtering on User Tag 1 in the Performance Reports Designer (in the Filters tab) or List Designer (in the filter fields of the New Group pane). To do so, you would set the filter to User Tag 1 is Europe or User Tag 1 is Asia.

In the Unified Service Manager portlet, you can create separate groups for your production and web servers and apply different monitoring templates to them. To create the groups, in the Filters section of the Edit Group dialog you would set the filter to User Tag 2 is production server for one group, and User Tag 2 is web server for the other group.

User Tag 1 and User Tag 2 can be used to filter for any system that has a Nimsoft Monitor robot running on it. You cannot use User Tag 1 and User Tag 2 to filter for network devices that do not have a Nimsoft Monitor robot.

For information about automatically creating groups according to User Tag, see Automatic Groups (see page 390).

**Filter Menus and Buttons**

Filters have these menus and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>and/or pull-down menu</td>
<td>Choose the and or or operator to apply to this row of the filter definition. This operator is present only in the second and subsequent rows.</td>
</tr>
<tr>
<td>(Blank)/not pull-down menu</td>
<td>Choose not in order to search for all systems except those that meet this row of the filter definition. Otherwise, leave blank.</td>
</tr>
<tr>
<td>Criterion pull-down menu</td>
<td>Choose the criterion to filter for, such as Name, IP Address, and so on.</td>
</tr>
</tbody>
</table>

For more information on using the Filters section, see "To create the groups..."
Operator pull-down menu | Choose the appropriate operator, such as is, contains, starts with, and so on.
---|---
Text field | Enter the appropriate text for the criterion you chose.
Add Filter/Remove Filter icons | Click to add or remove rows for the filter definition.
Move up/Move down icons | Click to move the row up or down. Filter rows are applied in sequential order.
Apply Filters icon | Click to see the results of applying the filter in the Members table. Although you see the list of systems in the Members table, the group is not saved until you click OK.

**Note:** The special characters \, %, and _ must be preceded with an escape character when using basic search, advanced search, or filters in Unified Service Manager or filters in Performance Reports Designer. In the case of advanced search and filters, this applies when the contains, starts with, or ends with operator is selected.

The escape character required depends on the type of database you use. For MySQL, the backslash (\) is the escape character; for MS SQL, special characters are enclosed in square brackets ([ ]). Searching for special characters is not supported for Oracle.

The table shows how to enter special characters for each database type.

<table>
<thead>
<tr>
<th>Character</th>
<th>MySQL</th>
<th>Oracle</th>
<th>MS SQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>\</td>
<td>Not applicable</td>
<td>\ (No escape character required)</td>
</tr>
<tr>
<td>%</td>
<td>%</td>
<td>Not applicable</td>
<td>[%]</td>
</tr>
<tr>
<td>_ (underscore)</td>
<td>_</td>
<td>Not applicable</td>
<td>[_]</td>
</tr>
</tbody>
</table>
View Group Assignments

You can use the Groups tab of Unified Service Manager to view which groups a computer system is assigned to. This can help you determine whether any monitor collisions occur and how to set priority for your groups.

Follow these steps:
1. In a badge or tree view, click on a computer system.
2. Click the Groups tab in the right pane.
   The table displays the name of the group, the type of group (container, dynamic, or static), the priority set for the group, and the state set for the group (active or inactive).

Servers Group

The Servers group is an automatic group that comes preconfigured with UMP. The Servers group creates sub-groups according to OS Type (Windows, Unix, and so on).

You cannot edit the properties of the Servers group or its sub-groups. However, you can assign monitoring templates and report templates. For the sub-groups, you can also click the Apply Filters icon to view what the results will be the next time the group is updated.

Delete a Group

Delete a group if you no longer need it. For container groups, all sub-groups must be deleted before you can delete the container group. For automatic groups, you can delete the Parent (container) group if all the sub-groups are deleted or if you change the name of the Parent Group in the Configure Automatic Groups tab.

Follow these steps:
1. In a badge or tree view, click on a group that does not have child groups.
2. Choose Delete Group from the Actions menu. Or, in the tree view mouse over the name of the group and click the Delete Group icon (삭제).
Working with Monitors

Monitors are checkpoints that can be configured to monitor specific resources of a system (such as CPU usage, memory usage, or bandwidth utilization) or events that occur within a system (such as disk crash or network unavailability). You can choose which monitors to include in a monitoring template and you can set the properties for each monitor to meet your specific monitoring requirements.

Once you create monitoring templates, you can assign them to groups of systems. Unified Service Manager automatically deploys the probes that support the monitors in the template and configures the appropriate probe settings.

This section of the help tells you how to create and configure monitors, assign monitors to monitoring templates, and assign monitoring templates to groups. It also tells you how to override monitor settings, apply a monitor an individual computer system, and check monitor status.

Note: You must have the **USM Edit Monitoring Templates** permission set in the Access Control List (ACL) to create, edit, and delete monitors and monitoring templates. You must have the **USM Modify Individual Monitors for Computer Systems** permission in order to apply a monitor directly to a system (without a monitoring template).

Local vs Remote Monitors

Each monitor is either a local or remote monitor, indicated in parentheses after the name of the monitor. For example, you can choose either the CPU Usage (local) monitor or the CPU (remote) monitor. The terms local or remote mean:

- Local - The monitor runs on the target system (the system being monitored). A Nimsoft robot must be installed on the system.
- Remote - The monitor runs on a system other than the target. To use remote monitors the Nimsoft discovery agent must be running in your environment to discover the systems to monitor. For example, you may run a discovery agent on a hub. A Nimsoft robot must also be installed on the system. Nimsoft calls the system where the discovery agent and robot are running a monitoring station. Devices discovered by a monitoring station will be remotely monitored by the same monitoring station. (Note: You can use the UMP Remote Admin application to configure remote discovery agents.)

When you choose a remote monitor, the appropriate probe is automatically deployed to the corresponding Monitoring Station. In general, choose a local monitor if a robot is installed on the target system. Otherwise, choose a remote monitor.

Note: Do not run both the local and remote versions of a monitor on the same system. Note also that auto-deployment does not occur in the case of the VMware probe.
If you choose a local monitor but no robot is installed on the system, you will see a "no robot found" error in the Monitor Status (see page 413) table.

**Understanding Precedence, Priority, and State**

Precedence, Priority, and State determine which version of a monitor is used if the same monitor is assigned to a system multiple times.

Precedence rules determine which monitors are applied within hierarchically related (parent-child) groups.

The Priority setting is used to determine which monitors are used among groups that are not related.

The State settings determine whether any monitors are applied to the system.

The following sections explain each of these in more detail.

**Precedence**

Precedence rules determine which templates, and therefore monitors, are applied first in hierarchical groups. Hierarchical groups are those with parent-child relationships.

For example, we have the hierarchical groups in the following diagram.

```
pes Customers (370)
+----+----+----+
|    |    |    |
| 🔘 | 🔘 | 🔘 |
|    |    |    |
| 🔘 | 🔘 | 🔘 |
|    |    |    |
| 🔘 | 🔘 | 🔘 |
|    |    |    |
| 🔘 | 🔘 | 🔘 |
|    |    |    |
+----+----+----+
```

The groups Customers, Pro Golf, and DB Servers are hierarchically related, as are Customers, Pro Golf, and Mail. The groups DB Servers and Mail are peer groups and are not hierarchically related.

In hierarchical groups, monitoring templates are inherited from ancestor groups. The templates assigned to the group are applied first, then templates from the parent group, then templates from the grandparent group, and so on. If multiple templates contain the same monitor, which may be configured with different settings, the monitor from the first template applied is the one that takes precedence.
In our example, the DB Servers group has its own monitoring templates, as well as those assigned to the Customers and Pro Golf groups. Monitoring templates assigned to the DB Servers group are assigned first, then templates from the Pro Golf group, and then templates from the Customers group. If, for example, monitoring templates assigned to DB Servers and Customers contain the same monitor, the monitor from the template assigned to the DB Servers group is used.

**Priority**

A group can have multiple monitoring templates assigned to it, and a system can belong to multiple groups. This means the same monitor, with different values defined, may be assigned to a system multiple times. This is called a monitor collision.

Within hierarchically related (parent-child) groups, monitor collisions are resolved by precedence rules. Among non-related groups, the **Priority** setting determines which version of a monitor is used. The monitor instance from the group with the highest priority is the instance that is used.

You can set the priority level for each group. The highest priority is 0, and the lowest priority is 10. When a group is created, by default it is assigned a priority of 0.

If monitoring templates containing the same monitor are assigned from two groups with the same priority, one instance of the monitor is selected at random. When this occurs, a message is written to the log file for the Automatic Configuration Engine (ACE). This log file can be viewed using the Log Viewer in Infrastructure Manager. Right-click on the `ace` probe and select **View Log**.

**Note:** Because it is not possible to predict which monitor will be used when monitors from groups of equal priority collide, it is recommended for new UMP installations that you monitor collision notices in the ACE log file and adjust the **Priority** settings to resolve any collisions that are of concern.

Monitoring templates are inherited from ancestor groups, but the priority setting is not. So, if the priority of the parent group is 0 and the priority of the child group is 2, the templates assigned to the parent group are inherited by the child group but the priority remains 2.

To view a list of groups assigned to a computer system and the priority for each group, see **View Group Assignments** (see page 399). To view the status of monitors assigned to a computer system, including whether there are any collisions, see **View Monitor Status** (see page 413).
Example

We have a computer system named Development that belongs to two groups, Group1 and Group2. Both groups have monitoring templates assigned to them that contain the Net_Connect monitor, but with different values for the configuration settings. Because Development belongs to both groups, the Net_Connect monitor is assigned to Development twice, so a collision occurs. However, Group1 has a priority of 3, and Group2 has a priority of 2. Therefore, the Net_Connect monitor associated with Group2 is used. If, however, Group1 and Group2 have the same priority assigned, one of the Net_Connect monitors is chosen at random.

Follow these steps:

1. Click on a group in a badge or tree view.
2. Choose Edit Group from the Actions menu. Or, in the tree view mouse over the name of the group and click the Edit Group icon (●).
   The Edit Group dialog is displayed.
3. Click the Properties tab.
4. Set a value for the Priority field.
   0 is the highest priority, and 10 is the lowest.
5. Click OK.

State

You can use state settings to determine whether or not Nimsoft Monitor monitors a system. If you have a system or group of systems that are not ready for production or are scheduled for maintenance, for example, you can choose settings so that the monitors assigned to those systems are not activated.

There are two ways you can do this. You can set the State property for an individual computer system, or you can set the Monitoring Template State property for a group.

The State property determines whether or not Nimsoft Monitor manages the system. When Nimsoft Monitor manages a system, it automatically deploys and configures the monitors that have been assigned to that system.

The Monitoring Template State property determines whether or not the monitoring templates assigned to a group are active.
Set the State for a System

You can set the State property for a computer system to determine whether that system is Managed, Unmanaged, or in Maintenance status.

The State you assign to a system carries across all groups the system is a member of. For example, if you have a system that is a member of two groups and you set the State for the system to Unmanaged, none of the monitors assigned by the two groups are deployed to the system.

**Note:** This is the same State property that in earlier releases (before UMP 6.0) was set for each system in Nimsoft Remote Admin. You can still set the State property in Remote Admin; however you can now set the State property from within UMP.

Follow these steps:

1. Do one of the following:
   - In a badge view, click on a device badge.
   - In tree view, click on the device name in the tree.
     The System details are displayed.

2. Choose the state you want to assign to the device from the State pull-down menu.

**Managed**

Nimsoft Monitor deploys and configures monitors assigned to the system. The monitors collect data, and any alarms defined for the system are generated.

**Unmanaged**

Nimsoft Monitor does not deploy or configure monitors for the system, and removes any monitors that have been deployed.

**Maintenance**

Any monitors deployed to the system are temporarily inactive. The monitors remain on the system, but data is not collected and alarms are not generated. You can set the State to Managed to resume these functions.

