Contact Nimsoft

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

At 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.
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.
# Contents

## Chapter 1: Infrastructure Manager Introduction

- Describing the Infrastructure elements ................................................................. 11
- Domain .................................................................................................................... 12
- Hub .......................................................................................................................... 13
- Robot ....................................................................................................................... 14
- Probes ...................................................................................................................... 15

## Chapter 2: System Description

- The Nimsoft Message flow .................................................................................... 21
- Nimsoft message handling ..................................................................................... 22
- Queues, subscribers and message delivery ............................................................. 23
- The Security Model ................................................................................................. 24
- System Overview .................................................................................................... 25
- User Security .......................................................................................................... 26
- Probe Security ......................................................................................................... 27
- Administration ........................................................................................................ 28
- Tunnels .................................................................................................................... 29
- Encryption ............................................................................................................... 30
- Alarm Solution ....................................................................................................... 31
  - Alarm Overview .................................................................................................... 32
  - Alarms .................................................................................................................... 33
  - Handling Alarms ................................................................................................. 34
- SLM Components .................................................................................................. 35
  - How it all fits together .......................................................................................... 36
  - Developing your own probes and utilities ........................................................... 37
    - Introduction ....................................................................................................... 38
    - Portable Data Stream (PDS) ............................................................................. 39
    - Installation ......................................................................................................... 40
    - Designing Probes .............................................................................................. 41
    - Using the Code Wizard ...................................................................................... 42

## Chapter 3: Infrastructure Manager Reference Guide

- The Menu Bar ......................................................................................................... 43
- The File menu ......................................................................................................... 44
- The View menu ....................................................................................................... 45
- The Security menu ................................................................................................. 46

---

Title page: The Menu Bar

Chapter 3: Infrastructure Manager Reference Guide

How it all fits together

SLM Components

Alarm Solution

The Security Model

The Nimsoft Message flow

Describing the Infrastructure elements

Chapter 2: System Description

- Domains
- Hubs
- Robots
- Probes

Chapter 1: Infrastructure Manager Introduction

Contents

The View menu

The File menu

Using the Code Wizard

Designing Probes

Portable Data Stream (PDS)

Installation

Chapter 3: Infrastructure Manager Reference Guide

The Menu Bar

The File menu

The View menu

The Security menu

Chapter 2: System Description

The Nimsoft Message flow

Nimsoft message handling

Queues, subscribers and message delivery

The Security Model

System Overview

User Security

Probe Security

Administration

Tunnels

Encryption

Alarm Solution

Alarm Overview

Alarms

Handling Alarms

SLM Components

How it all fits together

Developing your own probes and utilities

Introduction

Portable Data Stream (PDS)

Installation

Designing Probes

Using the Code Wizard

Chapter 3: Infrastructure Manager Reference Guide

The Menu Bar

The File menu

The View menu

The Security menu

Chapter 2: System Description

The Nimsoft Message flow

Nimsoft message handling

Queues, subscribers and message delivery

The Security Model

System Overview

User Security

Probe Security

Administration

Tunnels

Encryption

Alarm Solution

Alarm Overview

Alarms

Handling Alarms

SLM Components

How it all fits together

Developing your own probes and utilities

Introduction

Portable Data Stream (PDS)

Installation

Designing Probes

Using the Code Wizard

Chapter 3: Infrastructure Manager Reference Guide

The Menu Bar

The File menu

The View menu

The Security menu
Chapter 4: Infrastructure Manager User Guide

Logging on Infrastructure Manager ................................................................. 135
Working with Infrastructure Manager ............................................................... 136
  Connecting a Robot .................................................................................. 137
  Configuring a probe using the internal editor (raw configure) .................. 139
  The Probe Utility ................................................................................. 140
  Viewing a Probe's log-file ...................................................................... 143
  Login to Another Hub ........................................................................... 144
  Moving a Robot .................................................................................... 145
  Adding a new Probe Definition .............................................................. 147
  Finding Nimsoft components ................................................................. 151
  Probe administration ........................................................................... 152
  Creating Mobile Panels ....................................................................... 153
  Defining user-actions .......................................................................... 153
  Workspace printing ............................................................................... 154
  Downloading and Distributing Probes .................................................. 155
  Technical Tips ...................................................................................... 164
  Non-valid licenses Notification ............................................................ 180
  How to install a license for a HUB ......................................................... 181
  Setting up audio-visual alarm notification ........................................... 182
  The Infrastructure Manager Error Log ................................................ 183
Managing the Robot on a AS400 computer ................................................................. 183
Modifying the Infrastructure....................................................................................... 183
Installing Nimsoft in an active/passive Microsoft Cluster ........................................ 184
Report_engine not installed on the same server as the main hub? ........................... 193
Moving the SLM database from one SQL server to another .................................... 195
Alarm Server Mirroring within a Domain ................................................................... 196
Alarm Server Mirroring Across Domains .................................................................... 198
Setting up Passive robots .......................................................................................... 201
Setting up Robot Fail-over ......................................................................................... 206
Installing multiple Robots on the same server ......................................................... 208
Configuring Hubs to send all the alarms to a central Hub ........................................ 210
Setting up a tunnel between two Hubs that are separated by a Firewall ................. 212
Setting up a Tunnel in a NATed network .................................................................. 218
About renaming a Hub or Robot computer ............................................................... 219
Adding a slave report_engine and/or a slave sla_engine ......................................... 219

Chapter 5: Alarm SubConsole ................................................................................. 221
The Alarm SubConsole Window ................................................................................ 221
Modifying the layout of the list in the window ......................................................... 224
Right-clicking in the Alarm Window ......................................................................... 225
The Toolbar in the Alarm Window .......................................................................... 243

Chapter 6: Distribution Application ........................................................................ 247
Starting the Distribution Application ....................................................................... 248
Login ........................................................................................................................... 248
The Distribution Window ......................................................................................... 249
The Navigation Pane ............................................................................................... 250
The List Panes ......................................................................................................... 251
The Menu Bar ......................................................................................................... 253
The Toolbar .............................................................................................................. 255
Drag & drop .............................................................................................................. 268

Chapter 7: Probe Report ............................................................................................ 269
Starting the application ............................................................................................ 269
Login .......................................................................................................................... 270
The Probe Report Window ....................................................................................... 271
Right-clicking in the window .................................................................................... 271
The Menubar .......................................................................................................... 272
The Toolbar .............................................................................................................. 275
Generating reports ................................................................................................. 277
Generating a Probe Summary Report ................................................................. 277
Generating a Probe Configurations Report ...................................................... 278
Generating a Probe Statistics Report ............................................................... 279
Exporting a report to Excel ........................................................................... 280

Appendix A: Registry Options ........................................................................ 283
General ............................................................................................................. 283
Registry Keys ................................................................................................... 283
  HKEY_CURRENT_USER .............................................................................. 284
  HKEY_LOCAL_MACHINE ............................................................................ 286
Registry Options Keys .................................................................................... 287
Overview: Permissions and Ownership .......................................................... 291
User Administration ....................................................................................... 292
  Creating a new user .................................................................................. 293
  Creating a new profile ............................................................................. 295
  Managing the Access Control List ............................................................ 296
  Adding a new ACL .................................................................................... 297
Working with Alarms ..................................................................................... 322
  The Alarm Window .................................................................................. 322
  Handling Alarms ..................................................................................... 323
Account Administration ................................................................................ 325
  Creating an Account ............................................................................... 326
Working with Views in Lists ......................................................................... 331
  The Toolbar in the list ............................................................................. 332
  Right-clicking a column header .............................................................. 333
  Right-clicking in a list ............................................................................. 336

Appendix B: Glossary of Terms .................................................................... 343
Nimsoft Infrastructure .................................................................................... 343
  Domain .................................................................................................. 343
  Hub ......................................................................................................... 343
  Infrastructure Manager ........................................................................... 343
  Nimsoft Address ..................................................................................... 344
  Probe ...................................................................................................... 344
  Publishing messages .............................................................................. 344
  Quality of Service (QoS) ....................................................................... 345
  Robot ...................................................................................................... 345
  Subject .................................................................................................... 346
  Subscribe ................................................................................................. 346
Alarms ............................................................................................................. 346
  Acknowledge .......................................................................................... 346
Alarm Levels .........................................................................................................................346
Alarm message ......................................................................................................................347
History ..................................................................................................................................347
Regular expressions ...........................................................................................................347
Subsystem .............................................................................................................................351
Suppression ...........................................................................................................................351
Chapter 1: Infrastructure Manager
Introduction

This document describes how to use Infrastructure Manager to manage your system.

The document is meant to be a helping hand for those who are not familiar with Nimsoft products. It will help you through the installation process and show how to start working with the product.

The document describes tasks such as:

- Terms and definitions.
- System components.
- Testing and configuring the installed products.
- How to start using the products.

Infrastructure Manager provides monitoring and management solutions for systems, applications and networks.

It is the primary interface for configuration and management of your Nimsoft system. It provides:

- A windows explorer style overview of systems being monitored.
- A management and administration tool.
- An alarm window to view all alarms and messages.

Describing the Infrastructure elements

Infrastructure Manager connects to an active Hub and allows you to control, configure and manage all robots and probes connected to that hub.

![Infrastructure Manager screenshot]

**Navigation Pane,** displaying the infrastructure of your Nimsoft installation.

**Dock Pane,** which can be selected to show either the Alarm window or the Message window.

**Status Bar,** displaying login information, the number of alarms received and a graphical representation of the alarms, where different colors represent the different alarm severities.
Chapter 2: System Description

This chapter describes the Infrastructure Manager application.

This section contains the following topics:

- Describing the Infrastructure elements (see page 13)
- The Nimsoft Message flow (see page 23)
- The Security Model (see page 27)
- Alarm Solution (see page 35)
- SLM Components (see page 44)
- How it all fits together (see page 46)
- Developing your own probes and utilities (see page 47)

Describing the Infrastructure elements

This section gives a description of the most important terms and elements of the infrastructure. Knowing these terms will make the work with Nimsoft components a lot easier.
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.

Various security aspects, such as e.g. user-profiles, user-permissions and access-rights are distributed within the Domain.

Note the different Domain status symbols, as they appear in the Infrastructure Manager:

- Active Domain. You will receive update events from all Hubs within this Domain.

- Non-active Domain. A manual refresh is required to obtain the latest status.
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 components can connect to the Hub to receive dedicated messages and perform other specific activities. One such component is the Alarm Server (nas).

Note: It is recommended that at least two Hubs should be installed on the same Domain and network to ensure you have a backup of the user/security data.

![Hub Diagram]

Note that the Hub icons may have different color, depending on the Hub status:
Describing the Infrastructure elements

- **Light green**
  The Hub that you are connected to (your login Hub).

- **Dark green**
  Other accessible Hubs under the domain (auto-discovered or static).

- **Yellow**
  The Hub has an unknown status.

- **Red**
  The Hub is not accessible.

**Overview**

As mentioned, the Hub is a connection/message center in the network. Its main responsibility is to respond quickly to incoming messages, dispatch these messages to the connected subscribers and/or queues and to moderate/maintain various system information, such as name-tables etc. The Hub may be used to 'group' a set of robots that perform the same operations, have the same geographical locations, have the same departmental code etc. It is designed to handle a large amount of messages posted/published by its robots, and dispatches the messages to its clients. Messages published under a subject without subscribers or queues will automatically be discarded.

The figure above shows the Hub/Robot relationship. The Hub listens to port (TCP/48002) for commands and requests. The illustration shows a Robot with Hub capabilities and two active probes. The Hub does not require any special hardware or system software.

For more details, please see the hub chapter in the Probe documentation (NimbusDoc.chm help file).
The Robot-Hub message flow

All postings performed by the various probes will be handled by the spooler within the Robot. The spooler will attempt to pass the message over to its current Hub, and will de-spool the messages when the Hub responds positively to the request. When the Hub receives the message it takes a look at the message subject field, and dispatches the message to the appropriate recipients of this posting. The recipients may be other probes functioning as gateway processes (converting "alarm" postings to e.g. SNMP traps) or dedicated servers listening on subjects specifically designed for this.

The figure below shows probes sending a message (yellow dot) via the spooler to the Hub and into the various recipient processes. The flashing green/red dots signify the active/inactive state of a timed probe.

The subscribe mechanism

The Subscribe mechanism will enable clients of the Nimsoft to select messages based on their subjects rather than on e.g. the sender address. Whenever a client decides to receive message postings from the Nimsoft, it sends a subscribe request to the Hub. The client will receive messages matching the subscribed subjects from the Hub. A client may use the following methods when subscribing:

1. Subscribe - connects to the Hub, and gets messages as long as the client is alive/running on the session.
2. Attach - the Hub configures a Message queue to hold the messages if the client is passive (not running). So when the client comes back up, all messages will be passed on (even the ones that were received when the client was inactive).
Describing the Infrastructure elements

The message queues

The Hub is designed to handle large amount of incoming messages and requests. To maintain a high message throughput, message queues are used. A message queue is a FIFO (first in first out) queue used to temporarily hold the messages until a client is ready to read the data. As mentioned earlier, messages without subscribers will be discarded. Therefore it is vital to use message queues to ensure reliability and to be able to guarantee the message delivery. The Hub messages queues are found in the Nimsoft/hub/q directory.

The Name Service

All probes controlled by a Robot will be registered in a probe list managed by the Robot controller. In addition to the probe list, a list of all active probes (probes that listen to a bound port, and respond to a command set), is distributed to the Hub for rapid delivery upon request (from e.g. the Infrastructure Manager). The names found in these tables are the basis for the name to IP/port resolution, and is what we define as a Nimsoft Address. A client may query the controller for a name/IP resolution ala DNS and WINS, based on the service name (e.g. the Alarm Server, nas).

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. Each computer that is being monitored by a Probe will need a Robot installed on it.
Note the different color of the Robot symbols, as they appear in the Infrastructure Manager:

- Robot is running as a Hub, status OK.
- Robot is running, status OK.
- Robot is not responding, status ERROR.
- Robot has an unknown status.
**Robot Description**

A Robot is often referred to as a device that imitates human behavior. The Robot has two dedicated tasks:

- Control the 'probes' attached to the Robot.
- Ensure that messages 'published' by the probes reach the Hub.
- Provide a simple database service for its probes.

The Robot will on a 24 hour, 7 days a week basis ensures that the attached probes run without human intervention. It will relieve the system administrator of repetitive, time consuming tasks such as performing system surveillance, application monitoring, network monitoring, etc.

A Robot consists of two major elements, the controller and the spooler. The controller manages the probes with respect to startup time and running modes. A probe may be configured to run every night between 22:00 and 23:00 (known as a timed probe), or it may be configured to run continuously (as a daemon probe).

The spooler will in most cases forward the messages directly to the current Hub. It attempts to 'bulk' the messages whenever possible, to decrease network load. You may configure the spooler to store the messages locally (to a disk file), and send them when given criteria (severity, time and amount) are met.

Many tasks in a Nimsoft solution involve the storage of data for threshold monitoring and data trending. The third part of the Robot is called the "Hub Database server" or hdb. The hdb is a database service used by the two system probes described above (and possibly other probes with storage needs) as a lightweight database service.

The figure below shows a Robot (without distinguishing the controller or spooler) with two configured probes. One probe (with a green indicator on the connection) is active (due to being configured as a daemon), while the other is configured as a timed probe and therefore marked as red.
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.

Note the different Probe status symbols:

- Green. The Probe is running and is controlled by the Robot.
- Yellow. The Probe is not controlled by the Robot, but has registered a remote command port.
- Grey. The Probe is disabled/deactivated.
- Red. The Robot detected an error situation during the startup period of the Probe.
- Red with a lock symbol. The Robot denies startup of Probe due to missing security permissions.
- Red with a license symbol. The Robot denies startup of Probe due to an invalid license.
Describing the Infrastructure elements

Probe Description

Probes are programs installed on the computers which are connected to the Nimsoft, providing a link between the system and the Nimsoft. Seen from Nimsoft, the Robot controls a set of probes and provides the necessary communication ports for all of them. Seen from the connected system, the probe is an internal process capable of:

- Accessing internal system resources from probe-specific program code.
- Sending messages on the Nimsoft via the messaging features in the Nimsoft API.
- Receiving commands from the Nimsoft and maintaining a configuration file via the command features of the Nimsoft API.

Usually, the probe has its current configuration stored in a local configuration file. This file is maintained via commands in the Nimsoft API, and the settings are typically used to define the behavior of the probe-specific functions.

All of the probes in the Alarm solution use the three features described above like this:

- The probe-specific functionality checks the system for symptoms of error situations.
- When such a symptom is found, the probe issues a call to the API for sending an alarm message.
- When working with the probe from Infrastructure Manager, your input to the GUI is passed to the probe as commands to be interpreted by the API. This can be direct commands like "Stop", "Start" and "Restart", or more complex ones like "read the current contents from the config file". The last command is issued when you select Configure to launch the configuration tool for the selected probe.
The Nimsoft Message flow

The message flow on the Nimsoft is briefly described as shown on the figures below.

The upper figure illustrates how messages (letters etc.) are sent and received between people, the lower figure shows the same actions on the Nimsoft.

- The sender (e.g. a probe) puts the message in his mailbox for outbound mail.
- The message is fetched and transferred to the post office.
- The post office decides what to do with the message:
  - Does the message have an address? In this case it is forwarded directly to the receiver (e.g. a probe or a GUI).
  - If no address, the post office has to decide what to do. All Nimsoft messages contain a Subject ID, which is a text string classifying the message for all components on the Nimsoft, allowing them to subscribe to some messages and ignore others). Based on this Subject ID, the message is either put onto a queue destination, where anyone interested (e.g. a probe or a GUI) may fetch it, or the message is simply deleted.
The Nimsoft Message flow

Nimsoft message handling

The Nimsoft should be viewed as a message-bus serving client and server processes connected to it by providing a set of services. The two major components of the Nimsoft are the Robot and Hub processes. They provide the client/server applications with an entry-point (Robot) and an exit-point (Hub) to/from the Nimsoft. The messages flow on the bus using routing and naming schemes.

The illustration below shows the relationships between the various key components in the Nimsoft system. Whenever a message is generated by a probe (by issuing a publishing request), the message is picked up by the Robot spooler and passed on to the Robot’s primary Hub. The Hub dispatches the message to clients subscribing to the subject which the message is posted under.
### Nimsoft Message Model

The Nimsoft message model is based on the *request/response* and the *publish/subscribe* models. *Request/Response* is the standard way of communicating over the network. A client issues a request to a server and the server responds to the request. The *publish/subscribe* model is useful when a client wishes to send some kind of data without a designated receiver. This could be messages containing performance-data, an alert, and data to be inserted into some database, or messages targeted for gateway servers. The server merely listens on one or more specific subjects (registered by the Hub), and is notified by events whenever data is available.

### Queues, subscribers and message delivery

The transfer of messages to and from a Hub is done through queues. There are different ways of configuring queues, allowing a wide range of communication setups. In most everyday situations, the queue is a transparent part of the infrastructure. All you as an administrator normally will need to do is to define communication links between components (robots, probes and hubs), and the necessary queues are automatically set up for you. The queues fall into two main categories:

A permanent queue is stored in the local Hub database, and survives a restart of the Hub. This type of queue is set up where it is important to ensure that the message is delivered even if the receiver is down when the message is sent. Typically, this is the case when sending messages to a nos (Nimsoft ODBC server) or nas (Alarm Server) to be stored in a database. The controller at the receiving Robot attaches to the queue at startup and fetches all the messages queued up while it was down, if any. After that, new messages are fetched as soon as they are received by the Hub and put into the queue.

A temporary queue is a more ad-hoc type of mechanisms used for less critical communication paths. For example, when you open a Enterprise console, you want all alarm messages which the Hub receives while you have the console open to be displayed in your console. When the console is opened, it opens a subscription to alarm messages from the Hub. Then, a temporary queue is created on the Hub, and messages are forwarded to this queue as long as the console is active. When you close the console, the queue is removed.
When the probe publishes messages

The figure below shows a Robot with the active probe publishing messages (the yellow indicator) onto the Nimsoft. The message is received by the Robot spooler, which sends (unless configured to spool to disk) the message to the Hub that manages this Robot. Note that messages will be bulked together in order to increase the message flow from the Robot to the Hub. The client will perceive that the message it passed on to the spooler, is sent immediately.

When the Robot is configured to spool messages

The figure below shows the Robot with a spooler configured to be on, meaning it holds/queues messages locally until criteria for sending the message out on the Nimsoft is met. The criteria may be a combination of

1. The message priority (level)
2. The message count
3. The message time (how long its been in the queue)

The message may also be flushed by the operator through the spooler command set. If you compare the two figures above, you’ll discover the essentials regarding the spooling mechanism. The spooler will hold the messages until the flushing criteria are met, and pass the queued messages along to the Hub for further processing.
The Security Model

This document describes the security models found within the system. Our main security issues are to determine whether to restrict users and/or probes based on predefined permissions within the Domain. The security topics discussed in this document are:

- **Access**
  who has permission to do what

- **Authentication**
  is the client who he/she/it claims to be?

- **Encryption**
  make it impossible for others to read the data

I am using the terminology *node* for a **Hub**, **robot** or **probe**. **Client** is a GUI or a probe that can execute a command on other nodes. A complete solution with GUI’s and probes that logically belong together is called an **application**. A **domain** is a collection of one or more Hubs with robots and probes that are logically grouped together. The **robot** is consists of the **controller** and the **spooler**.

System Overview

![Diagram of system overview](image)

*Figure 1: NimBUS Overview*
The Nimsoft consists of Domains, Hubs, Robots and probes. A typical installation may look like this.

Consider the following scenario:
- A user performs a Login and wants to configure a probe

The security steps involved in the above scenario is explained in detail below:
1. The user performs a login on a Domain with a user name and a password before he can start managing the nodes in the domain. If the login succeeds the user will be granted session identification (SID) that contains information about the user identity. It is the Hub that issues the SID’s and it is the Hubs that verify the SID’s upon request by the controller.
2. The SID is attached to all requests and the node forwards it to the local Robot for verification of the users’ permissions. The robot forwards the request to the Hub which first checks the domain signature and then the users’ permissions, and accepts or denies the request.

The Session Identification (SID)

The SID is used to control the users/probes access to execute commands within the Nimsoft. When a client sends a request to a node it must have a valid SID. The SID is issued by the nearest Hub (Domain login) and will require a user name and a password if it is a user or verification from the controller if it is a probe.

The SID contains the following information:
- Signature (16 bytes) - the signature is based on a password set by the administrator (HMAC)
- Version (2 bytes)
- Expire time (EPOCH)
- Hub (Login)
- Client IP-address
- Client Ethernet address
- Client type (user or probe)
- Client identity (user-name or probe-name)
- The SID is encoded with Base64 to make it easier to transfer between applications.

User Security

An administrator creates user-accounts in the Domain, he/she also decides the access permissions for that user within the Domain.
Login

Login requests are sent from user applications (and probes with special requirements). These requests are checked against the security setup in the Hub. A typical login request is described below:

When a user is logging in, a login request is sent to the controller. The request contains:

- user name
- password

The controller receives the request and forwards it to the Hub after adding the following fields:

- IP address of the source
- MAC address of the source
- The Hub checks the information against the security configuration and sends a reply with a SID if the login request is valid.
Verifying a SID

A node receives a request and asks the controller to verify the SID. The request is forwarded to the Hub, which verifies the signature of the SID and checks the rest of the information against the access required by the node.

Whenever a request is sent to a probe, the SID for that user is attached. The SID and information about the client is sent to the Hub to check that the user has the access level required to execute the requested command.

The information added by the node is:

- Client IP-address
- Client MAC address
- The commands required access.
Probe Security

Probes have different tasks. Most of them have simple tasks such as monitoring something and sending an alarm if a threshold is reached. Other have more complex tasks such as collecting information from and executing commands on other probes. The first type does not need a SID, because all they do is to send messages on the Nimsoft. The other one needs permission to connect to and execute commands on remote probes; these probes are a potential security risk.

To obtain a SID without a login, two conditions must be fulfilled.

1. The robot must install the probe in order to get a signed checksum generated. This requires administration rights and cannot be performed by intruders or operators.
2. The controller must start the probe. A magic number scheme ensures that this cannot be circumvented.

If these requirements are met and the probe needs a SID; the controller connects to the Hub to get the appropriate SID for the probe. This again requires that the probe has been added to the security configuration with the appropriate permissions and IP-mask.

Signed checksum installation

To prevent that unauthorized probes are installed and started on a robot have we devised a system that ensures that only probes installed by a user with administrator rights can obtain a SID on start up.

The controller generates a signed checksum (HMAC) during installation; this HMAC is saved and is later used to verify the probe identity each time it is stared. If the checksum has changed the probe will not be started by the controller and cannot do any harm.

The signed checksum is generated from the main binaries/script in the probe package, it is based on the IP address + secret key.

Magic number scheme

A magic number is generated into the probe-environment just before the probe is started. When a probe starts, the magic number is passed to the controller to ensure that the controller is in full control of the probe that is started, thus making it impossible for intruders to use probes.

Administration

Please note that all changes to the security configuration must be done with the Infrastructure Manager; manual changes of the security file will render it invalid!!
The configuration file

The Hub has a security setup file that contains information about the users and probes that have access to the Nimsoft and what permissions they have.

The setup section contains generic configuration items such as how long the SID is valid and the signature.

The users section contains user information such as user name, access rights and password. See also the section Access Control Lists (ACLs). The Infrastructure Manager uses the profile variable to set the look and feel for the GUI.

The Probes section is used for giving probes access to other probes.

The Filters section can be used to give access-rights to hosts instead of users and should not be used.

Please note that this file is monitored with a checksum, so tampering causes the Hub to invalidate the configuration.

Access Control Lists (ACLs)

Access Control Lists consists of a set of access properties and permissions. When the administrator creates new users, or modifies the properties for an existing user, he attaches the user to an ACL. Users attached to an ACL will have the properties and permissions defined for that ACL.

The administrator can also create new ACLs or modify the properties for the existing ones.

The ACLs can be administered from the Infrastructure Manager, selecting Security > Manage Access Control List from the Menu bar.

See the section User Administration for details.

The signature

On initial startup of the Hub, security is disabled.

The first time a Manager connects to the Hub, the user is prompted to create an administrator user. The signature for the Hub is initially equal to the administrator’s password.

A new Hub is added to the domain. The manager is told by the Hub upon login that there is a new Hub without security enabled in the Domain, and is prompted to manage the unsecured Hub. The signature and the users are distributed to the new Hub. If the administrator logs on to the new Hub he is forced to login on a secure Hub.
Tunnels

Most companies today have one or more firewalls in their network, both internally between different networks and externally against a DMZ or Internet.

See also the sections Setting up a tunnel between two Hubs that are separated by a Firewall.

Network administrators are often reluctant to open a firewall for a lot of IP addresses and ports in order to make it possible for Management applications to work. This makes it difficult to administrate and monitor the whole network from a central location.

The solution is to set up a Tunnel between two Hubs that is separated by a Firewall. The Tunnel sets up a VPN-like (Virtual Private Network) connection between the two Hubs and enables all Nimsoft requests and messages to be routed over the Tunnel and dispatched on the other side. This routing will be transparent to all the users within Nimsoft. The only requirement for setting up a Tunnel is that one of the Firewalls opens for connection to the target Hub on one port.

Security is the main issue when opening a Firewall for external connections. The Tunnel is implemented using the SSL (Secure Socket Layer) protocol, which is currently the most widely deployed security protocol today (e.g., it is the protocol behind Secure HTTP (HTTPS)). See also the section Encryption. The security is handled in two ways; certificates to authenticate the Client and encryption to secure the network traffic (e.g., over Internet):

- **Authorization and Authentication**
  
The Tunnel provides authorization and authentication by using certificates. Both the Client and the Server need valid certificates issued by the same CA (Certificate Authority) in order to set up a connection. In the case of setting up a Tunnel, the machine receiving the connection (the Server) is its own CA and will only accept certificates issued by itself.

- **Encryption**
  
The encryption settings span from None to High. No encryption means that the traffic is still authenticated and is therefore recommended for Tunnels within LAN’s and WANs. You should be careful when selecting higher encryption level since this will be more resource intensive for the machines at both ends of the tunnel.
Encryption

The infrastructure supports Open SSL (Secure Socket Layer), thus encrypting the data-channels in the Nimsoft.

This excerpt is from the http://www.openssl.org documentation and states the goal for the SSL protocol.

"The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently.

The SSL protocol provides connection security that has three basic properties:

- The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES, RC4, etc.)
- The peer’s identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.).
- The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations."
The Alarm server (nas) connects to a Hub and collects any messages with a subject of Alarm. These Alarms are sorted and stored in the Alarm Database and then posted back through the Hub to the Alarm Sub Console (which is integrated into the Enterprise Console and the Infrastructure Manager.)
Alarm Solution

Alarm Overview

The Alarm solution is an application based on the Nimsoft Infrastructure. This application consists of three main parts in addition to the Nimsoft infrastructure:

- The Alarm Monitoring probes check the host computer for symptoms of error situations. This may be checking free disk space, log-file contents, performance problems or stopped system processes. When a problem is found, a Nimsoft message describing the problem is sent via the Robot to the Nimsoft.

- Nimsoft AS delivers several standard probes for monitoring a wide range of operating systems and applications for error situations which are known to be likely to occur in that particular type of system. Nimsoft AS works closely with the vendors of such systems to provide focused monitoring for the everyday problems troubling their users and support staff.

- The infrastructure (basically: the hubs) route the message to an Alarm server (nas). The nas stores the message in a small, local database.

Alarms

The ALARM product utilizes the infrastructure to create system and network monitoring solutions. Nimsoft AS delivers out-of-the-box solutions for a wide range of operating systems and applications. These solutions provide a quick start and will cover about 80% of the needs for server and workstation monitoring in most organizations. However: experience has shown that covering the remaining 20% is very costly. These needs vary from site to site, and a product covering them all will be extremely difficult both to develop and to learn. Also, the load on the monitored system will be higher than we believe is necessary.

We believe that most customers are best served by providing an infrastructure where they can develop their own solutions, targeted directly at the problems causing them the most trouble. This approach requires a development platform which:

- Does not force people to waste time on learning a proprietary programming language or scripting language (or, for that matter, a standard language they do not already know)

- Does not force people to waste time on inventing network access and security solutions to all the different operating systems used

- Does not force people to waste time on distributing and installing their solutions on all the monitored machines.
Alarm Server (nas)

The nas’s main purpose is to receive and manage incoming alarm-messages. The nas
- Supports message suppression.
- Provides clients with services such as:
  - Update events.
  - Repository services (get, list, close etc.).
- Supports message filtering.
- Supports automatic actions (auto-operator).
- Mirroring capabilities.

Alarm message handling

The Alarm Server (nas) is a service probe that attaches itself to a Hub-queue (nas), and receives alarm messages distributed by the Hub. An alarm message is generated by a probe somewhere on the Nimsoft. This is a "broadcast-type" message without any particular receiver (a posting) that may be picked up by any processes subscribing to the "alarm" subject. The nas subscribes to the "alarm" subject and acts upon the incoming message by storing information about the alarm into a database in the nas subdirectory.

Enterprise Console / Nas interaction

The Alarm Server responds to a command-set reachable by anyone with the correct access, as well as notifying through the use of message postings whenever state changes occur. Anyone may listen to the postings (notifications) made by the nas.
Message suppression

Many error situations in the monitored system can result in a huge number of alarms. For example, this can be the case if the logmon probe monitors a logfile for an application which enters an eternal loop, logging errors within the loop. This may result in a huge number of identical alarms, creating unnecessary load on the system, network and the Nimsoft. This can be avoided by using the message suppression mechanism.
The message suppression models supported by the nas, are:

- **Standard suppression** is a simple model that suppresses messages with an exact match on message subsystem id, severity level and message text.

- **Key suppression** is a model based on a suppression key that follows a message. When the key suppression is enabled messages with matching suppression key will be suppressed.

**Example**

With Key suppression on, these two messages from the same probe are equal:

- Filesystem '/usr' is filled 95% (suppkey: FsProbe-/usr)
- Filesystem '/usr' is filled 55% (suppkey: FsProbe-/usr)

The result of this would be one message in the alarm server database, but it would have recorded both of them as valid transactions (and therefore logged them in the transaction log). So if the sequence was as displayed (95% first, then 55% as the last status) then the administrator would experience the state as a filesystem with 55% filling grade (which is the correct way to see things).

An administrator may choose to ignore the suppression mechanism based on key, due to the fact that he/she wants to view the messages as they are reported by the probes.