Set the Monitoring Template State for a Group

You can use the Monitoring Template State property to choose whether monitoring templates are applied to a group.

When templates are Active, all templates assigned to the group are applied to all members of the group (unless a system has a State of Unmanaged or Maintenance). When templates are Inactive, none of the templates are applied to members of the group. However, the same monitoring templates remain active for other groups.
For example, you have a monitoring template named Basic assigned to groups named Web Servers, Database Servers, and Production Servers. If you set the Monitoring Template State property to Inactive for the Database Servers group, no templates are applied to the Database Servers group. The Basic template continues to be applied to the Web Servers and Production Servers groups.

Follow these steps:

1. Do one of the following:
   - In a badge view, display a group and choose Edit Group from the Actions menu.
   - In tree view, click on a group and choose Edit Group from the Actions menu, or click the Edit Group icon (.RequestBody) next to the group name in the tree.
   The Edit Group dialog is displayed.

2. Choose the Monitoring Template State from the pull-down menu.
   - Active
     Monitoring templates assigned to the group are implemented for systems that are members of the group (unless the State property for the system has previously been set to Unmanaged or Maintenance).
   - Inactive
     The monitoring templates assigned to the group are not implemented.

3. Click OK.

Applying Monitors to Groups

You can use monitoring templates to assign a set of monitors to a group of computer systems. This allows you to configure the monitor settings once and reuse the set of monitors across your environment.

Multiple monitoring templates can have the same monitor, and the same monitor can be used within a template multiple times with different configurations.

Note: Some probes, such as the VMware probe, allow only a single instance of a monitor per template. For monitors with this restriction, once the monitor is added to a template, if you click the Add Template (RequestBody) icon again, that monitor definition is excluded from the list of potential monitors from which to choose.
Create a Monitoring Template

Create a monitoring template to configure a set of monitors that can then be applied to a group of systems.

Follow these steps:

1. Click the Administration icon ( ).
   The Administration dialog is displayed.
   **Note:** You must have the USM Edit Monitoring Templates ACL permission set in order to edit monitoring templates. If the permission is not set, the Administration pane is not visible. ACL permissions are set in the Account Admin portlet or Infrastructure Manager.

2. Click the Edit Monitoring Templates tab.

3. Click the Add Template icon ( ).
   A new template is added to the Template list with the name New Template.

4. Enter a name and description in the text fields.

5. Choose an account from the Account pull-down menu if you want to assign the template to an account.

6. Click the Save Template icon ( ).

   **Note:** If you make changes to the Name, Description, or Account fields, save the template. Other changes, such as adding or editing a monitor, are applied immediately and you do not need to save the template.

7. To add a monitor to the template, with the name of the template selected in the Template list, click Add.
   The Add Monitor dialog is displayed. The dialog lists the monitors available to you. This list is populated with the monitors for the probes listed in the hub’s Nimsoft Monitor Archive.

8. Choose a category of monitors from the pull-down menu to narrow the list of monitors displayed, if wanted. Or, click on a column header to sort by that column.

   For more information about monitors, such as an explanation of local vs. remote monitors, see Monitors (see page 400).

9. Click a monitor to select it, then click OK.

   A configuration dialog displays properties similar to those you see in the Infrastructure Manager probe configuration windows. The properties vary for each monitor. For information on the properties for a specific monitor, see the SOC Probes Configuration Reference (SOC-probes/index.htm).

   **Note:** The properties you set for a monitor will be in effect for all computer systems in the group(s) the monitoring template is assigned to, unless you set monitor overrides. For more information, see Set a Monitor Override (see page 412).
10. Enter values for the monitor properties, then click **OK**.
    The monitor is added to the list of monitors for the template.

11. Repeat these steps to assign additional monitors to the monitoring template if wanted.
    **Tip:** Select the name of a monitor, then click **Summary** to see a pop-up window listing some of the properties for the monitor.

12. When you are finished adding and configuring monitors, click **Close**.
    The Administration dialog closes.

### Assign a Monitoring Template

Assign a monitoring template to a group to apply those monitors to the systems in the group.

**Follow these steps:**

1. In a badge or tree view, click on a group and choose **Edit Group** from the **Actions** menu. Or, in the tree view mouse over the name of a group and click the Edit Group icon.
   The Edit Group <Group Name> dialog is displayed.

2. Click the **Monitoring Templates** tab.

3. In the **Available** list, click the name of the monitoring template you want to assign to the group.

4. Click the **<<** button to move the monitoring template to the **Linked** list.
   The monitoring templates in the **Linked** list are linked, or assigned to, the selected group.

5. Use the **Move Up** and **Move Down** buttons below the **Linked** list to rearrange the order of monitoring templates. If there is a collision, the monitor associated with the monitoring template higher in this list takes precedence.

**Note:** Applying monitors results in a restart of the probe. If you are applying monitors to a large group of systems, you may want to test the configuration on a small group of systems first to avoid multiple restarts for the large group. The exception to this is the VMware probe, which monitors its configuration file and restarts itself when you apply a monitor using Service Oriented Configuration.
Copy a Monitoring Template

You can copy an existing monitoring template. You may wish to do this if you want to create a monitoring template that is similar to an existing template.

Follow these steps:

1. Click the Administration icon ( ).
   The Administration dialog is displayed.
   
   **Note:** You must have the **USM Edit Monitoring Templates** ACL permission set in order to edit monitoring templates. If the permission is not set, the Administration pane is not visible. ACL permissions are set in the Account Admin portlet or Infrastructure Manager.

2. Click the **Edit Monitoring Templates** tab.

3. Click the name of the monitoring template you want to copy in the **Template** list.

4. Click the Copy Template icon ( )
   A new template is added to the Template list with the name **Copy of <Template Name>**. The settings for the template are the same as the template you copied.

5. Edit the name and description as desired.

6. Choose an account from the **Account** pull-down menu if you want to assign the template to an account.

7. Click the Save Template icon ( ).
   **Note:** If you make changes to the **Name**, **Description**, or **Account** fields, save the template. Other changes, such as adding or editing a monitor, are applied immediately and you do not need to save the template.

8. To edit settings for a monitor already assigned to the template, click the name of the monitor, then click **Edit**.
   A configuration dialog displays properties similar to those you see in the Infrastructure Manager probe configuration windows. The properties vary for each monitor. For information on the properties for a specific monitor, see the SOC Probes Configuration Reference (SOC-probes/index.htm).
   **Note:** The properties you set for a monitor will be in effect for all computer systems in the group(s) the monitoring template is assigned to, unless you set monitor overrides. For more information, see **Set a Monitor Override** (see page 412).

9. Edit values for the monitoring properties as desired, then click **OK**.

10. To add a monitor to the template, click **Add** in the **Edit Monitoring Templates** tab.
    The **Add Monitor** dialog is displayed. The dialog lists the monitors available to you. This list is populated with the monitors for the probes listed in the hub’s Nimsoft Monitor Archive.
11. Choose a category of monitors from the Category pull-down menu to narrow the list of monitors displayed, if wanted. Or, click on a column header to sort by that column.

For more information about monitors, such as an explanation of local vs. remote monitors, see Monitors (see page 400).

12. Click a monitor to select it, then click OK.

A configuration dialog displays properties similar to those you see in the Infrastructure Manager probe configuration windows. The properties vary for each monitor. For information on the properties for a specific monitor, see the SOC Probes Configuration Reference (SOC-probes/index.htm).

**Note:** The properties you set for a monitor will be in effect for all computer systems in the group(s) the monitoring template is assigned to, unless you set monitor overrides. For more information, see Set a Monitor Override (see page 412).

13. Enter values for the monitor properties, then click OK.

The monitor is added to the list of monitors for the template.

14. Repeat these steps to edit or assign additional monitors to the monitoring template if wanted.

**Tip:** Select the name of a monitor, then click Summary to see a pop-up window listing some of the properties for the monitor.

15. When you are finished editing the monitors, click Close.

The Administration dialog closes.

**Reapply a Monitoring Template**

You can reapply monitoring templates to an individual computer system. You may wish to do this if you have changed the hardware configuration for that computer system, or if you have edited a monitoring template and do not want to wait for the updated settings to be pushed out to that computer system.

**Follow these steps:**

1. **Do one** of the following:
   - In the tree view, click the system you want to reapply a monitoring template to.
   - In a badge view, drill down to the system you want to reapply a monitoring template to.

2. **Click the Monitoring tab.**

3. **Right-click** in the table.
4. Choose **Update Monitoring Now** in the pop-up menu.

   The monitoring templates assigned to that computer system are reapplied to that system.

   **Note:** To see updates to the status area in this table, click the **Refresh group** icon (🔄). The refresh may take a few minutes.

### Applying Monitors to Systems

Typically you will want to create monitoring templates and assign them to groups in order to streamline monitor configuration. However, you can also apply a monitor to an individual computer system. You might want to do this if you want to apply a monitor that is not included in the monitoring template for the group(s) the system is a member of. Or, you may want to do this if you have a system that you want to apply only one monitor to.

Applying a monitor to an individual system is different than a monitor override, which allows you to apply different monitor settings than those specified in the monitoring template. With a monitor override, the monitor is included in the monitoring template, but the configuration settings are altered for the specified system.

Monitors applied to individual systems always take precedence over other monitors. If the same monitor is also included in a monitoring template for a group that the system is a member of, the configuration settings of the monitor applied to the system individually are used and the monitor settings in the monitoring template are ignored.

If the individual system monitor is deleted, the monitor settings from the monitoring template become the active settings.

**Note:** You must have the **USM Modify Individual Monitors for Computer Systems** permission in order to apply a monitor directly to a system (without a monitoring template).

### Apply a Monitor to a System

You can apply a monitor to an individual computer system.

**Follow these steps:**

1. Do one of the following:
   - In the tree view, click the system you want to apply a monitor to.
   - In a badge view, drill down to the system you want to apply a monitor to.

2. Click the **Monitoring** tab.

3. Click **Apply Monitors** in the bottom right of the Monitoring pane.

   The **Apply Monitors** dialog is displayed.
4. (Optional) To filter the list so you see only a certain category of monitors, choose a category from the Filter pull-down menu.

5. Click the Add monitor icon ( ).
   The Add Monitor dialog is displayed.

6. Click the monitor you want to add to select it.
   To filter the list so you see only a certain category of monitors, choose a category from the Category pull-down menu.
   If you do not see the monitor you want to apply in the list, verify that the probe that contains that monitor is installed and activated on the robot that manages the computer system.

7. Click OK.
   The configuration dialog for the monitor is displayed.

8. Enter configuration settings for the monitor.
   For information about monitor configuration settings, see the SOC Probe Configuration Reference (SOC-probes/index.htm).

9. Click OK.
   The monitor appears in the list in the Apply Monitors dialog.

10. Click Close to dismiss the Apply Monitors dialog.

11. To see the monitor in the Monitoring Status table of the Monitoring tab, click the Refresh groups icon ( ).
   It may take several minutes for the monitor to be added to the table.

**Delete a Monitor from a System**

You can delete a monitor that was applied to an individual computer system.

**Follow these steps:**

1. Do one of the following:
   - In the tree view, click the system you want to delete a monitor for.
   - In a badge view, drill down to the system you want to delete a monitor for.

2. Click the Monitoring tab.

3. Click Apply Monitors in the bottom right of the Monitoring pane.
   The Apply Monitors dialog is displayed.

4. (Optional) To filter the list so you see only a certain category of monitors, choose a category from the Filter pull-down menu.
Working with Monitors

5. Click the row of the monitor in the **Apply Monitors** dialog to select it.

6. Click the **Delete monitor** icon (❌).

**Edit a Monitor for a System**

You can edit a monitor that was applied to an individual computer system. Do this if you want to change the configuration settings for the monitor.

**Follow these steps:**

1. Do one of the following:
   - In the tree view, click the system you want to edit a monitor for.
   - In a badge view, drill down to the system you want to edit a monitor for.

2. Click the **Monitoring** tab.

3. Click **Apply Monitors** in the bottom right of the Monitoring pane.
   
   The **Apply Monitors** dialog is displayed.

4. (Optional) To filter the list so you see only a certain category of monitors, choose a category from the **Filter** pull-down menu.

5. Click on the name of the monitor in the **Apply Monitors** dialog.
   
   The configuration dialog for the monitor is displayed.

6. Edit the settings, then click **OK**.

7. Click **Close** in the **Apply Monitors** dialog.

**Set a Monitor Override**

You can set monitor properties to be applied to a specific computer system that are different than the properties configured in the assigned monitoring template. This is called a monitor override.

A monitor override is different than applying a monitor to an individual system. Applying a monitor to an individual system allows you to assign a monitor that is not included in the monitoring template.

**Follow these steps:**

1. In the tree, expand the group node that the system belongs to.

2. Click on the computer system.

3. Click the **Monitoring** tab in the right pane.

4. Click the <n> link in the **Overrides** column for the monitor you want to override.

5. In the **Configure Monitor Overrides** dialog, click **Add**.
6. In the Key field, choose the property from the pull-down menu that you want to override.

7. Enter a value in the Value field, then click OK.

**View Monitor Status**

You can view information about the monitors assigned to a computer system.

**Follow these steps:**

1. Do one of the following:
   - In the tree view, click the system you want to view monitoring information for.
   - In a badge view, drill down to the system you want to view monitoring information for.

2. Click the Monitoring tab.

   You see a table that contains this information:

   **Name**
   
   Name of the monitor assigned to the system.

   **Status**
   
   Status of the monitor, such as OK, no robot found, or collision. No robot found means that a Nimsoft robot is not installed on the computer system. If there is a collision, you can designate which monitor takes precedence in one of the following ways:
   
   - If the collision occurs because the system is assigned to multiple groups that have monitoring templates with the same monitors, you can assign priorities to the groups. For information on setting priorities, see *Priority* (see page 402), and for information on viewing the groups assigned to a system, see *Viewing Group Assignments* (see page 399).
   
   - If the collision occurs because the system is assigned to a single group that has multiple monitoring templates with the same monitors, you can arrange the order of monitoring templates assigned to the group. In the Monitoring Templates tab, use the Move Up and Move Down icons below the Linked list to designate the order of monitoring templates. The monitor associated with the monitoring template higher in this list takes precedence.

   **Group**
   
   Group the monitoring template is assigned to.

   **Last Update**
   
   Date and time the monitor properties were last updated.
Working with Alarms

**Template**

Monitoring template that the monitor is associated with.

**Overrides**

Number of monitor overrides. This number is also a link to the Configure Monitor Overrides dialog. For more information, see Set a Monitor Override (see page 412).

---

**Working with Alarms**

Administrators and other authorized users can view and manage alarms in USM.

You can view alarms for a group or for an individual system. Alarm data is summarized in a bar chart, and alarms can be displayed in a list or a table. You can filter alarms or change the way the data is sorted. You can also view a graph of the associated performance metric, if there is one, and view alarm history.

Authorized users can assign and acknowledge alarms. Administrators can set alarms to invisible so they are hidden from other users, and can view invisible alarms.

To support multi-tenancy, you see and can take action only on alarms from your origin.

**Note:** You must have the **Acknowledge**, **Accept**, **Assign**, or **Unassign** permissions set in the Access Control List (ACL) in order to take those actions on alarms. You must have the **Invisible Alarms** permission in order to set alarms as invisible and to view invisible alarms.

---

**View Alarms**

You can view alarms for a group or for a system in the USM **Alarms** tab. The **Alarms** tab includes a summary chart and a list view or table view that you can toggle between.

**To access the Alarms tab, follow these steps:**

1. In the USM tree view, click on the name of the group or system you want to view alarms for.
2. Click the **Alarms** tab.

**Note:** Some alarms are not associated with a group or a system. These alarms are displayed under the **Groups** node in USM.
Alarm Summary Chart

The alarm summary chart displays a bar graph of alarm data for the selected group or system.

By default, the data is grouped by severity. To change the grouping, choose an item from the pull-down menu at the top of the summary chart.

Click on a column in the summary chart to display only that data in the list or table view. To return to viewing all data for the group or system, do one of the following:

- Click the column again.
- Click the X next to the name of the filter in the toolbar above the alarm list or alarm table.
- Choose Clear Filters from the Actions menu. Locked filters are not removed by choosing this menu option.

Click the arrow in the upper right corner of the summary chart to hide the chart; click it again to display the chart.

Alarm List

The alarm list displays details about alarms for the selected group or system. Click the List icon ( ) in the Alarms tab to access the alarm list.

Hover over an item to see what type of information the item contains. For example, the first line contains the Alarm Status icon, Member Details icon, host name, subsystem, origin, and update time. Hover over the alarm message to see the entire message.

Click the following items to filter by that value in the alarm summary chart and the list:

- Alarm Status icon
- Host
- Subsystem
- Origin
- Owner

Click the item again to clear the filter. Or, click the lock icon ( ) next to the filter name to retain the filter when you view alarms for other groups or systems.
Click the MORE button to access more items you can click on to filter the data:

- Hub
- Robot
- Source
- Probe
- Assigned By
- User Tag 1
- User Tag 2
- Custom fields (by default named Custom 1 through Custom 5)

Click the Member Details icon, displayed as the icon for the device, to display the device view for the system. To return to the alarm list, click an Alarm Status icon in the device view.

Click the check box next to an alarm to select the alarm. If at least one alarm is selected, the Actions menu is activated. You can also choose Select All and Clear Selected from the Actions menu to select or deselect all alarms.

Click the following icons:

- Acknowledge icon (✓) to acknowledge an alarm
- Set visible/Set invisible icons (☐/☐) to set whether the alarm is hidden
- Assign icon (✎) to change who owns the alarm

Click the MORE button to view more information about the alarm in the Details, History, and Metric tabs.

**Details tab**

Displays information about the alarm, such as the hub and robot that issued the alarm, the probe that collected the data, and any User Tags assigned to the robot.

**History tab**

Displays a table listing timestamps, messages, and assignment actions for the alarm.
Metric tab

Displays a graph with data for the performance metric the alarm was generated for, if appropriate. For example, if the alarm was generated because a threshold for CPU usage was exceeded, the graph displays CPU usage data. The alarm occurrence is indicated on the chart by a circle. Data is displayed for the last 24 hours, unless the alarm is more than 24 hours old, in which case data is displayed for 12 hours before and after the alarm time. Click the Show current data icon to view data for the last 24 hours; click the Show alarm data icon to return to 12 hours before and after the alarm.

Click the Pop out icon in the upper right corner of the graph to display the data as a Performance Report in a new window. This allows you to use additional features in Performance Reporter, such as changing the time interval for the data displayed.

If the alarm is not related to performance data, you see a message stating No metric available when you click the Metric tab. For example, alarms stating that a system rebooted or that a process failed to start do not have performance data associated with them.
Set Custom Alarm Fields

Authorized users can enter text in five custom fields for selected alarms, and the text is displayed in the alarm list view. You may want to use these fields to enter information about who to contact when certain alarms occur, instructions on how to resolve the alarms, or general notes about the alarms. Or, the Nimsoft alarm_enrichment probe can be used to automatically add information such as device information (serial numbers, for example) or contact information to the custom text fields. For more information about the alarm_enrichment probe, see the documentation for nas in the *Library of Nimsoft Probe Guides*.

You must have the **Alarm Management** permission in your Access Control List (ACL) in order to enter text in the custom alarm fields.

By default, in USM these fields are named **Custom 1** through **Custom 5**. Administrators can change the name of these fields in the Raw Configure window for the Nimsoft Alarm Server (nas).

The text you enter in the custom fields is viewed by clicking the **More** button in the alarm list view. Or, you can add the columns for the custom fields to the alarms table view.

**Note:** The custom text fields are displayed in the alarms list view only if text has been entered for the field.

Click on a custom field to filter alarms by that field. You can also group information in the alarm summary chart by custom fields by choosing a custom field from the pull-down menu.

**Follow these steps:**

1. In the tree view, click the name of a group or a system that you want to view alarms for.
2. Click the **Alarms** tab.
   
   The alarms are displayed.
3. Select one or more alarms by clicking the check box next to the alarm(s) or by choosing **Select All** from the **Actions** menu.
4. Choose **Set Custom** from the **Actions** menu.
   
   The **Set Custom** dialog is displayed.
5. Select the fields you want to enter a value for, then enter the desired text.
   
   **Note:** Existing text for custom fields is not displayed in the Set Custom dialog. Text you enter overwrites any existing text.
6. Click **OK**.
7. In the alarms list view, click More for one of the alarms you selected. Or, in the alarms table view choose Edit Columns from the Actions menu and select one or more custom fields.

The custom fields you entered text for are now displayed.

**Change Names of Custom Fields**

The default names for the custom text fields for alarms are Custom 1 through Custom 5 in USM. Administrators can change the name of these fields in the Raw Configure window for the Nimsoft Alarm Server (nas).

**Follow these steps:**

1. Use Infrastructure Manager to open the Raw Configure window for the nas probe:
   a. Select the nas probe.
   b. Press the Ctrl key and right-click on the nas probe.
   c. Choose Raw Configure.
2. Add the setup > custom_headers folder, then open the folder.
3. Click New Key.
   The New Key dialog is displayed.
4. Enter the following values:
   a. Key name = custom_1 through custom_5
   b. Value = The name you want as the label for the field
5. Click OK, then click OK again to close the Raw Configure window.
6. Restart the USM webapp in the wasp probe:
   a. In Infrastructure Manager, double-click on the wasp probe to launch its configuration GUI.
   b. Click the webapps tab.
   c. Right-click USM.
   d. Click Stop.
   e. Click Start.

**Delete Text from Custom Fields**

You can delete text from a custom alarm field.

**Follow these steps:**

1. In the Alarms tab, select one or more alarms by clicking the check box next to the alarm(s) or by choosing Select All from the Actions menu.
2. Choose **Set Custom** from the **Actions** menu.
   The Set Custom dialog is displayed.

3. Select the fields you want to remove text for.

4. Leave the text field(s) blank.
   **Note:** Existing text is not displayed in the Set Custom dialog. Leaving it blank removes any existing text.

5. Click **OK**.

6. In the Alarms list view, click **More** for one of the alarms you selected.
   The custom fields you removed text for are no longer displayed.

**Alarm Table**

The alarm table displays information about alarms in a table format for the selected group or system. Click the table icon (tablise) in the **Alarms** tab to access the alarm table.

Click the check box next to an alarm to select the alarm. If at least one alarm is selected, the **Actions** menu is activated. You can also choose **Select All** and **Clear Selected** from the **Actions** menu to select or deselect all alarms.

Click the Alarm Status icon to display only alarms of that status in the alarm summary chart and the table. Click the Alarm Status icon again to clear the filter.

Click the Member Details icon, displayed as the icon for the device, to display the device view for the system. To return to the alarm list, click an Alarm Status icon in the device view.

Click a column header to sort the table data by that column.

You can change the columns displayed in the table by choosing **Edit Columns** from the **Actions** menu and selecting the columns you want to display.

**Note:** You can set values for the columns **Custom 1** through **Custom 5** by selecting one or more alarms and choosing **Set Custom** from the **Actions** menu.
Manage Alarms

You can accept, assign, unassign, or acknowledge (clear) alarms in the USM Alarms tab.

Note: You must have the Acknowledge, Accept, Assign, or Unassign permissions set in the Access Control List (ACL) in order to take those actions on alarms.

Follow these steps:
1. In the tree view, click the name of a group or a system that you want to manage alarms for.
2. Click the Alarms tab.