**Automated acknowledge**

The suppression key described above can also be used to automatically clean up in the alarm list when the probe detects that the critical situation is resolved. This is done by enabling automatic acknowledge based on key. This means that alarms with severity level "clear" automatically acknowledges any previous alarms with the same suppression key. In the example above, a reasonable configuration of the disk-monitoring probe would be to send the first alarm (95% full) with severity level "serious", while the last one (55% full) could have severity level "clear". When the last alarm arrives, everything is back to normal, and the administrator does not have to respond to the first alarm after all. Then the alarm is automatically acknowledged by the nas, leaving the administrator with a "to-do list" with as little "noise" as possible.
Alarm transactions

It is quite useful to follow the complete message life from the initial message and to when the message is closed (acknowledged) and via multiple suppressions. The Alarm Server is capable of logging all transactions to a specific transaction logfile. This is accomplished through a filtering mechanism tunable by the administrator. To keep the transaction logfile as manageable as possible, it is automatically administered (copied to a 'save' location) at configured intervals. The saved transaction logs are renamed to the following format: trans_timestamp.log where timestamp is the time (in seconds since epoch) it was managed.
Subsystems

In the Alarm window, the different alerts are classified by their subsystem ID, identifying which part of the system the alert relates to. This is a hierarchical list of codes, allowing you to group alarms in as wide or narrow groups as you want. This list is stored in the nas, and if you develop your own probes or customize the standard ones, you may also define your own list of subsystems. This list also maps the subsystem code into a text string for improved readability.

Notification messages

The Alarm Server notifies the world about changes to its alarm database by issuing postings on the Nimsoft. When an alarm message is received and its footprint is not previously recorded, an alarm_new message is generated. However, if the footprint already exists, an alarm_update message is generated. Whenever a client closes (acknowledges) an alarm it will be removed from the currently active alarms, and an alarm_close message will be generated. All transactions such as new, suppress and close are logged to the transaction log, and may be viewed through the nas configuration tool.

Handling Alarms

Alarms will appear in the Alarm window. This Windows application displays the alarm messages in the nas database for the operator. Alternatively, you can install a gateway for forwarding the alarms to other messaging infrastructures such as E-mail, GSM/SMS, pager or SNMP messages, or integrate Alarm more tightly to a systems management framework using one of the available framework integration kits. Either way, the operator is automatically informed about the problem a few seconds or minutes after the symptom appears, rather than having to check manually.
Alarms automatically handled by the auto operator

Alarms can also be automatically handled by setting up profiles in the Auto operator in the nas probe.

For more details, please see the nas chapter in the Probe documentation (NimbusDoc.chm help file).

Handling alarms from a cellular phone

Also note the Mobile Panel Solution, which allows you to view, assign and acknowledge Alarm messages directly on your mobile phone, and also provides QoS, SLO and SLA data.
The WAP Reader uses WebServices to interface with the Mobile Panel Probe through Tunnel technology and converts data from the probe to WAP panels. The Mobile Panel Probe retrieves QoS data from the Variable Server Probe and alarm data from the Dashboard Server Probe. The probe also contains an editor for creating WAP panels.

The operator will gain access to the Mobile Panel definition calling the appropriate URL using his cellular phone.

The installation of the Mobile Panel solution components is described in the Client Installation section of the Nimsoft Server documentation.

For more details about mobile_panels probe, please see the mobile_panels chapter in the Probe documentation (NimbusDoc.chm help file).

For more information on alarm handling, see the sections Nimsoft Alarm SubConsole and Working with Alarms in this document.
SLM Components

Most Probes can feed the SLM (Service Level Management) system with Quality of Service data.

The three following components are important parts of the SLM product line:

- Data Engine
- SLA Engine
- Report Engine

The **Data Engine** has two primary focus areas:

- Subscribe to Quality of Service messages.
- Insert QoS data in the database.
For more details, see the `data_engine` chapter in the Probe documentation (NimbusDoc.chm help file).

The **SLA Engine** (SLA= Service Level Agreement) has one primary focus area:

- Calculate SLA compliance.

For more details, please see the `sla_engine` chapter in the Probe documentation (NimbusDoc.chm help file).

The **Report Engine** has the following primary focus areas:

- Generate SLA reports based on the computations done by the `sla_engine`.
- Generate Quality of Service related graphs and reports.
- Run a light-weight web server for QoS and SLA reports.
- Perform file transfer (FTP) services to publish the reports to e.g. inter/intranet web servers.
- Possibility to customize the reports by modifying templates.

For more details, please see the `report_engine` chapter in the Probe documentation (NimbusDoc.chm help file).
How it all fits together
Developing your own probes and utilities

Introduction

Nimsoft AS has designed the general purpose message-bus, Nimsoft, to be as open as possible with respect to the various (and specific) user needs. In order to be able to interface the Nimsoft, extensions to existing programming environments are available.

We have developed a tool (CodeWizard) that generates code for the languages mentioned below. It is an ideal tool, and starting point for probe-developers as well as application developers.

The Software Development Kit (SDK) allows you to develop probes and utilities that integrate with the Nimsoft environment. The SDK is available for the following programming languages:

- Perl
- C
- Java
- Visual Basic

Portable Data Stream (PDS)

Nimsoft uses the proprietary Portable Data Stream (PDS) format as a way to represent data across the network. In general, a PDS formatted message contains a stream of data, tagged by descriptive labels. You may extract the data in a sequential manner, or get the data using the tags. The Nimsoft API offers several functions to read from or write to a PDS. The general idea is to store name, type and value information into the data stream on one end, and to extract the data on the other end of a network communication channel. The Nimsoft API will automatically translate the data in the stream to the correct format for that platform.
Developing your own probes and utilities

Installation

The SDK packages can be downloaded from the Nimsoft Internet Archive. Using Infrastructure Manager, the packages are installed by selecting them in the Nimsoft Internet Archive and dragging / dropping them into the Archive on the Hub you are logged on to. From there they can be dragged / dropped to the target Robot(s).

The packages are installed in the SDK directory under the Nimsoft root directory. Default locations are C:\Program Files\Nimsoft on Windows platforms and /opt/Nimsoft on UNIX platforms.

Depending on which SDK you have installed, you may need to modify your environment settings to allow Nimsoft libraries to be included in the build process, or, in the case of Perl, program interpretation.

Designing Probes

You should consider these questions when designing your probe:

■ Do you want to include the advanced log-facilities available in the API?
■ Do you need to read configuration variables from a file?
■ Should the probe run as a daemon or should it be timed?
  ■ Timed probe
    A *timed* probe runs once and then terminates, awaiting the next point in time when it is configured to start.
    ■ Started by the Robot at intervals or a given schedule.
    ■ Runs through all checkpoints and reports all threshold breaches.
    ■ Must keep all states between runs if needed.
  ■ Daemon probe
    A *daemon* probe is always active if activated by the operator. If it stops, the Robot immediately restarts it.
    ■ Runs always. Will be restarted by the Robot if it stops.
    ■ Is network aware and supports command interface.
    ■ Can subscribe to messages on the Nimsoft.
■ What QoS Definition do you want to set up (take a look at the ones already defined).
Using the Code Wizard

The Code Wizard is a tool for creating a probe framework.

You start the wizard by double-clicking the codewizard.exe file.

The codewizard.exe file is located in the Program Files\Nimsoft\sdk\bin folder, provided that the SDK is installed.
When the wizard is started, you select the programming language you are going to use.

Available options are:

- Perl
- Visual Basic
- Java
- C

In addition, you can select one or more of the program properties available in the wizard:

- Use logging facility.
- Add example on how to generate an alarm.
- Add support for configuration-file input.
- Add command-set interface.
- Subscribe to messages from Hub.
- Add example on how to generate Quality of Service (QoS).
- Include timeout handler.
- Publish user-defined messages.

Select the relevant options and click the *Generate* button, and the wizard generates example code for your new probe. The generated code can be saved and copied into your programming environment for further development.

For further information, see the *Nimsoft SDK Documentation* available on the Nimsoft Download Site.
Chapter 3: Infrastructure Manager Reference Guide

This section contains the following topics:

The Menu Bar (see page 51)
The Status Bar (see page 78)
The Navigation Pane (see page 78)
The Main Window pane (see page 96)
The Toolbar (see page 131)
The Dock Pane (see page 133)

The Menu Bar

This section gives a short description of the different functions and tools found in the Menu Bar. Note that some of the menus are partly restricted, depending if your user is classified as operator or superuser.

The File menu

This menu contains the following four options:

- Print Setup
- Print Preview
- Print
- Exit
Print Setup

It is possible to print the contents of the Main Window Pane or the Alarm Window. The *print setup* option enables you to:

- Select printer
- Edit the options and properties for the printout.
  - paper size
  - paper source
  - paper orientation (portrait or landscape)
  - paper quality
  - a set of advanced options

![Print Setup dialog box](image)
Print Preview

Placing the cursor in the Main Window Pane or the Alarm Window, enables you to print the contents of the window.

Selecting the Print Preview option opens a window with the contents of the selected window.

The toolbar in that window offers a set of options, such as:

- Zooming in or out
- Moving to next/previous page
- Select to view one or two pages in the window
- A Print button, opening the printer properties dialog, letting you modify the printer settings and start the printout of the contents.

Print...

Placing the cursor in the Main Window Pane or the Alarm Window enables you to print the contents of the window.

Selecting the Print option opens the printer properties dialog, letting you modify the printer settings and start the printout of the contents.

Exit

Exits the Infrastructure Manager.

Note the menu choice Tools > Options, described in the section Options.

Profiles define and control the appearance of the application window, such as layout of columns in the alarm window, what is displayed in the main window etc.).

A checkbox in the Options dialog lets you select to automatically save the current configuration profile on exit.

If you have modified the layout, this will be saved to your current profile at application exit, and this layout will be selected the next time you launch the application.
The View menu

Profiles

Different profiles can be created to define and control the appearance of the application window. This option lists all defined profiles, highlighting the profile your user currently is associated with, allowing you to select one of the other profiles.
Manage Profiles

Opens the Manage Profiles dialog, where you can create new profiles, or delete existing ones. See also the description here.

![Manage Profiles dialog]

Save Current Profile

Save the current profile with any changes you may have done. Also note the menu choice Tools > Options, described in the section Options.
A checkbox in the Options dialog lets you select to automatically save the current configuration profile on exit.

Save Current Profile as

Allows you to save the current profile with the profile name you specify. This enables you to use an existing profile, modify it and save it as your own.

Show All Domains

The Domains node in the Navigation Pane can, when expanded, list all defined Domains, or just the Domain you are connected to. When the Show All Domains option is selected, all Domains will be displayed in the Navigation Pane. Deselecting the option hides all other Domains.

Note! Regardless of which hub you log onto within a domain, you should get the same list of hubs for that domain since this information is being synchronized between the hubs in the domain. However, the set of other domains displayed in the Show All Domains mode will vary according to which hub you are logged on to within a domain. This information is not shared and synchronized between the hubs, so the list of other domains will just reflect the knowledge of the particular hub that you have logged on to.
Navigation Pane

*The Navigation Pane* will, when selected, appear in the left part of the Infrastructure Manager Window, otherwise not.

The Pane contains the following Nodes:

- Domains.
- Groups.
- Archive.
- Applications.
- URLs

Dock Pane

*The Dock Pane* will, when selected, appear in the lower part of the Infrastructure Manager Window, otherwise not.

By default, either the *Alarm Window* (displaying alarms received) or the *Message Window* (showing system- and communication-messages) can be displayed in the Dock Pane, depending on what is selected in the Menu Bar (alarm window or message window).

Alarm Window

The *Alarm window* when selected appears in Dock Pane, replacing the Message Window.

The window displays a list of alarms received, and the window is divided into a number of columns with different alarm information, such as:

- Alarm ID number
- Alarm Message text
- The time the alarm was received, time of origin and Arrival.
- Alarm severity
- Host name
- Probe name etc.
Message Window

The Message Window will, when selected, appear in Dock Pane, replacing the Alarm Window.

The window shows console internal messages indicating what events and actions are taking place, and can be used as a debugging tool.

The window can also show Trace info, which is a console internal message at a more detailed level.

Toolbar

The Toolbar (below the Menu Bar) will, when selected, appear in the Infrastructure Manager Window, otherwise not.

The Toolbar includes a sub set of functions also found in the menu bar.

Status Bar

The Status Bar will, when selected, appear at the bottom of the Infrastructure Manager Window, otherwise not.

The Status Bar displays different login and alarm information:
- Domain Login
- User
- Profile
- ACL

Alarm Indicator in Status Bar

When selected, the Alarm Indicator will appear in the Status Bar, otherwise not.

Alarm indicator, indicating total number of alarms and a graphical indication of alarms with the different severity levels.

Refresh

Refreshes the Infrastructure Manager Window to display current information.

Pressing the F5 key on your keyboard has the same functionality.
The Menu Bar

The Security menu

The Security menu contains the following options:

- **Login...**
- **Change Password...**
- **User Administration...**
- **Account Administration...**
- **Manage Access Control List...**
- **Set Login Expiration Time...**
- **Probe Administration...**

**Login...**

Opens the Login dialog, enabling you to log in as another user.

The Domain drop-down list allows you to log on another Domain, while the **Advanced** button, expanding the dialog, enables you to log on to a specific Hub on a specific Domain. Finish by clicking the **OK** button.

![Login dialog]

**Note**: With Infrastructure Manager Version 3.70.2 or newer, it is also possible to log on the Nimsoft consoles as a LDAP user. See the section **Logging on Infrastructure Manager** for further information.

Avoid creating Nimsoft Users and LDAP users with identical user names.
Change Password...

Opens the Password dialog, enabling you to change the password for the user currently logged on. Enter the new password in the upper field, and then retype it in the lower field. Finish by clicking the OK button.

Note that this is the password for the current Domain.

User Administration...

Opens the User Administration dialog, enabling you to:

- Add, delete or edit the properties for existing Nimsoft users (change password, profile, ACL etc.).
- Manage access Control Lists (ACLs)
- Manage Profiles (add or delete profiles).

See also description here.
**Account Administration...**

Opens the Account Administration dialog, where you can add, edit or delete accounts.

You may also define contacts (‘users’) for each account.

For details, see the section Account Administration.

**Manage Access Control List...**

Opens the Manage Access Control List, where you can add, edit or delete ACLs.

An ACL consists of a set of access properties and permissions. Users attached to an ACL will have the properties and permissions defined for that ACL. See also the description here.
Set Login Expiration time...

Specifies how long (days-hours-minutes) you can be logged on the Infrastructure Manager before the system automatically logs you off. The minimum value is 10 minutes.

Note that you will not be logged off the Infrastructure Manager itself (which automatically receives a re-login from the system), but applications launched from the Infrastructure Manager (such as a Probe configurator) will be stopped if has been opened for a longer time than the defined expiration time. You will receive a message like the one shown below. You then have to click the OK button to perform a re-login, or click the Cancel button and close the Probe configurator and start it again to continue working on it.
**Probe Administration...**

Opens the Probe administration dialog, where you can define the security level for the different Probes when they attempt to access other Probes within the same Domain. If the entry for a certain Probe is missing in this list, the Probe will have the lowest security level set. That means it can perform very limited actions against other Probes.

The four security access levels defined are:

- Open
- Read
- Write
- Admin

You can also limit the computers the Probe has access to by assigning the corresponding IP addresses.

Also see the section Probe administration.

**The Tools menu**

![Infrastructure Manager Menu](image)

**Find...**

Opens the *Find* dialog, where you can search for other Nimsoft components (Hubs, Robots or Probes).
There are three common searching criteria for all three Nimsoft components (Hub, Robot and Probe):

- **Restrict find to login domain**
  The utility will search only within the Domain you are logged on.

- **Name**
  The name of the component.

- **Match case**
  Means that the entry in the Name field is case sensitive (the name must be correctly written regarding UPPERCASE and lowercase).

Further you can specify different searching criteria, depending on type of Nimsoft component you want to search for:

- **Hub**
  Only the common criteria, described above.

- **Robot**
  Matching criteria:
  - **OS Major and OS Minor**
    Specify an OS, and Robots running this OS will be found.

    *Major* describes the general OS groups (Unix, windows and IBM), while *Minor* describes a more specific OS within these groups (e.g. windows98, linux etc).

  - **Tag 1 and Tag 2**
    Under Setup > Misc in the configuration dialog for the controller probe, it is possible to specify an identification tag.

    ![Configuration dialog](image)

    E.g. Robots within a department in a company can be attached a tag. Using this tag as a searching criterion, you will search for all Robots in that department.
- **Probe**

- **Class**

  Probe indicates a probe which is not listening to an attached port. This can be because it is inactive or because it runs at specific intervals and is not controlled by the Infrastructure Manager (like the logmon probe, for example). Probe/Port indicates a probe which is actively listening on an attached port.

  Port means a Probe/program that has been started (and attached a port), but the controller does not recognize it. It can typically be a custom made program for test purposes.

- **Group**

  The logical group the Probe belongs to. Probes are divided into different groups, depending on monitoring purposes (Network probes, Database probes, System probes, Gateways etc).

**Example:**

![Find window](image)
To find all cdm Probes installed on the Domain you are logged on:

- Ensure the option Restrict find to login domain is checked.
- Select Tools > Find.
- Specify searching criteria in the Find dialog and click the OK button. All instances of the cdm Probe found will be listed in a separate window, including detailed Probe information (version number, Robot etc.)

**Connect Robot...**

This option opens the Connect Robot dialog, which can be used to restart a Robot or connect a Robot to another Hub.

![Connect Robot dialog]

See the section Connecting a Robot.

**Distribution**

Starts the Distribution application. You can distribute Probe packages to Robots, using the Infrastructure Manager, or you can start the standalone Distribution application. This application offers drag & drop capabilities the same way as in the Infrastructure Manager, but most important is the ability to create distribution tasks, making it easy to initiate a distribution of certain packages to a set of destination Robots. The built-in task scheduling mechanism enables you to start the actual distribution at some preferred time, thus eliminating the interactivity required when distributing within Infrastructure Manager.

See the section Distribution Application (see page 247).
Service Controller...

A utility for starting or stopping the Service Controller (the process controller.exe) on the computer you are working on. When stopped, the computer will not be available on the Nimsoft (the icon in the Navigation pane will turn into red). It is not possible to run the Infrastructure Manager or the Enterprise Console on the computer where the Service Controller is stopped.

Note the icon on the status line of your desktop.

Clicking the icon enables you to start or stop the Service Controller. In addition, you can define the startup mode.

By default, the startup mode Auto is selected, which means that the Service Controller is started when you start the computer.

If selecting Manual, it means that you manually have to start the Service Controller before attempting to launch the Infrastructure Manager or the Enterprise Console.

Clicking the Force Stop button stops Nimsoft immediately.

Clicking the Shutdown button enables the core components to finish their current tasks (e.g. the nas is allowed to process the alarms) before shutting down Nimsoft.

You may specify a Max wait time before shutting down. If not, the components are allowed to use the time necessary to finish their tasks.
Alarm Notifier...

Starts the Alarm Notifier. This is a small program that shows the highest severity level of current alarms, and notifies you either visually or with a user-defined sound whenever the severity level defined in the Alarm Notifier setup is reached.

You may also specify an application to be launched when an alarm with the defined severity level is reached.

When launched, the icon will appear on the status line.

The application may run and keep you informed of the alarm status, even if the Consoles are not running.

Right-clicking the icon lets you open the setup dialog, enabling you to define sound, severity properties, actions etc.

Also see the section Setting up audio-visual alarm notification.

Options

Opens the Options dialog, where you can set different options for the Infrastructure Manager.
The Menu Bar

Note: If you change some of the settings in this dialog, you must perform a re-login before your new settings will be activated.

Options

Login
Primary Hub: <none>
Secondary Hub: <none>

- Attempt automatic login when selecting hub nodes
- Receive domain events
- Enable automatic login at application startup
- Show Groups node

Multiple Network Interface Card Settings:
- Bind to IP
- Automatic
- IP: ...

Probe Request
Timeout value: 10 (sec)

Find Utility
- Execute as an external process

Profiles:
- Save configuration profile on exit

Message Beep
- Beep activated on error messages

Internet Archive
- Attempt Internet Archive integration with local archive

Salesforce Self-Service Center user credentials:
User: 
Password: 
- Attempt automatic login when downloading from the Internet Archive

Alarms
Alarm Server: <default>
- Strip host name
- Display indicator in statusbar

NIS Database
Data Engine: /Support/xplesa/xplesa/data_engine

- Login

Primary Hub
Here you can select which Hub to log on at Infrastructure Manager startup.

Secondary Hub
If primary Hub is not found at Infrastructure Manager startup, you will be logged on to the Hub selected as the secondary Hub.
Further, if logged on to the primary Hub, and this Hub stops, you will automatically be logged on to the Hub selected as the secondary Hub.

In addition there are four checkboxes:

- **Attempt automatic login when selecting hub nodes:**
  Attempt automatic login with your current name and password when selecting a Hub node in the Navigation Pane.

- **Enable automatic login at application startup:**
  Enable for automatic login without prompting for a user name and a password at application startup if you already are logged on another Nimsoft application.

- **Receive domain events:**
  Enable all hubs within the domain to send status events. The result of leaving this field unchecked is that only events from the login hub will be processed.

- **Show Groups nodes:**
  The Groups node (containing user-composed groups of Probes, Robots or Hubs) will appear in the Navigation Pane when this option is selected, otherwise not.

**Multiple Network Interface Card Settings**

The Network Interface Card Settings is useful for setting the IP for the NIC.

- **Bind to IP:** Select this check box to set the IP for the NIC.

- **Automatic:** This option is available only if the Bind to UP check box is selected. Select this option to automatically let NumBUS set the IP for the NIC.

- **IP:** This option is available only if the Bind to UP check box is selected. Select this option to explicitly specify the IP address. Specify the IP address in the given box.

**Request**

*Timeout values when executing Nimsoft requests.*

The timeout value used when executing Nimsoft requests is by default set to 10 seconds.

In some cases it is necessary to increase this value (e.g. when executing requests over lines with heavy traffic, tunnel configurations, etc.).

The value must be in the range between 10 seconds and 300 seconds. However, avoid setting this value higher than necessary, as this may slow down the system, e.g. spending time on waiting for response from components that are not available.
- **Find Utility**

  When launching the *Find utility* (available from the Toolbar) with this option checked, the *Find utility* will run as a separate process.

  This means that you may continue working with the Infrastructure Manager even if the find dialog is active.

- **Profiles**

  *Save configuration profile on exit*

  If checked, the current configuration profile is automatically saved on exit. This means that any changes you have made, affecting the Profile (e.g. created Groups or one or more User Actions) will be saved on your current profile.

  If you have made any such changes, and this option is not checked, the following warning will appear, allowing you to select whether you want to save the changes to the profile or not.

- **Message beep**

  Activates a sound (beep) on internal console messages.

- **Nimsoft Internet Archive**

  *Attempt Nimsoft Internet Archive integration with local archive*

  When the option *Attempt Nimsoft Internet Archive integration with local archive* is checked, the Infrastructure Manager attempts to connect to the Nimsoft Internet Archive at application startup. This enables you to see packages located in the Nimsoft Internet Archive in addition to packages downloaded to your local archive when the Archive node is selected in the Navigation pane (see The Archive Node).

  A status line at the bottom of the package list (marked with a horizontal red line on the figure below) indicates if you are connected to the Nimsoft Internet Archive or not. Green text means OK, red text indicates that you are not integrated with the Nimsoft Internet Archive.

  The status line will typically appear like this:

  **Nimsoft Internet Archive Mode:** GA –
  **View:** Packages in local archive only.
This means that packages from the **GA** (General Availability) section of the Nimsoft Internet Archive can be accessed.

It also indicates that the user has selected to view packages located in the local archive only (see The Archive Node).

For more information about the Nimsoft Internet Archive, see also the section Downloading Probe packages from the Nimsoft Internet Archive.

This connection ensures an easy method for downloading packages from the Nimsoft Internet Archive into your local package archive.

**Note:** On installations where this web connection can not be established (e.g. due to firewall configurations), a timeout (and an error message) will appear each time the Infrastructure Manager application is started. Turn off this option to avoid this timeout.

**Attempt automatic login when downloading from the Nimsoft Internet Archive**

**Note:** This option is activated when the Attempt Nimsoft Internet Archive integration with local archive is selected, otherwise it is greyed out and can not be selected.

Fill in Salesforce Self-Service Center user credentials and tic this option to be automatically logged in to the Salesforce Self-Service Center.

Otherwise you will be asked to enter Salesforce Self-Service Center user credentials to log in when you attempt to download a package from the Nimsoft Internet Archive.

All customers with an active Maintenance contract and a Self-Service Center login, will be granted access to the Nimsoft Support Site.

To obtain a login account, please contact Nimsoft Support.

- **Alarm Server**

  This pull-down menu enables you to connect to an alternative Alarm Server (nas). You are by default connected to the nas on the HUB you are logged on to.
- **Strip hostname**
  A checkbox where you can select to remove the Domain name part in the *hostname column* in the Alarm Window for incoming alarms.

  When selected, the hostname will be stripped from the first *dot (.)* found in the name, starting from left.

  Note that you can modify this functionality by editing one of the two strings in Registry:

  HKEY_CURRENT_USER > Software > Nimsoft Software > Infrastructure Manager > Options > StripHostDot

  By default set to 0 and does not influence on the Strip Hostname functionality. When set to 1, the hostname will be stripped from the last dot (.) in the name, starting from right; when set to 2, the hostname will be stripped from the second dot (.) in the name, starting from right; and so on.

  HKEY_CURRENT_USER > Software > Nimsoft Software > Infrastructure Manager > Options > StripHostDomain

  By specifying a part of a hostname here, this part will be stripped from the hostname.

  E.g. specifying `nimsoft.no`, `nimsoft.no` will be stripped from the hostname.

  **Note:** If checking/unchecking this option, the GUI's needs to be restarted in order for the change to take effect.

- **Display indicator in Status Bar**
  If checked, the Alarm indicator is displayed in the Status Bar at the bottom of the Infrastructure Manager Window.

- **NIS Database**
  Specify the name of the *Data Engine*, which is a link to the NIS database containing your QoS data.

  **NOTE:** Otherwise the The Dynamic Views Node node will not shown in the Navigation pane.

  The Infrastructure Manager is also the tool for creating *accounts* and *contacts* (see Account Administration...), typically defining a customer/company and the associated privileges. This information is also written to the database.
The Window menu

Launch Main Window Pane

Launches the Main Window Pane as a separate window. You will now have two instances of the Main window Pane - the ordinary one inside the frame of the application window and the one you launched as a separate window.

You may now continue working in the Infrastructure Manager, modifying the contents of the Main Window Pane, while the separate window remains unchanged.

You may work separately in both windows, using right-click menus and tool buttons.
The Menu Bar

The separate window may either be closed, or you may dock it (send it to the Dock Pane, where normally the Alarm Window or Messages Window appear.

Even when the window is placed in the Dock Pane, you may work in the window, using right-click menus and tool buttons.

Also see Dock Window...

Dock Window...

If the Main Window Pane is opened as a separate window, it can be moved to the Dock Pane when selecting Dock Window.

Normally the Alarm Window or Message Window appears in the Dock Window.

Using the Docked Window List option, you can toggle between the different windows to appear in the Dock Pane.

Previous Window in Dock Pane...

Displays the previous window from the Docked Window List in the Dock Pane.

This list normally contains the Alarm Window and the Messages Window. In addition it may contain one or more instances/views of the Main Window Pane, which is sent to the Dock Pane.
Next Window in Dock Pane ...

Displays the next window from the Docked Windows List in the Dock Pane.

This list normally contains the Alarm Window and the Message Window. In addition it may contain one or more instances/views of the Main Window Pane, which is sent to the Dock Pane.

Docked Window List

Opens the Docked Windows List, displaying the windows that have been displayed in the docked window.

The list normally contains the Alarm Window and the Message Window. In addition it may contain one or more instances/views of the Main Window Pane, which is sent to the Dock Pane.

The Docked Windows dialog enables you to:

- Activate one of the windows in the list
- Remove one or all of the entries in the list.

When launching the Infrastructure Manager application the list contains the Alarm Window and the Message Window.
Removing all entries from the Docked Windows list, the Dock Pane will be empty.

To add the Alarm Window and the Message Window to the list, you select View > Alarm Window and View > Message Window from the Menu bar, or double-click the Alarm indicator or the Messages icon in the Status bar.

The Help menu

Infrastructure Manager

Opens the Nimsoft on-line documentation, describing the Infrastructure Manager application and the infrastructure.

Getting Started

Opens the on-line documentation, pointing directly to the Getting Started section.

Using a few moments going through this documentation hopefully will help you to understand the Nimsoft products and make it easier to start using them. The document is not meant as a product description, but more as a walkthrough of some important and visible functions of the main applications.

The following main tasks are covered:
- Infrastructure Manager and Infrastructure.
- Service Level Manager.
- Alarm Console Overview.
Installation Guide

Opens the on-line documentation, pointing directly to the Nimsoft Server documentation. This document describes the Nimsoft Server application.

Nimsoft Server is the tool for downloading and installing Nimsoft Software products.

Nimsoft Server will, when installed on your site, act as a portal that you may access from other computers on your network via a web browser.

You may then:
- Launch Nimsoft applications.
- Install Nimsoft products on your clients.
- View your Dashboards and reports.

Probes

Opens the Probe on-line documentation.

This on-line documentation contains description of probes that have been released for General Availability.

Configuration Guide

Opens the on-line Configuration guide.

About Infrastructure Manager

Displays the Infrastructure Manager product version.
The Status Bar

The Status Bar, located at the bottom of the Infrastructure Manager application window displays login and alarm information:

- Login Hub
- Nimsoft User name
- ACL (Access Control List)
- Profile
- Alarm indicator
- Message icon

The Navigation Pane

The navigation pane displays the complete structure of your installation. The Pane contains the following Nodes:

- Domains.
- Dynamic Views.
- Groups.
- Archive.
- Applications.
- URLs
The Domains Node

The Domain is the top-level node in the Nimsoft hierarchy, and a site is normally set up with one Domain. Various security aspects in the Nimsoft such as user-profiles, user-permissions and access-rights are distributed within the Domain.

The Domain is used to group one or more Hubs in a logical set such as a company or enterprise.

The Hub is a message concentrator and re-distributor. It is the collection point for all messages coming from the various installed Robots.

Right-clicking a Hub enables you to log on the hub.
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. Each computer that is being monitored by a Probe will need a Robot installed on it.

The 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.

By left-clicking a Robot, all Probes installed on that Robot will be displayed in the Main Window Pane, while left-clicking one of the Probe-groups under the Robot; only Probes in that group will be displayed.

- The Robot where the Hub software is installed is marked with a light-green indicator.
- The Hub that you are currently logged on to is also marked with a light-green indicator.

For more information on the objects found under this node, see the section Describing the Infrastructure elements.
The Navigation Pane

The Dynamic Views Node

The Group Server probe collects and analyzes information about your infrastructure. All Robots present will be detected, and the information will be organized in database tables in the NIS database.

The Dynamic Views node reflects the Infrastructure by reading the contents from these tables in the database, which is addressed by the Data Engine selected in the Options dialog. All Robots found will be listed grouped on the OS-type the Robot is running.

**Note** the color of the robots in the list. They are either grey or light blue:

- Light blue means that the group_server probe produces QoS data for this robot.
- Grey means that the group_server probe does NOT produce QoS data for this robot.

In addition, you can create your own groups in the group_server probe. Creating groups of type Nimsoft will be presented under the Dynamic Views node. The SQL statement used when creating the group defines which robots to be placed in the group.

**NOTE:** If the Data Engine is not selected in the Options dialog, the Dynamic Views node will not be shown in the Navigation pane.

**NOTE:** It is possible to hide this node from the Navigation Pane for certain Nimsoft Users, using an Access Control List (ACL, see User Administration for further description). This is done by deselecting the Dynamic Views option for this ACL.
Nimsoft users associated with this ACL will not see the Dynamic Views node.

You can launch the ACL options dialog by selecting Security > Manage Access Control List from the menu bar in Infrastructure Manager.

The Dynamic Views node lists all Robots sorted on the OS the Robot is running:
Example:

The *Windows* child-node lists all Robots installed on *Windows* computers.
Selecting one of the Robots, all Probes hosted by the Robot will be listed in the main window pane.

**Note** the color of the robots in the list. They are either grey or light blue:

- White means that the group_server produces QoS data for this robot.
- Grey means that the group_server probe does not produce QoS data for this robot.
Distributing Probe packages to multiple Robots

Distributing a probe package to a child-node, the probe package will be distributed to all Robots found under that child-node.

Example: Distributing a probe package to the UNIX child-node, the probe package will be distributed to all UNIX Robots.