   The alarms information is displayed. By default, the list view of alarms is displayed. Click the table icon ( ) and list icon ( ) to toggle between the two alarm views.
3. In the list view, do one of the following:
   - Click the Acknowledge icon ( ) to acknowledge an alarm.
   - Click the Assign icon ( ). In the popup menu, choose Accept, Assign, or Unassign.
   - Click the check box to select one or more alarms, then choose Accept, Assign, Unassign, or Acknowledge from the Actions menu.
   - From the Actions menu, choose Select All, then choose Accept, Assign, Unassign, or Acknowledge.
4. In the table view, do one of the following:
   - Click the check box to select one or more alarms, then choose Accept, Assign, Unassign, or Acknowledge from the Actions menu.
   - From the Actions menu, choose Select All, then choose Accept, Assign, Unassign, or Acknowledge.

Working with Invisible Alarms

Administrators can set whether or not an alarm is visible to other users. You may want to set some alarms to invisible to hide them if they are not relevant to other users.

You can quickly set a single alarm to invisible (or visible) by clicking an icon, or you can select multiple alarms and set them to invisible (or visible) by choosing a menu item.

Note: You must have the Invisible Alarms permission in order to set alarms as invisible and to view invisible alarms.
Set a Single Alarm to Invisible

You can quickly set whether a single alarm is visible by clicking an icon in the alarms list view.

**Note:** You must have the **Invisible Alarms** permission in order to set alarms as invisible and to view invisible alarms.

**Follow these steps:**
1. In the tree view, click the name of a group or a system that you want to manage alarms for.
2. Click the **Alarms** tab.
   The alarms information is displayed.
3. Click the list view icon (imulator).
4. Click the Set visible/Set invisible icons (imulator) to set whether an alarm is hidden for users who do not have the **Invisible Alarms** permission.

Set Multiple Alarms to Invisible

Administrators can filter or sort to find certain types of alarms and then set multiple alarms to invisible (or visible).

**Note:** You must have the **Invisible Alarms** permission in order to set alarms as invisible and to view invisible alarms.

There are several tools that allow you to filter and sort visible and invisible alarms.

To see what other users (who do not have the **Invisible Alarms** permission) will see, choose **Hide Invisible** from the **Actions** menu. All invisible alarms are hidden, and the Visibility filter is listed on the toolbar. Choose **Show All** or click the X icon next to the filter to display the invisible alarms again.

To see how many alarms are visible and invisible, in the list view group the alarm summary chart by choosing **Visibility** from the pull-down menu. To see only invisible alarms, click the **Invisible** column in the alarm summary chart.

In the table view, you can add the Visibility column to the table (choose **Edit Columns** from the **Actions** menu). As with all columns in the table, click the **Visibility** header to sort the table by that column.

**Follow these steps:**
1. In the tree view, click the name of a group or a system that you want to manage alarms for.
2. Click the **Alarms** tab.
   
   The alarms information is displayed.

3. Click the list view icon ( '..' ).

4. Select the alarms you want to set to invisible. You can do this by:
   
   - Clicking check boxes next to the alarms
   - Choosing **Select All** from the **Actions** menu
   - Clicking a column in the alarm summary chart to filter for alarms in that column, then choosing **Select All** from the **Actions** menu
   - Entering text in the **Quick Filter** field to display only alarms that contain that text, then choosing **Select All** from the **Actions** menu

5. Choose **Set Invisible** from the **Actions** menu.

### Filter Alarms

There are several ways you can filter alarm data to display only the data you want to see.

- Click a column in the alarm summary chart to display only that data in the summary chart and in the list or table. For example, if the chart is sorted by severity, click on the column for major alarms to see only alarms of major severity.

- Enter text in the Quick Filter field to do a full-text search of alarm data. For example, to find alarms for the dashboard_engine probe, enter `dashboard_engine` in the Quick Filter field and all alarms with "dashboard_engine" in a text field, such as the alarm message, are displayed.

- Click items in the alarm list or table (the Alarm Status icon, host, subsystem, and so on). For example, to view only alarms related to SLA agreements, click a subsystem item that says **SLA**.

You can combine these methods or click multiple items in the alarm list to apply multiple filters. Active filters are listed in the toolbar above the alarm list or alarm table.

You can lock a filter by clicking the lock icon (  ) next to the filter name. When a filter is locked, it is retained when you view alarms for a different group or system.
For example, you are viewing alarms for a group named Servers and you click the Critical column in the alarm summary chart so that you are filtering for only critical alarms. You click the lock icon to lock the Critical filter, then click on a system in the group named db_server. Because the Critical filter is locked, you see only critical alarms for db_server.

You can lock multiple filters, and you can lock some filters and leave others unlocked.

There are several ways to clear filters:

- Choose Clear Filters from the Actions menu to remove all unlocked filters. Locked filters are not removed by choosing this menu option.
- Click the X next to the name of the filter in the toolbar above the alarm list or alarm table.
- If you clicked a column in the alarm summary chart, click the column again to remove the filter.
- If you clicked an item in the alarm list or alarm table, click the item again to remove the filter.

**Sort Alarms**

You can change the sorting of alarm data in the alarm list and alarm table.

To change the sorting of data in the alarm list or alarm table, choose an item from the pull-down menu in the toolbar above the alarm list or table. The sorting you choose is retained when you switch between the alarm list and alarm table.

In the table, click a column header to sort by that column. This updates the Sort by pull-down menu and also sorts the list.

**Viewing System Information**

You can view information about individual computer systems. The System tab displays information about system properties and performance. The Metrics tab displays data for the metrics monitored on the system.

**Follow these steps:**

1. Do one of the following:
   - In the tree view, click the system you want to view system information for.
   - In a badge view, drill down to the system you want to view system information for.
2. Click the System tab or Metrics tab.
View System Properties

The **System** tab displays information about system properties, disk usage, interface traffic, and system performance. The information displayed depends on the data available. Items that have no value available for the system are omitted.

The icons in the **Alarms** section indicate the number of alarms of each severity level for the system. Click an alarm icon to view the related alarms in the **Alarms** tab.

If disks are monitored on the system, the **Disk Usage** table is displayed. Disks are monitored if the cdm (local) or rsp (remote) probe, or a storage probe, is installed and configured to monitor disks on the system.

The **Disk Usage** table contains a bar for each disk indicating percent of disk usage (or, in the case of some storage probes, percent of disk free). Click the bar to view a Performance Reports chart of disk usage data for the past 24 hours.

**Note:** You can use the time selection buttons on the bottom toolbar to change the time interval for Performance Reports.

The alarm status icon in the **Disk Usage** table indicates the highest severity alarm for the disk. Click the alarm icon to view related alarms in the **Alarms** tab.

If interfaces are monitored on the system (the interface_traffic probe is installed and configured), the **Interface** table is displayed. Click an interface name in the table to view a Performance Report with data about interface traffic for the past 24 hours.

The alarm status icon in the **Interface** table indicates the highest severity alarm for the interface. Click the alarm icon to view related alarms in the **Alarms** tab.

If performance and network response are monitored on the system, you see Performance Reports charts in the right pane of the **System** tab. The charts displayed depend on which probes are deployed and configured to monitor the system. For example, if the cdm (local) or rsp (remote) is collecting data, charts with data on CPU and memory usage are displayed. The charts include an icon indicating alarm status for the metric displayed on the chart.

The charts display data for the previous 24 hours. If data is missing for that interval (for example, if the probe is disabled), the chart is not displayed.

**More information:**

[Device Performance Charts Reference](see page 426)
# Device Performance Charts Reference

The following table lists the performance charts displayed for each device type.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Performance Charts</th>
</tr>
</thead>
</table>
| VMware      | ■ CPU Reserved Capacity  
             | ■ CPU Usage            
             | ■ CPU Overall Usage (pool)  
             | ■ Disk Latency          
             | ■ Disk Read Rate        
             | ■ Disk Write Rate       
             | ■ Memory Balloon        
             | ■ Memory Granted        
             | ■ Memory Reserved Capacity  
             | ■ Memory Usage          
             | ■ Network Data Receive Rate  
             | ■ Network Data Transmit Rate  
             | ■ VM Count              
             | ■ VM Count Active       
             | ■ Datastore Free        
             | ■ Memory Overall Usage  
             | ■ CPU Usage             
             | ■ Guest Disk Free       
             | ■ Guest Memory Usage    
             | ■ Host Memory Usage     
             | ■ Overall CPU Usage     
<pre><code>         | ■ Power State           |
</code></pre>
<table>
<thead>
<tr>
<th>Device Type</th>
<th>Performance Charts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>CPU Last 5 Minutes</td>
</tr>
<tr>
<td></td>
<td>Memory Free</td>
</tr>
<tr>
<td></td>
<td>Big Buffer Misses</td>
</tr>
<tr>
<td></td>
<td>Huge Buffer Misses</td>
</tr>
<tr>
<td></td>
<td>Very Large Buffer Misses</td>
</tr>
<tr>
<td></td>
<td>Large Buffer Misses</td>
</tr>
<tr>
<td></td>
<td>Medium Buffer Misses</td>
</tr>
<tr>
<td></td>
<td>Small Buffer Misses</td>
</tr>
<tr>
<td>Server</td>
<td>Total CPU Load</td>
</tr>
<tr>
<td></td>
<td>Processor Queue Length</td>
</tr>
<tr>
<td></td>
<td>Memory Paging</td>
</tr>
<tr>
<td></td>
<td>Total Memory Used</td>
</tr>
<tr>
<td></td>
<td>Physical Memory Used</td>
</tr>
<tr>
<td></td>
<td>Memory Swap</td>
</tr>
<tr>
<td></td>
<td>Total Memory Used</td>
</tr>
</tbody>
</table>
View Metrics

The **Metrics** tab allows you to see data for all metrics that are monitored on a system.

Metrics are listed in a hierarchical tree. Click a node in the tree to view graphs of the last 24 hours of data, if available, for that node. Nodes at any level of the tree may have data, and available data is indicated by the ➔ icon next to the node name.

**Note:** if you want to view data for an interval other than the last 24 hours, click the Pop out icon (⃣) in the upper right corner of the graph to display the data in Performance Reports Designer. From there you can use the time selection buttons at the bottom of the chart to change the time interval.

Any system that has ever had monitoring data collected is displayed as a node in the **Metrics** tree. However, if the system is no longer monitored, no data is displayed.

For virtual machines (VMs), data is grouped under either the **Virtual Machine** or **Hypervisor** nodes in the tree. Under the **Virtual Machine** node, the VM server, physical host, and VMs (guests) are all displayed.

**Note:** VMs, the VM server, and the physical host are all displayed under the **Virtual Machine** node in the **Metrics** tab. It is recommended that you use a naming convention that allows you to distinguish these components.

Click the **Hypervisor** node to view data about the number of VMs installed and active. You may see more VMs listed in this data than appear in the tree under the **Virtual Machine** node since only monitored VMs appear in the tree. Nodes under the **Hypervisor** node display data about CPU, memory, and resource pool usage.

Display Metrics for Custom Probes

If you have a custom probe, you must include functions provided by the Nimsoft SDK so that data from the probe is displayed in USM. Your probe must create:

- Configuration Items (CIs) to represent monitored items (devices, disks, virtual machines, etc.)
- QoS metrics to contain data from the probe
- Devices to represent the local or remote system that is being monitored

Your probe must link these items to the appropriate alarms and QoS metrics.

For more information about the SDK, see the [Nimsoft Monitor Solution > SDK Products](#) documentation in the [Nimsoft Library](#).
Following are two examples.

**Example Perl Script for Monitoring a Local Directory**

This example creates a CI that represents a directory on the local system where the probe is running and a QoS metric for available space in the directory. The example uses the function `ciOpenLocalDevice` to create the device to represent the local system. If the item you are monitoring is remote from the system where the probe is running, use the function `ciOpenRemoteDevice` to create a device to represent the system.

```perl
#!/bin/perl
use lib "perllib/";
use Nimbus::API;

$ENV{'NIM_ROOT'} = '/opt/nimsoft';
nimInit(0);

# NIS2 - Local device example
#
# This example shows how to create a CI representing
# a directory on the local system, and a metric representing
# the available space on that directory. A device that represents
# the local computer system where this probe is running is
# also created by the ciOpenLocalDevice function.
#
my $dirName = "/var";
my $dirCiType = "1.11"; # System.Directory
my $dirMetric = "3"; # Directory Space in KB
my $dirSpace = 100; # Measurement - 100 KB remaining
my $hCI = ciOpenLocalDevice($dirCiType, $dirName);

# Send an alarm for the CI and metric ID
my ($rc,$szId) = ciAlarm($hCI, $dirMetric, 3, "$dirName space is low");

# Define a QoS metric for directory space
my $qosName = "QOS_DIRECTORY_SPACE";
my $qosGroup = "QOS_MACHINE";
my $qosDescr = "Directory Space";
my $qosUnit = "Kilobytes"
my $qosUnitAbbr = "KB";
my $qosInterval = 300;
my $qosSource = ""; # Nimsoft SDK will use the local host address

my $rc = nimQoSSendDefinition($qosName, $qosGroup, $qosDescr, $qosUnit, $qosUnitAbbr);
my $hQoS = nimQoSCreate($qosName, $qosSource, $qosInterval);

# Bind the CI to QoS (establish their relationship)
```

my $rc = ciBindQoS($hCI, $hQoS, $dirMetric);

# Send the QoS data point
my $rc = nimQoSSetValue($hQoS, $dirName, $dirSpace);

# Clean up
my $rc = ciUnBindQoS($hQoS);
my $rc = nimQoSFree($hQoS);
my $rc = ciClose($hCI);

nimEnd(0);
Example NimRecorder Script for e2e_appmon Probe

This example, created using the NimRecorder scripting wizard provided with the developer edition of the probe (e2e_appmon_dev), creates CIs that represent each web page that is monitored ("Support" and "Downloads"). The example also sends QoS measurements for the time it took to render each web page.

The NimRecorder is launched by choosing the Programs > Nimsoft Monitoring > E2E Scripting menu option. For more information about using NimRecorder, see the documentation accessed from the Help menu in the NimRecorder application window.

```nim
include "NimBUS-functions.src"
nimSetCi("3.21", "Support", ",", "1")
nimInit()

StartBrowser("IE", "www.nimsoft.com", 3)

target\$= "Support"
nimQoSStart()

UsePage("ITSM + Service Desk + IT Monitoring: Better Together - Nimsoft")
  ClickHTMLElement("A[INNERTEXT= 'support']")

nimQoSStop()

nimQoSSendTimer(target\$)

nimSetCi("3.21", "Downloads", ",", "1")
nimInit()
target\$= "Downloads"
nimQoSStart()

UsePage("ITSM and ITIL-based Support and Service That You Can Count On - Nimsoft")
  ClickHTMLElement("A[INNERTEXT= 'Downloads',INDEX='2']")

nimQoSStop()

nimQoSSendTimer(target\$)

CloseWindow("IEXPLORE.EXE|IEFrame\|Nimsoft - Windows Internet Explorer",1)

CloseWindow("IEXPLORE.EXE|IEFrame\|ITSM and ITIL-based Support and Service That You Can Count On - Nimsoft - Windows Internet Explorer",1)

nimEnd()
```
Working with Reports

In USM administrators can assign report templates to groups. Once a report template is assigned to a group, users can view the report for any system in the group.

USM comes with a default report template. In addition, there are ready-made report templates with server usage and performance information. You can find these in the Reports Template dialog (see Assigning Report Templates to Groups (see page 432)), in a folder named USM Dynamic Report Templates. These reports are:

**Server Basic**

Displays information on total CPU usage, system CPU usage, user CPU usage, idle CPU usage, wait CPU usage, percent of memory used, percent of physical memory used, megabytes of memory used, megabytes of swap memory used, paging memory used, and disk space usage.

**Server Load**

Displays information on CPU and processor queue length and megabytes of physical and swap memory used.

**Server Performance**

Displays information on total CPU usage, user and system CPU usage, CPU processor queue length, percent memory used, megabytes of physical and swap memory used, total megabytes of memory used, and disk space usage.

Administrators can also create reports in the Performance Reports Designer and assign them as report templates to groups in USM.

Administrators can designate which report template is the default report. The default report is launched when users click the Reports button. There must be one report template designated as the default, and the default template cannot be deleted.

Assigning Report Templates to Groups

Administrators who have the USM Group Modification permission can assign report templates to groups in USM. Once you assign the report template to a group, users can view the report for any system in the group.

To assign report templates to a group:

1. In a badge or tree view, click on a group and choose Edit Group from the Actions menu. Or, in the tree view mouse over the name of a group and click the Edit Group icon.

   The Edit Group <Group Name> dialog is displayed.

2. Click the Report Templates tab.
3. Click Add Template.
   The Report Templates dialog is displayed. If you are an account user, you see only
   the report templates that are not private to another account or to another user.
   Otherwise, you see all report templates that are not private to another user.

4. Select the report template you want to add, then click Add.
   The report template you added is assigned to the selected group and all groups and
   systems under it in the tree.

5. (Optional) To select a report template as the default report for the group, click the
   radio button in the Default column for that template.
   The default template is the report launched when users click the Reports button in
   USM. There must be one report template designated as the default, and the default
   template cannot be deleted.

Viewing Reports

To view a report for a computer system:

1. Do one of the following:
   ■ In the tree view, click the system you want to view a report for.
   ■ In a badge view, drill down to the system you want to view a report for.

2. To view the default report, click the Reports button. To select another report, click
   the arrow next to the Reports button and choose the report from the pull-down
   menu.
   The report data is displayed in a new browser window.

Launching a Standalone USM

You can launch USM in a browser window as a standalone application (outside of UMP). You
may want to do this if you want to link to USM from another application, or if you
want to display data for a group or system in USM on a web page.

The standalone USM opens in a new browser window. Because it is a standalone version
of USM, you cannot navigate to other UMP portlets or change UMP settings from this
window.

There are two ways to launch a standalone USM window: using a URL, and using an
HTML file. Using a URL is simple and flexible. Using an HTML file allows you to hide the
user name and password or to incorporate USM in another web page (displaying it in a
frame, for example).
Launching USM with a URL

You can launch a standalone version of USM using a URL with the following syntax:

\[
\text{http://<host name or IP address>/usm/jsp/standalone.jsp?user=<user name>&password=<user password>}
\]

This displays USM in the tree view with the root Group node selected.

You can omit the user name and password from the URL. In this case, the user is prompted for a user name and password when the URL is executed.

Specify a Group OR a System

You can specify a group or computer system to display by appending the parameters described in the following table to the URL. USM searches from the top of the tree and displays the first instance of the group or system name in the tree.

For group or system names that contain a space, you can enter either a space or a + in the URL. The parameters are not case-sensitive.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Example(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Name of the group you want to display. Enter the full name of the group.</td>
<td>ump_server/usm/jsp/standalone.jsp?user=admin&amp;password=myump&amp;group=acme</td>
</tr>
<tr>
<td>grp_id</td>
<td>ID number of group from the cm_group table. Obtain the ID number by querying your Nimsoft database.</td>
<td>ump_server/usm/jsp/standalone.jsp?user=admin&amp;password=myump&amp;grp_id=530</td>
</tr>
</tbody>
</table>
| device    | Host name or IP address. If you specify the fully-qualified host name, the first instance of the host is displayed. If you enter part of the host name, the first instance of a host that contains that text in the name is displayed. If the system you specify exists but does not belong to a group, the standalone USM displays it under the Search node of the tree. | ● ump_server/usm/jsp/standalone.jsp?user=admin&password=myump&device=server1.acme.com  
  ● ump_server/usm/jsp/standalone.jsp?user=admin&password=myump&device=172.24.135.16  
  ● ump_server/usm/jsp/standalone.jsp?user=admin&password=myump&device=server1 |
| cs_id     | ID number of the computer system from the cm_computer_system table. Obtain the ID number by querying your Nimsoft database. | ump_server/usm/jsp/standalone.jsp?user=admin&password=myump&cs_id=271  |
**Parameter** | **Value** | **Example(s)**
--- | --- | ---
view | USM view to display. If no view is specified, the standalone USM opens in the tree view. Possible values are:
| badge or badge 1 - Displays USM in the badge 1 view
| badge2 - Displays USM in the badge 2 view
| badge3 - Displays USM in the badge 3 view
| alarms - Displays USM with the **Alarms** tab displayed

### Specify a Group AND a System

You can specify both a group and a system by using the `group` or `grp_id` parameter and the device or `cs_id` parameter. For example:

```java
ump_server/usm/jsp/standalone.jsp?user=admin&password=myump&group=acme&cs_id=271
```

### Specify a Path

You can display a specific group or system, rather than having UMP search from the top of the tree, by including the path to the group or system in the USM tree structure.

Begin the path with a slash; you can use either forward slashes (`/`) or back slashes (`\`). If you have a group with a forward slash in the name, use back slashes to specify the path, and vice versa. Do not include the root **Group** node in the path.

For example:

- `ump_server/usm/jsp/standalone.jsp?user=admin&password=myump&group=\customers\acme`
- `ump_server/usm/jsp/standalone.jsp?user=admin&password=myump&device=/customers/acme/server1`

### Which Item is Displayed?

This topic looks at some examples to illustrate how the URL syntax works. We have the following tree structure.
The following table lists values for the group parameter and describes the results for each value.

<table>
<thead>
<tr>
<th>Group Value</th>
<th>Group Selected</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group=test</td>
<td>![Test (30)]</td>
<td>The first group in the tree named Test is selected.</td>
</tr>
<tr>
<td>group=/test/test</td>
<td>![Test (30)]</td>
<td>The initial slash indicates a path, so the Test subgroup is selected.</td>
</tr>
<tr>
<td>group=test/test</td>
<td>![Test (30)]</td>
<td>Without an initial slash the text is treated as a group name, not a path, and the Test/Test group is selected.</td>
</tr>
</tbody>
</table>

**Errors**

This section describes error messages you may see when launching a standalone USM with a URL.

**System Not Found**

_The member <system name or cs_id> was not found._

**Reason:**
The specified system name or cs_id does not exist.

**Action:**
Enter a valid system name or ID.
Group Not Found

The group <group name> was not found.

Reason:
The specified group name or grp_id does not exist.

Action:
Enter a valid group name or ID.

Launching USM using an HTML File

You can use an HTML file to launch the standalone USM. You may want to do this if:

■ You do not want to pass parameters, such as user name and password, in a URL
■ You want to display the standalone USM as part of an HTML page, such as in a frame

Follow these steps:

1. Create an HTML file with the following syntax:

   <html>
   <body onload="javascript:document.autoForm.submit()">
   <form name="autoForm" method="post" action="http://<UMP SERVER>/usm/jsp/standalone.jsp">
       <input type="hidden" name="group" value="<GROUP NAME>">
       <input type="hidden" name="device" value="<DEVICE NAME OR IP>">
       <input type="hidden" name="user" value="<USER NAME>">
       <input type="hidden" name="password" value="<USER PASSWORD>">
   </form>
   </body>
   </html>

2. Execute the HTML file.

   For example, enter the path to the file as a URL in a browser:

   http://<SERVER>/<PATH TO HTML FILE>

   The standalone USM opens in a browser window without displaying parameters in the URL.
3. (Optional) To display the standalone USM as part of an HTML page, refer to the HTML file created in step 1 on your HTML page.

For example, to display USM in an iframe, include syntax similar to the following in your HTML page:

```html
<html>
<body>
  <iframe src="http://<SERVER>/<PATH TO HTML FILE>" width="100%" height="300" frameborder="0">
  </iframe>
</body>
</html>
```
Chapter 25: Unified Dashboards Guide


This document contains information about:

- How to update dashboards for existing users
- Which probes and QoS must be enabled to collect data for each dashboard
- A description of each dashboard
Chapter 26: Administration

This section contains the following topics:
- Single Sign On (see page 441)
- Set Automatic HTTPS Redirect (see page 442)
- Probe Updates (see page 442)
- Set Permissions for UMP Portlets (see page 443)
- Set up Email for UMP (see page 446)

Single Sign On

UMP supports SAML (Security Assertion Markup Language) 2.0-compliant single sign-on. Single sign-on allows users, once logged into your systems, to access UMP without logging in again.