Configuring Probes

Selecting a Robot under a child-node, you may also launch the configuration tool for a probe installed on that robot by double-clicking the probe in the main window pane, provided that you are logged on the Hub controlling the Robot.

The Groups Node

Note that this node will be hidden if the option Show Groups node is NOT selected in the Options dialog. The Options dialog is launched by selecting Tools > Options in the menu bar.

The Groups Node may contain user-composed groups of Probes, Robots or Hubs.

It is often useful to group a set of Probes to simplify configuration and to speed up the task of locating the Probe in a large environment.

Distributing a probe package to a group of Robots, the probe package will be distributed to all Robots in that group.
You may also group a set of Probes related to a task. E.g. a database administrator needs to configure/monitor database Probes as well as a disk monitoring Probe (cdm).

By left-clicking one of the groups, all defined elements under that group will be displayed in the Main Window Pane.

To create a new group:

Right-click in the Navigation Pane, select New > Infrastructure Group.

The New Infrastructure Group dialog pops up, and you can select the type of group you want to create (Hub, Robot or Probe).

Use the find ( ) command from The Toolbar to locate the objects that you want put into your groups. You may then drag the objects onto the newly created group.

The Archive Node

The Archive Node contains information about Probe packages and licenses stored in the archive on the Hub you are currently logged on.
Clicking the Archive node, a link to the Nimsoft Internet Archive appears in the Main window.

Clicking this link, the Nimsoft Internet Archive will appear in a separate window:
For more information about the Nimsoft Internet Archive, see the section Downloading Probe packages from the Nimsoft Internet Archive.

Expanding the Hub icon under the Archive node, you will find that the Probe packages are divided into logical groups (Application, Database, Gateway etc).

The main window pane will now list the probe packages.

What packages are listed depends on the following selections options selected:

- The option ‘Attempt Nimsoft Internet Archive integration with local archive’ option set in the Options dialog in the Tools menu. With this option selected, you will also be able to see packages located in the Nimsoft Internet Archive in addition to the packages downloaded to your local archive. The status line in at the bottom of the window (marked with a horizontal red arrow on the figure below) indicates if this option is selected or not.
Also note the four icons in the Main Window Pane’s Toolbar (marked with a vertical red arrow). Here you can select the view of the list of packages.

■ Also note the four icons in the Main Window Pane’s Toolbar when the Probe Packages sub node is selected in the Navigation Pane.
By left-clicking the Licenses icon, all licenses installed will be displayed in the Main Window Pane.

Applications
The Navigation Pane

This Node by default contains shortcuts to some Nimsoft applications. You may also define other applications frequently used to be started directly from the Navigation Pane. You may *drag* an application (.exe files) from the desktop or the Windows Explorer and *drop* it onto the *Applications* Node.

The applications icon will now appear as a Node child under the Application Node, and you can start the application by double-clicking the icon.

To create a new shortcut to an application:

Right-click in the Navigation Pane, select *New > Application*.

Give the new application a descriptive name, and you may *drag* an application from the desktop or the Windows Explorer and *drop* it onto the *Applications* Node.
This node by default contains shortcuts to some Nimsoft URLs. You may also define other URLs to be started directly from the Navigation Pane.

Open the URL in your browser and move the cursor to the icon in the URL’s address field of your Web browser, left-click, drag and drop it onto the URLs Node.

The URL icon will now appear as a Node child under the URLs Node, and you can start it by double-clicking the icon.
Right-click Menu in the Navigation Pane

Right-clicking in the Navigation Pane opens a small menu:

- **Show All Domains**
  This option is only available when right-clicking the Domain Node. By default, only the Domain you are logged on to will be shown in the Navigation Pane. By selecting this option, all defined Domains will be shown. However, the set of other domains displayed will vary according to which hub you are logged on to.

- **New**
  Allows you to add new Applications, URLs and Infrastructure Groups.

- **Application**
  Add new shortcuts for starting applications that are frequently used. You may drag an application from the desktop or the Windows Explorer and drop it onto the applications icon. It will now be accessible from the profile, and thus available to all users of the profile.

- **URL**
  Add new shortcuts for opening URLs. You may drag URL's from your favorite web-browser onto the URLs folder.

- **Infrastructure Group**
  Add new Infrastructure groups. The group folder may contain user-composed groups of Probes, Robots or Hubs. It is often useful to group a set of Probes to simplify configuration and to speed up the task of locating the Probe in a large environment.
- **Rename**
  Allows you to rename Applications, URLs or Infrastructure Groups, except the standard ones included with the Nimsoft software.

- **Delete**
  Allows you to delete Applications, URLs or Infrastructure Groups, except the standard ones included with the Nimsoft software.

- **Properties**
  Using this option, you can check and modify the various properties, depending on what you have selected in the Navigation Pane.

- **Login**
  Right-clicking a Hub and selecting the *Login* option lets logs you on to the selected Hub.

- **Move**
  Right-clicking a Robot and selecting the *Move* option opens the *Move* dialog, letting you move the Robot to another Hub on the same or another Domain. Note that you cannot move the Robot running the Hub software.

  See also the section *Moving a Robot*.

- **Remove**
  Right-clicking a Robot and selecting the *Remove* option lets you remove the Robot from the Hub.

  This is useful if you have e.g. have disconnected a computer with a Robot installed. The Robot will then appear in the Infrastructure Manager with a red indicator. Even if the computer running the Robot software is stopped (or removed), the Robot will still exist in the Hub’s list of Robots.

  Selecting the *Remove* option removes the Robot from the List.

- **Restart**
  Right-clicking a Robot and selecting the *Restart* option lets you restart the Robot.
The Main Window pane

Note the counter at the right-hand bottom of the Main Window Pane.

The counter indicates the total number of items (Tot) listed in the window (e.g. number of Probes) and the number of items selected (Sel).

You can select one item by left-clicking it and multiple items by using Ctrl + left-click.
The Main Window Pane displays different parts and levels of the structure of your Nimsoft installation, depending on what is selected in the Navigation Pane.

- If a **Domain** is selected in the Navigation Pane, the Main Window displays all Hubs under that Domain.

  **Note** the different Hub status symbols, as they appear in the Infrastructure Manager:

  - **Light green**
    The Hub that you are connected to (your login Hub), and it is up and running.
  
  - **Dark green**
    Other accessible Hubs under the domain (auto-discovered or static), and they are up and running.
  
  - **Yellow**
    The Hub has an unknown status.
  
  - **Red**
    The Hub is not accessible.
    May indicate that the Hub computer is shut down or disconnected, the Service Controller on the Hub is stopped, or the Hub license is expired.

The following columns are available in the Main Window Pane:

- **Name**
  The names of the Hub computers connected to the Domain. The one you are logged on to is marked with a light green indicator.

- **Address**
  The addresses of the Hub computers on the format:
  
  `<Domain name> / <Hub name> / <Name of the computer running the Hub software> / Hub.`
The Main Window pane

- **Security**
  This column indicates if the *security concept* is enabled for the Hub. Security is initialized during the Nimsoft installation.
  
The security includes the following topics:
  
  - **Access** - who has permission to do what?
  - **Authentication** - is the client who he/she/it claims to be?
  - **Encryption** - make it impossible for others to read the data.

- **Status**
  The status of the Hub. Should display OK.
  
  Error, which also is indicated with a red icon, means that the Hub is unavailable (e.g. computer shut down, the Service Controller on computer stopped or the Hub license is expired.)
  
  Intermediate, which also is indicated with a yellow icon, means that the status of the Hub is unknown

- **License**
  License information for the Hub Probe. Should display OK if the license is valid (and not expired).

- **Version**
  The version number and compilation date of the Hub software the Hub computer is running.

- **IP**
  The Hub computer’s IP address.

- **Port**
  The port on the Hub computer allocated for Nimsoft communication (usually 48002).

- **Domain**
  The name of the selected Domain, on which the Hub is installed.

- **Robot**
  The name of the Robot running on the Hub computer, normally the computer’s hostname.
If a Hub is selected, the Main Window displays all Robots under that Hub.

**Note** the different Robot status symbols, as they appear in the Infrastructure Manager:

- Robot is running as a Hub, status OK.
- Robot is running, status OK.
- Robot is not responding, status ERROR.

The following columns are available in the Main Window Pane:

- **Robot**
  The names of the Robot computers connected to the selected Hub. The one running the Hub software is marked with a light-green indicator.

- **Address**
  The addresses of the Robot computers on the format: <Domain name> / <Hub name> / <Robot name>.

- **License**
  License information for the Hub Probe running on the Hub computer. Should display OK, indicating that the number of licenses used and expire date is not exceeded.

- **IP**
  The IP address of the Robot computer.

- **Status**
  The status of the Robot. Should display OK. If status is Error (also indicated by a red indicator), it probably means that the Robot computer is stopped or disconnected.

  If the Hub is stopped or disconnected, all Robots controlled by that Hub will search for a secondary Hub as defined in the Robot’s configuration tool (the Controller).

- **Version**
  The version and compilation date of the Robot software.

- **Type**
  Indicates the Robot’s ‘connection’ to the Hub.
  The two main types are Regular and Passive.

- **Created**
  When the Robot was created/installed or moved to the Hub.
The Main Window pane

- **Updated**
  The last time the Robot was updated by the Hub.

- **OS Major, OS Minor and OS description**
  A description of the operating system the Robots are running.

- **Tag # 1 and Tag # 2**
  User-defined tags used for defining identification properties for computers in the infrastructure. The tags are defined under Setup > Misc in the configuration dialog for the controller probe.

- **Port**
  The port the Robot computer allocated for Nimsoft communication, normally 48000.

- **Domain**
  The name of the Domain the Hub is connected to.

- If a Robot is selected in the Navigation Pane, the main window displays all Probes installed on that Robot.

  **Note** the different Probe status symbols:
  - Green. The Probe is running and is controlled by the Robot.
  - Yellow. The Probe is not controlled by the Robot, but has registered a remote command port.
  - Grey. The Probe is disabled/deactivated.
  - Red. The Robot detected an error situation during the startup period of the Probe.
  - Red with a lock symbol. The Robot denies startup of Probe due to missing security permissions.
  - Red with a license symbol. The Robot denies startup of Probe due to an invalid license.

  The following columns are available in the Main Window Pane:

  - **Probe**
    The name of the Probe.

  - **Robot Address**
    The full address of the Robot hosting the Probe: <Domain><Hub><Robot>.
■ Class
Identifying the type of probe (Probe or Probe/Port).
Probe indicates a probe which is not listening to an attached port. This can be because it is inactive, or because it runs at specific intervals and is not controlled by the Infrastructure Manager (like the logmon probe, for example).
Probe/Port indicates a probe which is actively listening on an attached port.
Port means a Probe/program that has been started (and attached a port), but the controller does not recognize it. Can typically be a custom-made program for test purposes.

■ Description
A short description of the Probe.

■ Group
The logical group the Probe belongs to.
Probes are divided into different groups, depending on monitoring purposes (Network probes, Database probes, System probes, Gateways etc).

■ Address
The Probe address: <Domain><Hub><Robot><Probe>.

■ Port
The Probe’s communication port.

■ Pid
The Probe’s process identification number.

■ Active
If the Probe is active or not.
Possible states:
Yes means the Probe is activated.
No means the Probe is deactivated.
Error indicates an error condition for the Probe, the Probe icon should also be red.
Right-clicking the Probe, selecting View Log, opens the Log Viewer window. Here you probably can find the reason why the error condition occurred.

■ Command
The name of the Probe’s executable (the process started when the Probe is activated).

■ Arguments
The argument list accompanying the command.
■ Working Directory

The working directory of the Probe (within the Program Files/Nimsoft folder). The working directory normally is probes, hub or robot.

■ Configuration File

Name of the configuration file (<Probe name>.cfg) found in the working directory.

■ Log File

The name of the Probe’s log file (normally <Probe name>.log) found in the working directory.

In the Probe’s configuration tool, it is possible to rename the log file and set the level of details written to the file.

The probe logs information about its internal activity. The file is a text file and can be opened in for example Notepad.

It is advisable to log as little as possible during normal operation to minimize disk consumption, and rather increase the amount of detail only when debugging.

■ Data File

Name of the data file accompanying the Probe. Only a few of the probes are accompanied by a data file (e.g. ntevl and ntpref).

■ Type

The type of the Probe, either daemon, on_demand or timed.

■ Daemon probe

A daemon probe is always active if activated by the operator. If it stops, the Robot immediately restarts it. However, note that it is also possible to specify a time range within which the Probe will run.

- Runs always. Will be restarted by the Robot if it stops.
- Is network aware and supports command interface.
- Can subscribe to messages on the Nimsoft.

■ On_demand

The probe is not automatically started, but can be started explicitly when required.
■ Timed probe
   A timed probe runs once and then terminates, awaiting the next point in
time when it is configured to start.
   - Started by the Robot at intervals or a given schedule.
   - Runs through all checkpoints and reports all threshold breaches.
   - Must keep all states between runs if needed.

■ Time Specification
   Specifies when the Probe is active (see interval for timed Probe and time range
for deamon Probe above).

■ IP address
   The IP address of the computer hosting the Probe.

■ Package
   The name of the Probe package.

■ Version
   The Probe software version.

■ Robot
   The name of the Robot where the Probe is installed.

■ Groups
   See Probes, Robots and Hubs described above.

■ Archive
   By left-clicking the Hub icon under the Archive Node, all Probe packages installed
will be displayed in the Main Window Pane.
Note the four extra tool buttons added to the toolbar at the upper part of the window. The tool buttons are present only when the Hub icon under the Archive Node in the Navigation Pane is selected. See description in the section The Toolbar in the Main Window.

Symbols:

- New version available in Nimsoft Internet Archive (unlicensed Probe).
- New version available in Nimsoft Internet Archive (licensed Probe).
- Distributed Probe with valid license.
- Distributed unlicensed Probe.
- Distributed Probe without valid license.
- Distributed unlicensed Probe, beta version.
- Distributed licensed Probe, beta version.
- Licensed probe in the local archive with version number higher than the probe found in the Nimsoft Internet Archive/beta-archive.
- Unlicensed probe in the local archive with version number higher than the probe found in the Nimsoft Internet Archive/beta-archive.
The following columns are displayed in the Main Window Pane:

- **Name**
  The name of the Probe package.

- **Description**
  A short description of the Probe package.

- **Status**
  The Probe status (OK, License expired, New version available etc.).

- **Version**
  The Probe package software version.

- **Web Version**
  The version number of the newest version available from the Nimsoft Internet Archive.

- **Group**
  The logical group the Probe belongs to.

- **License Info**
  The name of the owner of the license.

- **License Expires**
  The date when the license expires, if not unlimited.

- **Required**
  If a license is required or not.

- **Date**
  The date the current Probe package was generated.

- **Size**
  The size of the Probe package (in KB).

- **Release Note**
  The name of the Probe package’s release notes html file.

By left-clicking the License icon under the Archive Node, all licenses installed will be displayed in the Main Window Pane. The following columns are displayed:

- **Product**
  The name of the product for which the license is valid.

- **Info**
  The name of the owner of the license.
The Main Window pane

- **Expiration Date**
  The date when the license expires.

- **IP**
  The IP address of the computer for which the license is valid.

- **#**
  The number of licenses included in the license string.

- **Code**
  The license code.

**The Toolbar in the Main Window**

The Main Window Pane also includes a set of functional tool buttons making it easier to navigate in the pane.
See a description of the tool buttons in the section *The Toolbar in the List*.

Note the four extra tool buttons added to the toolbar when the Hub icon under the Archive Node in the Navigation Pane is selected:

- When selected, only packages located in your local archive will be listed.
- When selected, probes with valid license and with newer versions available in the Nimsoft Internet Archive will be listed.
- When selected, packages available in the Nimsoft Internet Archive, but not in your local archive will be listed.
- When selected, all packages (either located in your local archive or in the Nimsoft Internet Archive) will be listed.

**Right-clicking in the Main Window Pane**

Right-clicking in the Main Window Pane opens a menu, giving a lot of possibilities. The number of available options depends on what is displayed and selected in the Main Window Pane.

```
View
Up
Configure... Ctrl+Z
Activate
Deactivate
New...
Edit...
Delete
Log Viewer Ctrl+V
Map Viewer Ctrl+M
Update Version...
Print Preview
Print...
Security
Edit
```
Common options

For a description of the common options available, independent of what is displayed in the window, see the section Right-clicking in a list.

Options available when Robots are displayed in the Main Window Pane

This section describes options available (in addition to the Common options) when Robots are displayed in the Main Window Pane.

View

- View
  - Up
  - Actions
  - Restart
  - Move...
  - Remove
  - Maintenance
  - Print Preview
  - Print...
  - Edit
Views: The view function is used to manipulated the view of the robots in the window. There are various types of views available. Refer views for more information.

Sort By: This option let you sort the robots by different robot properties such as Robot name, address, License etc.

Row Details: This option opens the Row Details dialog showing robot information.

### Row Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robot</td>
<td>thillai</td>
</tr>
<tr>
<td>Address</td>
<td>/Nimsoft/Nimbus/thillai</td>
</tr>
<tr>
<td>License</td>
<td>OK</td>
</tr>
<tr>
<td>IP</td>
<td>172.18.4.5</td>
</tr>
<tr>
<td>Status</td>
<td>OK</td>
</tr>
<tr>
<td>Version</td>
<td>3.52 Jun 9 2009</td>
</tr>
<tr>
<td>Type</td>
<td>Child</td>
</tr>
<tr>
<td>Created</td>
<td>07/22/09 13:14:43</td>
</tr>
<tr>
<td>Updated</td>
<td>06/12/09 11:21:53</td>
</tr>
<tr>
<td>OS Major</td>
<td>Windows</td>
</tr>
<tr>
<td>OS Minor</td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td>OS Description</td>
<td>Service Pack 3 Build 2600</td>
</tr>
<tr>
<td>Tag #1</td>
<td></td>
</tr>
<tr>
<td>Tag #2</td>
<td></td>
</tr>
<tr>
<td>Pot</td>
<td>48000</td>
</tr>
<tr>
<td>Domain</td>
<td>Nimsoft</td>
</tr>
<tr>
<td>Maintenance Until</td>
<td></td>
</tr>
</tbody>
</table>

[Image showing the Row Details dialog]
**Sort**: Select this option to sort the robot records. You can apply sorting of three different levels on the different robot properties. You can also set sorting orders and perform case sensitive sorting too.

![Sort dialog box]

**Columns**: Use this option to select property columns to be displayed for the Robot. See Columns for more details.

**Toolbar**: Include or remove toolbar from the window by selecting or not selecting the option respectively.

**Status bar**: Include or remove status bar from the window by selecting or not selecting the option respectively.

**Properties**: Opens the properties box for the robot, to specify or update the robot properties.

![Properties dialog box]
Up

Selecting this option brings you one step up in the infrastructure hierarchy; the Hubs are displayed.
**Actions**

Using the *Actions > Configure* option, you can create actions (command and argument).
The defined actions will, when created, appear as shortcuts in the menu.

You can add your own user defined menu commands that will show up in the popup menu when you right click on the Robot list. Press the ‘New’ button if you want to add a new command. You can determine the menu command ordering by using the ‘Move Up’ and ‘Move Down’ buttons. In the argument field you have the option to specify a great number of tokens, which will be expanded to the correct value when you actually initiate the command.

E.g. $ROBOT in the argument list will be replaced with the name of the Robot selected when you activate the command. The tokens available are the same as the column name headers in the Robot list. Just add a $ to the column name and uppercase the letters. So e.g. Address will become $ADDRESS. You need to save your user defined menu configurations to a profile if you want them to persist between sessions.

**Note: User actions can also be defined when right-clicking in the alarm list.**

This option lets you define your own actions to be performed on alarms.

You can add your own user defined menu commands that will show up in the popup menu when you right click on an alarm in the list.

Select Configure to bring up the dialog to configure your action. Press the ‘New’ button if you want to add a new command. You can determine the menu command ordering by using the ‘Move Up’ and ‘Move Down’ buttons. In the argument field you have the option to specify a great number of tokens, which will be expanded to the correct value when you actually initiate the command.

**Restart**

Restarts the Robot software on the selected Robot.
Move

Option for moving the Robot to another Hub.

Opens the *Move* dialog, where you can select to which Hub to move the Robot. Note that you cannot move the Robot running the Hub software (marked with a light-green indicator).

See also the section Moving a Robot.

Remove

Removes the selected Robot, and the Robot is not managed by a Hub anymore.

Note that the removed Robot can be found and moved to a Hub, using the Connecting a Robot option.
Maintenance

**Note:**

The prerequisite for the Maintenance option is to install the infrastructure Manager version => 3.60 (rev. 4), HUB version => 4.30 and Robot version => 2.80. The option is not available otherwise.

The Maintenance option has two sub options:
1. **Set Maintenance Mode Until**
2. **Leave Maintenance Now**

**Set Maintenance Mode Until:** This option lets you set the selected Robot (s) in maintenance mode for the period specified.
This is useful if you want to stop the computer where the robot is running due to maintenance etc.

The Robot stops all probes and stop sending messages on the Nimsoft.

This is reflected by the icon coloring in the Robot and Probe lists. When set in maintenance mode, the Robot icon will first be red for a short while with status Error, and then be white with status Maintenance.

The probe icon of other probes indicates that these probes are suspended while the robot is in maintenance mode.

Probe distribution and activation can be performed while the robot is in maintenance mode, however the affected probes will be suspended and not actually started.

The Robot will automatically be started when the specified maintenance period is exceeded.

**Leave Maintenance Now:** To manually exit the maintenance mode immediately, select this option. The following warning appears before leaving the maintenance.

![Warning dialog](image)

Click **Yes** to leave the maintenance mode, otherwise **No**.

**Print Preview:** Select this option preview the page to be printed, which includes Robots’ details.
Print: This option opens the Print dialog to print the robot details.

![Print dialog]

Edit: This option let you select Robot(s) from the list.

Select the Select command to select or deselect robots from the list. You can invert your selection too.
The Main Window pane

**Filter**: This option opens the Filter dialog to filter the robot with specific characters in their property from the list.

![Filter dialog]

**Copy to Clipboard**: Select this option to copy the Robot properties in the clipboard. Information message is displayed after the copy is done.

![Information message]

**Enterprise Console Compatibility**

Note that you may select Robot(s) (multi-select supported) from the list and drag and drop on a dashboard in the Enterprise Console (if in design-mode).

**Options available when Probes are displayed in the Main Window Pane**

This section describes options available (in addition to the Common options) when Probes are displayed in the Main Window Pane.

**Up**

Selecting this option brings you one step up in the infrastructure hierarchy:

Selecting this option when Probes are displayed in the window, Robots will be displayed.
Configure...

Opens the configuration tool for the selected Probe. When configuration modifications have been made, you must restart the Probe.

See the Probe on-line documentation, launched by selecting Help > Probes in the Toolbar in Infrastructure Manager, for configuration parameters for the different probes.

Configuration Lock

If someone else has already opened the configuration tool for the same probe, you get the following message:

![Configuration Lock dialog]

You now have two options:

- Select No to open the configuration tool in read mode. You can not make any changes to the probe configuration, but you can see the current settings.
- Select Yes to take over control of the probe configuration. The other user loses control and will not be able to make changes to the probe configuration.

Activate

Activates (starts) a Probe that has stopped or has been deactivated, using the Deactivate option.

Deactivate

Deactivates (stops) a running Probe. The Probe can be activated again, using the Activate option.

New...

This option let you define a new Probe (see the section Adding a new Probe Definition).
The Main Window pane

Edit...

Opens the Edit dialog for the selected Probe, allowing you to edit the Probe definition.

See the section Adding a new Probe Definition for the different properties.

![Edit dialog](image)

Delete

Deletes the selected Probe. You will be asked if you want to delete it permanently, or not.

![Delete dialog](image)

If selecting Delete permanently, the probe will be completely deleted. If not checking the Delete permanently option, the Probe package will still be found in the Hubs archive, making it possible to distribute it to the Robot again later if you wish.
View Log

Opens the Log Viewer window, reading the Probe’s logging file, where most Probes record various run-time events. See also the section Viewing a Probe’s log-file.

View Dashboard

Launches a Configuration Dashboard, if existing, for the selected probe. Configuration Dashboards are designed to control probe configuration files, and is a powerful feature truly integrating the Enterprise Console with the Infrastructure Manager.

Update Version

This option allows you to update to a newer version of the selected Probe. The utility checks if your local Hub archive contains a newer version of the Probe. If found, you are asked if you want to update to the newer version.
Security

Here are two security options:

- **Set Access**

  Opens the *Set Probe Access* dialog for the selected Probe, where you are allowed to set the IP access to the Probe.

  You are not allowed to modify the access properties for Probes where the access already is set, using the Probe Administration (*Security > Probe Administration…*)

- **Validate**

  Allows you to validate (manually start) the selected Probe if the Robot Controller is not able to start it. The probe icon will appear like this in the Probes list in the Main Window, and status shown in the *Active* column will be *Error Validation*.

  In the *Package Editor*, used when designing Probe packages, a *Check CRC flag* can be set. The checksum is written to the controller.cfg file at Probe distribution, and will be compared each time the Probe is started. If the controller detects that the checksum has changed, it refuses to start the Probe.

  You may then either re-distribute the Probe, or (if you know that nothing seriously is wrong) select *Validate* to start the Probe.

**Options available when Probe packages are displayed in the Main Window Pane**

This section describes the options available (in addition to the Common options) when the Probe packages in the Archive are displayed in the Main Window Pane.

First, Note the four extra tool buttons added to the toolbar at the upper part of the window. The tool buttons are present only when the Hub icon under the Archive Node in the Navigation Pane is selected. See description in the section *The Toolbar in the Main Window*. 
Refresh

Refreshes the window, updating the window with the most current information.

New

This option opens the Package Editor dialog, enabling you to create new Probe packages. Probe packages are used for Probe distribution to Robots. The new probe package will be placed in your local package archive.

For more details, please see the package editor chapter in the Probe documentation (NimbusDoc.chm help file).

Edit...

This option is available when packages in your local archive are listed.

Opens the Package Editor dialog, where you can edit the selected Probe package. Probe packages are used for Probe distribution to Robots.

For more details, please see the package editor chapter in the Probe documentation (NimbusDoc.chm help file).

Delete

This option is available when packages in your local archive are listed.

Deletes the selected Probe package(s) from the local archive on your Hub. You are asked if you really want to delete the package(s). Clicking Yes permanently deletes the package(s) from your Hub archive.
Configure archived configuration

This option lets you modify the configuration files distributed with the probe package.

This option was introduced in the version of Infrastructure Manager delivered with Nimsoft Server 3.60 or newer, and the first probe package enabled to take advantage of this feature is the logmon probe, version 2.20 or newer.

Note that you must start the configuration tool with an installed probe first so that the configuration tool is fetched from the Archive.

The option is also available in the distsrv version 4.7.x or newer, where you right-click the probe package listed on the Status tab and select Configure archived configuration.

The dialog shown below appears, letting you select which configuration file to configure.
When selected, the GUI for the probe appears, letting you set the options and parameters you want.

Click the **Apply** button when finished. The configuration file in the probe package is now updated, and the package can be distributed to the robots with the modified configuration file.
Distribute

Opens the Distribute dialog, where you can distribute the selected package(s) to one or more hubs attached to the Domain you are currently logged on.

Expand the tree list on the lower left-hand side and drag either a Hub or a Robot from that tree and drop in onto the initially empty Destination Robots list on the right side. If a Hub is dropped, the system will automatically expand the Hub into the set of Robots it represents. Another way to make your selection is to select either a Hub or a Robot in the tree in this dialog, and press the Add button. Note that Robots placed in the destination list can be removed by selecting them, and then pressing the Remove button.

Clicking the OK button starts the distribution job.

Note that you may also distribute packages manually by dragging one or more packages from the package-list and dropping it/them onto a Hub (distributes to multiple Robots) or to a single Robot.

The package-list will appear in the Main Window Pane if you expand the node named Archive in the Navigation Pane on the left side. A list containing all the available packages in will appear on the upper right-hand side. The list contains detailed information about the packages available for distribution, such as version and licensing information.
View Progress

If you have started a Probe package distribution job, the Progress dialog will show the distribution progress.

If you have closed the progress dialog, you may open it again, using the View Progress option.

Import

Selecting Import enables you to import probe packages into your local package archive. An explorer window will be opened, letting you browse to the location where probe package you want to import is located.

Select the package and click the Open button. The package will be added to your archive.
Download

This option is activated when packages that are present in the Nimsoft Internet Archive only (and not in your local archive) are selected.

You can download the selected package(s) from the Nimsoft Internet Archive and store them in your local package archive.

A window appears on your screen, informing about the distribution progress.

![Distribution Progress Window](image)

Note that you will be asked if you want to overwrite the existing version of the package already present in your local Hub archive.

![Data Transfer Window](image)

Explore Nimsoft Internet Archive

Opens the Nimsoft Internet Archive in a separate window. Note that it is possible to select packages in the Nimsoft Internet Archive window, drag and drop them into your local package archive. Also note the different archive modes, described in the section Nimsoft Internet Archive Mode. The selected mode determines what packages are available and possible to download.

See also the section Downloading Probe packages from the Nimsoft Internet Archive.
Product Information

Opens a separate window containing a short piece of information about the selected probe package.

Nimsoft Internet Archive Mode

This option lets you select between three different archive modes, determining what part of the Nimsoft Internet Archive that will be shown in the window.

The Nimsoft Internet Archive is divided in the following three sections:

GA (General Availability)

This is the section you should use when downloading probes. It contains the final version of the probes, tested and verified by the Nimsoft QA department.

CR (Control Release)

This section contains probes that are in the Control Release phase. Prior to releasing the probes for General Availability, they stay in Control Release for a limited period of time. The probes are tested and verified by the Nimsoft QA department, but problems reported by customers may be corrected before the GA release. Probes in the CR section are made available to a limited number of users who want to participate in the final test and verification process of the probe.

Beta

This section of the archive contains probes that are in the Beta phase. Initial testing by the Nimsoft QA department has been conducted, but the probes may still be modified as the test program moves forward. Customers may download Beta versions to have a closer look at new features and functionality.

In addition the archive contains a selection of unsupported probes.

Options available when Licenses are displayed in the Main Window Pane

This section describes options available (in addition to the Common options) when the Licenses in the Archive are displayed in the Main Window Pane.

Refresh

Refreshes the window to display the most current information.
Add License

This option lets you add a license to the Archive. The Add License dialog appears, enabling you to type or paste the license text string into the license field and click the OK button.

You can paste multiple licenses into the window. Use <Return> to shift to a new line to paste additional licenses into the window.

An information text appears, informing you that the license has been successfully added. Click the OK button.

Delete

Deletes the selected license(s) from the Archive.

You will be asked to confirm that you really want to delete the selected license(s). Clicking the Yes button completely deletes the license(s) from your local archive.
The Toolbar

The Toolbar includes a subset of functions also found in the menu line:

- **Show Navigation Pane**
  
  Shows / hides (toggling) the Navigation Pane from the application window.

- **Show Dock Pane**
  
  Shows / hides (toggling) the Dock Pane from the application window.

- **Launch Main Window Pane**
  
  Launches the Main Window Pane as a separate window. You will then have two instances of the Main Window Pane, enabling you to work with different views in the two windows.

  **Example:**

  Having selected one Robot node in the Navigation Pane, the Probe list for that Robot will be listed in the Main Window Pane. Launch the Main Window Pane as a separate window and select another Robot in the Navigation Pane. You will now be able to see and work on Probes from both of the Robots.
- **Dock Window**
  If a window (e.g. the Main Window Pane) is opened as a separate window, it can be moved to the Dock Pane by clicking this button. The window will be added to the Docked Windows list (see below).

- **Undock Window**
  Removes the current docked window from the Dock Pane and opens it as a separate window. The window will be removed from the Docked Windows list (see below).

- **Previous Window in Dock Pane**
  Selects the previous Window in Dock Pane. Windows sent to the Dock Pane are added to the Docked Windows list, and this function will display the previous window on the list in the Docked Window.

- **Next Window in Dock Pane**
  Selects the next Window in Dock Pane. Windows sent to the Dock Pane are added to the Docked Windows list, and this function will display the next window on the list in the Docked Window.

- **Docked Windows list**
  Windows sent to the Dock Pane are added to the Docked Windows list. Using the previous and next buttons described above, you can select the window to be listed in the Dock Pane.

- **Login**
  Opens the login dialog, where you can log on with a valid Nimsoft user name and a password. If not clicking the Advanced button, you will log on the Hub you are currently logged on, with the user name and password you specify.

  Clicking the Advanced button, you will have the option to log on another Hub (also Hubs on other Domains).

- **Find**
  Opens the Find dialog, where you can search and locate Hubs, Robots, or Probes. You have the option to restrict the search from to the current login Domain (timesaving), or from all Domains.

  The dialog also offers more advanced search functionality, such as:
  - Class or/and group of Probes
  - OS type (when searching for Robots).
Hold Events

This option is useful in situations where a large number of events occur, causing this might slow down and result in a slower response from the Infrastructure Manager. No events will be received and managed by the Infrastructure Manager as long as this option is activated. You will notice that the option is turned on by the flashing status bar at the bottom of the window.

The option can be selected by clicking the button, but it will also be automatically turned on if the number of events exceeds a value set in the registry. You can adjust this threshold value by modifying the registry key `IgnoreNimEventsCount`, located in:

```
HKEY_CURRENT_USER > Software>Nimsoft Software > Nimsoft Manager > Options.
```

The Dock Pane

The Dock Pane appears in the lower part of the Infrastructure Manager Window (if the menu option `View > Dock Pane` is checked).

By default, either the Alarm Window (displaying alarms received) or the Message Window (showing system- and communication-messages) can be displayed in the Dock Pane, depending on what is selected in the Menu Bar:

- View > Alarm Window or
- View > Message Window.

But also the contents of the Main Window Pane, when first launched in a separate window, can be directed to the Dock Pane.

Launching the contents of the Main Window Pane can be done by selecting `Window > Launch Main Window Pane` in the Menu Bar, or by moving the cursor towards the right edge of the window until the cursor appears as shown below and left-clicking.

```
Selecting Window > Dock Window Pane in the Menu Bar directs the separate window to the Dock Pane.

Windows that have been moved to the Dock Pane appear in the Docked Window List. This list pops up if you select Window > Docked Window List from the Menu Bar. In this list, you can activate or remove windows from the Dock Pane.
The Dock Pane

The Alarm Window

See description in the section The Alarm SubConsole Window for a description of the Alarm Window.

The Message Window

The Message window displays Nimsoft-internal messages and trace information.

By right-clicking in the Message window, you get the following options:

- Show messages (default). The messages shown are console internal messages indicating what events and actions have taken place, and can be used as a debugging tool.
- Show Trace, displaying the events at a more detailed level.
- Clear messages, which removes all messages from the Message window (trace information is still available).
Chapter 4: Infrastructure Manager User Guide

This section contains the following topics:

- Logging on Infrastructure Manager (see page 135)
- Working with Infrastructure Manager (see page 136)
- Managing the Robot on a AS400 computer (see page 183)
- Modifying the Infrastructure (see page 183)

Logging on Infrastructure Manager

You can do almost all of the configuration, control and management of your system through Infrastructure Manager.

Launch Infrastructure Manager by selecting Start > Programs > Nimsoft Monitoring > Infrastructure Manager.

The login dialog appears, and you must log in with a valid Nimsoft user and password.

With Infrastructure Manager Version 3.70.2 or newer, it is also possible to log on the consoles as a LDAP user. Thus the LDAP group structure can be used, and it is no longer necessary to define the users as Nimsoft users. Using ACLs (Access Control Lists), users belonging to different groups in LDAP can be assigned different permissions in Nimsoft.

Avoid creating Nimsoft Users and LDAP users with identical user names.

If this is a first time login, and no other Nimsoft users have been created, you must use the user and password specified as Initial user during the Nimsoft Server Installation.
Clicking the **Advanced** button, you will have the option to log on another Hub (also Hubs on other Domains).

---

**Working with Infrastructure Manager**

This section describes how to manage the Nimsoft infrastructure, using Infrastructure Manager.

The following tasks will be described:

- Distributing Probes (to archive on Hub and to local archive)
- Getting license keys
- Managing the Infrastructure
Connecting a Robot

Infrastructure Manager enables the operator to manage the infrastructure. One of the major elements in this infrastructure is the Robot. The Robot will, when it’s installed on a LAN, attempt to connect to the nearest Hub. The only requirement for this **plug and play** functionality to work is that at least one Hub is installed on the same subnet as the Robot. Otherwise, you’ll have to manually "tell the Robot where to find the Hub". This is done by using Infrastructure Manager.

Follow these steps if you want to connect to an unmanaged Robot (one that is not visible in Infrastructure Manager)

1. Launch Infrastructure Manager.
2. Select Tools > Connect Robot....
3. Type in the IP-address/name of the remote system.

Follow these steps if you want to connect a managed Robot (one that is visible in Infrastructure Manager)

1. Launch Infrastructure Manager.
2. Select/highlight the Robot you wish to connect to in the tree control.
3. Right-click and select **Connect Robot...** or press **Ctrl + R**.
4. Press the **Get Info** button.
This will perform a request to the remote Robot, returning information about which Hub it is managed by.

You have now obtained information about where the Robot is connected. The information area will contain the names of the primary and secondary Hubs (or "NO Hub" if it is unmanaged) the Robot relates to.

You may:
- Move the Robot to another Hub by clicking the Move button (see Moving a Robot (see page 145)).
- Issue a restart command to the Robot by clicking the Restart button.
- Exit the window by clicking the Close button.
Configuring a probe using the internal editor (raw configure)

As you initiate a probe configuration, Infrastructure Manager will attempt to launch an external configuration program from the *util* directory. If such a configuration program is not present for a certain probe, the manager will get the configuration file from the Robot (remote), and present it in a *regedit*-like editor. The various configuration tools/programs are documented in the technical reference chapters.

You may add, delete and modify the nodes in the configuration file, as well as the variable name/value elements.

**Note:** This method is also available (as an advanced feature) when a configuration program exists. You may activate it by pressing *Shift+Right-Click* and selecting *Raw Configure...*

**Note:** If the selected probe configuration contains references to a *data-file*, then the user is presented with an option to view/edit the *data-file* or the raw-configuration file.
The Probe Utility

Using the Probe Utility, you will be able to access and run the selected probe’s command set and watch the output returned in a window. This can be very useful for debugging purposes. To start the Probe Utility for a specific probe, you select the probe in Infrastructure Manager (left-click the probe) and click $<\text{CTRL}> + P$ simultaneously.

The Probe Utility window contains the following four sections:

- The Toolbar, containing six buttons.
- The Probe Command set section, consisting of:
  - a drop-down menu where you can select one of the commands available.
  - a parameter list, where parameters belonging to the selected command will be listed. Note that note all commands have associated parameters.
  - an input field, where you can specify a value for the parameter selected in the parameter list.
- The Command output window, listing the output based on the command you run.
- The Status bar (located at the bottom of the Probe utility window) showing status of the last command sent (OK, Communication error etc.).
The Toolbar

The toolbar contains the following six buttons:

- The **Info** button. Clicking this button, the Command output window will list available general probe information, such as probe name, probe version, lib. version, etc.

- The **Restart** button. Clicking this button restarts the probe. You will be asked to confirm that you really want to restart it.

- The **Stop** button. Clicking this button stop the probe. You will be asked to confirm that you really want to stop it.

- The **Run** button. Clicking this button runs the command selected in the Commandset section (optionally with the selected command parameter).

- The **Options** button. Clicking this button opens the properties dialog for the probe.

The option box contains:

- A Nimsoft address field, showing the the probes address <Domain><Hub><Robot><probe name>.

- The IP address of the computer hosting the probe.

- Request timeout, indicating the maximum time to wait for a response from the probe on the command sent. No response within this period results in an error status.
■ Show variable type (and size). When checked, the command output field will, in addition to the variable name and value, also show the variable type (integer, PDS, string) and size.

■ Expert Mode. When checked, a set of additional commands for advanced use are added to the Probe commandset list.

The Print button. Clicking this button opens the printout properties dialog, allowing you to print the contents of the command output window.

Running probe commands from the dos prompt:

Note that you can also run the probe commands from the dos prompt, using the pu command. The example below runs the get_info command for the cdm probe on /Development/wsrun/wsrun (user name rune and password 1234admin):

pu -u rune -p 1234admin /Development/wsrun/wsrun/cdm get_info
Viewing a Probe's log-file

Most Probes record various run-time events to a log-file. This log-file may be viewed from the Infrastructure Manager by right-clicking the Probe and selecting View Log.

This opens the Log Viewer window, which will display lines from the log-file. Please note that most Probes have a way to set their levels of detail for the logging facility.
Infrastructure Manager is an event-driven application that needs to be "hooked" up to the Nimsoft via a Hub. Therefore, you will need to select a Hub to log on to within the Domain where you want to receive the events generated on the Nimsoft.

Select Security > Login... from Infrastructure Manager to connect to other Hubs than your primary connection point.

You can also right-click on a Hub in the tree control and select the 'Login' menu item. If the current user name and password is applicable for the Hub in question, you will automatically be logged on to this Hub without the "Login dialog" being displayed.

A list of available Hubs is presented. This list will only contain the "well-known" Hubs on the LAN. These include

- Hubs running on the same subnet
- Hubs with "static routing" definitions

In cases where you need to connect to a Hub that you don't see, type in the hostname/IP-address in the Hub IP input field and click OK.
Moving a Robot

The Infrastructure Manager enables the operator to manage the infrastructure. One of the major elements in this infrastructure is the Robot. The Robot will when installed on a LAN attempt to connect to the nearest Hub. The only requirement for this plug 'n play functionality to work, is that at least one Hub is installed on the same subnet as the Robot. Otherwise, you'll have to manually "tell the Robot where to find the Hub". This is done by using the Infrastructure Manager:

1. Connect to the Robot (see the section Connecting a Robot), or right-click the Robot you want to move in the Navigation Pane and select Move. The following dialog appears:
Selecting *Show hubs in all domains*, all hubs will be listed. If the option is NOT selected, only Hubs in the domain you are currently logged on will be listed.

2. Select a Hub from the list, and press **OK**.

   The Infrastructure Manager attempts to instruct the remote Robot to be managed by the selected Hub.

3. The information area is updated with the correct relationships.

   **Note** the *Use DNS Lookup* option. If ticking this option, the Hubs in the list will be greyed out and cannot be selected. The **DNS Name** field at the bottom of the dialog will be enabled, allowing you to specify the DNS name of the computer hosting the Hub to which you want to move the Robot.

   **Hint**: You may also use the drag ’n drop feature in the Infrastructure Manager to move a Robot from one Hub to another. Select/highlight the Hub that manages the Robot you want to move (in the Navigation Pane), drag the Robot (from the list of Robots displayed in the Main Window Pane) and drop it onto the destination Hub.
Adding a new Probe Definition

The Infrastructure Manager enables the operator to manage the Probe definitions on any Robot. Selecting a Robot in the Navigation Pane, all Probes installed on the selected Robot will be displayed in the Main Window Pane. Right-clicking in the Main Window Pane opens a small menu, enabling you to create a new, edit or delete a Probe definition.
Probe
The name of the Probe.

Type
The type of the Probe, one of daemon, on_demand and timed.

Command
The name of the executable, relative to the working directory or the full path if specifying an executable elsewhere in the directory structure.

Arguments
The argument list accompanying the command.

Working directory
The working directory of the Probe, often Probes/...

Configuration file
The name of the configuration file found in the working directory.

Data file
The name of the data file accompanying the Probe.

Time specification
Specifies when the Probe is active; see more in the section Time Specification Format.

Execution
Specifies when and/or how often the Probe is executed.

Group
The name of the Probe group it belongs to.

Description
A short description of the Probe.

Log file
Name of the log file used by the Probe.
Time Specification Format

The format of the time specification used in the Range From / To and Execution / Start at fields are as follows:

- <minute>
- <hour>:<minute>
- <weekday> <hour>:<minute>
- <day of month> <hour>:<minute>
- <month> <day of month> <hour>:<minute>

Examples:

- **Range From**: 03:15, **Range To**: 06:00.
  This means:
  Activate the Probe in this interval. The Probe is terminated when it passes its window of time.

- **Start at**: 04:20.
  This means:
  Start the timed Probe at 04:20.

- **Interval**: 5 min.
  This means:
  Start the timed Probe at 5 min interval. This may be combined with a range specification.

A daemon probe, running from 04:00 to 08:00 every day:
A timed probe, running once every Sunday at 08:45:

A timed probe, running once at 08:45 the first day of every month:

A timed probe, running at 5 minutes intervals, Monday to Friday:
Finding Nimsoft components

The dialog is invoked from the Menu bar in Infrastructure Manager by selecting: Tools > Find...

Use this dialog to locate Hubs, Robots, or Probes cross-Domain in the system.

Example:

To find all cdm Probes installed on the Domain:

- Select the Domain Node in the Navigation Pane.
- Select Tools > Find.
- Specify searching criteria in the Find dialog as shown above and click the OK button. All Probes found will be listed in a separate window, including detailed Probe information (version number, Robot etc.)


**Probe administration**

The dialog is invoked from the Menu bar in Infrastructure Manager by selecting *Security > Probe administration...*

This dialog enables you to set the upper access level a certain Probe will have in the system.

![Probe Administration Dialog]

In effect that means the security level the Probe has when accessing other Probes within the same Domain. If the entry for a certain Probe is missing in this list, the Probe will have the lowest security level set. That means it can perform very limited actions against other Probes.

If the probe needs access to other probes or parts of the Nimsoft, other than for sending messages, one of following access permissions can be given:

- Open
- Read
- Write
- Admin

The security settings for the Probes is defined in the Probe

You can also limit the computers the Probe has access to by assigning the corresponding IP addresses. No value in this field means general access rights to all computers within the Domain. Limited computer access is specified by a row of IP addresses separated with the '|' character.
Creating Mobile Panels

Creating Mobile Panels, you are allowed to view, assign and acknowledge Alarm messages directly on your mobile phone, and also provides QoS, SLO and SLA data.

You can create and make Mobile Panels available, using the mobile_panels probe.

For more details, please see the mobile_panels chapter in the Probe documentation (NimbusDoc.chm help file).

Defining user-actions

You can add your own user defined menu commands that will show up in the popup menu when you right click on the Robot list.

Activate user actions dialog by selecting any Hub-node in the tree-list (on your left) and right-clicking the Robot list and selecting the Actions > Configure... menu-item.
Press the ‘New’ button in the dialog if you want to add a new command.

You can determine the menu command ordering by using the ‘Move Up’ and ‘Move Down’ buttons. In the argument field you have the option to specify a great number of tokens, which will be expanded to the correct value when you actually initiate the command. E.g. $ROBOT in the argument list will be replaced with the name of the Robot selected when you activate the command. The tokens available are the same as the column name headers in the Robot list. Just add a $ to the column name and uppercase the letters. So e.g. Address will become $ADDRESS. You need to save your user defined menu configurations to a profile if you want them to persist between sessions.

**Workspace printing**

Use the ‘Print’ or ‘Print Preview’ command to print the list content of the Main Window or the Alarm Window. You can rearrange the columns and set the sort order to reflect the data layout you want for the print. Use the ‘Print Preview’ command to verify the output before initializing the actual print.

- Activate printing by clicking the printer icon on the toolbar or by selecting Print... from the popup menu.
**Downloading and Distributing Probes**

There are two separate ways to distribute archive packages using Distribution. You can distribute within the Infrastructure Manager or start the standalone Nimsoft Distribution application.

The obvious difference of use is the interactive character when using Infrastructure Manager. You simply drag a package from the archive list and drop it on a domain node, hub node, or a robot node. A progress dialog will provide information in detail about the ongoing distribution. Note that you can close down this dialog and continue working in the Manager without interfering with the actual distribution. If you would like an update of the distribution status, reactivate the dialog using the View Distribution Progress menu command in the Archive node of the Manager. This is invoked through the right-click menu. As an alternative to drag & drop, you can also perform distribution within the Manager by invoking the Distribute dialog from the archive list.

The other way to distribute is using the standalone Nimsoft Distribution application. Indeed you will find drag & drop capabilities here in the same way is in the Manager, but most important is the ability to create distribution tasks. These tasks are saved and make it easy to reinitiate a distribution of certain packages to a set of destination robots. The built-in task scheduling mechanism enables you to start the actual distribution at some preferred time, thus eliminating the interactivity required when distributing within Infrastructure Manager. Setup parameters will let you determine how the application should handle error situations when a specific distribution fails. A destination robot is perhaps turned off, and you can specify a number of retry attempts and the time interval between the attempts. A generated log file will provide full information of a task distribution.

**Downloading Probe packages from the Nimsoft Internet Archive**

Log on your Hub and select the logon Hub icon under the Archive node in the Navigation Pane. Probe packages are listed in the Main Window.

There are two ways of downloading Probe packages from the Nimsoft Internet Archive to your local archive:
Alternative 1: Click the "Packages in Nimsoft Internet Archive only" icon (see figure below). Select the Probe package(s) you want to download. Drag and drop them onto your archive node.

Note: Unless you have checked the option Attempt Nimsoft Internet Archive integration with local archive, and filled in Salesforce Self-Service Center user credentials in the Tools > Options menu, you will be asked to enter Salesforce Self-Service Center user credentials to log in when you attempt to download a package from the Nimsoft Internet Archive.

To obtain a login account, please contact support@nimsoft.com.
Alternative 2:

Download the Probe package by clicking the link to the Nimsoft Internet Archive in the Main Window Pane.

**Note:** In WINDOWS 7 and WINDOWS 2008R2, the probe GUI will be launched from user’s temporary folder to avoid file access issues.

![Nimsoft Internet Archive](image)

The Nimsoft Internet Archive, containing all Probe packages available, will pop up in a separate window.

Click the login icon at the top of the Nimsoft Internet Archive window, and the login dialog appears. Enter your Salesforce Self-Service Center user credentials and click the Login button to log in.
To obtain a login account, please contact support@nimsoft.com.

Select the Archive tab, and the packages in the archive are available.
Note that the archive contains different archive modes, determining what part of the Nimsoft Internet Archive that will be shown in the window. **Normally the GA mode should be used.**

**GA (General Availability)**

This is the section you should use when downloading probes. It contains the final version of the probes, tested and verified by the Nimsoft QA department.

**CR (Control Release)**

This section contains probes that are in the Control Release phase. Prior to releasing the probes for General Availability, they stay in Control Release for a limited period of time. The probes are tested and verified by the Nimsoft QA department, but problems reported by customers may be corrected before the GA release. Probes in the CR section are made available to a limited number of users who want to participate in the final test and verification process of the probe.

**Beta**

This section of the archive contains probes that are in the Beta phase. Initial testing by the Nimsoft QA department has been conducted, but the probes may still be modified as the test program moves forward. Customers may download Beta versions to have a closer look at new features and functionality.

In addition the archive contains a selection of unsupported probes.

Find the Probe package you want to download, mark it, drag and drop it onto the Archive node.
The Probe package will now appear in the Main Pane in Infrastructure Manager, together with other Probes previously downloaded.

Note that the Probe icon is probably now is red, which means that you have no valid license.

**Entering the Probe License**

Order a license for the Probe by sending an email to support@nimsoft.com. You will then receive an e-mail, containing the license as a text string.

With the Licenses icon under the Archive Node in the Navigation Pane selected, mark the complete text string and drag and drop it onto the Main Window Pane. A message like the one shown below appears on the screen.

```
Information
License has been added successfully
```

The Probe icon is green, which means that you have a valid license.

Note that the Probe is now located in your local archive (on the Hub). The next step is to distribute the Probe to the Robot(s).
Distributing Probes from your local archive

Distributing a Probe package to all Robots on your Hub

If you want to distribute the Probe to all Robots on your Hub, you mark the Probe in your archive, drag and drop it on your Hub in the Navigation Pane.

Distributing a Probe package to single Robots

If you just want to distribute the Probe to some of the Robots, you must drag and drop the Probe directly to the Robots in the Navigation Pane.

Distributing a Probe package to all Robots in a group

Note that you may also distribute a Probe package to all Robots in a group, created under the Groups node in the Navigation Pane. This is done by dragging and dropping the Probe directly to the Group in the Navigation Pane.

Distributing a Probe package to all Robots running the same OS

You can also distribute a Probe package to all Robots installed on computers with the same OS-type (e.g. Windows). This is done by dragging and dropping the Probe directly to the OS group under the Dynamic Views node in the Navigation Pane.
A progress window appears on the screen when the distribution process starts.

The following dialog appears if dropping the Probe package on a Hub. Note the Update only option. With this option ticked, the probe package will only be distributed to robots on which it already exists.

If dropping the probe package directly on a Robot, the Update only flag is turned off.

Click the OK button to continue.
The Progress window appears, informing you about the progress of the distribution. This is interesting information when distributing multiple packages, resulting in a long distribution time.

All previous distributions will be displayed in the window.

By clicking the New button at the bottom of the window, a new session is created, and you start with an empty window.

The option ‘Automatically close dialog when distribution is complete’ closes the window when the distribution is successfully finished.
Technical Tips

Example, Copying a probe configuration to another probe

This is useful if you have configured a probe on one robot and you want to copy the configuration parameters on the same type of probe installed on other Robots. In this example we use the `emailgtw` probe.

1. Log on to the Hub where Robot with the probe configuration you want to use as source is installed. Select the `emailgtw` probe from the probe list in the Infrastructure Manager. Drag and drop the probe into the Archive.
2. The *Update packages* dialog will then appear. Press the Rename button and give the package a descriptive name (e.g. emailgtw-master).

3. Ensure that the *Configuration Only* option is checked and press the OK button. You will now end up with a new package in the archive. Now you can select the Probe configuration package and drag and drop on the selected robot(s).
4. The distribution progress window will appear, and the configuration of the probe is completed as soon as the distribution process is finished.

![View Distribution Progress](image)

**Distributing multiple probes and configuration files together as a "super-package"**

This is convenient if you want to distribute multiple probes and configuration files to a number of computers as one package and in one operation. These computers will then receive the same probes with identical configuration parameters.

**Cdm probe Note:** When including the cdm probe in a package, you must ensure that the target computers have the same disk partitions as defined in the cdm configuration file (*cdm.cfx*) distributed with the package.

Example:

If the configuration file has defined a C: and a D: partition, and you distribute the package to a computer with only a C: partition, the cdm probe on this computer will try to monitor a D: partition (which is missing) and report an error.

**Documentation reference:**

If you during this procedure want additional information about the packageEditor, please see the packageEditor description in the Probes on-line documentation (launched by selecting Help > Probes in Infrastructure Manager Menu bar.)
In the following example we will make a packet called super-package, containing the \texttt{cdm} and the \texttt{ntevl} probes. You may of course add as many probes as you like in the package.

1. Open your local package archive, right-click in the list and select \textit{New} to launch the \textit{packageEditor}.

In the following example we will make a packet called super-package, containing the \texttt{cdm} and the \texttt{ntevl} probes. You may of course add as many probes as you like in the package.

1. Open your local package archive, right-click in the list and select \textit{New} to launch the \textit{packageEditor}.
2. We will now create the distribution package. Give the new package a name (in this example we call the package *super-package*). You may also create a new group (e.g. Super) for the package.

![New Package dialog box](image)

3. Click the **OK** button, and the new package will appear in the list in the package archive.
4. Drag and drop the cdm probe into the package archive.
5. Ensure that *Configuration Only* is selected, and rename the package to *cdm-cfg*. Click the OK button, and the *cdm-cfg* package will appear in the list in the package archive.

6. Select the *cdm-cfg* package in the package archive, right-click and select *edit*. Right-click the file *cdm.cfx* in the list, select *Save file as...* and save the file on a destination of your own choice (you will need the file later in this procedure).
Important! When saving the file as another filename the new filename cannot have more than one "." in the name. You will receive an error message and the package will not be transferred to the central archive. Examples: incorrect filename "cdm.new.cfx"; valid filename "cdm_new.cfx"

**Note:** The Save file as... function is working properly with Nimsoft ver. 3.2 and newer.

With older versions, you have to select Edit file..., copy / paste (use CTRL + C and CTRL + V) the contents to a file in e.g. Notepad and save the file as cdm.cfx.

1. Now you drag and drop the ntevl probe into the package archive. Ensure that **Configuration Only** is selected, and rename the package to ntevl-cfg. Click the OK button, and the ntevl-cfg package will appear in the list in the package archive. Select the ntevl-cfg package in the package archive, right-click and select edit. Right-click the file ntevl.cfx in the list, select Save file as... and save the file on a destination of your own choice (you will need the file later in this procedure). Also see the note in step 6.

2. Select the super-package in the archive, right-click and select Edit. You are now going to define the contents of the super package.

3. Click the tab for OStype and select Add section to make a section.

Give the section the name win32 and select OStype = windows and OS = win32 for distribution to windows computers.
For other platforms, see the packageEditor description in the *Probes on-line documentation* (launched by selecting Help > Probes in Infrastructure Manager Menu bar.)

4. Click the Dependencies tab, click in the window and select *Add dependencies*. Type probe name (cdm) and optionally the Version number. If you just use the probe name, the package will only distribute the probe to target computers where the probe does not exist.
If you also use a version number, the package will only distribute the probe to target computers where the probe does not exist, and to target computers where the probe exists in an older version.

5. Make a new tab called cdm-cfg. Select the option Configuration of existing probe and type cdm in the Probe name field. Click the OK button.

6. Repeat steps 10 to 11 for the ntevl probe.

7. Select the cdm-cfg tab and click the Files tab. Right-click in the window and select Add file.
8. Select Browse to find the cdm.cfx file you saved in step 6 and click the OK button.

9. Select the ntevl-cfg tab and perform steps 13 to 14 for the ntevl probe.

10. Finally, click the OK button in the super-package dialog to finish the procedure.

Now the super-package (including the two probes with their configuration parameters) can now be distributed, using drag and drop.

The package can be distributed to:
- a single Robot.
- a Hub, including all underlying Robots.
- a Domain, including all underlying Hubs and Robots.

About upgrading Nimsoft components

Robot_update

- Upgrade the hub robot separately, in other words do not drop this package on hub or domain levels. Use Find functions in Infrastructure Manager to create the lists of robots.
- Turn off the ‘update only’ flag, as this will only upgrade robots which have previously been upgraded.
- Some added functionality in the controller becomes available with a new configurator, which is installed with Infrastructure Manager.
Probes - general

- Packages can be dropped on a hub or domain level with ‘update only’ turned on – the probe will then only be distributed to robots on which it already exists.

- On distribution, the probe definition is recreated and the probe is set to the active state as defined in the package (active for most probes, inactive for data_engine and report_engine).

  This also means that any changes made in time specifications on individual robots are lost. Check this specifically for the logmon probe, which is a timed probe.

- The probe packages contain a default configuration file, and the entries here will be merged into the probe configuration.

  This means that in most cases re-distribution of the probe does not create any problems. Example profiles which have been removed may be re-created.

- Probes will normally function properly with old profiles, but you may want to edit the profiles to take advantage of new functionality.

  Refer to the release notes of individual probes for more information on this.

Quality of Service

Some probes may have additional QoS objects which must be manually turned on in the probe configurator.

For some probes the QoS table names have been modified.

Examples:

- url_response
  - QOS_URL_RESPONSE, QOS_NETWORK
    changed to
  - QOS_URL_RESPONSE, QOS_URL

- wintask
  - QOS_WINTASK_EXECUTION, QOS_APPLICATION
    changed to
  - QOS_WINTASK_RUN_TIME, QOS_WINTASK

You will need to check the SLO definitions in the SLM Manager of any SLOs using the changed QoS objects.
Modifications made on computers when Nimsoft is installed

Modifications made when Robot is installed (Windows NT/2000/XP).

.../Nimsoft

This is the product directory specified by the user and this is the directory where the Nimsoft product files reside.

Normally this is C:\Program Files\Nimsoft

Windows System directory

msvcrt.dll (Microsoft C library)

Only updated if the existing version is old. This should not be the case on Window XP or Windows 2000 with a recent service pack.

New Registry sections

- HKEY_LOCAL_MACHIN\Software\Nimsoft Software
- HKEY_LOCAL_MACHIN\Software\Nimsoft Software AS

Stores some variables internally used by Nimsoft

Start Menu\Programs\Nimsoft Software

A common menu choice to start the Service Controller.

<services>

A service called ‘Watcher’. The service can be managed with the service controller. The complete service can be removed with the command

.../Nimsoft/bin/Nimsoft -remove

Modifications made when Nimsoft Server or Infrastructure is installed (Windows NT/2000/XP).

When installing the Nimsoft Server or Infrastructure, a VB runtime can be selected. When this is done, the following additional components are installed:
windows system directory

\atl.dll

Only updated if the existing version is old. This should not be the case on Window XP or Windows 2000 with a recent service pack.

\asycfilt.dll

\stdole2.tlb

Only updated if nonexistent or the existing version is old.

\comcat.dll

\msvbm60.dll

\oleaut32.dll

\olepro32.dll

Only updated if nonexistent or the existing version is old. These last 4 are registered.

<registered>

...\Nimsoft\lib\Nimsoft.dll

This Nimsoft dll is registered.
**Turning DNS on or off**

You may turn the DNS system **on** or **off** by modifying the configuration parameters for the nas probe.

This is done by opening the raw-configuration tool (see Configuring a probe using the internal editor (raw configure)) for the nas probe.

In the Infrastructure Manager: Shift+right-click the nas and select *Raw Configure*.

Select the *Setup* section and click the *New Key* button to add the following new key:

```
name_lookup_mode = <value>
```

Use the value 0 to turn DNS off, use 2 to turn DNS on.

Valid values:

- 0 - DNS off
- 2 –DNS on
Unable to remove Netware robots from list

After uninstalling netware robots, you may experience that several netware robots still appear on the robot list (found under the Robot tab in hub configuration tool), even if the NLMs are uninstalled and the proxy is deleted.

If attempting to remove them manually from the robot list in hub configuration tool, they may reappear after a few seconds.

How to get rid of the unexisting robots in the list:

Start probe utility on the controller-probe on the robot where the proxy-probe is running by selecting the controller probe in Infrastructure Manager and clicking <CTRL>+P.

Select: ‘probe_unregister’ from the Probe commandset drop-down list and fill in the name of the machine:

remote_<name of the machine>_netware

Click the green arrow.
Now you can remove the robot from the robot list in the hub configuration tool.

Non-valid licenses Notification

When logging in to Infrastructure Manager, the system automatically searches for expired licenses.

If missing licenses are found, you will get a notification like the one shown below:
How to install a license for a HUB

Licenses can be ordered by sending an email to support@nimsoft.com. You will then receive an e-mail, containing the license as a text string.

To install a license for a Hub, you just double click the 'Hub' Probe in the Infrastructure Manager. The Hub configuration tool appears on the screen. Click the Modify button in the License Information field on the General tab.

The Edit License dialog appears.
The license you received from Nimsoft appears as a text string:

Example:

Nimsoft-v1.0/Nimsoft Demo/*/10/Unlimited/DIE BUSH GORM SAL PINK DARK

Type the text string, or mark the text string and copy it onto the 'Hub License' field. Click the OK button, and the Edit License dialog disappears. Click the Apply button and restart the probe.

**Setting up audio-visual alarm notification**

It is not required to keep the full WorkSpace up and running at all times in order to monitor your network. Your installation provides you with a small program that notifies you either visually or with a user-defined sound whenever the propagated (the highest) alarm-level has reached a defined level. You may launch the Alarm Notifier from the WorkSpace Tools menu, or link the executable nasspy.exe from your Nimsoft/util directory to your startup folder.

The spy will receive alarm status events from the configured Alarm Server (nas).

**Configuring the nasspy.**

Right-click the nasspy icon in your system tray (assuming that it is already started) to bring up a popup-menu. **Setup** will bring you to the property-sheet, where you can define:

- Which application that will be launched upon double-clicking the icon.
- Various sound settings.
- How the nasspy connects to the Nimsoft (automatically or configured).
The Infrastructure Manager Error Log

During installation of the Infrastructure Manager, the log file `Nimsoft_manager.log` is created in the directory

*Program Files/Nimsoft/AC/logs*

Events, trace and error info will be written to this log.

When the size of the file exceeds approximately 100 KB, a backup of the file will automatically be created. The name of the backup file is `_Nimsoft_manager.log`.

As soon as the backup file is created, the log file `Nimsoft_manager.log` is cleared and starts logging again. The next time the log file is full, the backup file will be overwritten and so on.

Managing the Robot on a AS400 computer

Use the following commands on the AS400 computer to manage the Robot.

Start the robot with the command

`STRSBS NIMSOFT/NIMSOFT`

The robot can be stopped with the command

`ENDSBS NIMSOFT/NIMSOFT`

**NOTES:** If you want to shut down the system/tcpip each night for backup, you should also stop Nimsoft and start it again after tcpip has been restarted.

Stopping and starting Nimsoft can be done in jobsdce as described in the example below (stop time 01.00.00 and start time 07.00.00, every day):