SAML is an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).* Support for SAML-based authentication is available in a Software-as-a-Service (SaaS) model from a third-party company, AssureBridge.

In order to use the AssureBridge SAML single sign-on solution for UMP, you must have an identity server with a public URL.

For more information or to obtain single sign-on, contact AssureBridge:
- Email: info@assurebridge.com
- Phone: 1-888-409-6995
- Visit www.assurebridge.com

Set Automatic HTTPS Redirect

After you configure UMP to use SSL communications, you can also configure UMP so that any attempt to log in via HTTP is automatically redirected to HTTPS.

Follow these steps:

1. Locate the following directory:
   `<Nimsoft_installation>/Nimsoft/probes/service/wasp/webapps/ROOT/WEB-INF/classes`.
2. Open the file `portal-ext.properties` in a text editor.
3. At the bottom of the `portal-ext.properties` file, add the line `web.server.protocol=https`.
4. Save the `portal-ext.properties` file and restart the wasp probe.

UMP is now configured to redirect an HTTP login attempt to HTTPS.

Probe Updates

Probes in the Nimsoft Archive are automatically deployed to Nimsoft robots. However, if an updated version of the probe is placed in the Archive, the updated version of the probe is not deployed to robots where an earlier version of the probe is already installed.

An upcoming version of the product will manage version updates of probes. In the meantime, if you need to update the version of a probe installed on a robot you can do it manually using Infrastructure Manager. To update a probe using Infrastructure Manager, drag the probe package from the archive list and drop it on a robot node.
Set Permissions for UMP Portlets

In order to use UMP portlets, you must have the appropriate permissions set in the NMS Access Control List (ACL) for the user. If you try to access a portlet that you do not have the permission for, you see a "Permission Denied" message. ACL permissions are set in the Account Admin portlet or the NMS Infrastructure Manager.

The following portlets do not allow access to account contact users, regardless of permissions set:
- Dashboard Designer
- Nimsoft Remote Admin
- SLM

The following table describes the permissions for UMP portlets.

<table>
<thead>
<tr>
<th>Portlet</th>
<th>Required Permission(s)</th>
</tr>
</thead>
</table>
| Account Admin      | ■ Account Administration  
|                    | ■ Manage ACL - allows the user to edit ACL permissions                                  |
| Alarm Console      | ■ Alarm Details - allows the user to load the Alarm Console application.  
|                    | The following permissions allow the user to take the indicated action or view the indicated information in the Alarm Console portlet:  
|                    | ■ Accept  
|                    | ■ Unassign  
|                    | ■ Invisible Alarms  
|                    | ■ Alarm History  
|                    | ■ Acknowledge  
|                    | ■ Alarm Management  
|                    | ■ Assign  
|                    | ■ Reassign  
| Change Password    | ■ Change Password  

**Note:** In addition to having the Change Password permission set in the ACL, the user must be an account contact user in order to access this portlet.
### Set Permissions for UMP Portlets

<table>
<thead>
<tr>
<th>Cloud User Experience Monitor</th>
<th>Cloud UE Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Dashboards</td>
<td>Custom Dashboards</td>
</tr>
<tr>
<td>Dashboard Designer</td>
<td></td>
</tr>
<tr>
<td>Discovery Status</td>
<td>Discovery Pie</td>
</tr>
<tr>
<td>Dynamic Views</td>
<td>Dynamic Views Dashboards, Dynamic Views Reports</td>
</tr>
<tr>
<td>List Designer</td>
<td>List Designer</td>
</tr>
<tr>
<td>List Viewer</td>
<td>List Viewer</td>
</tr>
<tr>
<td>Maintenance Mode</td>
<td>Maintenance Mode</td>
</tr>
<tr>
<td>My Tickets</td>
<td>Service Desk</td>
</tr>
<tr>
<td>Nimsoft Remote Admin</td>
<td>Basic Management</td>
</tr>
<tr>
<td>Performance Reports Designer</td>
<td>QoS Access</td>
</tr>
<tr>
<td>Reports</td>
<td>Custom Reports</td>
</tr>
<tr>
<td>Report Scheduler</td>
<td>Report Scheduler</td>
</tr>
<tr>
<td>Service Desk</td>
<td>Service Desk</td>
</tr>
<tr>
<td>SLA Reports</td>
<td>SLM View</td>
</tr>
<tr>
<td>SLM</td>
<td>SLM Admin</td>
</tr>
<tr>
<td>Unified Reports</td>
<td>Unified Reports</td>
</tr>
</tbody>
</table>
| Unified Service Manager | USM Basic - allows the user read-only access to the portlet  
Note: The Basic Management permission also grants access to USM. However, Basic Management allows you to take additional actions in other Nimsoft Monitor applications, such as starting and stopping probes. MSPs who want to grant account contact users access to USM but want to restrict them from starting and stopping probes should enable the USM Basic permission and disable the Basic Management permission.  
USM Edit Monitoring Templates - allows the user to create, edit, and delete monitoring templates  
USM Group Modification - allows the user to create, edit, and delete groups  
USM Automatic Robot Installation - allows the user to enable and configure automatic deployment of agents (robots).  
USM Modify Individual Monitors for Computer Systems - allows the user to add a monitor directly to a system, without adding the monitor to a monitoring template. Also allows the user to edit these monitors.  
Alarm Management - Allows the user to enter text in five custom fields (by default named Custom 1 through Custom 5) for alarms.  
Invisible Alarms - Allows administrators to set whether an alarm is hidden for other users.  
The following permissions allow the user to take the indicated action on alarms in the USM Alarms tab:  
Accept  
Acknowledge (clear)  
Assign  
Unassign |
Set up Email for UMP

To enable UMP portlets, such as Report Scheduler, to automatically send emails you can configure email settings for UMP.

**Note:** To set up email for UMP you must be either a Nimsoft Monitor user with at least administrator privileges or an account contact user with administrator privileges.

To set up email for UMP:
- Configure Outgoing Mail Settings (see page 446)
- Configure the From Email Address (see page 447)

**More information:**

Choose a Job Delivery Method (see page 227)

Configure Outgoing Mail Settings

To have UMP automatically send emails, configure the settings for your outgoing mail server.

**To Configure Outgoing Mail Settings**

1. Choose the Manage, Control Panel menu option in UMP.
   
   The Control Panel is displayed.

2. Scroll down and click Server Administration.
   
   The Server Administration settings are displayed in the right pane.

3. Click the Mail link near the top.
   
   The mail server settings are displayed.

4. Enter information for your mail server in the Outgoing SMTP Server and Outgoing Port fields.

5. Enter information in other fields if appropriate for your mail server.

6. Click Save.
Configure the From Email Address

To have UMP automatically send emails, configure the From address to be used by these emails. Depending on your environment, the email feature may not work unless a valid From address is set.

**To Configure the From Email Address**

1. Open Infrastructure Manager.
2. Click on the robot for the primary hub in the tree view.
3. Click the wasp probe to select it in the top right pane.
4. Press CTRL and right-click, then choose Raw Configure from the popup menu.
5. Expand the webapps folder in the tree view of the Raw Configure window.
6. Click reportscheduler in the tree view.
   The Report Scheduler keys are displayed in the right pane.
7. Click New Key.
   The New Key dialog is displayed.
8. Enter email_from_address in the Enter key name field.
9. Enter the email address you want to use as a From address in the Enter value field.
   This must be a valid email address for your SMTP server.
10. Click OK, then click OK again to close the Raw Configure window.
11. Restart the wasp probe.
Chapter 27: Troubleshooting

This section contains the following topics:

- Single Time Zone Required (see page 449)
- LDAP Authentication with Active Directory Groups (see page 450)
- Custom Logo Missing (see page 450)
- Unified Service Manager Displays Non-localized Text (see page 450)
- Relationship Services Not Supported on Solaris (see page 451)
- I Cannot Access a Wiki Page I Created (see page 451)
- Page Titles May Contain Garbled Text (see page 452)
- Garbled Text in Console Installer (see page 452)
- Relationship Viewer Dependent upon Root Cause Analysis and Topology Manager (see page 453)
- Close Browser When Logging Out (see page 453)
- Size of Dashboard Panels (see page 453)
- Do Not Edit QoS Properties in SLM Portlet (see page 453)
- Turn Off Compatibility View with IE 8 or 9 (see page 454)
- Internet Explorer 8 Performance Issue (see page 454)
- Internet Explorer 8 Displays Page Title Incorrectly (see page 454)
- Portlet Not Resizing in Chrome (see page 455)
- User Names (see page 455)
- Internet Explorer 8 Cross-Site Scripting Issue (see page 456)
- Login Fails on Solaris (see page 457)
- Slow Performance on Internet Explorer 7/8 (see page 457)
- Non-ASCII Characters Stored Incorrectly in the Database (see page 457)
- Numeric Login IDs Do Not Work (see page 458)
- I Cannot Access the Control Panel (see page 458)
- Logging In Takes Me to the Login Page (see page 459)
- CSV File is Incorrect in Chinese or Japanese (see page 459)

Single Time Zone Required

For data time-stamping to work correctly across a distributed Nimsoft deployment, the Nimsoft Server, the UMP server, and the database server must all be set to the same time zone, regardless of the geographic locations of the servers.
LDAP Authentication with Active Directory Groups

In the Account Admin portlet, you can link a Nimsoft ACL to an Active Directory group so that users can authenticate using LDAP. However, a user’s primary group in Active Directory cannot be the same as the LDAP group you select for the Nimsoft ACL.

Custom Logo Missing

Symptom:
After I upgraded to UMP 2.5.x, my custom logo is missing.

Solution:
This is due to a change in the behavior of the third-party portal software, Liferay 6. In Liferay 5 custom images were stored in the database. In Liferay 6 custom images are stored on the file system, and Liferay cannot find existing custom images in the database. To resolve this, specify the custom image for the logo again.

Do the following steps:
1. Log into UMP as an administrator.
2. Click Manage, Control Panel from the menu bar.
3. Click Settings under Portal.
4. Click Display Settings under Miscellaneous on the right.
5. Click Change under Logo and browse to the image you want to use for the logo.
   A small .jpg file works best.
6. Click Save.
   Your pages now display the logo you specified.

You may also need to specify other custom images, such as for a user or organization, again.

Unified Service Manager Displays Non-localized Text

Valid after upgrading from NMS 5.12 to NMS 5.60 with non-English locales

In the Unified Service Manager portlet, if you select the Windows or UNIX server group in the left-hand navigation pane, the Description field in the right-hand pane displays English text, instead of the localized language.
Relationship Services Not Supported on Solaris

The Relationship Viewer portlet requires the IP address and port of the Graph Services within the relationship_services probe.

However, in this release of UMP, the relationship_services probe does not run on a Solaris hub. So if you run the installer from a Solaris primary hub, you are not presented with the option to specify the relationship_services probe location.

However, the relationship_services probe does not have to be on the primary hub, and it may actually be present somewhere else in your environment.

The installer will try to find a robot that is running the relationship_services probe. If that search is successful, the installer will use it to configure the Relationship Viewer portlet. If the search fails, the installer will not attempt to configure the Relationship Viewer portlet.

I Cannot Access a Wiki Page I Created

Symptom:
I create a page for a global wiki, but when I try to view the page I see this error: You do not have the required permissions.

Solution:
To resolve this, the owner of the wiki must grant Power User permissions for the wiki page.

Follow these steps:

Note: These steps must be done by the owner of the global wiki (the user who created the wiki).