```
ADDJOBSCE JOB(ENDNIMSOFT) CMD(ENDSBS SBS(NIMSOFT) DELAY(120)) FRQ(*WEEKLY) SCDDATE(*NONE) SCDDAY(*ALL) SCDTIME('01.00.00') USER(NIMSOFT) TEXT('End Nimsoft')
ADDJOBSCE JOB(STRNIMSOFT) CMD(STRSBS SBSD(NIMSOFT/NIMSOFT)) FRQ(*WEEKLY) SCDDATE(*NONE) SCDDAY(*ALL) SCDTIME('07.00.00') USER(NIMSOFT) TEXT('Str Nimsoft')
```

If you later want to change the schedules, use `WRKJOBSCE`.

Modifying the Infrastructure

This section describes various tasks related to modifications of the Infrastructure.
Installing Nimsoft in an active/passive Microsoft Cluster

This section describes the steps to install the Nimsoft Server (or Hub/Robot) in an active/passive Microsoft Cluster. By doing so you minimize the risk of having a single point of failure due to hardware problems or maintenance. All client applications (as well as other interconnecting Hubs) will operate as if nothing had happened if the cluster nodes changes state.

The illustration below shows the various elements in the resource group that we need to define later.

One of the initial tasks is to install the Nimsoft infrastructural component that you require to run in a clustered environment. Typically a Nimsoft Server (or Hub) will be the target for an installation. Our example will install a Nimsoft Server to the S:\Nimsoft drive. This drive will in turn be part of the resource group together with a virtual IP address, name and service resource.
Modifying the Infrastructure

Chapter 4: Infrastructure Manager User Guide

Preparations

We are assuming that you have administrative access to a 2-node cluster, and that you have the appropriate disk hardware (RAID). All resources should be made available to both cluster nodes.

We recommend NOT to install the Consoles (Infrastructure Manager, Enterprise Console and Service Level Manager) on the cluster nodes, but rather install them on a workstation.

Installing and configuring

1. Start Cluster Administrator from the Administrative Tools menu (fig.1).
2. Create a cluster group named **Nimsoft**.
3. Add an **IP address** resource from the action menu, e.g. **10.1.1.100** (fig.2,3).
4. Add a **Network name**, e.g. **cl-Nimsoft**, enable the update dns checkbox. (fig. 4).
5. Add a **Physical disk**, e.g. **S:** (fig. 5).

Test that the above configuration works by moving it from one cluster node to the other. Bring up a command shell from the **Start/Run** menu, and check that the virtual IP address is available using the ipconfig command, that you may access the disk resource by **dir S:**

1. Prepare to install the infrastructure component of your choice.
   We chose to install a complete Nimsoft Server.
2. Modify the install directory to e.g. **S:\Nimsoft** (the physical disk from step 5).
3. Give the hub a name, e.g. **CL-NIMSOFT** and complete the installation acc. to your needs. Do not install consoles.
4. The installation program will detect multiple network interfaces and will present them in a list. Choose "Automatic".
5. Log in with Infrastructure Manager from another machine.
6. Configure the controller to use a specific IP address (use the virtual address set, see fig. 3) and override the robot name to e.g. **2003cluster**. (fig. 7).
7. Let the Robot and Hub restart and check for the changes made. If experiencing trouble with the data_engine and/or dashboard server probes, you can solve this by restarting the computer.

**Note:** Changing IP invalidates security information in the Hub. If this is NOT the only Hub in the Domain, the Hub will get updated with security information from one of the other Hubs.
Otherwise, you should set the probes shown in the figure below to the access and IP-mask as shown (using the Security > Probe administration from the menu bar in the Infrastructure Manager) and then restart the computer.

8. Create a Generic Service resource in the Cluster Group Nimsoft, and enter NimsoftWatcherService as the service name. Add dependencies to the disk resource, IP address and network name. Add the following root-key to the Registry replication list, SOFTWARE\Nimsoft Software\Nimsoft Installation. (fig. 6).

   Note on 64-bit systems should look like this: SOFTWARE\Wow6432Node\Nimsoft Software\Nimsoft Installation

9. Bring the Nimsoft Service resource to an online state in the Cluster Administrator using the action menu on the selected item.

10. If Nimsoft Server 3.60 or later:
    Install the vs2008_redist_x64 and vs2008_redist_x86 packages, available from Microsoft on the other cluster machines.

Complete the installation on the second cluster node

1. Move the Nimsoft Cluster Group in the Cluster Administrator, observe that all resources should move, and that the Nimsoft Service resource is still in an online state.

2. Register Nimsoft.dll on the other computer (the one you are NOT installing from).

   Example:
   regsvr32 S:\Nimsoft\lib\Nimsoft.dll.

3. Move the Nimsoft Cluster Groups between the nodes and verify that the Probes comes up on both nodes.
You should now have a Nimsoft running in your cluster.

Fig. 1 – The Cluster Administrator
Fig. 2 – Defining a new cluster resource

![Virtual IP Address Properties](image_url)
Fig. 3. – Defining a Virtual IP Address resource
Fig. 4 – Defining a Network Name resource
Fig. 5 - Defining a Disk resource
Modifying the Infrastructure

Fig. 6 – Defining a Generic Service resource

Fig. 7 – Configuring the Robot
Reinstalling Nimsoft in an active/passive Microsoft Cluster

When reinstalling Nimsoft in an active/passive Microsoft Cluster, you should follow the steps below.

Perform an upgrade/reinstallation on the same server you did the previous installation of Nimsoft.

- Bring the Nimsoft Service offline in the Cluster Administrator.
- Upgrade/reinstall Nimsoft.
  
  Just ignore warnings that probes like data_engine, report_engine, sla_engine, group_server and so on, couldn’t be enabled.

  Also ignore the warning "The installation did not complete successfully due to the following probe(s) that did not start...." and the recommendation for a full reinstalltion.

- Bring the Nimsoft Service online again in the Cluster Administrator.

- Log into Infrastructure Manager and activate the probes which are not running.
- If upgrading to Nimsoft Server 3.60 from an older version of Nimsoft Server:
  
  Install the following files on the second cluster node:

  **vcredist_x64.exe**
  
  ![Link to vcredist_x64.exe](http://www.microsoft.com/downloads/details.aspx?familyid=ba9257ca-337f-4b40-8c14-157cfdf4ee4e&DisplayLang=en)

  **vcredist_x86.exe**
  
  ![Link to vcredist_x86.exe](http://www.microsoft.com/downloads/details.aspx?familyid=9b2da534-3e03-4391-8a4d-074b9f2bc1bf&DisplayLang=en)

Report_engine not installed on the same server as the main hub?

If the report_engine is not homed on the same server as the main hub and the httpd probe, you must configure the httpd server to see the report_engine. Otherwise you will not be able to see the Dynamic Dashboards.

This is possible in version 1.21 of the httpd probe by configuring the address to the report_engine in the setup section.

Open the configurator for the httpd probe by double-clicking it in the Infrastructure Manager. The Raw Configure dialog for the probe will be launched.
Create a new Key by clicking the New Key... button. The New Key dialog pops up.

Fill in the Key name: report_engine_address
and the Value: report engine address on the format

Click the Apply button to activate the new setting and exit the Raw configure dialog.
Moving the SLM database from one SQL server to another

This procedure describes how you can move the SLM database from one SQL server to another. The example below shows how to move the database NIS_MAVERICK (owned by maverick) on NIMDB (MSSQLS2000) to database NIS_GMH (owned by gmh) on XPGUHU\STD01 (MSSQL2005):

1. Deactive the data_engine.
2. Make a full database backup of NIS_MAVERICK on NIMDB.
3. Transfer the backup to XPGUHU.
4. Create the new login gmh on server XPGUHU\STD01.
5. Restore the database NIS_MAVERICK to database NIS_GMH on XPGUHU\STD01 as user sa.
6. Change NIS_GMH’s owner to maverick.
7. Edit the data_engine’s properties (DBMS;DB;USER;PW) to (XPGUHU\STD01;NIS_GMH;maverick;*).

8. Activate the DataEngine

Now new (as well as data queued during step 1 and 8) qos-data are inserted into corresponding R_QOS_DATA-tables OK.
Alarm Server Mirroring within a Domain

The Alarm Server (nas) is capable of performing full or partial mirroring. This feature may be activated due to various reasons such as:

- Organizational reasons, central IT department with one or more subsidiaries.
- Geographical reasons, IT staff on every location.
- Availability reasons, at least one alarm repository must be active at any time.

The mirroring is configured in the Infrastructure Manager by bringing up the nas configuration tool, and selecting the Import/Export tab.

Various scenarios

Full mirroring solution

The figure above shows a simple full mirroring solution. All alarm messages are mirrored (copied) between both alarm servers.

The configuration in the nas configuration tool under the Import/Export tab is:

- A: Import from B, export (new, update, close) to B.
- B: Import from A, export (new, update, close) to A.

One-way mirror

The configuration in the nas configuration tool under the Import/Export tab is:

- A: Import from B, export (new, update) to B.
- B: Import from A, export (new, update) to A.
The figure above shows a one-way mirroring solution. We want to achieve a solution where the alarms in B are mirrored to A, reflecting the changes etc., but we do not want to mirror the messages in A to B. The red arrow indicates that only close alarm-events are exported to B.

The configuration in the nas configuration tool under export/Export tab is:
- A: Import from B, export (close) to B.
- B: Import from A, export (new, update, close) to A.

Mixed solution

![Diagram](image)

Figure 3. shows a typical departmental (hierarchical) organization with the IT-department (center for Enterprise management) sits on the top A. The department denoted by B has an IT-staff - C does not have any. We want to achieve the following:

1. A wants the full picture (enterprise view), with alarms from A, B & C.
2. B wants a 'local' perspective, just seeing and maintaining his 'own' alarms.
3. C doesn't want to see nor handle any alarms, thus only implementing a Hub with permanent queues.

The configuration in the nas configuration tool under export/Export tab is:
- A: Import from B, export (close) to B.
- B: Import from A, export (new, update, close) to A.
- C: no alarm server is present.
Alarm Server Mirroring Across Domains

In this example we use the following configuration:

- Two Domains: Domain1 and Domain2
- Two Hubs: Hub1 and Hub2.
- Two servers running the Hubs: server1 and server2.

The full addresses of the two Hub Probes are:

- /Domain1/Hub1/server1/Hub
- /Domain2/Hub2/server2/Hub

To set up nas mirroring, you have to set up the nas and the Hub on BOTH servers, and in addition set up the timedQ Probe to fetch and send alarms between the two Domains.

Setting up the nas on server1:

1. In the Infrastructure Manager: Shift+right-click the nas to bring up Raw Configure.
2. If the section 'imports' does not exist, create it at the root level by clicking 'New Section'. Enter 'imports' as the section name and click the 'Create at root' checkbox.
3. Create a section 'Hubs' under the 'imports' section. This is done by selecting the 'imports' section and clicking the 'New Section' button. Enter the name 'Hubs' and make sure that the 'Create at root' checkbox is NOT checked.
4. In the 'Hubs' section: Create the key 'Hub_0' with the value 'Hub2'.
5. If the section 'exports' does not exist, create it (see step 2).
6. Create a section 'Hubs' under the 'exports' section (see step 3).
7. In the 'Hubs' section: Create the key 'Hub_0' with the value 'Hub2,/Domain2/Hub2/server2/Hub'.
8. In the 'exports' section: Create the keys
   - 'flag_new'
   - 'flag_update'
   - 'flag_close'
   - 'export_imported'.
   All keys should have the value 'no', except 'flag_close', which has the value 'yes' for partial mirroring.
   For full mirroring: Set the 'flag_new', and 'flag_update' should also have the value 'yes'.

Setting up the nas on server2:

This procedure is the same as for server1, just change the names.
The difference is that this server should have the 'flag_new' and 'flag_update' keys set to 'yes' so that the alarms are mirrored to 'server1'.

**Setting up the Hub on server1:**

1. In the Infrastructure Manager: Double-click on the Hub to bring up the properties GUI.
2. Go to the 'Setup' tab, with the 'Queues' tab selected there.
3. Right click in the 'Queues' tab and select 'New'.
4. Input the name 'NAS-EXPORT-TO-Hub2'.
5. Set the type to 'Attach'.
6. Input the subject 'NAS-EXPORT-Hub1'.
7. Click 'OK'.
8. Select the 'nas' queue. Right-click and select 'Edit'.
9. Edit the subject, adding ',NAS-EXPORT-Hub2' so that it reads 'alarm,NAS-EXPORT-Hub2'.
10. Click 'OK'.

**Setting up the Hub on server2:**

The procedure is the same as that for server1, just change the Hub names.

**Setting up the timedQ Probe**

The last step is to set up the timedQ Probe to fetch and send alarms between the two Domains on interval:

The timedQ Probe creates a connection between two Hubs on interval and manages the queues for you. This is required if you have a firewall that takes down inactive connections or have an ISDN line which you use to connect the remote sites.

To set up timedQ to handle the setup mentioned above do the following:

1. Install the timedQ Probe to Hub1.
2. In the Infrastructure Manager: Double-click on the timedQ Probe.
3. In the 'profiles' section: Add a new section 'Hub1-to-Hub2'.
4. In this new section: Add the following key-value pairs:
   - active = yes
   - timespec = 00:00:00 interval 00:15:00
   - msg_src = server1
   - msg_dst = server2
5. In the 'Hub1-to-Hub2' section: Add the new subsection 'flush' with the key-value pairs:
   - active = no
   - threshold = 5

6. In the 'Hub1-to-Hub2' section: Add the new subsection 'alarm' with the key-value pairs:
   - active = yes
   - alarm_level = 4
   - error_count = 3

7. In the 'profiles' section: Add the new section 'Hub2-to-Hub1'.

8. In this new section: Add the following key-value pairs:
   - active = yes
   - timespec = 00:00:00 interval 00:15:00
   - msg_src = server2
   - msg_dst = server1
   - src_queue = 'NAS-EXPORT-TO-Hub1'
   - queue_timeout = 20
   - max_connection_time = 120

9. Add the subsection 'flush' (see step 5)

10. Add the subsection 'alarm' (see step 6)

You have now set up timedQ to trigger a connection between the two Hubs every 15 minutes.
Setting up Passive robots

Communication between Hubs and Robots is usually 2-ways, meaning that both Hub and Robot can initiate communication. You can, however, define that only the Hub should initiate communication. This is done by setting robots to Passive mode.

This feature is an additional security measure for Hub/Robot communication.

Setting robots to passive mode can either be done during installation or for individual robots from the probe GUI.

To add passive robots to a hub, you need to complete the following steps in this order:
1. Set the relevant robots to passive, either during installation or using the controller for the robot(s) (see Setting Robot mode to passive).
2. Add the passive robot(s) to the hub (see Adding/Editing a Passive Robot).

This feature is an additional security measure to Hub/Robot communication.

Setting Robot mode to passive

If you have not already set Robot mode to Passive during installation, you can do this using the robot’s process and port controller:
1. In the infrastructure, locate the robot you want to set to passive mode.
2. Double-click the controller probe. The controller GUI dialog opens.
3. Select the **Setup** tab, and then the **Misc.** tab.

4. In the Robot mode section, select the **Passive - must be contacted by hub** option.

5. Click **OK**.

You must now add the passive robot to the hub, as described below.

**Note:** If you set a passive robot to normal (regular) mode, you must remove the passive robot from the **Registered Robots** list for the hub in question. You can do this by right-clicking the robot and selecting **Remove Passive Robot**. Since the robot runs in normal/regular mode, the robots list will be automatically updated.
Adding/Editing a Passive Robot

If a robot is set to passive, it will no longer contact the hub, and will subsequently be removed from the Registered Robots list for the hub. You can add the passive robot to the list as follows:

1. Navigate to the relevant hub and double-click it.
2. Select the Robots tab. In the Registered Robots list, the Type column indicates whether the various robots use passive or regular mode.
Note: To edit an existing passive robot, right-click a robot (with Type = Passive) in the list and select Edit Passive Robot.

4. In the Add Passive Robot dialog, enter the necessary information in the following fields:
   ■ Robot IP/Name: Enter the IP address to the passive robot you want to add.
   ■ Port: Enter the port number of the robot.

5. Click the Verify button to check that the Hub can communicate with the Robot.

6. Click OK in the dialog confirming that verification was successful.
   Or
   If the verification was not successful, try editing the robot IP/port information and try again.

7. Click OK in the dialog when you are done. The passive robot displays in the Registered Robots list.

Repeat this procedure for any other passive robots you want to add.

Troubleshooting: A Firewall is blocking Hub communication with Probes on a Passive robot

Some firewalls only allow communication on a limited number of ports for security reasons. If this is the case, a Hub may not be able to communicate with some or all Probes on a robot (unless all Probe ports are opened in the firewall).

To solve this problem, you must do as follows:
■ Enable the Passive robot’s Proxy mode. By doing this, all Hub/Probe communication will be channeled through the Passive robot’s port.
■ Open the robot’s port in the firewall.

To enable Proxy mode for a Passive robot:
1. In the infrastructure, locate the robot for which you want to enable Proxy mode.
2. Select the controller probe, press the SHIFT key and right-click the controller.
3. Select **Raw Configure** from the menu. The **Raw Configure** dialog opens.

4. Click the **New Key** button and enter the following values:
   - Key name: `proxy_mode`
   - Value: `1`

5. Click **Apply** and close the dialog boxes.

6. Ensure that the correct port for the Passive robot is opened in the firewall.

### Migrating Passive robots between hubs

To migrate a Passive robot from one hub to another, do as follows:

1. Remove the Passive robot from Hub #1 (the hub you are migrating FROM). To do this, right-click the passive robot and select **Remove Passive Robot**.
2. Add the Passive robot on Hub #2 (the hub you are migrating TO). See the procedure **Adding/Editing a Passive Robot** above.
3. Restart Hub #1 for changes to take effect.
4. Restart Hub #2 for changes to take effect.

The Passive robot has now been removed from hub #1 and added to hub #2.

**Note!** To prevent the possibility of a Hub on another domain taking over a Passive robot on your domain, you should restrict access to the relevant ports on your firewall.
Setting up Robot Fail-over

One of the primary tasks of the Robot is to maintain connectivity to the Nimsoft 24 hours a day, 7 days a week. In order to accomplish this, we have implemented built-in fail-over mechanisms into the Robot's controller. It attempts to stay connected to the Nimsoft by operating in two modes:

1. Automatic, roaming the LAN (using broadcast within the same subnet) for a Hub.
2. Fixed, using a preset ip-address or hostname.

All connectivity is restricted to Hubs within the same Domain.

It will automatically "roam" the LAN for a secondary Hub in the same Domain. Please note that this is restricted within the same network subnet. You may however, define a "fixed" secondary Hub on any network address, as long as the Hub is within the Domain constraints.

Note: Remember that if the Robot is unable to connect to a Hub, messages will be spooled and kept (under certain criteria) until a Hub connection is achieved.

Configuring a secondary Hub

Bring up the Robot Controller Configuration Tool (by double-clicking the controller Probe), and select the Setup/Nimsoft tab.
You may then choose to setup an automatic or a specified secondary Hub.

Possible solutions

A "balanced" solution

Figure 1 (above) shows a balanced solution consisting of two Hubs: B acts as a backup solution for A.

Let's assume that the system could run its alarm server (nas) on A. B is configured with a permanent queue (post) directed towards Hub A. All the Robots managed by Hub A will connect to Hub B upon failure of A. All messages will be collected by Hub B, and queued until Hub A comes back on-line. The alarm server (nas) on A will now receive the messages queued by B.

A dedicated backup solution
Figure 2. (above) shows a dedicated backup solution that only acts as a backup solution for the primary Hub (A). The alarm server (nas) still runs on A. Hub B will take the Hub responsibility for all the Robots managed by A, as long as A is down. All messages will be queued for A, and forwarded as soon as Hub A reports as well behaved. The orphaned Robots will then switch back to their primary Hub (A). The only difference from the situation described in figure 1. is the fact that the backup Hub is just waiting for orphaned Robots, and not taking part of the 'active' solution.

A departmental structure

Figure 3. shows a typical departmental structure where another 'department' helps in maintaining full connectivity. Lets assume that the IT department is denoted by A. The alarm server is located here as well. It is quite natural that A should become the secondary Hub for all the Robots in this scenario due to the fact that all of the messages eventually end up here anyway.

**Installing multiple Robots on the same server**

It is possible to install additional Robots on a server where already one Robot is installed and running.

**Note:**
- Not all Probes are verified to work properly when multiple instances of the same probe are running on the same server.
- It is not possible to install more than one Hub on each server.
Procedures

Windows systems:

1. Each Robot needs its own file set. Create a new installation directory for the additional robot and give it a name such as c:\Program Files\Nimsoft_XXX.
2. Create the two folders bin and robot in the new directory.
3. Copy the file Nimsoft.exe from the bin folder in the original Nimsoft directory and paste into the bin directory created in step 2.
4. Copy the files controller.exe and robot.cfg from the robot folder in the original Nimsoft directory and paste them into the robot directory created in step 2. Edit the following parameters in the robot.cfg file (these parameters must be unique for the new robot:
   - robotname: give the new robot an unique name.
   - controller_port: select an unused port, e.g. 50000 if this port is free.
   - spooler_port: select an unused port. Use <controller port +1>, e.g. 50001 if free.
5. Each Robot needs its own watcher service. Create a new watcher service for the new robot by using the following command from a dos window (give the new watcher service a name like for example Nimsoft_xxx):
   
   bin\Nimsoft -servicename <new watcher service name> -install
6. Find the new robot in Infrastructure Manager. Launch the controller GUI and select the Setup > Misc. tab. Select the option Set QoS source to robot name instead of computer hostname. Save the changes and restart controller.
7. Finally deploy robot_update package 2.90 (or newer) to the robot to achieve full robot functionality.
   
   Note that the Service Controller will only display the status of the original robot. The new robots can be individually stopped and started using normal service handling tools in Windows.
   
   If you want to remove the robot, use the command
   
   bin\Nimsoft -servicename <new watcher service name> -remove
   
   and remove the folders created.

Unix systems:

1. Use nimldr version 2.28 and upwards, install_packages 3.58 and upwards.
   
   When running nimldr from the command line, you must set these hidden options:
   
   -P port_number. Select an unused port, e.g. 50000 if this port is free.
   -N robot_name. Give the new robot an unique name.
   -F <directory containing local installation file> Installation file on the local machine.
2. Run the the install script. Make sure to select robot installation, when prompted.
When finished, the robot should be installed and running.

3. Find the new robot in Infrastructure Manager. Launch the controller GUI and select the Setup > Misc. tab. Select the option Set QoS source to robot name instead of computer hostname. Save the changes and restart the controller.

**Configuring Hubs to send all the alarms to a central Hub**

Configuration for HUB 1 and HUB 2 to send all alarms to HUB 3:

Open the configuration tool for HUB 1 and HUB 2 by double-clicking the probe in Infrastructure Manager.
Select the Queues tab.

In the Queue window, right click and select *New*.

The Queue properties dialog appears.

Fill in:

- **Name**
  
  <type a name>

- **Type**
  
  post

- **Subject**
  
  alarm

- **Nimsoft Addr**

  Select HUB 3 from the list menu: /<domain>/<hub>/<robot>/hub

Ensure that the Active is checked and click OK. Click the Apply button.
Setting up a tunnel between two Hubs that are separated by a Firewall

Many companies today have one or more firewalls in their network, both internally between different networks and externally against a DMZ or Internet. Network administrators are often reluctant to open a firewall for a lot of IP addresses and ports in order to make it possible for Management applications to work. This makes it difficult to administrate and monitor the whole network from a central location.

The solution is to set up a Tunnel between two Hubs that are separated by a Firewall.

The Tunnel sets up a VPN-like (Virtual Private Network) connection between the two Hubs and enables all Nimsoft requests and messages to be routed over the Tunnel and dispatched on the other side. This routing will be transparent to all the users within Nimsoft. The only requirement for setting up a Tunnel is that one of the Firewalls opens for connection to the target Hub on one port.

**NOTE:** Do not use Static Hubs if setting up a tunnel!
Security

Security is the main issue when opening a Firewall for external connections. The Tunnel is implemented using the SSL (Secure Socket Layer) protocol, which is currently the most widely deployed security protocol today (e.g., it is the protocol behind Secure HTTP (HTTPS)). The security is handled in two ways; certificates to authenticate the Client and encryption to secure the network traffic (e.g., over Internet):

- **Authorization and Authentication**
  The Tunnel provides authorization and authentication by using certificates. Both the Client and the Server need valid certificates issued by the same CA (Certificate Authority) in order to set up a connection. In the case of setting up a Tunnel, the machine receiving the connection (the Server) is its own CA and will only accept certificates issued by itself.

- **Encryption**
  The encryption settings span from *None* to *High*. No encryption means that the traffic is still authenticated and is therefore recommended for Tunnels within LAN’s and WANs. You should be careful when selecting a higher encryption level since this will be more resource intensive for the machines at both ends of the tunnel.

Setting up the tunnel

Decide in which direction the connection should be made. This decides which side should be set up as a Server in the Tunnel configuration.

On the Hub on the Server side:

**Setting up the Server**

1. Open the *hub configuration tool* on the Hub computer by double-clicking the Hub Probe in Infrastructure Manager.
   - Check the *Enable Tunneling* option on the General tab.
2. Go to the *Tunnels > Server Configuration* tab and check the *Active* option.
The Certificate Authority (CA) Setup dialog appears.

![Certificate Authority Setup dialog](image)

Fill in organization and address information, give the CA a name, select a password and specify expire days (number of days before the server certificate expires).

Click the OK button to finish this dialog.

The CA and the Server Certificate is now generated.

3. Select one of the predefined security settings None, Low, Medium or High, or you can select Custom, where you define your own security setting.

4. Click the **Apply** button in order to start the Server.
Creating Client certificate(s)

1. Click the New button in the Issued Certificates field. The Client Certificate dialog appears.

   Fill in organization and address information, fill in the IP-address of the hub on the client side in the Common name field, select a password and specify expire days (number of days before the client certificate expires).

   Click the OK button.

2. Click the view button in the Issued Certificates field, and the Certificate Information pops up. Click the Copy button, and the certificate is now copied to the clipboard.

   Now, open up a text editor (such as Notepad) and paste the certificate into a new blank file. Save the file to a floppy, USB, or network drive where the Tunnel client can access it.

   Exit Notepad and click the OK button to exit the Certificate Information dialog box.

3. Click the Apply button and click on Yes when asked to restart the probe.
On the Hub on the Client side:

1. Open the *hub configuration tool* on the Hub computer by double-clicking the Hub Probe in Infrastructure Manager.
   
   Check the *Enable Tunneling* option on the General tab.

2. Go to the Tunnels > Client Configuration tab.

3. Click the *New* button, and the *New Tunnel Connection* dialog pops up.

4. Fill in the IP address of the Hub on the server side, the password used when generating the certificate, and copy the Certificate from the file into the *Certificate* field. Ensure that the Active Tunnel option is checked and click the OK button to close the dialog.

5. Click the *Apply* button to activate the Client.

The Tunnel should now be up and running!
Setting up a Tunnel in a NATed network

Networks that use NAT affect how a Tunnel is configured. Some of the possibilities are described in the three scenarios below.

You should be aware that when a Tunnel is configured, it replaces the Static Hub and NAT setup in the Hub configuration.

Client address is NATed

193.71.55.111

Client

10.2.1.111

101.1.1.1

Server

The Client certificate must be issued to (CommonName) the IP address that is visible to the Server, in this case 10.2.1.111, not 193.71.55.111.

Server address is NATed

193.71.55.111

Client

202.1.1.1

10.1.1.1

Server

The Client must uncheck the 'Check Server CommonName' option in the Tunnel Client Setup Window. The reason for this is that the Server certificate has 10.1.1.1 as CommonName, not 202.1.1.1 that is what the Client sees.

Server and Client addresses are NATed

193.71.55.111

Client

202.1.1.1

10.2.1.111

101.1.1.1

Server

Combine the two methods described above. The Client certificate must be issued to (CommonName) the IP address that is visible to the Server (10.2.1.111) and the Client must uncheck the 'Check Server CommonName' option in the Tunnel Client Setup Window.
About renaming a Hub or Robot computer

When renaming a Hub or a Robot computer, or changing the IP address, you should be aware of the following consequences:

- **QoS**
  When computers hosting QoS enabled probes are renamed, the QoS objects will be stored in new tables in the QoS database.

- **Alarms**
  Alarm filtering will be affected if the renamed computer is defined with host name as Alarm source in the filtering definition.
  This may also affect objects in Dashboards in the Enterprise Console.

- **Queues**
  Defined queues between Hubs will be affected if one of the Hub computers is renamed.

- **Mirroring**
  NAS mirroring (alarm messages are mirrored (copied) between both alarm servers) will be affected if one of the Hub computers are renamed.

- **Tunnels (if changing IP-address)**
  Defined tunnels will be affected if one of the HUB computers changes IP-address.

- **Licenses**
  License strings containing an IP address will not be valid any more if the computer hosting the probe/application requiring the license changes IP-address.

Adding a slave report_engine and/or a slave sla_engine

The primary task of the SLA Engine is to compute Service Level Agreement compliance for the SLAs, and the primary task of the Report Engine is to generate SLA and QoS reports.

You may speed up these tasks by installing another SLA Engine and/or Report Engine on another Robot controlled by the SLM Hub.

These components will then automatically be defined as slave components and assist the master components doing their job.
The Alarm SubConsole shows the list of alarms received.

The Alarm SubConsole can be started separately by selecting Start > Programs > Nimsoft Software > Tools > Nimsoft Alarm SubConsole.

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

This section contains the following topics:
The Alarm SubConsole Window (see page 221)

The Alarm SubConsole Window

The Alarm SubConsole window displays a list of alarms received, and the window is divided into a number of columns with information.
The information about the alarms in the list is divided into the following columns:

- **ID**
  Each alarm is assigned a unique ID-number by the Alarm Server.

- **Host Name**
  The name of the computer sending the alarm.
  **Note:** Occasionally host computers are represented with their IP address in this column.
  You may try to convert these by setting the following string in Registry to 1:
  HKEY_CURRENT_USER > Software > Nimsoft Software > Nimsoft Manager > Options > StripHostNameIp
  However, be aware of that this may result in timeouts!

- **Source**
  The IP-address of the computer sending the alarm.

- **Message**
  This field contains the alarm text message, describing the error condition.

- **Time Received**
  The last time the alarm was received by the nas.

- **Time Origin**
  The time when the alarm was sent from the probe.

- **Time Arrival**
  The time when the alarm was received by the nas.

- **Severity**
  All alarms are stamped with a code indicating the severity level, indicating the seriousness of the alarm. Note that the severity level also appears as colored icons in the ID column, making the most important ones stand out. The severity levels are:
  - Clear (Green)
  - Informational (Cyan)
  - Warning (Blue)
  - Minor (Yellow)
  - Major (Orange)
  - Critical (Red)
■ **Subsystem**
This identifies which part of the monitored computer the alarm was sent from (CPU, disk network etc.).

■ **Subsystem ID**
The subsystem ID is a field, containing one or more numbers separated by dots. This ID identifies which part of the monitored computer the alarm was sent from (CPU, disk network etc.).

■ **Count**
This field shows how many times the alarm has been received from the probe.

■ **Domain**
The name of the Domain associated with the Probe sending the alarm.

■ **Robot**
The Robot hosting the Probe sending the alarm.

■ **Probe**
This is the name of the probe that sent the alarm.

■ **Assigned To**
If the alarm is assigned to an operator, this field shows the name of this operator.

■ **Assigned By**
If the alarm is assigned to an operator, this field shows the name of user who assigned the alarm to the operator.

■ **Time Assigned**
If the alarm is assigned to an operator, this field shows at which time the alarm was assigned to the operator.

■ **Hub**
The Hub controlling the Robot hosting the Probe that sent the alarm.

■ **Nas**
This is the name of the nas storing and managing the alarm.

■ **Origin**
QoS data from probes are tagged with a name to identify the origin of the data. The origin name is normally set in the controller probe GUI.
If not, the Hub name will be used.
Note however, that the Origin field under *Advanced Settings* in the Hub GUI lets you specify an origin name of your own choice to be used, rather than the Hub name.
The Alarm SubConsole Window

- User Tag 1 & User Tag 2
  
  These are user-defined tags to be used as a grouping / locating mechanism. The tags are set in the controller probe GUI.

- Visible
  
  Normally all alarms are listed in this window and marked Yes in this column. However, the administrator can, using the nas GUI, set an alarm invisible. The alarm can then be seen only by users enabled through ACL to see invisible alarms.

Modifying the layout of the list in the window

If you want to modify the layout of the list in the window, you have a set of options available:

- If you want to have the columns placed in another order, the columns can be moved, using drag and drop.
- Left-clicking the column border, dragging to the preferred width and releasing the mouse button can also modify the width of columns.
- Right-clicking in a column header or inside the list also gives many options.

For details, see the section Right-clicking a Column Header.
Right-clicking in the Alarm Window

- View
- Accept
- Assign
- Unassign
- Acknowledge
- [Del]

**Alarm Details**
- Locate Probe
- Configure Probe...
- Hold Alarms
- ✓ Show Invisible Alarms
- Set Visibility
- Actions
- Notes
- Launch URL Ctrl+U
- Alarm Filter...
- Set Alarm Filter Based on
- Clear Alarm Filter
- Transaction History
- History
- Edit

- View
- Print
- Print Preview
- Edit

See description in the section *Right-clicking in a list*.

- Accept
- Assign
- Unassign
- Acknowledge
- Alarm Details

See the description in the section *Handling Alarms* for these options.
The Alarm SubConsole Window

Locate Probe

Right-clicking an alarm message and selecting this option searches and finds the probe that sent the selected alarm message.

If the option is selected in the Alarm SubConsole integrated in the Infrastructure Manager, the probe will be selected in the Main Window Pane.

If the option is selected in the Alarm SubConsole integrated in the Enterprise Console, or when the Alarm SubConsole is running stand-alone, a message will appear on the screen, displaying the complete probe address (Domain/Hub/Robot/Probe).

Configure Probe...

Right-clicking an alarm message and selecting this option opens the Probe configurator for the probe that sent the selected alarm message.

This enables you to edit the options and configuration parameters for the Probe.

Hold Alarms

The alarm window will not be updated when this function is active. This functionality may be useful when the alarm traffic is heavy.

Alarm Visibility

- **Set Visibility**
  - Visible
  - Invisible

**Hide Invisible Alarms/ Show invisible Alarms**

Selecting *Hide Invisible Alarms* hides alarms set invisible from the list. This option changes name to *Show Invisible Alarms*, letting you show alarms set invisible in the list again.

**Set Visibility**

Use this option to set the selected alarm visible or invisible.

- **Set Invisible**: Sets the selected alarm invisible. If the Show invisible Alarms option is selected, the invisible alarms are listed.
- **Set Visible**: Sets the selected alarm visible.

Note: The users require access rights in order to use the alarm visibility functionality.
The administrator can add textual notes to alarms. This can be done, using the NAS window or by selecting Notes > Attach from by right clicking in the message window.

**Show notes:**

Notes attached to an alarm can be seen by right-clicking the alarm in the alarm list, selecting Notes > Show.
If more than one note attached to the alarm, each note will have its own tab. In the example below you will find that two notes are attached to the alarm.

Clicking the Comment button lets you add a comment to the note.

Your logon user name and the current time will automatically be filled in. Write your comment, click the Apply button and then the OK button.
Attach notes

Selecting Notes > Attach lets you add notes to the alarm.

The following dialog appears, listing all notes available: Those defined in the NAS GUI and those defined using the New Note button (see below).

Tick the one(s) you want to attach to the alarm, or click the New Note button to create your own note.

Detach notes:

You may also detach note(s) that are attached to an alarm by selecting Note > Detach.

The following dialog appears, listing the alarms attached to the alarm. Tick the one(s) you want to detach and click the Detach button.
Another option is to click the note description text in the window. This activates the Delete Note button (which otherwise is grayed out). Clicking this button will detach the note from any alarm referring the note and permanently delete the note. The following warning will be given.

![Delete Note](image)

Creating a new note

Click the New Note button to create your own note.

**NOTE**: If no notes are previously defined, you must right-click the alarm and select Manage Notes to create a new note.

![New Note](image)

Fill in a name of the note in the Name field and the note text in the Description field.
Notes may also contain URLs. If a note contains an URL, the URL can be launched when right-clicking the alarm to which the note is attached and select *Show*.

If the note contains one or more URLs, a drop-down list at the bottom of the dialog lets you select which URL to launch.

Also note the option "Automatically remove this note when no active alarms refer to it". When this option is ticked, the note will be permanently deleted when no alarms refer to the note anymore.
Click the OK button and observe that the new note is added to the list.

Click the Attach button to attach the note to the alarm.

Managing notes

Selecting Note > Manage lets you manage the notes available.
The Manage Notes window lets you *add*, *edit* and *delete* notes.

- **New**: This button opens the New Note dialog.

- **Edit**: Select a note and click the Edit button. This option opens a dialog similar to New note with the details of the selected note.
  
  Refer the Notes section to know more about add operation.

- **Delete**: Select a note and Click the Delete button. A confirmation message appears before deleting the note.

![Warning dialog](image)

### Launch URLs

Alarms may contain URLs in the text field. If an alarm messages contains a URL, you will see that the option ‘Launch URL’ is activated when right-clicking the alarm in the alarm list. Selecting the ‘Launch URL’ option will launch the URL in a separate window.

### Actions

This option lets you define your own actions to be performed on alarms.

You can add your own user defined menu commands that will show up in the popup menu when you right click on an alarm in the list.

Select Configure to bring up the dialog to configure your action. Press the ‘New’ button if you want to add a new command. You can determine the menu command ordering by using the ‘Move Up’ and ‘Move Down’ buttons. In the argument field you have the option to specify a great number of tokens, which will be expanded to the correct value when you actually initiate the command.
For example, $HOST in the argument list will be replaced with the name of the Host sending the alarm when you activate the command. The tokens available are the same as the column name headers in the alarm list.

**Useful options to this feature:**

- ACL management of who can access the alarm actions Configure dialog.
- Alarm message extraction argument in order to obtain specific parts of a message.
- Parent popup menu to group menu items.
**ACL Management**

Enter the ACL Management window and use the Alarm Management and Modify Profiles switch to determine whether users of a specific ACL should be allowed to enter this dialog.

For the Infrastructure Manager SubConsole and the Enterprise Console alarm lists, the Configure menu item will not be present if the above ACL permission is not set. For the standalone SubConsole, the menu item will be grayed out.

**Alarm Message Extraction**

An extension has been added to support message text extractions from the alarm line. In the arguments field, specify as many $MSG{AA,BB}$ type of arguments you need. You will need to substitute the AA part with a text token that precedes the value you want to extract from the alarm message. The BB must be substituted with a text string that marks the end of the requested value.

Example:

Alarm message: Disk D:\ has 16% free space, which is at or below the threshold (20%)

Argument: $MSG{ threshold (,)} $MSG{ has, free}

The resulting argument will be: 20% 16%

Notice that $MSG{ has, free}$ and $MSG{has, }$ will both return the value 16% from the alarm message. It’s all about finding a text that will mark the start and some text (here in this latter case, just a space) that marks the end of what should be contained in the value.
Menu Action Grouping

In order to be able to organize the set of menu actions, the possibility to add a parenting popup menu has been added.

Use the pipe character | in order to specify the name of the parenting popup menu. The below figure indicates that 2 parenting popup menus will be created; Check and Help. For both, there will be 2 actual alarm actions contained in their child menu. The alarm action Calc in the below figure does not have a parenting popup menu specified, and will therefore reside on the same level as the Check and Help popup menus.
The menus will now look like this:

```
View
Accept
Assign
Unassign
Acknowledge [Del]

Alarm Details
Locate Probe
   Configure Probe...

Hold Alarms
✓ Show Invisible Alarms
   Set Visibility

Actions
Check.  Message
   Configure...
   Source

Notes
Launch URL Ctrl+U

Alarm Filter...
Set Alarm Filter Based on
   Clear Alarm Filter

Transaction History
   History

Edit
```

Alarm Filter...

Using the alarm filter, you can configure the alarm list to display:

- Only alarms from selected source(s):
  - Host name
  - Source
  - Nas
  - Origin
  - Subsystems
  - Probe
  - etc.

- Only alarms containing specific message text.
- Only alarms with severities as specified.
- Only alarms received, origin or arrival before or later than:
  - Time Received
    The last time the alarm was received by the nas.
  - Time Origin
    The time when the alarm was sent from the probe.
  - Time Arrival
    The time when the alarm was received by the nas.

- Only alarms assigned to or by specific users, or only alarms assigned before or later than n hours.

- User tags 1 or 2
  Only alarms containing the user tag specified. These are user-defined tags to be used as a grouping / locating mechanism. The tags are set in the controller probe GUI.
Also note the two options Set Alarm Filter Based on and Clear Alarm Filter (see below).

**Set Alarm Filter Based on**

Selecting (by left-clicking) one of the alarms in the window, you can use this option to filter on parameters like:

- Source
- Severity
- Host Name
- Probe
- Etc.

Then only alarms sent by the source, probe etc. that sent the selected alarm will be displayed in the window.

Another example: If selecting an alarm with severity Warning and filtering on Severity, only alarms with severity Warning will be displayed.

**Clear Alarm Filter**

Clears alarm filters (as described under Set Alarm Filters based on, see above), if any.
Transaction History

This option opens the Transaction History window for the alarm selected. This window shows the transaction log for the alarm. This makes it possible to study and follow the complete message life from the initial message and to when the message is closed (acknowledged) and via multiple suppressions.

History

Even if an alarm message is acknowledged, it can still be traced in the nas history database.

Using the History option, you can list and see alarms from the selected time frame (today, last hour, last week, last month, last 24 hours, last 3 days or last 7 days).
The alarms will be opened in a separate window.

Selecting the *Query* option, a filter dialog appears, enabling you to filter the historical alarms you want to see for the period specified.

You can select one of the same predefined time periods as mentioned above, or you can select *Custom* and specify a custom period (*From* time and *To* time).
You can filter on one or more of the columns in the alarm window, and regexp is supported. The example above will pick alarms from all probes on the host xpruha with severity level Minor and above for the custom period specified.

Setting the filter and clicking the Open button, the alarms matching the filter will be opened in a separate window.

Clicking the Save button, the query will be saved to a local repository. Then clicking the Open button, this repository will be opened, enabling you to paste the query for other use.
Clicking the OK button, the filter dialog will be filled in according the selected query.

Clicking the Delete button will delete the query from the repository.

**Note:** Double-clicking a query will open the query in a new dialog, making long queries easier to read.

---

**The Toolbar in the Alarm Window**

The upper part of the Alarm Window contains a toolbar, enabling you to find, sort and handle alarms, manage views etc.
The Alarm SubConsole Window

See the description in the section *Handling Alarms* for the following (leftmost) tool buttons.

- Accept
- Assign
- Unassign
- Acknowledge
- Hold Alarms
■ **Alarm Filter...**

Using the alarm filter, you can configure the alarm objects to display:

- Alarms from selected source(s), subsystems, probes, etc.
- Only alarms with severities as specified.
- Alarms containing specific text.
- Time when the alarms were received.
- Alarms assigned to or by specific users, etc.

For details, see the section **Alarm Filter...**

See the description in the section *Right-clicking a column header* for the following tool buttons:

- Select
- Filter
- Find
- Find next
- Find Previous
See description in the section *Right-clicking in a list* for a description of the right-most buttons:

- Sort
- Columns
- Print
- Save views
- Manage views
Chapter 6: Distribution Application

There are two separate ways to distribute archive packages. You can distribute within the Infrastructure Manager or start the standalone Nimsoft Distribution application.

Using the Infrastructure Manager:

The obvious difference of use is the interactive character when using Infrastructure Manager. You simply drag a package from the archive list and drop it on a Domain node, Hub node, or a Robot node. A progress dialog will provide information in detail about the ongoing distribution.

Note that you can close down this dialog and continue working in the Manager without interfering with the actual distribution. If you would like an update of the distribution status, reactivate the dialog using the View Progress menu command in the Archive node of the Manager. This is invoked through the right-click menu.

As an alternative to drag & drop, you can also perform distribution within the Manager by invoking the Distribute dialog from the archive list.

Using the Nimsoft Distribution application:

The other way to distribute is using the standalone Nimsoft Distribution application. You will find drag & drop capabilities here in the same way is in the Manager, but most important is the ability to create distribution tasks (Task = profile containing information about what packages to distribute and the set of destination Robots).

These tasks are saved and make it easy to reinitiate a distribution of certain packages to a set of destination Robots. The built-in task scheduling mechanism enables you to start the actual distribution at some preferred time, thus eliminating the interactivity required when distributing within Infrastructure Manager.

Setup parameters will let you determine how the application should handle error situations when a specific distribution fails. A destination Robot is perhaps turned off, and you can specify a number of retry attempts and the time interval between the attempts.

A generated log file will provide full information of a task distribution. The rest of this documentation will focus on the use & functionality of the standalone Nimsoft Distribution application.
Starting the Distribution Application

You start the Nimsoft Distribution application by double-clicking the shortcut to Nimsoft Distribution found under the Applications Node in the Navigation Pane in the Infrastructure Manager, or by selecting Tools > Nimsoft Distribution from the menu bar.

Login

The Login dialog is the same as that found in the Alarm Sub Console. It is simpler than that of the Infrastructure Manager and Enterprise Console.

Note: If the Nimsoft Distribution application is launched directly from Infrastructure Manager, you will automatically be logged into the Hub, which was the current login Hub for the Infrastructure Manager.

You need to specify the Hub you want to log on to (or its IP address) in the Hub field.
The Distribution Window

The application window is divided into three window panes: The Navigation Pane on the left and two List Panes on the right.
The Navigation Pane

The tree structure in the Navigation Pane contains the Domain structure associated with the Hub you are currently logged into.
The List Panes

The **Upper List Pane** displays:

- The tasks that we define, using the Create Task option. A task is a profile containing information about what packages to distribute and the set of destination Robots.

  **Note:** When a distribution has been initiated by starting a task, the task entry itself will display the distribution status.

- The distribution jobs contained in the distribution server.

  **Example:** If distributing a Probe package, using drag and drop (in the Infrastructure Manager or in the Nimsoft Distribution application), the distribution will appear in the upper list pane.

The fields in the upper list pane are:

**Name**

The name of the job or task.

**Description**

A short description of the job or task.

**Status**

The distribution progress when the job or task is running (starting at 0%, ending at 100% when successfully finished).

**Information**

Status information during the distribution (In progress, Completed, etc.).
Start at

Start time for the task if scheduling is defined.

Last started

The last time the task was started.

The **Lower List Pane** displays the packages currently contained in the archive you are logged into. As in the Infrastructure Manager, you can do a quick interactive distribution simply by dragging one or more packages and dropping them onto a Domain node, Hub node, or a Robot node.

The fields in the lower list pane are:

**Name**

The name of the probe package.

**Description**

A short description of the probe package.

**Version**

The probe package version number.

**Group**

The logical group the package belongs to.

**License Info**

Short license info (owners name, demo license etc.).

**License expires**

The date when the license expires.

**Required**

"Yes" if a license is required for the probe package, otherwise this field is empty.
The Menu Bar

The Nimsoft Distribution application menu bar contains the following menu items:

- File
- Action
- View
- Tools
- Help

Help

Help Nimsoft Distribution

This option opens the online documentation for the Nimsoft Distribution application.

About Nimsoft Distribution

This option displays the application version number.

File Menu

You can perform the following tasks from the file menu:

Update Tasks

Updates the tasks in the List Pane.

Login

Opens the Login dialog.

Exit

Exits the Nimsoft Distribution application.

Action Menu

You can perform the following tasks from the Action menu:

Create Task

Opens the Create Task wizard (see Creating Tasks).

Start

Starts a distribution task.

Cancel

Cancels a running distribution task.

Reattempt

Restarts a distribution that has failed.
View Menu

You can perform the following tasks from the view menu:

View Progress
  Opens the Progress View window for the selected task.

View Log
  Opens the log dialog, described in the section The Log Window.

Toolbar
  Shows or hides the toolbar.

Refresh
  Refreshes the contents of the window panes.

Tools Menu

The Setup submenu provides the ability to make changes to the distribution server setup, see The Setup Dialog section for more information.

Help Menu

You can access the following information from the help menu:

Distribution
  Opens the online documentation for the Nimsoft Distribution application.

About Distribution
  Displays the application version number.
The Toolbar

- **Update Tasks**
  Updates the task.

- **Create Task**
  Starts the Create Tasks Wizard.

- **Start**
  Starts a distribution task.

- **Cancel**
  Cancels a running distribution task.

- **View Progress**
  Opens the Progress window for the selected task.

- **View Log**
  Opens the Log window.

- **Setup**
  Opens the Setup dialog, where you will be able to tune the distribution server.

- **Login**
  Opens the Login dialog.
Creating Tasks

You create a new task by invoking the Create Task wizard.

![Create Task dialog box]

- **Name:** Task 3
- **Description:** Distribution of new probes
Specify a name and a description and click the Next button.
Select the packages to be distributed in this Task in the *Available packages* frame and click the Add button. Ensure that the selected packages appear in the *Packages to distribute* frame before clicking the Next button.

![Create Task Window](image)
Here you must specify the destination Robots. Note that you are not necessarily expected to specify exactly which Robots to distribute to in a static manner. You are supposed to enter criteria that will result in a set of Robots. You can test the set of Robots by activating the Test Extracted Target Output button. When an actual distributions starts, the distribution server will itself extract the target output as it initiates the distribution. You are free to use regular expressions in any of the fields.

In this example (see the figure above) the destination Robots will be: all Robots controlled by the Hub wrune.

Click the Next button to continue the wizard.
The last dialog lets you set up a start time for the task if scheduling is desired (if you check the *Enable scheduling* option).

If checking the *Update only* button (this option can only be selected if the *Enable scheduling* option is checked), packages will only be distributed to target computers where the package has previously been installed.

Finally, click the *Finish* button.

Defined Tasks can be modified, using the *Properties* option.

The Property option is found by right-clicking a task in the Upper List Pane and selecting *Properties*. 
In addition to parameters defined and described during the Creating Tasks Wizard, you will be able to specify unique Retry parameters for the Task in question:

- Number of attempts.
- Timeout duration (time between each attempt).
The Distribution Window

Starting a Task

Once a Task has been created you can start it by:

- Clicking the Start button found in the Toolbar.
- Selecting the menu command Action > Start
- Right-clicking a task in the Upper List Pane and selecting Start.

The following dialog appears. If checking the Update only, packages will only be distributed to the target computers where the package has previously been installed.

Click the OK button to start the distribution.

![Start Dialog](image)

Note that tasks also can be started automatically at a specified date and time, using the Schedule functionality in the task setup dialog.

Canceling a Task

You can cancel an ongoing distribution, but please note this command will not lead to an immediate distribution halt. The distribution server might not be able to stop an already posted distribution request, and in that case the system will have to wait until it finishes.
Progress View

A detailed status view of a distribution can be seen by double-clicking a job or a task, or by selecting the menu command View > View Progress. That is, if the job or task is currently not active, double-clicking it will result in the Log window being activated. Otherwise, when the job or task is running, the Progress window will be activated.

The following columns of information is found in the Progress window:

- **Package**
  The name of the probe packages to be distributed by the task.
  - Green symbol when in progress or successfully finished.
  - White symbol when queued.
  - Red symbol when distribution failed.

- **Robot**
  The name of the robot to which the probe packages are distributed.

- **Message**
  The current status of the distribution process (queued, finished etc.).

- **Sections**
  This column displays which section of the probe package is currently being transferred.

- **File**
  The name of the file currently being transferred.
The Distribution Window

- **Kb**
  Displays the number of Kilobytes currently transferred.

- **Version**
  Displays the version of the probe packages being distributed.

- **Update**
  Yes means that the probe package is updated to the newest version.
  No means a complete distribution of the package.

- **Time Entered**
  The time the job is entered into the distribution server's job list.

- **Time Scheduled**
  The time when the transfer is expected to start.

- **Time Started**
  The time when the transfer starts.

- **Time Finished**
  The time when the transfer is finished.

If a job or task does not complete with a 100% success of distribution, the Reattempt command (*Action > Reattempt* in the Menu bar) can be used to tell the distribution server to reinitiate distributions to the failed targets only.
The Log Window

The Log window provides detailed information about each distribution. The window is opened by selecting View > View log in the Menu bar.

Once inside the log window, you can choose to see all available logs (using the File > Set Log option) or just the logs corresponding to a single job or task.

When looking at the log data, you can further choose to view all log information (View > All Distributions) or just the data produced since the last run (View > Since Last Run).

The following columns of information are found in the Log window:

- **Task**
  The name of the task running the probe package distribution.

- **Package**
  The name of the distributed probe package.

- **Robot**
  The name of the robot to which the probe package was distributed.

- **Status**
  The status of the transfer; OK or error.
The Distribution Window

- **Description**
  The description of the distribution task.

- **Time Entered**
  The time the job was entered into the distribution server’s distribution job list.

- **Time Scheduled**
  The time when the transfer was expected to start.

- **Time Started**
  The time when the transfer started.

- **Time Finished**
  The time when the transfer was finished.

- **Result Code**
  A code, reflecting the result of the transfer as described in the Result String (see below).

- **Result String**
  Describing the result of the transfer (finished, cancelled, failed etc.)

- **Attempt**
  The number of attempts before finishing the transfer or giving up.

- **Remote**
  Yes in this column indicates that the package was distributed from a remote distribution Robot.

- **Source**
  The address of the source distribution server in case of remote distribution.

- **Version**
  Displays the version number of the distributed probe package.

- **Update**
  Yes means that the probe package is updated to the newest version.
  No means a complete distribution of the package.

Double-clicking one of the log entries (rows) opens the row in a separate window with detailed log information.

There are manual maintenance functions here that enable you to either totally clear the log or just to compress it. The compression logic will remove all "older" entries of a package/Robot combination. That is, only the very latest entry of a specific package distribution to a certain Robot appears in the log.
The Setup Dialog

The Setup dialog is opened by selecting the menu command **Tools > Setup**. The Setup enables you to tune the distribution server.

- **Distribution**
  - **Number of concurrent distributions**
    You can limit the number of concurrent distributions by specifying an upper number.
  - **Enable remote distribution**
    Enabling remote distribution is recommended. This enables the distribution server on your Hub to transfer a distribution task to the Hub (its distribution server) where the destination Robot resides.
  - **Accept remote distribution request**
    The distribution server on your Hub may be requested by other servers to perform a distribution. You can decline any such request by un-checking his option.
Drag & drop

- **Log History**
  
The log file contains detailed distribution history data.

  When *Enable automatic cleanup* is checked, the system automatically removes entries older than the specified number of days. See also  The Log Window.

- **Retry parameters**
  
Here you can decide the number of distribution attempts and the time interval between those attempts in case of failed distributions.

- **Poll interval**
  
These parameters specify how often the application GUI should request updated information from the distribution server. In addition you can also perform a total refresh by pressing F5.

Drag & drop

You can drag packages from the package archive window and drop them onto a Domain Node, a Hub node, or a Robot node. This will lead to an immediate interactive based distribution.

Also, using the drag & drop feature, you can drop a Task definition onto a Domain, Hub, or Robot. In this case the destination targets contained in the Task will be overruled. The only thing retrieved from the task is the set of packages to distribute. You will in fact note that in this way of distributing, a new job entry will appear in the Task list. So in fact, it is not the Task itself that has been started. Package information residing in the Task has been extracted to create a new job.
Chapter 7: Probe Report

Probe Report is an application for searching and finding probes and probe configuration parameters.

If your installation consists of more than one domain, reports will be made for the domain you are currently logged on.

Reports can be printed, or they can be exported into Microsoft Excel.

It is possible to make three different reports:

- **Probe Summary Report**
  This report contains a list of all probes installed on computers controlled by the selected hub(s) on the domain you are currently logged on.

- **Probe Configurations Report**
  This report lists the configuration parameters for the selected probe(s) on the selected hub(s).

- **Probe Statistics Report**
  This report lists the statistics for all probes on the selected hub(s), such as number of probes, probe status etc.

This section contains the following topics:

- [Starting the application](#) (see page 269)
- [Login](#) (see page 270)
- [The Probe Report Window](#) (see page 271)
- [Generating reports](#) (see page 277)

### Starting the application

Currently you can start the Probe Report application by double-clicking the icon located under the `program files/Nimsoft/bin` folder.

![ProbeReport.exe]

In the next release, it will be possible to start the application from the Infrastructure Manager.
If your installation consists of more than one domain, reports will be made for the domain you are currently logged on.

To log on to another domain, you select *File > Login* from the Menu bar, or you click the Login icon in the Toolbar.
The application window contains a list pane, where the generated report will appear as a list, a toolbar and a menu bar.

<table>
<thead>
<tr>
<th>Probe</th>
<th>Editor</th>
<th>Class</th>
<th>Description</th>
<th>Group</th>
<th>Address</th>
<th>Port</th>
<th>PID</th>
<th>Active</th>
<th>Command</th>
<th>Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Right-clicking in the window

In addition to ordinary right-click functions as described in the section Right-clicking in a list, you can generate three different reports from this menu:

- **Probe Summary Report**
  This report contains a list of all probes installed on computers controlled by the selected hub(s) on the domain you are currently logged on.

- **Probe Configurations Report**
  This report lists the configuration parameters for the selected probe(s) on the selected hub(s).
The Probe Report Window

- **Probe Statistics Report**
  This report lists the statistics for all probes on the selected hub(s), such as number of probes, probe status etc.

---

**The Menubar**

**File**

- **Probe Report**
  - File
  - Report
  - View
  - Help
  - Probe
  - Robot
  - View
  - Probe Summary Report
  - Probe Configurations Report
  - Probe Statistics Report
  - Print Preview
  - Print...
  - Edit

---

272 Infrastructure Manager
Chapter 7: Probe Report

The Probe Report Window

- **Login**
  Opens the Login dialog, enabling you to log in as another user, or to log in on another Domain.

- **Print Setup**
  Here you can select printer and edit the printer options (paper size, paper source, paper orientation etc).

- **Print Preview**
  The Print Preview option opens a list with the contents of the main window.

- **Print**
  The Print option prints the contents of the main window.

- **Exit**
  Exits the Probe Report application.

Report

![Probe Report Window](image)
The Probe Report Window

- **Probe Summary Report**
  Generates a *Probe Summary Report*. This report contains a list of all probes installed on computers controlled by the selected Hub(s) on the domain you are currently logged on.

- **Probe Configurations Report**
  Generates a *Probe Configurations Report*.
  This report lists the configuration parameters for the selected probe(s) on the selected hub(s).

- **Probe Statistics Report**
  Generates a *Probe Statistics Report*.
  This report lists the statistics for all probes on the selected hub(s), such as number of probes, probe status etc.

**View**

- **Toolbar**
  When this option is checked, the toolbar will appear below the Menubar.

- **Status Bar**
  When this option is checked, a status bar at the bottom of the window will be shown.

**Help**
The Probe Report Window

Chapter 7: Probe Report

- **Probe Report**
  Opens the Probe Report on-line documentation, describing the application.

- **About Probe Report**
  This option displays the application version number.

- **Display Login Information**
  This option displays the current login status.

![Login Information Window](image)

The Toolbar

- **Login**
  Opens the Login dialog, enabling you to log in as another user, or to log in on another Domain.

- **Print**
  This option prints the contents of the main window.

- **Export Report to Excel**
  When clicking this button, the report currently displayed in the main window will be copied to the clipboard.

  You can now start Excel and paste the contents into a worksheet.
The Probe Report Window

- **Probe Configuration Reports View**
  This button is activated when a Probe Configuration Report has been generated. Clicking this button allows you to select different report views. Currently three views are supported: CPU, Disk and Memory (for the cdm probe).

- **Abort Report**
  Clicking this during the generation of a report will abort the report. You are asked if you want to display the aborted report.

- **Probe Statistics Report**
  Generates a **Probe Statistics Report**.
  This report lists the statistics for all probes on the selected hub(s), such as number of probes, probe status etc.

- **Probe Configurations Report**
  Generates a **Probe Configurations Report**.
  This report lists the configuration parameters for the selected probe(s) on the selected hub(s).

- **Probe Summary Report**
  Generates a **Probe Summary Report**. This report contains a list of all probes installed on computers controlled by the selected Hub(s) on the domain you are currently logged on.
Generating reports

Generating a Probe Summary Report.

Click the Probe Summary Report button on the Toolbar or select Report > Probe Summary Report from the Menubar.

The following dialog appears, and you can select one or more Hubs. When clicking the OK button, a report will be generated for probes on the selected hubs.

This report contains a list of all probes installed on computers controlled by the selected Hub(s) on the domain you are currently logged on.
Generating a Probe Configurations Report.

Click the Probe Configurations Report button on the Toolbar or select Report > Probe Configurations Report from the Menubar.

The following dialog appears, and you can select one or more Hubs and one or more probes. When clicking the OK button, a report will be generated for selected probes on the selected hubs.

Generates a Probe Configurations Report.

This report lists the configuration parameters for the selected probe(s) on the selected hub(s).
Generating a Probe Statistics Report.

Click the Probe Statistics Report button on the Toolbar or select Report > Probe Statistics Report from the Menubar.

The following dialog appears, and you can select one or more Hubs. When clicking the OK button, a report will be generated for probes on the selected hubs.

This report lists the statistics for all probes on the selected hub(s), such as number of probes, probe status etc.
Exporting a report to Excel.

When you have generated a report, you can easily export the report into a worksheet in Excel.

Click the Copy Report to Excel button.

The following dialog appears, telling that the contents of the report are copied to the clipboard.
Click the OK button to close the information dialog.

Start Excel, select a worksheet, place the cursor in a row/column, right-click and select Paste.

The report is now copied into the worksheet.
Example:

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Probe</td>
<td>Hub</td>
<td>Count</td>
<td>Active</td>
<td>Total</td>
<td>Total.Active</td>
<td>Robot(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>cdm</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>controller</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>data_eng</td>
<td>wosume</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>distv</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>emailgw</td>
<td>wosume</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>hdp</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>httpd</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>hub</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>lparepos</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>informix</td>
<td>wosume</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>interface</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>login</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>mgc</td>
<td>wosume</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>nas</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>net_con</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>ntp</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>nsc_services</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>omm</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>process</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>remedy_run</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>report_engine</td>
<td>wosume</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>smtpgw</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>spooler</td>
<td>wosume</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>spoolnik</td>
<td>wosume</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Development/Avsnare/Aworse</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix A: Registry Options

This section contains the following topics:

- **General** (see page 283)
- **Registry Keys** (see page 283)
- **Registry Options Keys** (see page 287)
- **Overview: Permissions and Ownership** (see page 291)
- **User Administration** (see page 292)
- **Working with Alarms** (see page 322)
- **Account Administration** (see page 325)
- **Working with Views in Lists** (see page 331)

**General**

The Infrastructure Manager efficiently lets you manage and configure probes in your IT infrastructure. It also offers features for downloading new probe packages from the Nimsoft Archive for distribution. Additionally, the Infrastructure Manager also handles the license management.

The Enterprise Console offers you advanced users interface to Alarms/Events and Quality of Service data generated and collected by probes in your IT infrastructure. A complete dashboard suite containing a designer and a web-publishing tool also follows the solution.

**Registry Keys**

This document aims to explain the various Registry options for Infrastructure Manager and Enterprise Console. The sections are found under:

- HKEY_CURRENT_USER\Software\Nimsoft Software
- HKEY_LOCAL_MACHINE\Software\Nimsoft Software
- HKEY_LOCAL_MACHINE\Software\Nimsoft Corporation

The most important keys are the Options keys, which are placed at the following location: HKEY_CURRENT_USER\Software\Nimsoft Software\Nimsoft Manager\Options. The Manager and EC share these keys since they by implementation share many binary components.
HKEY_CURRENT_USER

The following figure shows the Registry structure for Nimsoft in the HKEY_CURRENT_USER section. Here you can view various console applications and persistency settings based on their application name.
Additionally, some simple Option values are available for the applications such as Nimsoft DashboardViewer and Nimsoft Web Publish. However, the focus is on the Nimsoft Manager section and some of the more relevant subsections.

- **NcListCtrl**
  This folder contains persistency data and user preferences for the extended List Control used by EC and the Manager. If any uncommon problem arises for a certain list, you can identify the list with its attributes and delete in order to reset it.

- **NcSplitFrame**
  EC and Manager save the Login keys before the applications are closed. You can delete these keys in order to reset the login dialog values. The other key of less interest, but worth mentioning is WebServer. The WebServer key holds the address of httpd. Web dashboards use this address to download standard documentations/images when any web dashboard is accessed first time.

- **Options**
  This folder contains the most important keys for the EC and the Manager. Many of them can be set in the Tools/Options dialog and the associated help for the dialog provides the necessary explanation. The Option keys are explained in detail in the last section.
HKEY_LOCAL_MACHINE

The following figure shows the Registry structure for Nimsoft in the HKEY_LOCAL_MACHINE section.

- Nimsoft Software/Nimsoft Manager

In the Labels and URLs sections, text labels and URL addresses used by EC and the Manager can be changed in order to customize the appearance for lighter OEM purposes. The Probe Version section contains archive version the Manager stores and check against, in order to manage archive version updates.

- Nimsoft Corporation

This folder contains installed version tags, useful to the Nimsoft Server for informing the users about possibly newer versions of Manager (Nimsoft section) and EC (Nimsoft Enterprise Console section).
# Registry Options Keys

Following table lists registry keys and their explanation:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[HKEY_CURRENT_USER\Software\Nimsoft Software\Nimsoft Manager\Options]</td>
<td></td>
</tr>
<tr>
<td>&quot;ActivateSummarize&quot;=&quot;1&quot;</td>
<td>EC: Alarm Summary is activated.</td>
</tr>
<tr>
<td>&quot;AlarmIndicator&quot;=&quot;1&quot;</td>
<td>EC/Manager: Alarm summary bar is displayed in status bar.</td>
</tr>
<tr>
<td>&quot;AttemptQosInit&quot;=&quot;1&quot;</td>
<td>EC: This status indicates an attempt to reinitialize a database connection, if the connection is broken during the dashboard execution. The performance is affected if the connection cannot be resumed.</td>
</tr>
<tr>
<td>&quot;AutoAppLogin&quot;=&quot;1&quot;</td>
<td>EC/Manager: Application automatically logs on to active session (held by NimLogin) at the startup.</td>
</tr>
<tr>
<td>&quot;AutoDesignRefresh&quot;=&quot;1&quot;</td>
<td>EC: Automatically updates dashboard when closing the design mode.</td>
</tr>
<tr>
<td>&quot;AutoLogin&quot;=&quot;1&quot;</td>
<td>Manager: automatically attempts to log in to the hub, selected in the navigation tree.</td>
</tr>
<tr>
<td>&quot;AutoMapRefresh&quot;=&quot;6&quot;</td>
<td>EC: A value greater than 0 and less than 100 sets the number of hours between an automatic reload of the active dashboard by the system.</td>
</tr>
<tr>
<td>&quot;CentralSubscription&quot;=&quot;1&quot;</td>
<td>EC: The dashboard gets a nas events from the login hub and thus overrides any other nas setting.</td>
</tr>
<tr>
<td>&quot;ConnectionString&quot;=&quot;26/xc39ar7nWz7tvWNqq6EWTsXAYAWQuMzDdqoghiSaEb90rJNd1BUAYIchKMl380fwswPkrS8IxP1c7is7rec/bPFBysLheZShqhiJHhjwjgQ/at039R9rOo12PV+k6akcwz9C160Tpf3QnjKT89nmV7ewK4809P1TszoMpuGtM19yELTe43EgMNz71mp&quot;</td>
<td>EC/Manager: The last successful connection string obtained from the Data Engine is stored and reused if no contact with Data Engine at login.</td>
</tr>
<tr>
<td>&quot;ConvertHostNameIp&quot;=&quot;1&quot;</td>
<td>EC/Manager: It is a client side attempt to convert an IP in an alarm, from nas to the corresponding host name. It reduces the performance a lot.</td>
</tr>
<tr>
<td>&quot;DashboardLinkEventReceiverModel&quot;=&quot;0&quot;</td>
<td>EC: Switch between new and old mechanism for distributing state notifications from Dashboard Server. New mechanism is used when value is one. Default value is zero since this switch is not proven more efficient.</td>