1. Click Manage, Control Panel.
   The Control Panel is displayed.
2. Click Wiki under My Community.
3. Click the name of the wiki.
4. In the All Pages table, click Actions, Permissions for the page you want to allow access to.
   The permissions dialog for the wiki page is displayed.
5. Select all the check boxes for Power User, then click Save.
   All users can now access the wiki page.
Page Titles May Contain Garbled Text

Valid for non-English instances of UMP

Symptom:
I imported a LAR file, and now page titles in UMP are not displaying correctly.

Solution:
If this occurs, you may need to add an additional Java startup option to the wasp configuration to set the encoding to UTF-8.

Follow these steps:
1. In Infrastructure Manager, double-click the wasp probe.
2. Click the Setup tab.
3. At the bottom of the window, under the heading Extra Java VM arguments, enter the following text:
   -Dfile.encoding=UTF-8
4. Click OK.
5. Deactivate the wasp.
6. Activate the wasp.

Garbled Text in Console Installer

Valid on Windows systems

Symptom:
I see garbled characters when I run the installer in console mode for the Spanish or Brazilian Portuguese version of UMP.

Solution:
This is due to a defect in the third-party installation tool. We have requested a fix for this issue. In the meantime, the workaround is to run the installer in its default mode, which displays a graphical user interface (GUI).
Relationship Viewer Dependent upon Root Cause Analysis and Topology Manager

At present, the only source of data for the Relationship Viewer is the Nimsoft Root Cause Analysis and Topology Manager. Attempting to use Relationship Viewer without it generates an error message stating that there is no data to display. Contact Nimsoft sales for more information about Root Cause Analysis and Topology Manager.

Close Browser When Logging Out

When you log out of UMP it is important to also close the browser. This fully terminates active sessions. Otherwise, you may see unexpected behavior.

Size of Dashboard Panels

The size of the data returned for a dashboard panel should not exceed 5 MB. If it does you may observe either a slow response or scrollbars freezing or not scrolling the content in the dashboard. To estimate the data sent for a panel, use the following guidelines:

- Gauge, meter, slider: on average 50 bytes
- Chart: on average 50 bytes for each sample
- Table: size of data returned from query + overhead for each cell equal to (the length of the column name x 2) + 5 bytes

If the data for a panel is too large UMP logs a message and sends notification to the requesting client.

Do Not Edit QoS Properties in SLM Portlet

In the SLM portlet, you can expand the Quality of Service pane and view the various QoS in the database. If you open the Properties dialog for a QoS Definition, the fields in the dialog are editable. However, if you edit these fields, the data in the S_QOS_DEFINITION database table changes and conflicts with other database tables. This causes unwanted behavior in other portlets and with other functionality.

The only supported way to change QoS definitions is in the interface of QoS-enabled probes.

Important! Do not edit the fields in the Properties dialog of a QoS in the SLM portlet.
Turn Off Compatibility View with IE 8 or 9

If you use Microsoft Internet Explorer 8 or 9 to access UMP, you must turn off the Compatibility View for navigation menus to work properly. Check the Compatibility View Settings under the Tools menu in Internet Explorer to be sure Compatibility View is turned off for UMP.

Internet Explorer 8 Performance Issue

The 64-bit versions of Internet Explorer 8 and 9 do not work with UMP in a stable and consistent manner on all platforms of Windows. Currently only the 32-bit versions of Internet Explorer 8 and 9 are supported for use with UMP.

Internet Explorer 8 Displays Page Title Incorrectly

If you open certain portlets with Internet Explorer 8, and then click within the portlet, the pound or hash symbol (#) is displayed in the browser tab, rather than the portlet name.

This may occur with the following portlets:
- PRD
- SLM
- List Designer
- Custom Dashboards
- Unified Services Manager
- SQL Server Load (My SQL Server)
- Exchange
- Power
- Vblock
- Network
- Unified Reports
Portlet Not Resizing in Chrome

Valid for Google Chrome

Symptom:
When I resize my browser window, the portlet I'm using becomes unresponsive. If I try to close the window, a message referencing a memory error appears.

Solution:
A number of portlets may become unresponsive if you resize the browser window while using Google Chrome. This is due to an issue with Flash player in Chrome that can occur if you make the browser window very small, and then increase its size again.

If you experience this issue, refresh the browser to make the portlet display correctly again, and then avoid resizing the window while using Chrome.

User Names

Nimsoft Account Contact login IDs and user names must be in all lowercase characters.

Important! Do not use mixed-case names or uppercase names as they will not work properly in UMP.
Internet Explorer 8 Cross-Site Scripting Issue

Valid on Internet Explorer 8 Browser

Symptom:

When I use Internet Explorer 8 to launch a Performance Reports Designer report from a URL, I see an Information triangle that states:

Unable to locate new series.

http://10.0.4.113:8084/qoschart/jsp/standalone.jsp?user=administrator&password=t3sti9&def={'title':'My Report', 'info':'This is a test','tref':'S+10min,E-13hour','series':[{'sqt':'w2k8-vm5.i9.x|QOS_CPU_USAGE|System','style':'area','color':'666666'},{'sqt':'w2k8-vm5.i9.x|QOS_CPU_USAGE|User','style':'line','color':'222244'},{'sqt':'10.0.4.222|QOS_INTERFACE_PACKETS|PACKETS_IN-Intel(R) PRO/100 VE Network Connection - Packet Scheduler Miniport.','style':'col','color':'FFFF33'},{'sqt':'Phantom.i9.x|QOS_CPU_USAGE|User','scale':2,'style':'area','color':'008000'},{'sqt':'10.0.4.226|QOS_INTERFACE_PACKETS|PACKETS_IN-bge3','style':'line','color':'006633'},{'sqt':'w2k8-vm5.19.x|QOS_CPU_USAGE|User','series':[]}

Data not located for: 10.0.4.222|QOS_INTERFACE_PACKETS|PACKETS_IN-Intel(R) PRO/100 VE Network Connection - Packet Scheduler Miniport.

The IE information bar displays this message:

Internet Explorer has modified this page to prevent cross-site scripting.

Solution:

Usually this means a report template was applied to a system for which not all of the QoS objects were defined or that a QoS object was incorrectly specified in the URL.

To resolve this issue:

1. Choose Tools > Internet Options from the Internet Explorer menu bar.
2. Click the Security tab.
3. Click Trusted Sites.
4. Click Sites.
5. Add the site to the zone.
6. Uncheck Require server verification (https:) for all sites in this zone.
7. Click Close.
8. Click Custom level.
9. Scroll to near the bottom of the list of Settings and for Enable XSS filter click Disable.
10. Click OK to close the dialogs.
Login Fails on Solaris

Symptom:
After I install UMP on Solaris I try to log in as the administrator user and the login fails.

Solution:
Use Infrastructure Manager to log into the hub. This prompts Nimsoft Monitor to create the administrator user in the database, and you can now log into UMP as the administrator user.

Slow Performance on Internet Explorer 7/8

Symptom:
You may experience that UMP works slowly using IE7, possibly due to IE7’s caching strategy.

Solution:
You can optimize this by changing the settings for browsing history. Go to Tools-InternetOptions-General-BrowsingHistory-Settings, and set the strategy for checking pages to Automatic.

For IE8 it may also help to select the CompatibilityView mode.

Non-ASCII Characters Stored Incorrectly in the Database

Depending on the database collation used, the database may not store non-ASCII user input correctly. For example, if a user enters Japanese characters in a community string in the Nimsoft Remote Admin portlet, the database may store the Japanese characters incorrectly, causing authentication to fail.
Numeric Login IDs Do Not Work

Symptom:
I cannot log in using a numeric user name.

Solution:
Do the following steps:
1. Deactivate the wasp probe in Infrastructure Manager.
2. Open the following file for editing: `<UMP Installation directory>/probes/service/wasp/webapps/ROOT/WEB-INF/classes/portal-ext.properties`.
3. Add the following line:
   `users.screen.name.allow.numeric=true`
4. Activate the wasp probe.

I Cannot Access the Control Panel

Symptom:
After upgrading from UMP 2.1.x (or earlier) to UMP 2.5.x (or later), when I click Manage, Control Panel I see my private home page instead of the Control Panel.

Solution:
Users not assigned to the Liferay administrator role may not be able to access the Control Panel after upgrading.

Do the following steps:
1. Deactivate the wasp probe in Infrastructure Manager.
2. Open the probes/service/wasp/webapps/ROOT/WEB-INF/classes/portal-ext.properties file for editing.
3. Add the following line, or if it is present uncomment it by removing the hash sign character (#):
   `permissions.user.check.algorithm=5`
4. Activate the wasp probe in Infrastructure Manager.
**Logging In Takes Me to the Login Page**

**Symptom:**
After upgrading from UMP 2.1.x (or earlier) to UMP 2.5.x (or later), when I log in I see the UMP login page again instead of my private home page.

**Solution:**
Do the following steps:
1. Deactivate the wasp probe in Infrastructure Manager.
2. Open the `probes/service/wasp/webapps/ROOT/WEB-INF/classes/portal-ext.properties` file for editing.
3. Add the following line, or if it is present uncomment it by removing the hash sign character (#):
   ```
   virtual.hosts.default.community.name=
   ```
4. Activate the wasp probe in Infrastructure Manager.

**CSV File is Incorrect in Chinese or Japanese**

**Symptom:**
When I export a Performance Report to a CSV file in Chinese or Japanese, there are incorrect characters and incorrect times in the report.

**Solution:**
This may occur if the locale in UMP is set to a multi-byte language (Chinese or Japanese) and your default application associated with CSV files is Microsoft Excel. Excel does not always correctly identify the encoding (UTF-8) of the exported CSV file.

To resolve this, use the Excel Import function. The following steps are an example for Excel 2007:
1. Click the Data tab in the top ribbon in Excel.
2. Click From Text in the Get External Data section.
3. Browse to the CSV file and click Import.
4. Click the Delimited radio button for the Original data type.
5. Choose 65001: Unicode (UFT-8) from the File Origin pulldown menu.
6. Click Next, then click the Comma check box in the Delimiters section.
   - Make sure only the Comma check box is checked.
7. Click Next, then click Finish.
$PASSWORD Substitution in Alarm Console • 50

A

About Layout Styles • 211
About the Relationship Viewer • 205
Accessing the Relationship Viewer • 206
Account Admin • 23
Account Admin Pane • 23
Account Tables • 262
Actions Dialog • 39
Add a Note to a Ticket (Self Service Users) • 176
Add a Page • 18
Add A Work Log Item to a Ticket (Agent or Admin Users) • 177
Add an Attachment to a Ticket • 177
Add Column Panes • 157
Add Portlets • 18
Administering Report Scheduler • 234
Administration • 441
Adobe Flash Player Settings Dialog • 40
Advanced Search • 372
Alarm Components • 104
Alarm Console • 29
Alarm Console Loses Filters with Internet Explorer • 50
Alarm Console Table • 34
Alarm Console Table Popup Menu • 37
Alarm Console Toolbars • 29
Alarm Data Format Pane • 163
Alarm Filter Bar • 31
Alarm Filter Dialog • 40
Alarm Filter Expression Dialog • 40
Alarm History Dialog • 41
Alarm List • 415
Alarm Notification Tab in SLA Form • 282, 290
Alarm Summary Chart • 415
Alarm Table • 420
Apply a Monitor to a System • 410
Applying Monitors to Groups • 405
Applying Monitors to Systems • 410
Assign a Host Variable • 92
Assign a Monitoring Template • 407
Assign a QoS Variable • 91
Assign a Robot Variable • 91
Assign a Text Variable • 92
Assign To Dialog • 41
Assigning Report Templates to Groups • 432
Assigning Variables • 90
Asynchronous data type • 349
Attach Notes Dialog • 41
Automatic (Interval) data type • 349
Automatic Agent Deployment • 373
Automatic Groups • 390
Automatic Replacement of Fields in PRD Templates • 193
Automatic Weight Distribution • 296
Automatically Create Tickets from Alarms • 244