</tr>
<tr>
<td>&quot;DashboardServer=&quot;/SDP/xppesu/xdell/dashboard_server&quot;</td>
<td>EC: Nimsoft address to dashboard_server probe.</td>
</tr>
<tr>
<td>Registry Key</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&quot;DataEngineVersion&quot;=&quot;7.11 [Nov 6 2008]&quot;</td>
<td>EC/Manager: The last successful version string obtained from the Data Engine is stored and reused if no contact with Data Engine at login.</td>
</tr>
<tr>
<td>&quot;DisplayRangeError&quot;=&quot;1&quot;</td>
<td>EC: If meter controls in dashboards get out-of-range values, then an error message is displayed instead of the object. It is rarely used.</td>
</tr>
<tr>
<td>&quot;EnableDynamicViewsModification&quot;=&quot;1&quot;</td>
<td>EC: The dynamic views dashboard templates are accessible for modifications.</td>
</tr>
<tr>
<td>&quot;FindExternal&quot;=&quot;1&quot;</td>
<td>Manager: The Find command starts an out-of-process external utility instead of the built-in one. This way processing Find does not affect the Manager GUI response.</td>
</tr>
<tr>
<td>&quot;GroupServerTree&quot;=&quot;1&quot;</td>
<td>Manager: Display the dynamic views servers in accordance with the group setup in the Group Server.</td>
</tr>
<tr>
<td>&quot;HubUpLogin&quot;=&quot;1&quot;</td>
<td>EC/Manager: Re-login to system in ten seconds after the login hub has started (after being down) in order to ensure proper data and states.</td>
</tr>
<tr>
<td>&quot;IgnoreNimEvents&quot;=&quot;0&quot;</td>
<td>EC/Manager: Most events sent to consoles are ignored if it is set to one.</td>
</tr>
<tr>
<td>&quot;IgnoreNimEventsCount&quot;=&quot;200&quot;</td>
<td>EC/Manager: If, more than N events arrive during a 10-second window, than Hold Events turns On automatically.</td>
</tr>
<tr>
<td>&quot;IgnoreAlarmCountEvents&quot;=&quot;0&quot;</td>
<td>EC/Manager: Insignificant alarm updates due to change in count status. It is ignored only if the registry is set to 1.</td>
</tr>
<tr>
<td>&quot;IgnoreWebDataCollect&quot;=&quot;0&quot;</td>
<td>EC: Dashboard initial probe requests to obtain domain status are ignored if set to one. Some dashboard objects require this data to work as intended (Robot/Hub objects).</td>
</tr>
<tr>
<td>&quot;IntegratedDynViews&quot;=&quot;1&quot;</td>
<td>EC: Dynamic Views dashboards are not launched in a separate window.</td>
</tr>
<tr>
<td>&quot;IntegratedToolbox&quot;=&quot;1&quot;</td>
<td>EC: The Designer toolbox is not launched in a separate window.</td>
</tr>
<tr>
<td>&quot;InternetArchive&quot;=&quot;1&quot;</td>
<td>Manager: The Manager attempts to contact the Nimsoft Internet Archive.</td>
</tr>
<tr>
<td>&quot;LaunchDashboardNewWindow&quot;=&quot;0&quot;</td>
<td>EC: Linked dashboards is launched in a new window if set to 1.</td>
</tr>
<tr>
<td>&quot;LoginHub&quot;=&quot;&quot;</td>
<td>EC/Manager: Primary login hub.</td>
</tr>
<tr>
<td>&quot;LoginHub2&quot;=&quot;&quot;</td>
<td>EC/Manager: Secondary login hub.</td>
</tr>
<tr>
<td>&quot;LoginHubIp&quot;=&quot;&quot;</td>
<td>EC/Manager: Primary login hub IP.</td>
</tr>
<tr>
<td>&quot;LoginHubIp2&quot;=&quot;&quot;</td>
<td>EC/Manager: Secondary login hub IP.</td>
</tr>
<tr>
<td>&quot;LogLevel&quot;=&quot;2&quot;</td>
<td>EC/Manager: Will set the log level using the LogSet method in the Nimsoft COM library.</td>
</tr>
<tr>
<td>Registry Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&quot;MessageBeep&quot;=&quot;1&quot;</td>
<td>EC/Manager: For event messages in the Messages/Trace window that are signaling an error, a beep alarm is generated.</td>
</tr>
<tr>
<td>&quot;MultibyteFormat&quot;=&quot;0&quot;</td>
<td>EC: Dashboards will be stored in a binary format that can be interpreted properly on multi-byte OS systems. The format itself is not multi-byte.</td>
</tr>
<tr>
<td>&quot;MultiThreadConsole&quot;=&quot;1&quot;</td>
<td>EC: Dashboard requests/queries using the multiple threads to speed performance.</td>
</tr>
<tr>
<td>&quot;MultiThreadManager&quot;=&quot;1&quot;</td>
<td>Manager: The Manager Navigation tree does not freeze and wait when nodes are clicked on, but rather obtain data in threads and display results when ready.</td>
</tr>
<tr>
<td>&quot;MultiThreadWeb&quot;=&quot;0&quot;</td>
<td>EC: Web dashboards also uses multi-thread mechanism if set to 1. This can have unexpected consequences in IE and is by default turned off.</td>
</tr>
<tr>
<td>&quot;NasAddress&quot;=&quot;&quot;</td>
<td>EC/Manager: IT is the location from where nas retrieves alarms, if other than the default one following the login hub.</td>
</tr>
<tr>
<td>&quot;NasVersion&quot;=&quot;3.22, Nov 11 2008&quot;</td>
<td>EC/Manager: It is the version string set by system, in order to determine the new nas support.</td>
</tr>
<tr>
<td>&quot;QosAddress=&quot;/SDP/van01/van01/data_engine&quot;</td>
<td>EC/Manager: t is the Nimsoft address to the data_engine holding the NIS connection string to use.</td>
</tr>
<tr>
<td>&quot;QosDefaultTimeZone&quot;=&quot;1&quot;</td>
<td>EC: Use default time zone for dashboards as opposed to time zone adjusted for local time.</td>
</tr>
<tr>
<td>&quot;ReceiveDomainEvents&quot;=&quot;1&quot;</td>
<td>Manager: Subscription channel is established to all the hubs in the domain and the registry ensures full domain event update.</td>
</tr>
<tr>
<td>&quot;RefreshLogin&quot;=&quot;0&quot;</td>
<td>Manager: If set to one, a login is performed on on refresh event (using F5 key) in order to ensure the fullest possible update status.</td>
</tr>
<tr>
<td>&quot;RegExp=&quot;/</td>
<td>!&quot;</td>
</tr>
<tr>
<td>&quot;ReleaseQosConnection&quot;=&quot;0&quot;</td>
<td>EC: If the value of this registry is set to one, the shared NIS connection for an active dashboard is reset, in case one of the objects in a dashboard fails on a request. It is mandatory to use this setting with care since its behavior can affect the performance for dashboard with no apparent problems.</td>
</tr>
<tr>
<td>&quot;RequestTimeout&quot;=&quot;10&quot;</td>
<td>EC/Manager: Requests in the Nimsoft COM library will in general be set up with this timeout value. Be aware that the COM library for the time being does not seem to use this value correctly so that in effect the timeout for requests using the COM library is fixed ten seconds.</td>
</tr>
<tr>
<td>&quot;RequestTimeoutDashboard&quot;=&quot;30&quot;</td>
<td>EC: For dashboard request objects, this timeout value is used. However, the same limitation applies here regarding the COM library as for the &quot;RequestTimeout&quot; value described above.</td>
</tr>
<tr>
<td>Registry Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>&quot;SaveConfiguration&quot;=&quot;0&quot;</td>
<td>EC/Manager: If set to one, the changes to the current user profile are saved automatically on exit.</td>
</tr>
<tr>
<td>&quot;SF-AutoLogin&quot;=&quot;1&quot;</td>
<td>Manager: Attempts automatic login to SalesForce in order to connect to the Nimsoft archive.</td>
</tr>
<tr>
<td>&quot;SF-Passwd&quot;=&quot;&quot;</td>
<td>Manager: The encrypted password for connecting to SalesForce.</td>
</tr>
<tr>
<td>&quot;SF-User&quot;=&quot;&quot;</td>
<td>Manager: The user for connecting to SalesForce.</td>
</tr>
<tr>
<td>&quot;ShowConfigurationControls&quot;=&quot;0&quot;</td>
<td>EC: Show the advanced branch containing dashboard objects for Nimsoft probe configuration management in the EC Designer toolbox.</td>
</tr>
<tr>
<td>&quot;ShowGroupsNode&quot;=&quot;0&quot;</td>
<td>Manager: Show the manually managed group nodes for hubs, robots and probes in the Manager.</td>
</tr>
<tr>
<td>&quot;StartupMap&quot;=&quot;&quot;</td>
<td>EC: Specify a dashboard to automatically load EC with at startup. A path pointing at subpanels can be used e.g. Example/host.</td>
</tr>
<tr>
<td>&quot;StripHostDomain&quot;=&quot;&quot;</td>
<td>EC/Manager: Specify a string representing a domain that will be stripped off the host name in alarms.</td>
</tr>
<tr>
<td>&quot;StripHostDot&quot;=&quot;0&quot;</td>
<td>EC/Manager: Number of domain parts separated by dots that are cut off the end of the host name in alarms.</td>
</tr>
<tr>
<td>&quot;StripHostName&quot;=&quot;1&quot;</td>
<td>EC/Manager: Attempt to strip the host name in alarms based upon the above strip host settings.</td>
</tr>
<tr>
<td>&quot;SubscriptionCheckInterval&quot;=&quot;5&quot;</td>
<td>EC/Manager: It is the check interval in minutes, useful for checking a valid subscription channel to Nimsoft. A value of zero means no check.</td>
</tr>
<tr>
<td>&quot;SuppressInitialQuery&quot;=&quot;0&quot;</td>
<td>EC/Manager: Suppress initial query at application startup to obtain proper domain data used typically in list combo-boxes in dialogs like Options.</td>
</tr>
<tr>
<td>&quot;TraceDashboardObjects&quot;=&quot;0&quot;</td>
<td>EC: If set to one, then the trace messages appearing in the Message or Trace window appears for the dashboard objects.</td>
</tr>
<tr>
<td>&quot;TrendGraphPoints&quot;=&quot;1000&quot;</td>
<td>EC: Number of data point to store in Registry for trend probe request dashboard objects. This ensures some current history at full refresh.</td>
</tr>
<tr>
<td>&quot;TurnOffEvents&quot;=&quot;1&quot;</td>
<td>EC: Turn off incoming events when in Design mode. Dashboard objects are not real time updated, however this prevents abrupt behavior such as many incoming alarms during the design mode.</td>
</tr>
<tr>
<td>&quot;WebDashSrvAddress=&quot;/SDP/xpessu/xpdell/dashboard_server&quot;</td>
<td>EC: Web dashboards obtain the Dashboard Server address to use through this Registry key.</td>
</tr>
<tr>
<td>&quot;WebDistSrvAddress&quot;=&quot;&quot;</td>
<td>EC: Web dashboards obtain the Distribution Server address to use through this Registry key. If you do not specify anything, the address is derived from the login hub address.</td>
</tr>
<tr>
<td>&quot;WebNasAddress&quot;=&quot;&quot;</td>
<td>EC: Web dashboards obtain the Nas address to use through this Registry key if you do not specify anything, the address is derived from the login hub address.</td>
</tr>
</tbody>
</table>
Overview: Permissions and Ownership

Defining permissions for users

You have three different types of users in Nimsoft Infrastructure Manager:

- Nimsoft users
- LDAP users
- Account contacts

You can set permissions for these three user types based on the Access Control List (see Adding a new ACL), but the functionality and procedure is different for each type.

- For Nimsoft users, you create a user and assign an Access Control List which defines the permissions, see Creating a new user.

- For LDAP users, the users must first be included in a specific LDAP group which you define in your LDAP system. Then you can assign an ACL to the LDAP group, see Setting LDAP Group.

- For account contacts, you define permissions by assigning an ACL to each contact, see "Creating a Contact".

**NOTE:** Some of the permissions in an ACL will by default not be applicable for account contacts.

Defining ownerships/origins for users

The origin (data owner) that is assigned to a user, defines which alarm data and QoS data the user gets access to. Origins are set for accounts in the Ownership list, and all contacts under an account will therefore have the same ownerships. See "Creating an Account" for more information.

To set ownership for LDAP users and Nimsoft users, you need to create an account and define the applicable ownerships, and then link the account to an ACL. When Nimsoft users and LDAP users that are attached to the ACL, are logging on the Nimsoft Service Delivery Portal (SDP), they will be treated as contacts in the linked account and get access to the data from the origins set for the account. See Setting an Account link for more information.
The main tasks in user administration are:

- **Creating users**
  Users are created with a username and a password and attached to a profile and an ACL (see below).

- **Creating profiles**
  The profile controls the appearance of the application window, such as:
  - Which entries are accessible under the URL-, Group- and Application Nodes in the Navigation Pane.
  - The contents of the Dock Pane at application startup.
  - Defined actions, created in the right-click menu when robots are displayed in the Main Window Pane.

- **Creating Access Control Lists (ACLs).**
  Using ACLs, you can:
  - Define the permissions for users attached to the ACL.
  - Set filter options for users attached to the ACL.

These tasks can be executed, using the right-click menu in the User Administration dialog, opened by the Security > User Administration option in the Menu Bar.
Creating a new user

Use the menu choice Security > User Administration. The following dialog box appears.

**Note:** Avoid creating Nimsoft users and LDAP users with identical user names.
Select New User from the right-click menu, and the New User dialog box pops up.

[Image of the New User dialog box]

Fill in the username, the user’s full name and a short description. Select Access Control List and Default profile from the pull-down menus.

If you don’t find a suitable profile for the user, you can create a new profile; see the section Creating a new profile.

Click the Set password button to create a password for the user.

Enter the password, retype it and click the OK button.

Click OK to quit the New User dialog box, and the user is created.

Note that you can edit the user profile (change profile, user type and password) by selecting the user in the User Administration dialog and clicking the Edit User button.
Creating a new profile

Select Manage Profiles from the right-click menu in the User Administration dialog.

Use this dialog to create new profiles, delete old ones, or to set profile attributes.

Click the New button to add a new profile.

Click OK, and then click OK in the Manage Profiles dialog.

To attach a user to a profile: See the section Creating a new user.
Managing the Access Control List

Selecting Security > User Administration in the Menu Bar opens the User Administration dialog. Using the Manage Access Control List option in the right-click menu of the User Administration dialog, you can define new Access Control Lists (ACLs). Using ACLs, you can:

- Define the permissions for users attached to the ACL.
- Set filter options for users attached to the ACL.

Note the Extended Security option in the ACL List.

This option enables:

- When right-clicking a probe in the Infrastructure Manager, the Security entry in the right-click menu is enabled.

It is also required that the Basic Management option in the ACL is enabled.

The Security entry has the following two options:

- **Set Access**

  Opens the Set Probe Access dialog for the selected Probe, where you are allowed to set the IP access to the Probe.

  You are not allowed to modify the access properties for Probes where the access already is set, using the Probe Administration (Security > Probe Administration...)
■ **Validate**

Allows you to validate (manually start) the selected Probe if the Robot Controller is not able to start it.

In addition, the three following Security options in the Infrastructure Manager Menu bar are enabled:

■ Security > Set Login Expiration Time
■ Security > Set Signature
■ Security > Probe administration

For further information on ACL, see the section Adding a new ACL.

### Adding a new ACL

You can define different filters and permissions in an ACL in a way that restricts users attached to the ACL to see only parts of the infrastructure, alarms only from specific Hubs/Robots, etc.

Using the **Security > User Administration** option from the Menu Bar, you can attach a user to one of the ACLs. That means that you can create different ACLs with the permissions the different type of users need to do their work.

In this example, we make an ACL called *Intruder*:

■ Click the *New* button under the *Access Control List* field.
Give the new ACL a name. You can copy the permission and filter settings from another existing group by selecting from the combo box. Click the OK button. The ACL should now appear in the Access Control List field.

**Setting or modifying Permissions?**

You may want to change the permission settings, as you copied the settings from an existing ACL when you created this one.

Permissions are selected by checking / unchecking options in the right pane.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Enables a user to assign alarms to himself.</td>
</tr>
<tr>
<td>Unassign</td>
<td>Enables the user to unassign alarms that are previously assigned to a user.</td>
</tr>
<tr>
<td>Dynamic Views States</td>
<td>This option gives the user general access to Dynamics Views alarm state information</td>
</tr>
<tr>
<td>Invisible Alarms</td>
<td>The administrator can, using the nas GUI, set an alarm invisible. The Invisible Alarms ACL setting gives the user the possibility to see &quot;invisible alarms&quot; (alarms that are set invisible by the nas administrator) in the alarm list.</td>
</tr>
<tr>
<td>Reassign</td>
<td>This option overrides any assignment at Assign/Acknowledge</td>
</tr>
</tbody>
</table>
### Alarm History
This option activates the History node in Enterprise Console. The History node reveals the Query node and a user-defined collection of saved queries. The Query functionality enables you to inspect acknowledged alarms more closely. Queries performed may be saved, and will show up as independent nodes in the Navigation tree.

### Acknowledge
Enables the user to close alarms.

### Alarm Management
Enables the user to manage notes (add a note to an alarm) and configure Actions when right-clicking an alarm in the sub-console.

### Assign
Enables the user to assign alarms to another user.

### Alarm Details
This option gives the user general access to alarm lists and alarm details.

### Discovery
Enables the Discovery functionality in the Enterprise Console, used to discover and create template panels.

### Dashboard Design
Enables the user to create, modify and delete dashboards in the Enterprise Console.

### Dynamic Views
Makes the Dynamic Views node appear in the Navigation Panes of the Infrastructure Manager and the Enterprise Console. If not selected, this node is hidden.

### Web Publish
The Web Publish Applications made available and can be launched from the Applications node in the Navigation Pane of the Infrastructure Manager. This enables the user to make the following dashboards, consoles and reports available on your web server:
- Enterprise Console created Dashboards
- Infrastructure Manager
- Enterprise Console
- Alarm SubConsole
- SLA reports
- QoS reports
- Grouped SLAs
- HTML management.

### Dashboard Upload
Enables the user to upload dashboards to archive. This is done in Enterprise Console by right-clicking a dashboard and selecting Upload Dashboard. Otherwise this option is greyed out.

### Dashboard Download
Enables the user to download dashboards from archive. This is done in Enterprise Console by right-clicking a dashboard and selecting Download Dashboard. A small window listing all dashboards in the archive is opened, letting you select the one(s) to download. Otherwise this option is greyed out.
| Extended security | Enables for various security maintenance features. The following options under the Security menu option in Infrastructure Manager is made available:  
- Set Login Expiration Time...  
- Set Signature...  
- Probe Administration... |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>License Management</td>
<td>Enables the user to add and delete licenses.</td>
</tr>
<tr>
<td>Manage ACL</td>
<td>Enables the Security &gt; Manage Access Control List option in the Infrastructure Manager menu bar. This enables the user to create, modify and delete Access Control Lists.</td>
</tr>
<tr>
<td>User Administration</td>
<td>Enables the user to create, modify and delete users. Enables the User Administration and Account Administration options under the Security menu option in Infrastructure Manager.</td>
</tr>
<tr>
<td>Modify Profiles</td>
<td>Enables the View &gt; Save Profile and View &gt; Save Profile as options in the Infrastructure Manager menu bar. This enables the user to modify and save user profiles.</td>
</tr>
<tr>
<td>Distribution</td>
<td>Enables the user to distribute packages from the local archive to hubs/robots. If not enabled, the following error message will be displayed when attempting to distribute a package.</td>
</tr>
<tr>
<td>Program options</td>
<td>Enables the Tools &gt; Options menu option in the Infrastructure Manager. This option lets the user change various program attributes.</td>
</tr>
<tr>
<td>Basic Management</td>
<td>Enables the user to configure, restart, and move probes in the Infrastructure Manager. These options are made available by right-clicking a probe.</td>
</tr>
<tr>
<td>Manage Profiles</td>
<td>Enables the user to create, rename and delete profiles, using the View &gt; Manage Profiles menu option in the Infrastructure Manager. Otherwise this option is greyed out.</td>
</tr>
</tbody>
</table>
Management Tools | Enables for various management tools available under the Tools menu option in Infrastructure Manager (these options are greyed out):
---|---
Find | Opens the *Find* dialog, where you can search for other Nimsoft components (Hubs, Robots or Probes).
Connect Robot | This option opens the Connect Robot dialog, which can be used to restart a Robot or connect a Robot to another Hub.
Service Controller | A utility for starting or stopping the Service Controller (the process controller.exe) on the computer you are working on. When stopped, the computer will not be available on the NimBUS (the icon in the Navigation pane will turn into red).
Alarm Notifier | Starts the Alarm Notifier. This is a small program that shows the highest severity level of current alarms, and notifies you either visually or with a user-defined sound whenever the severity level defined in the Alarm Notifier setup is reached.

Archive Management | Create and modify packages.
---|---
Opening your local package archive in Infrastructure Manager, right-clicking in the list, you can select:
Edit | to launch the packageEditor for the selected package.
New | to create a new package.
Delete | to remove the package from the local archive.

Execution Level 1–3 | Generic ACL permissions that can be used by certain probes to differentiate between accesses to various operations.
---|---
If e.g. a user associated with *Execution Level 1* runs the probe, other operations and commands will be executed than if a user associated with *Execution Level 3* runs the probe.
Execution Level 3 is the highest level.

Alarm Summary | Displays alarm summary information
Custom Reports | Displays custom reports
Dashboard Publish | Makes published dashboards generally available
Dynamic Views Dashboards | Displays Dynamic Views Dashboards
Unified Reports | Gives the user access to unified reports
Discovery Pie | Displays discovery information
Custom Dashboards | Displays custom dashboards
Discovery Management | Enables the user to set computer system properties
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Administration</td>
<td>Enables the user to manage Account contacts and customize their SDP portal content</td>
</tr>
<tr>
<td>User Monitoring</td>
<td>Displays and disconnects user sessions</td>
</tr>
<tr>
<td>Topology Maps</td>
<td>Displays topology maps</td>
</tr>
<tr>
<td>Report Designer</td>
<td>Enables the user to create, modify and delete reports</td>
</tr>
<tr>
<td>Dynamic Views Reports</td>
<td>Displays Dynamic Views reports</td>
</tr>
<tr>
<td>Default Customization</td>
<td>Enables NimBUS users to customize their default SDP portal content</td>
</tr>
<tr>
<td>Dashboard Designer</td>
<td>Enables the user to create, modify and delete private dashboards</td>
</tr>
<tr>
<td>User Customization</td>
<td>Enables the users to customize their own portal content</td>
</tr>
<tr>
<td>Change Password</td>
<td>Enables the contacts to change their own password</td>
</tr>
<tr>
<td>SLM Admin</td>
<td>Run Service Level Manager with full access.</td>
</tr>
<tr>
<td></td>
<td>That means you are allowed to create SLAs and open existing SLAs and their underlying elements (SLOs, QoS’s etc.) and make any changes you want.</td>
</tr>
<tr>
<td>SLM View</td>
<td>Run Service Level Manager in read-only mode.</td>
</tr>
<tr>
<td></td>
<td>That means you are allowed to open SLAs and the underlying elements (SLOs, QoS’s etc.), but all fields are greyed out, so you are not allowed to make any changes.</td>
</tr>
<tr>
<td>Web Service</td>
<td>Enables the user to access to Web Service API.</td>
</tr>
</tbody>
</table>

**Setting Filters?**

You can set filters to limit the ACLs’ access to specific parts of the infrastructure:
- Click the *Set Infrastructure Filter...* button.
The *Filter* dialog appears. Click the *New* button, and the New filter dialog pops up:

![New Filter Dialog](image)

In the example on the figure above, we limit the ACLs’ access to see only the Domain *Development* and only Robots and Probes controlled by the Hub *wsrune* (note that you may also use the Robot and Probe fields to limit the access to specific Robots or Probes).

Click the *OK* button.

- The defined filter appears in the Filter window.

![Probe Filter Window](image)

Click the *OK* button to finish.
Setting Alarm Filters?

You may also set alarm filters, allowing the ACL to "see" only specific alarms in the Alarm Window.

(Note that the Alarm Indicator in the Status Bar, if displayed, counts all alarms, independent of this filtering).

Click the Set Alarm Filter... button, and the following dialog appears:

![Alarm Filter Dialog]

You can use one or more of the filtering parameters in the dialog. Using the example on the figure above, only alarms received from the host xpruha will be displayed in the Alarm Window for users attached to the ACL.

The following filtering fields are available:

**Note:** Regular expression may be used in the definitions described below.

- **Alarm Source**
  - **Host name**
    
    Here you specify one or more computers that you want your alarms filtered on.

  - **Source**
    
    Here you specify one or more IP addresses for the computers that you want your alarms filtered on.
- **Nas**
  Here you specify one or more Alarm Servers (nas) that you want your alarms filtered on.

- **Origin**
  QoS data from probes are tagged with a name to identify the origin of the data. The origin name is normally set in the controller probe GUI. If not, the Hub name will be used.

  Note however, that the Origin field under *Advanced Settings* in the Hub GUI lets you specify an origin name of your own choice to be used, rather than the Hub name.

- **Subsystem**
  Here you specify one or more subsystems that you want your alarms filtered on. A subsystem is a part of the monitored computer (CPU, disk network etc.)

- **Subsystem ID**
  Here you specify one or more subsystem IDs that you want your alarms filtered on. The subsystem ID is a field, containing one or more numbers separated by dots, identifying the subsystem.

- **Domain**
  Here you specify one or more Domains that you want your alarms filtered on.

- **Hub**
  Here you specify one or more Hubs that you want your alarms filtered on.

- **Robot**
  Here you specify one or more Robots that you want your alarms filtered on.

- **Probe**
  Here you specify one or more probes that you want your alarms filtered on.

- **Assignment**
  In this field you can filter on:
  - The alarms assigned to specific users.
  - The alarms assigned by specific users.

- **Tags**
  This field lets you filter on User Tags.

  User Tag 1 and User Tag 2 are user-defined tags to be used as a grouping / locating mechanism. The tags are set in the controller probe GUI.
User Administration

- **Message**
  This field lets you filter on text in the message field of the alarm message. Typing e.g. *URL*, the users associated with the ACL will only see alarms where URL is a part of the alarm message text.

- **Severity Level**
  This field lets you filter alarm messages Severity level.
  
  Selecting e.g. >= Minor, the users associated with the ACL will only see alarms with severity level Minor or higher.

  Click the OK button to activate the filter and finish.

**Setting Dashboard Web access restrictions?**

Using the Web Publish application, Dashboards can be made available and accessed via a Web browser.
You may set filters to restrict the ACL access to these Dashboards, using the *Set Dashboard Web access* option. Click the *Set Dashboard Web Access...* button, and the following dialog appears.

![Dashboard Access Dialog](image)

The Dashboards available in the archive are listed in the left pane.

If the right pane is empty, users attached to the ACL can access all of the dashboards.

If you want to filter the ACL access to some of these Dashboards, you do so by copying (select the Dashboards you want to make accessible for the ACL and click the *Add* button) the ones you want to be accessible over to the right pane.

Note that users attached to the ACL will now be able to access the Dashboards copied to the right pane only.
**Note** the *Set/Unset Restricted Access* button. When selecting a Dashboard made accessible (in the right pane) and clicking this button, the access to the selected Dashboard will be restricted. That means that users attached to the ACL will not be able to move upwards in the Dashboard hierarchy when accessing Panels. The button has toggle functionality; clicking the button once more for the selected Dashboard, removes the restriction.

Click the OK button to finish.

**Setting Dynamic Views access restrictions?**

The *Group Server probe* collects and organizes QoS data into database tables. The Enterprise Console and the Infrastructure Manager will, based upon these data, create a new top level branch called Dynamic Views in its navigation tree, exposing the data in a tree structure.

The Enterprise Console contains a set of preconfigured dashboard templates that are the basis for the Dynamic Views dashboard being launched and automatically populated with context related data when at the end node of a branch.

The Dynamic Views node in the Infrastructure Manager reflects the Infrastructure by reading tables in the database.

Using the *Dynamic Views Origin Ownership* option, you may restrict the part of the Infrastructure users associated with this ACL is allowed to see in the Dynamic Views Nodes of the Enterprise Console and the Infrastructure Manager.

In the *Dynamic Views Origin Ownership* list at the bottom of the dialog, you will find the Origin options available. By default these are NOT selected.
The Origin will normally be one of the following:

- The Hub.
- Any other Hubs, attached to the Hub via a queue.
- Robots controlled by the Hub, provided that the Robots are configured to override the data origin set by the Hub in the controller GUI (Setup > Advanced).

With none of the origins in the list selected, users attached to the ACL will see the complete Infrastructure in the Dynamic Views Node.
Selecting one or more of the origins in the list, users attached to the ACL will only see the part of the Infrastructure represented by the origins selected (e.g. a Hub).

Make your selection and click the OK button to finish.

**Setting LDAP Group**

ACL Management, accessible from the menu bar in Infrastructure Manager, lets you create Access Control Lists (ACLs) with belonging privileges. These ACLs can be associated with a specific LDAP groups. The HUB (version 4.70 or newer) can be configured to supply a list of groups found in the container specified in the HUB when attaching the ACL to a LDAP group). The users in the LDAP group will then be assigned the privileges for the ACL the group that is associated with.

When a LDAP user logs on a console (for example Infrastructure Manager), the request will be directed to the LDAP server for authentication. The user can be member of one or more LDAP groups. If the user name is found in one or more groups attached to an ACL, the user will be assigned privileges in Nimsoft as defined in the ACL.
If the user belongs to multiple groups connected to ACLs, the user will be assigned the privileges from the ACL with the most extended privileges.

The **Set LDAP Group** button is unavailable until LDAP integration has been configured and enabled in the HUB. Please refer the **LDAP Configuration** chapter in this document for further details.

In this example we will assign the ACL **Operator** to the users in a LDAP group called **QA**.

1. Select the ACL Operator and click the **Set LDAP Group** button.

2. The **Set LDAP Group** dialog appears. Scroll to find and select the **QA** entry in the list. Click the **OK** button.
3. Click the **OK** button in the *Manage Access Control List* dialog to exit and activate the new setting.

4. Test that the LDAP user login works by logging on Infrastructure Manager with a user in the LDAP group selected in step 2.

![Login dialog]

**LDAP Configuration**

Nimsoft Server has the Nimsoft LDAP solution, making it possible to log on the Nimsoft consoles as a LDAP user. This means that it is no longer necessary to be defined as a Nimsoft user to log on and use these consoles.

**Supported platforms:**
- Windows
- Linux

The Nimsoft LDAP solution requires certain configuration tasks on the Hub and the Infrastructure Manager as described in the next sections.

**Configuring your login Hub**

The HUB must be configured to forward login requests to a LDAP server and to access the container with the user groups in LDAP.
Launch the Hub in *Infrastructure Manager* and click the *Settings* button on the *General* tab of the HUB GUI. A dialog lets you define the LDAP authentication settings.

1. Select the LDAP Authentication option to activate the LDAP authentication feature. You can use this checkbox to activate/deactivate the LDAP authentication feature.

2. In the field Server Name, write the IP address or the host name for the LDAP server which the Hub should point to. You can use the Lookup button to test the communication.

3. Select the LDAP server type from the Server Type pulldown menu. Currently two server types are supported; Active Directory and eDirectory.

4. Select the Use SSL option if you want to use SSL during LDAP communication. Most LDAP servers are configured to use SSL.

5. In the fields User and Password, specify a user name and a password to be used by the HUB when accessing the LDAP server to retrieve information. In Active Directory, the user can be specified as an ordinary user name (as shown on the illustration above).

   In eDirectory, the user must be specified as a path to the user in LDAP on the format `CN=yyy,O=xxx`, where CN is the user name and O is the organization.

6. In the field Group Container (DN), specify a group container in LDAP to define where in the LDAP structure you want to search for users. You can click the Test button to check if the container is valid.

7. In the field User Container (DN), specify a user container in LDAP to define more specifically where in the LDAP structure you want to search for users.

See also the section Advanced LDAP Configuration for further Hub configuration information.
Connecting Access Control Lists to LDAP users

ACL Management, accessible from the menu bar in Infrastructure Manager, lets you create Access Control Lists (ACLs) with belonging privileges. These ACLs can be associated with a specific LDAP groups (the HUB will supply a list of groups found in the container specified in the HUB when attaching the ACL to a LDAP group). The users in the LDAP group will then be assigned the privileges for the ACL the group is associated with.

When a LDAP users logs on a console (for example Infrastructure Manager), the request will be directed to the LDAP server for authentication. The user can be found in one or more LDAP groups. If the name is found in one or more groups attached to an ACL, the user will be assigned privileges in Nimsoft as defined in the ACL.

If the user belongs to multiple groups connected to ACLs, the user will be assigned the privileges from the ACL with the most extended privileges.

Enter ACL management from the Infrastructure Manager by selecting Security > Manage Access Control List from the menu bar.