B

Background Alpha • 121
Background Color • 120
Background ImageURL • 122
Badge View • 367
Baseline Value Definition • 317
Basic Search • 370

C

Calculation Examples • 273
Calculation method • 349
Calculation Profiles • 347
Calculation Terms and Conditions for the QoS • 268
Calculation Terms and Conditions for the SLA • 270
Calculation Terms and Conditions for the SLO • 269
Calculations Tab in SLA Form • 284
Change Layout Style Selector • 210
Change Names of Custom Fields • 419
Change Password • 27
Changing What You See • 207
Charts Pane • 188
Choose a Job Delivery Method • 227, 230
Close Browser When Logging Out • 453
Cloud User Experience Monitor • 51
Cloud User Experience Monitor Configuration • 51
CMDB Integration • 245
Command Bar • 30
Compliance Calculation • 266
Compliance percentage • 351
Compliance period • 350
Configure Outgoing Mail Settings • 446
Configure the From Email Address • 447
Configuring a Widget to Use External DB Data • 88
Configuring the Table Widget • 86
Contact Nimsoft • 3
Converting Data Units • 76
Copy a Job • 232
Copy a Monitoring Template • 408
Create a Filter • 392
Create a Group • 389
Create a Job • 225
Create a Monitoring Template • 406
Create a New Service Level Objective (SLO) • 286
Create a Page • 18
Create a Variable • 90
Create Dashboard • 60
Create Groups Automatically • 392
Create NM Users • 246
Create Service Desk Users • 246
Create Tickets from Alarms • 244
Creating a Calculation Profile • 299
Creating a Compliance Period • 297
Creating a QoS Monitoring Profile • 317
Creating an Exclude Period • 304
Creating an Exclude Period, using the Add Exclude Period Wizard • 305
Creating an Operating Period • 298
Creating an SLA • 278
Creating an SLA Using the SLA Wizard • 310
CSV File is Incorrect in Chinese or Japanese • 459
Custom Dashboards • 55
Custom Logo Missing • 450
Customize Data Sources for Systems • 137
Customizing the Dynamic View Templates • 140

Data Types • 352
Default Fonts for Reports • 236
Define the XML File • 376
Defining a Quality of Service Object • 294
Defining QoS Constraints • 294
Defining Reports with a URL • 198
Defining the Calculation Terms and Conditions • 267
Defining the Quality of Service Object • 264
Definition of Compliance Percentage • 266
Definition of Multi-Series Calculation • 272
Delete a Group • 399
Delete a Job • 233
Delete a Monitor from a System • 411
Delete a Variable • 93
Delete Text from Custom Fields • 419
Deploy Agents Automatically • 374
Deploy Agents to Systems Listed in a File • 375
Deploying Widgets • 63
Design a List • 150
Designing a New Dashboard • 59
Detach Notes dialog • 42
Details Dialog • 42
Device Performance Charts Reference • 426
Dialogs • 39
Disable Public Reports • 167, 197
Discovery Status • 129
Discovery Status Pie Chart • 129
Discovery Status Table • 132
Display Metrics for Custom Probes • 428
Distributing Importance (Weight) • 296
Do Not Edit QoS Properties in SLM Portlet • 453
Drilling Down in List Viewer • 169
Duplicate Data Series are generated • 145
Dynamic View is not Displayed • 145
Dynamic Views • 135
Dynamic Views May Display Redundant Tree Nodes • 144

E

Edit a Dynamic View Template • 144
Edit a Job • 228
Edit a Monitor for a System • 412
Edit a Variable • 92
Edit ACLs Dialog • 24
Enabling the Alarm Console • 49
Error Console • 19
Errors • 436
Example • 93, 394
Example – Creating a SLA Based on the Selected SLA • 316
Example – Creating an SLA Based on a Service • 310
Example - Defining a Simple Service Level Agreement • 307
Example 1
  One QoS and One SLO • 273
Example 2
  Two QoSs and One SLO • 274
Example 3
  Two QoSs and One SLO, Using Calculation Method AND or OR • 274
Example 4
  Two SLOs, Each with Three QoS • 275
Excluded Periods • 285
Excluding Quality of Service Data • 303
Exporting QoS Data Using Export QoS Data Wizard • 326
Exporting the QoS Data Series • 325

F
Filter Alarms • 423
Filter Menus and Buttons • 397
Filters • 392
Filters Tab • 186
Find Dialog • 42
Flow Analysis • 147

G
Garbled Text in Console Installer • 452
Gauge Data Format Pane • 160
General Bar • 29
General Properties • 124
Generating a Graph • 324
Get Link URL Button • 216
Getting Started with Service-Oriented Configuration • 386
Getting Started with UMP • 15
Group Not Found • 437

H
History Bar • 32
How to Navigate the Help Topics • 20
How to Print Multiple Help Topics • 21
Hub • 352

I
I Cannot Access a Wiki Page I Created • 451
I Cannot Access the Control Panel • 458
Import the File • 385
Information Tab • 332
Internet Explorer 8 Cross-Site Scripting Issue • 456
Internet Explorer 8 Displays Page Title Incorrectly • 454
Internet Explorer 8 Performance Issue • 454
Introduction to SLA Reports • 249
Introduction to SLM • 255

J
Java Exception Displayed When Scheduling Reports • 240

L
Launch Relationship Viewer • 373
Launching a Standalone USM • 433
Launching the Relationship Viewer using the WebContent Portlet • 217
Launching USM using an HTML File • 437
Launching USM with a URL • 434
LDAP Authentication with Active Directory Groups • 450
Legal Notices • 2
List Designer • 149
List Designer Window • 153
List Viewer • 169
List Viewer Window • 170
Local vs Remote Monitors • 400
Logging In Takes Me to the Login Page • 459
Login Fails on Solaris • 457

M
Magnify Button • 212
Main Window Pane • 348
Maintenance Mode • 173
Manage Actions Dialog • 43
Manage Alarm Filter ACLs • 43
Manage Alarms • 421
Manage Notes Dialog • 43
Managing Alarms in Dashboards • 57
Managing Objects on the Canvas • 80
Managing Pages • 18
Managing your QoS Data • 333
Manual Weight Distribution • 296
Manually Create an Incident from an Alarm • 244
Meters • 105
Migration for Legacy Users • 180

Index 463
Mini Map Tool • 56
MiniMap Tool • 139
My Tickets • 175

Navigating in USM • 366
New Account/Edit Account Dialog • 26
New Action Dialog • 44
New Note/Edit Note Dialog • 44
Nimsoft Remote Admin • 179
No Access Error • 146
No Data Displayed in Alarm Console • 50
No Existing Interfaces Error • 146
Non-ASCII Characters Stored Incorrectly in the Database • 457
Note Icon Does Not Display in Report Scheduler Reports • 242
Notes (SLO Form) • 291
Notes Dialog • 45
Notes Tab in SLA Form • 283
NULL value • 352
Numeric Data Format Pane • 159
Numeric Login IDs Do Not Work • 458

Objectives (SLO) Tab in SLA Form • 281
Open View Dialog • 165, 171
Operating period • 352
Operating Periods • 346
Overview • 205
Overview of Creating Service Level Agreements • 278

Page Titles May Contain Garbled Text • 452
Paging • 367
Panel • 106
PDF Preferences Dialog • 166, 196
Performance Reports Designer • 183
Performance Reports May Convert Incorrectly to PDF • 204
Permissions in USM • 366
Pie Chart Detailed View • 130
Pop Out Graphs • 373
Populating the Quality of Service Tables • 265
Popup Menus • 36
Portlet Not Resizing in Chrome • 455
Precedence • 401
Preconfigured Reports • 357
Preferences Dialog • 45, 171, 198, 253, 341
Preparing the Canvas • 80
Preview a Job • 232
Priority • 402
Probe Updates • 442
Probes • 353
Properties Pane • 120

QoS • 354
QoS constraint • 354
QoS Data Tables • 260
QoS Definition Tab • 331
QoS Monitor Properties • 319
QoS Monitors List • 318
QoS object • 354
QoS Objects • 252
QoS Selection Tabs • 185
Quality of Service • 348
Quality of Service Reports • 221
Query Dialog • 46

Radar View Button • 210
Radius Slider • 213
Reapply a Monitoring Template • 409
Relationship Selector • 213
Relationship Services Not Supported on Solaris • 451
Relationship Viewer • 205
Relationship Viewer Control Bar • 208
Relationship Viewer Dependent upon Root Cause Analysis and Topology Manager • 453
Report Scheduler • 225
Removing an Account User’s Access • 239
Report Scheduler Does Not Display Estimated Values • 240
Report Scheduler Jobs Table • 234
Report Scheduler Shifts Time Axis in PDF Format • 240
Reports • 221
Reports Overview • 221
Reports with Integrated Data • 245
Requests List • 176
Right-Clicking Objects on the Canvas • 125
Robot • 353
Run a Job • 232
Run Query Dialog • 46
Running Unified Reports • 357

S

Save Dialog • 166, 196
Saving Information as a PDF • 253
Scaling Dashboards • 123
Schedule a Job • 226, 230
Search and Clear Search Controls • 213
Search for Computer Systems • 370
Select a Layout • 18
Selecting a Data Source--DB • 85
Selecting a Data Source--NIS • 82
Selecting a Data Source--Probe • 83
Selecting a Data Source--QoS • 81
Selecting a Data Source--SLA • 85
Selecting a Data Source--Variables • 83
Selecting the Data Source • 80
Sending SQL Queries to the Database • 336
Servers Group • 399
Service Desk • 424
Service Level Agreement (SLA) • 353
Service Level Agreement Form • 279
Service Level Agreement Reports • 224
Service Level Agreements • 343
Service Level Objective Form • 287
Set a Custom Font for Reports • 238
Set a Monitor Override • 412
Set a Single Alarm to Invisible • 422
Set Automatic HTTPS Redirect • 442
Set Custom Alarm Fields • 418
Set Custom Fields Dialog • 47
Set Default View Dialog • 47
Set Multiple Alarms to Invisible • 422
Set Permissions for UMP Portlets • 443
Set the Monitoring Template State for a Group • 404
Set the State for a System • 404
Set up Email for UMP • 446
Set Up Service-Oriented Configuration • 387
Set Where Reports are Stored on a Server • 234
Setting Permissions to Use SLM • 265
Setting Up a Probe to Deliver Quality of Service Data • 265

Single Sign On • 441
Single Time Zone Required • 449
Size Limits for SQL Queries • 337
Size of Dashboard Panels • 453
SLA Calculation Tables • 261
SLA Configuration Tables • 261

SLA Engine • 262
SLA Reports • 249
SLM • 255, 353
SLM Concepts • 258
SLM Database Structure • 260
SLM Interface Reference • 338
SLM May Allow Invalid Logical Expressions • 354
SLM Overview • 255
SLM Portlet Displays Incorrect Data Set • 355
SLM Terms and Definitions • 349
SLO • 353
SLOs • 252
Slow Performance on Internet Explorer 7/8 • 457
SOC Probes Configuration Reference • 388
Some Scheduled Jobs are Not Running • 241
Sort Alarms • 424
Sorting • 368
Source Data Format Pane • 165
Spark Data Format Pane • 159
Specify a Group AND a System • 435
Specify a Group OR a System • 434
Specify a Path • 435
Specify Job Information • 225, 229
SSO Credentials Configuration • 53
State • 403
Status Data Format Pane • 164
Step 1 – Define an Operating Period • 307
Step 2 – Create a new SLA and Define the Service Level Compliance Requirement • 308
Step 3 – Define the Individual Service Level Objectives • 309
Step 4 – Excluding Periods • 310
Summary • 271
Supported Variables • 142
System Not Found • 436

T

Template Names • 140
The Active Objects Tab • 327
The Application Window • 103
The Calculation Settings Tab • 293
The Dashboards Templates • 111
The Excluded Periods Tab • 292
The Menu Bar • 339
The Navigation Pane • 342
The Portal • 15
The QoS Probes Tab • 332
The Quality of Service Tab • 288