In this example we will assign the users in a LDAP group called QA the ACL Operator.

1. Select the ACL Operator and click the Set LDAP Group button.

2. The Set LDAP Group dialog appears, Scroll to find and select the QA entry in the list. Click the OK button.

3. Click the OK button in the Manage Access Control List dialog to exit and activate the new setting.
4. Test that the LDAP user login works by logging on Infrastructure Manager with a user in the LDAP group selected in step 2.

Verification

Launch the Infrastructure Manager and log in as a LDAP that does not exists as a Nimsoft user.

Verify that you can access the expected contents and have the privileges as described by the ACL the LDAP user is associated with (see the Connecting Access Control Lists to LDAP users).

Advanced LDAP Configuration

Keys in the /LDAP/server section

Below you will find tree keys that may be added to the HUB configuration file if you do not want to use the default parameters. These keys will be read by the Hub LDAP engine, and will have an impact on how the Hub communicates with the LDAP protocol.
use_ssl

If you want to use SSL, you don’t need to add this key. This key accepts the two strings: yes or no. Default is yes if the key is not supplied. This instructs the Hub LDAP library to turn on / off SSL during LDAP communication. A valid SSL certificate must be installed on your LDAP server.

Ports that will be used are 389 for normal LDAP connection, 636 for SSL connections.

Currently, these cannot be changed.

Timeout

This key accepts a numerical value indicating the number of seconds to spend on each LDAP operation, whether it be searching or binding (authentication) operations. The default value is 10 seconds if the key is not provided.

codepage

This key will allow the user to change which codepage to use when translating characters from UTF-8 encoding to ANSI, which is what the Hub and all other Nimsoft parts use internally. Text is coming from the LDAP library as UTF-8 encoded characters. Since Nimsoft products do not have true Unicode support, all characters will be attempted translated into ANSI using this codepage.

If you don’t not want to use the default codepages (see below), you must add this key.

On Windows platforms, the codepage must be a number representing the codepage you wish to use. See this page for a list of codepages:


On Windows, the Hub LDAP library will use MultibyteToWideChar and WideCharToMultiByte functions to translate to and from ANSI/UTF-8. These functions takes a codepage as a parameter.

On all other platforms, the Hub LDAP library will use iconv functions. Ref:
The codepage key is not shipped with the Hub configuration file.

The **default value if none is specified is:**

<table>
<thead>
<tr>
<th>Codepage Value</th>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28591</td>
<td>WINDOWS</td>
<td>ISO 8859-1 Latin 1; Western European (ISO)</td>
</tr>
<tr>
<td>ISO-8859-1</td>
<td>UNIX</td>
<td>ISO 8859-1 Latin 1; Western European (ISO)</td>
</tr>
</tbody>
</table>

On windows platforms, it’s a numerical value, on linux, it’s a text string which can be passed into `iconv_open` function.
Setting an Account link

This option lets you link an ACL to an account. By using this option, Nimsoft users and LDAP users attached to the ACL will, when logging on the Nimsoft Service Delivery Portal (SDP), be treated as contacts in the linked account.
Clicking the *Set Account Link* button, a dialog appears, listing the accounts available. You may select one of the accounts in the list, or you may create new accounts by clicking the *New Account* button.
Making ACL permissions available for Accounts/Contacts

Selecting the option *Make ACL permissions available for Account/Contacts* for an ACL, this ACL will be available and can be attached to contacts. Accounts and contacts can be created by selecting *Security > Account Administration* in the Infrastructure Manager Menu bar.

See the section Creating a Contact or details.
Working with Alarms

Once an alarm is generated, the Enterprise Console provides a powerful area where operators can view and manage the alarms. The basic alarm management architecture within Nimsoft ensures that alarms are positively assigned and acknowledged (closed) before they disappear from the screen. Obviously some alarms can be set to timeout after a certain period and other alarms can be automatically closed based on the receipt of a clearing event.

The basic flow of alarm management is:

- Alarm generated by the probe.
- Alarm appears on the Enterprise Console.
- An operator takes ownership of the alarm.
- The operator gets more detail about the problem and fixes it.
- The operator closes the alarm, and the alarm is therefore removed from the console.

The basic alarm window allows the operator to decide which columns to display (see the section Working with views in lists), in which order to display them and how to sort the display. The operator can save preferred methods of viewing the alarms for future use.

Selecting any one of the icons at the top of the screen will filter the display to show only alarms associated with that source, or multiple servers can be grouped together to create a technology or business view – e.g. see all alarms from File Servers.

Each alarm offers a menu of actions by right clicking on the alarm.

From this menu, the operator can assign the alarm, close the alarm or look at the history of an alarm (i.e. look at all previous occurrences and what state changes have occurred). Numerous other options are available to improve the operator’s efficiency.

The Alarm Window

When View > Alarm Window is selected from the Menu bar, the Alarm window displays alarms received by the nas belonging to the Hub you are currently logged on to.

If no alarm filters are active, the window will display all alarms received.

Note that if you click an alarm object in a Dashboard, you implicitly set a filter. Click on an empty part of the Dashboard to clear the filter, or go through the Set Filter dialog to clear it manually.
Handling Alarms

Alarm details

Double-clicking an alarm in the Alarm Window opens the alarm and displays it in a separate window called Alarm Details.

The window provides detailed alarm information (see figure below).

![Alarm Details window]

In addition the window contains some function buttons:

- **Accept**
  The user assigns selected alarms to himself.

- **Assign**
  The Assign function found in the alarm windows’ toolbar could be used when assigning an alarm to a specific user. You can also assign an alarm by right-clicking it and select Assign.

A white dot will appear in the lower right part of the colored alarm symbol when the alarm is assigned.

Assigned alarms can be unassigned again (see below).
- **Unassign**
  The *Unassign* function found in the alarm windows’ toolbar could be used when unassigning an alarm that has been assigned.

  You can also unassign an alarm by right-clicking it and select *Unassign*.

- **Acknowledge**
  Acknowledges an alarm. The alarm gets closed and disappears from the alarm window.

- **History**
  Opens the *Alarm History* window, showing the transaction log for the selected alarm.

- **Notes**
  Lets you read notes attached to the alarm. These notes can be added in the NAS GUI or by right-clicking an alarm in the alarm list, selecting *Note > Attach*.

![Notes](image)

Clicking the Comment button lets you add a comment to the note.
Account Administration

An account typically defines a customer/company. You may also define contacts (‘users’) for each account.

Open the Account Administration tool by selecting Security > Account Administration from the menu in the Infrastructure Manager.

This tool enables you to add, edit or delete Accounts.

Contacts

For each of the Accounts, you may define a number of Contacts, or ‘users’. 
Creating an Account

The Account Administration window lists all Accounts defined. In addition, the upper part of the window contains a row of tool-buttons, making it easier to manage the list:

- Select
- Filter
- Find
- Find next
- Find Previous
- Sort
- Columns
- Print
- Save views
- Manage views

See the section *Working with views in lists* for more information.

Right-clicking in the list gives you the possibility to:

- Add a new Account.
- Edit an Account.
- Delete an Account.
In addition, the two menu options View and Edit offers a set of options to manage the list, see the section Working with views in lists for more information.

Select New Account to bring up the New Account dialog.
The dialog contains three main parts:

- **General**

  This part describes the general Account information, such as *Account name* (e.g. the company name), a short description, the address and the phone/fax numbers.

  The Account name is mandatory and must be a unique name. If trying to specify a name that already exists, the field will be disabled (greyed out). The other fields in the general part are optional and of informational character.

- **Ownership**

  This field lists the different parts of the Infrastructure (hubs and robots) being the owner/origin of data collected by probes. Select the one(s) you want to be accessible for the account.

- **Contacts**

  This window lists all *Contacts* defined.

  For each of the Accounts, you may define a number of Contacts, or ‘users’.

  Right-clicking in the Contacts list opens a small menu enabling you to *add, edit or delete* Contacts. In addition, the *View* options give you the possibility to modify the layout of the list. The *Edit* options offers some *find, filtering and search* possibilities that are common for most lists in Nimsoft applications. In addition, the two menu options *View* and *Edit* offers a set of options to manage the list, see the section *Working with views in lists* for more information.

  See also the section Creating a Contact for more information about Contacts.

**Creating a Contact**

For each of the Accounts, you may define a number of Contacts, or ‘users’.
Open the Contact dialog by right-clicking in the Contacts list of the Account dialog, selecting *New Contact*.

![New Contact dialog](image)

To create a new Contact, the following fields in the dialog are mandatory:

- **Login ID**

  Specify a unique ID (name) of the Contact. Note that this name must be unique across all accounts. If trying to specify a Contact name that already exists (in this or another Account), the field will be disabled (greyed out). This is the ID the Contact uses when logging on the Nimsoft Service Delivery Portal (SDP).
■ **Set Password**

Optionally click the *Set Password* button to create a password for the Contact. This is the password the Contact uses when logging on applications or Web Portals that allows contacts to log in.

**Note:** If you choose not to set a password for the Contact here, the Contact will be asked to set a password the first time he/she logs on applications or Web Portals that allows contacts to log in.

A password must contain at least 6 characters. The password must be entered in both fields.

Click the *OK* button to continue.

■ **Access Control List**

Here you can attach an Access Control Lists (ACL) to the contact.

Access Control Lists consists of a set of access properties and permissions. Contacts attached to an ACL will have the properties and permissions defined for that ACL.

The ACLs can be created and modified by clicking the *Manage ACL* button (see below). Note that only ACLs with the option "Make ACL permissions available for Accounts/Contacts" selected will be available. See Adding a new ACL for more details.

■ **Manage ACL**

Clicking this button opens the *Manage Access Control List* dialog, where you can edit the properties for an ACL and even create new ones. See Adding a new ACL for more details.

All other fields in the dialog are optional and of an informational type:

■ A short description of the Contact.

■ First and last name of the Contact.

■ The Contact’s title.
The department the Contact belongs to.

The Contact’s phone and mobile phone numbers and his e-mail address.

When finished, click the OK button to store the Contact.

**Working with Views in Lists**

If you want to modify the layout of a list in a window (e.g. the alarm list in the Alarm SubConsole), you have a set of options available:

- Left-clicking the column border, dragging to the preferred width and releasing the mouse button can also modify the width of columns.

- If you want to have the columns placed in another order, the columns can be moved, using drag and drop. You left-click the column you want to move, drags it to the preferred position and drop it by releasing the mouse-button.

- Left-clicking the column border, dragging to the preferred width and releasing the mouse button can also modify the width of columns.

- Right-clicking a column header also gives many options.
See the section Right-clicking a column header.

- Right-clicking inside the list also gives many options. Some of the options are special for the different lists, and will be described in the sections describing the different lists.

  The other options, which are common for all lists are described in the section Right-clicking in a list.

- Further, the Toolbar in the upper part of the lists contains a set of functional buttons, see the section The Toolbar in the list.

### The Toolbar in the list

The Toolbar integrated in the upper part of the list includes a set of functional tool buttons making it easier to navigate in the pane. Note that this toolbar can be selected / deselected by right-clicking in the list and selecting View > Toolbar.

The options in the toolbar are also available when either right-clicking in the list or when right-clicking a column-header.

See the section *Right-clicking in a list* for an explanation of the following options in the Toolbar:

- Sort
- Columns
- Print
- Save view
- Manage views

See the section *Right-clicking a Column header* for an explanation of the following options in the Toolbar:

- Select
- Filter
- Find
- Find next
- Find previous
Right-clicking a column header

Right-clicking a column header gives many options.

Sort Ascending / Descending

The entries in the list can be sorted, ascending or descending, based on the entries in the column under the header you right-click.

Select

This option can be used to select specific rows in the list. Specify a select pattern in the Select what field and click the OK button. All rows matching the specified pattern will be selected.

Clicking the Match whole column value option, only rows containing exactly the pattern entered will be selected.

There is also an option for case sensitive selection. In this example, all list entries containing the word warning will be highlighted.

Note that you can select all rows by left-clicking in the list and clicking <ctrl> + a>.
To reset to normal view, with none of the rows selected, simply left-click in the list.

**Filter**

Entries in the list can be filtered by defining a select pattern (i.e. text). Only entries in the list containing this pattern will be displayed in the list, others will be hidden.

In this example, only alarms containing the word *wsrcue* will be displayed.

Using the option *Dynamic filtering*, the filtering starts immediately (while you are writing the select pattern).

To reset to normal view, with all list entries displayed, open the filter dialog again and click the *Reset* button.

**Find**

You can search for specific list entries by defining a select pattern (i.e. text), and the first list entry containing this pattern will be highlighted.

Clicking the *Match whole column value* option, the find function searches for a column with exactly the contents entered in the *Find what* field.

You may also select the find function to be case sensitive.

Clicking the *Find Next* button highlights the next entry containing the select pattern, while clicking the *Find Previous* button will find the previous entry containing the select pattern.
Columns

Columns can be removed from the list. You select the column you want to remove and click the <<Remove button. If you later want the removed columns back again, you simply select them and click the add>> button, or you click the Reset button.

You may also change the order of the columns. Selecting a column in the list and clicking the Move Up button, moves the column one step up, which means that the column will be moved one position leftwards in the list.

Properties

In the Properties dialog, you can modify the selected column's title. Note that for the Assign Time column, you may also specify the time format. You may also select between Fixed column width and Automatic Adjustment (the width is automatically adjusted to fit the length of the longest text string in the column.)
Right-clicking in a list

Right-clicking inside the list offers a lot options. Some of the options are special for the different lists, and will be described in the sections describing the different lists.

<table>
<thead>
<tr>
<th>View</th>
<th>Views</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Sort by</td>
<td>Assigned</td>
</tr>
<tr>
<td>Assign</td>
<td>Row Details</td>
<td>Message</td>
</tr>
<tr>
<td>Unassign</td>
<td>Sort…</td>
<td>Time</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>Columns…</td>
<td>✓ Persistent View</td>
</tr>
<tr>
<td>[Del]</td>
<td>Toolbar</td>
<td>Save View…</td>
</tr>
<tr>
<td></td>
<td>Status Bar</td>
<td>Manage Views…</td>
</tr>
<tr>
<td></td>
<td>Properties</td>
<td>Reset View</td>
</tr>
<tr>
<td>Hold Alarms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Show Invisible Alarms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set Visibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ctrl+U</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm Filter…</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set Alarm Filter Based on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear Alarm Filter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction History</td>
<td></td>
<td></td>
</tr>
<tr>
<td>History</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The other options, which are common for all lists are described in this section.

Right-clicking in a list in a window (e.g. the alarm list in the Alarm SubConsole) gives you the possibility to modify the appearance of the list.

Views

The View function can be used to manipulate the view (the appearance of the list in the window). You may create your own views or make modifications of the layout of a list and save the views, giving them descriptive names (see Save View).

You can then toggle between different defined views.
Persistent view

If you have no default view specified, you can turn on or off a switch telling the system whether you want to save the changes you have made to a list during an ongoing session or not. If the switch 'Persistent View' is set, the sort levels and column ordering will appear in the same manner at start-up as when you exited the application.

Save View

This option can be used if you want to define specific views. If you change the layout of the list to match your specific needs, you can save the view and give it a specific name.

Manage views

The View function can be used to manipulate the view (the appearance of the list in the window) and to create your own views.

The Manage View function can be used to manipulate these defined views.

You can:
■ Activate a view
■ Delete views that are no longer required
■ Specify which view should be set initially when the application is started. A blue arrow will indicate this selection in the list containing your defined views.
If you have no default view specified, you can turn on or off a switch telling the system whether you want to persistently save the changes you have made to a list during an ongoing session or not. If the switch Persistent view is set, the sort levels and column ordering will appear in the same manner at start-up as when you exited the application.

**Manage Views**

- **View**
  - History - Main
  - History - Transaction
  - History - Repeating

**Reset view**

Resets to a basic view, with application default values.

**Sort By**

This function can be used to sort the list based on the different columns in the view.

**Row Details**

Marking an entry in the list and selecting *Row Details* opens a separate window containing detailed information about the selected list entry.
Sort

A more sophisticated sorting function, where you can specify multiple sorting keys. You may sort by a first column, then by a second and finally by a third column. You may select to sort in ascending or descending order and also choose case sensitive sorting.

Columns

This function allows you to add or remove columns from the view.

Columns can be added by marking the column you want to add in the Available Columns field of the dialog and clicking the Add>> button. The column will move to the Displayed Columns field (note the Add All button, which moves all columns).

Columns can also be removed by marking the column you want to remove in the Displayed Columns field of the dialog and clicking the <<Remove button. The column will move to the Available Columns field (note the Remove All button, which removes all columns).
Further you may change the order of the columns by using the Move Up / Move Down button.

![Columns dialog box](image)

**Toolbar**

Lets you include or remove the Toolbar (see the section The Toolbar in the list) from the top of the list.

**Status Bar**

Lets you include or remove the Status Bar from the bottom of the list.

**Properties**

Opens the properties box for the list.

There is a General tab for selecting background color, text color and font etc. for the list.

Further you may select:

- The *Grid Lines* option, which will make the list appear with grid lines (as a table).
- The *Full Row* select, which makes it possible to select the full row in the list by left-clicking it.
In addition, there is a tab for each column, where you can modify the column title and column width.

![Properties dialog box](image)

**Print**

Prints the contents of the window. The printer dialog appears, allowing you to select a printer and to modify the printer properties, such as page orientation, number of copies etc.

![Skriv ut dialog box](image)
Print Preview

Displays a preview of the contents of the list, as it will appear on a printout.

Edit

This option enables you to select, filter and find alarms in the list. These functions are also available in the Toolbar, and more information about these functions can be found in the section The Toolbar in the list.

You may also copy selected alarms to the clipboard.
Appendix B: Glossary of Terms

Nimsoft Infrastructure

Domain

A Domain is by dictionary definition the set on which a function is defined.

The Domain is the top-level node in the Nimsoft hierarchy. It is used to group multiple Hubs in a logical set such as a company or enterprise. Various security aspects in the Nimsoft such as e.g. user-profiles, user-permissions and access-rights are distributed within the Domain.

Hub

A Hub is by dictionary definition a center of activity, a focal point.

The Hub is a service in the Nimsoft Infrastructure that:

- manages a group of Robots.
- collects and redistributes messages published by the robots.
- maintains several central services such as security issues, naming services etc.
- manages message subscribers such as Gateway services, applications and servers.

The Hub is operated and managed by a Robot (like any other service/probe), so it is correct to imply that a Hub is a Robot with Hub capabilities.

Infrastructure Manager

The Infrastructure Manager is dedicated to handle management operations within the Nimsoft environment. You may navigate in the Nimsoft structure by exploding elements in the tree-control, and configure the various components by double-clicking the components in the right-hand list control.
Nimsoft Address

A Nimsoft address consists of four basic elements, the Domain, Hub, Robot and probe. For example, the address /Nimsoft/oslo/wscase/nas resolves to the following information:

- Nimsoft is the Domain-name
- oslo is the Hub-name
- wscase is the Robot-name
- nas is the probe-name (in this case it is the Alarm Server)

The Nimsoft API has functions that resolve a Nimsoft address to an IP-address and a port.

Probe

A Probe is by dictionary definition a usually small object that is inserted into something so as to test conditions at a given point.

A probe is a program (usually quite small) developed using the Nimsoft API from any of the supported languages such as C/C++, VB, Perl, Java and COM. Thereby, it can be connected to the Nimsoft Infrastructure for sending and receiving messages, and be accessed from Infrastructure Manager for administration purposes. The functionality in any Nimsoft solution is typically located in a number of probes, each dedicated to one or a few tasks.

Timed probes vs. daemon probes

A timed probe runs once and then terminates, awaiting the next point in time when it is configured to start. A daemon probe is always active if activated by the operator. If it stops, it is immediately restarted by the Robot.

Publishing messages

A message is published on the Nimsoft when it is simply sent to the nearest Hub without being destined for any particular receiver. The Nimsoft Infrastructure automatically ensures that the message is delivered to all probes subscribing to the Subject ID found in the message.
Quality of Service (QoS)

Many probes are capable of sending trending data periodically. These messages are formatted and known as Quality of Service messages. They normally contain data such as response times, availability, etc. used for Service Level Monitoring and reporting. The data is captured by the Data Engine and is recorded into a SQL server.

The message layout is as following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>Name of Quality of Service</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the originator of the data</td>
</tr>
<tr>
<td>source</td>
<td>Specifies the source of the data. E.g. ping</td>
</tr>
<tr>
<td>sampletime</td>
<td>When the sample was recorded (epoch value)</td>
</tr>
<tr>
<td>samplevalue</td>
<td>The actual value.</td>
</tr>
<tr>
<td>samplerate</td>
<td>The rate of the sample interval</td>
</tr>
<tr>
<td>samplemax</td>
<td>The maximum value (if any). E.g. disksize.</td>
</tr>
</tbody>
</table>

Robot

A Robot is by dictionary definition a device that automatically performs complicated often-repetitive tasks.

The Robot is the software that connects a computer to the Nimsoft Infrastructure. Its primary task is to maintain and manage a set of probes, and to ensure a reliable flow of messages from its clients (The Probes) to the Hub. The Robot is the natural point of entry to the Nimsoft Infrastructure and it provides us with the following services:

- Automatic failover
- Naming services
- Scheduling services
- Software distribution services
- Handles 'local' security matters (such as e.g. access permissions, probe startup validation)

The Robot is capable of installing software in two ways:

1. By drag ‘n drop from the WorkSpace
2. Automatically during startup using a pull mechanism. This is a useful feature when you plan large rollouts into your organization.
The Robot uses the following well-known ports:

- TCP/48000 (controller)
- TCP/48001 (spooler)

**Subject**

All Nimsoft messages must contain a Subject ID. This is a text string classifying the message for all components on the Nimsoft, allowing them to subscribe to some messages and ignore others. All messages with the same subject should also have identical data structure.

Example: the "alarms" handled in the ALARM solution are simply messages with Subject="alarm". All components of the Alarm solution work on messages with this subject and ignore the subjects used by other solutions.

**Subscribe**

When a client of the Nimsoft (e.g. a probe or gateway) subscribes to Nimsoft Messages, it informs the Hub that it want a copy of all messages it detects on Nimsoft with a certain (set of) Subject ID(s). You may have several probes subscribing to the same subject. They will all automatically receive all messages with that subject ID.

**Alarms**

**Acknowledge**

All new alarm messages received by a Alarm Server (nas) are initially considered un-acknowledged and presented to an operator. When the operator has verified whether there was a problem and possibly fixed it, (s)he can acknowledge the message, indicating that the problem no longer exist. The message is then deleted from the nas database, but a copy is kept in the history database.

**Alarm Levels**

The Nimsoft API provides the developer with a method of sending an alarm. The supported alarm levels are:

<table>
<thead>
<tr>
<th>Constant</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIML_CLEAR</td>
<td>0</td>
</tr>
<tr>
<td>NIML_INFORMATION</td>
<td>1</td>
</tr>
</tbody>
</table>
Alarm message

An "Alarm" message is a general message defined with a specific format. The message is published onto the Nimsoft under the subject of "alarm", and is what we call a "raw alarm message". It is normally generated by a probe responding to a threshold breach, using the API function `nimAlarm (...)`. The API function will pack the parameters provided by the caller into a Message containing the following elements:

- Message text
- Message severity level
- Message subsystem
- Message originator/source
- Timestamp

History

When an Alarm message is acknowledged, it is deleted from the nas database, but it is still kept in a history database. The contents of this database can be viewed from e.g. Enterprise Console.

Regular expressions

Regular Expressions provide a mechanism to select specific strings from a set of character strings. The following text is extracted from the `perlre` man-page, and should be consulted for more in-depth understanding of regular expressions.
The patterns used in pattern matching are regular expressions such as those supplied in the Version 8 regexp routines. (In fact, the routines are derived (distantly) from Henry Spencer’s freely redistributable reimplementation of the V8 routines.) See the section on Version 8 Regular Expressions for details. In particular the following metacharacters have their standard egrep-ish meanings:

- \ Quote the next metacharacter
- ^ Match the beginning of the line
- . Match any character (except newline)
- $ Match the end of the line (or before newline at the end)
- | Alternation
- ( ) Grouping
- [ ] Character class

By default, the "^" character is guaranteed to match only at the beginning of the string, the "$" character only at the end (or before the newline at the end) and Perl does certain optimizations with the assumption that the string contains only one line. Embedded newlines will not be matched by "^" or "$". You may, however, wish to treat a string as a multi-line buffer, such that the "^" will match after any newline within the string, and "$" will match before any newline. At the cost of a little more overhead, you can do this by using the /m modifier on the pattern match operator. (Older programs did this by setting $*, but this practice is deprecated in Perl 5.) To facilitate multi-line substitutions, the "." character never matches a newline unless you use the /s modifier, which tells Perl to pretend the string is a single line— even if it isn’t. The /s modifier also overrides the setting of $*, in case you have some (badly behaved) older code that sets it in another module.

The following standard quantifiers are recognized:

- * Match 0 or more times
- + Match 1 or more times
- ? Match 1 or 0 times
- {n} Match exactly n times
- {n,} Match at least n times
- {n,m} Match at least n but not more than m times
(If a curly bracket occurs in any other context, it is treated as a regular character.) The "*" modifier is equivalent to {0,}, the "+" modifier to {1,}, and the "?" modifier to {0,1}. n and m are limited to integral values less than 65536. By default, a quantified subpattern is "greedy", that is, it will match as many times as possible without causing the rest of the pattern not to match. The standard quantifiers are all "greedy", in that they match as many occurrences as possible (given a particular starting location) without causing the pattern to fail. If you want it to match the minimum number of times possible, follow the quantifier with a "?" after any of them. Note that the meanings don’t change, just the "gravity":

- `*?` Match 0 or more times
- `+?` Match 1 or more times
- `??` Match 0 or 1 time
- `{n}?` Match exactly n times
- `{n,}?` Match at least n times
- `{n,m}?` Match at least n but not more than m times

Since patterns are processed as double quoted strings, the following also work:

- `\t` tab
- `\n` newline
- `\r` return
- `\f` form feed
- `\a` alarm (bell)
- `\e` escape (think troff)
- `\033` octal char (think of a PDP-11)
- `\x1B` hex char
- `\c` control char
- `\l` lowercase next char (think vi)
- `\u` uppercase next char (think vi)
- `\L` lowercase till `\E` (think vi)
- `\U` uppercase till `\E` (think vi)
- `\E` end case modification (think vi)
- `\Q` quote regexp metacharacters till `\E`
In addition, Perl defines the following:

- \w Match a "word" character (alphanumeric plus "_")
- \W Match a non-word character
- \s Match a whitespace character
- \S Match a non-whitespace character
- \d Match a digit character
- \D Match a non-digit character

Perl defines a consistent extension syntax for regular expressions. The syntax is a pair of parentheses with a question mark as the first thing within the parentheses (this was a syntax error in older versions of Perl). The character after the question mark gives the function of the extension. Several extensions are already supported:

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(?#text)</td>
<td>A comment. The text is ignored. If the /x switch is used to enable whitespace formatting, a simple # will suffice.</td>
</tr>
<tr>
<td>(?:regexp)</td>
<td>This groups things like &quot;()&quot; but doesn’t make backreferences like &quot;()&quot; does. So split(/b(?::a</td>
</tr>
<tr>
<td>(?=regexp)</td>
<td>A zero-width positive lookahead assertion. For example, /\w+(?=\t)/ matches a word followed by a tab, without including the tab in $&amp;.</td>
</tr>
<tr>
<td>(?!regexp)</td>
<td>A zero-width negative lookahead assertion. For example /foo(?!bar)/ matches any occurrence of &quot;foo&quot; that isn’t followed by &quot;bar&quot;. Note however that lookahead and lookbehind are NOT the same thing. You cannot use this for lookbehind: /(?!foo)bar/ will not find an occurrence of &quot;bar&quot; that is preceded by something which is not &quot;foo&quot;. That’s because the (?!foo) is just saying that the next thing cannot be &quot;foo&quot;—and it’s not, it’s a &quot;bar&quot;, so &quot;foobar&quot; will match. You would have to do something like /(?!foo)...bar/ for that. We say &quot;like&quot; because there’s the case of your &quot;bar&quot;.</td>
</tr>
</tbody>
</table>

Note that \w matches a single alphanumeric character, not a whole word. To match a word you’d need to say \w+. You may use \w, \W, \s, \S, \d and \D within character classes (though not as either end of a range).

Some examples:

<table>
<thead>
<tr>
<th>Regex</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/.+substring.+/</td>
<td>match substring somewhere in complete string (beginning to end)</td>
</tr>
<tr>
<td>/^at start.+/</td>
<td>match at start beginning at the first character position, match everything after start.</td>
</tr>
</tbody>
</table>
### Subsystem

The subsystem ID is a field in all Alarm messages, containing one or more numbers separated by dot’s (\`). This identifies the module within the monitored system the alarm should be related to. The Enterprise Console groups the incoming alarms according to subsystem, allowing you to view i.e. only alarms related to security issues or the disk system.

### Suppression

Probes sometimes generates several identical alarms. If suppression is enabled, such messages are treated as one to reduce network overhead and unnecessary messages presented to the operator.