

Nimsoft Server Installation Guide

Release: 5.0.0



Copyright Notice

Legal Notices

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 Corporation 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 Corporation 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 Corporation 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 Corporation 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 Corporation'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

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.

Contact Nimsoft

Contact Technical Support

For your convenience, Nimsoft provides one site where you can access the information you need for your 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.

Document History

Version	What's new?
Version 5.00	<ul style="list-style-type: none">■ Added details for MySQL and Oracle support■ Added Java requirements■ Added details for cloud installation■ Removed Nimsoft Web Service and Mobile Panel documentation

Contents

Copyright Notice	2
Contact Nimsoft	4
Document History	5
Contents	6
Chapter 1: Nimsoft Server Introduction	10
Chapter 2: Nimsoft Server Installation	12
Introduction.....	12
Prerequisites.....	12
Microsoft Windows platform	12
Linux platform	13
Solaris platform	13
Java Requirements	13
Installation requirements	14
System requirements	14
Preparing a database for a SLM installation.....	15
MS-SQL Server.....	16
MySQL	17
Oracle	18
Modifications made on computers when Nimsoft is installed.....	19
Modifications made when Nimsoft Server or Nimsoft Infrastructure is installed (Windows 2000/XP/2003/ Vista/2008/Windows 7).....	19
Modifications made when Robot is installed (Windows 2000/XP/2003/ Vista/2008/Windows 7)	20
Nimsoft Licenses.....	20
The Nimsoft Server Installation Wizard.....	20
Nimsoft Server First-time Installation	21
Nimsoft Server Upgrade	33
Chapter 3: Accessing Nimsoft Server	50
Introduction.....	51
Modifying the layout of the menu bar	53
Browser Setup	57

Chapter 4: Planning your installation 58

Introduction.....58

Planning and Establishing your Infrastructure58

 Defining your goals.....58

 What domains do you need?59

 Where do you need hubs?60

Planning and Establishing your ALARM Installation61

 Defining your goals.....61

 Planning the Infrastructure62

 Where do you need nas probes?62

Chapter 5: Client Installations 63

Introduction.....63

Installation in a firewalled environment67

 Introduction.....67

 Rather use an open Internet solution with Direct QoS Access?68

 What is a DMZ68

 What is a tunnel69

 Installation order69

 Deploying dashboards to the DMZ web server72

 Enabling Dashboards in the DMZ to receive alarm events from the outside74

Installing Enterprise Console75

Installing Infrastructure Manager79

Installing Service Level Manager83

Installing Nimsoft Infrastructure on Windows87

 Installing a Windows Robot.....87

 Normal installation.....90

 For Cloud setup94

 Installing Windows Robot, Hub, Distribution Server and Alarm Server97

Installing Nimsoft Infrastructure on Unix 107

 Installing Nimsoft Infrastructure on a Unix computer on your internal network 108

 Unix Installation Utility (nimldr) usage..... 109

 Robot installation from the Nimsoft Archive 110

 Infrastructure installation from local file 112

 Installing Nimsoft Infrastructure on a Unix computer in a DMZ 113

Infrastructure installation, Tunnel Server 116

Infrastructure installation, Tunnel Client 118

Installing the robot on AS400 121

 Installation procedure 123

 On the AS400..... 123

 On the workstation on the network..... 123

 On the AS400..... 124

 Example..... 124

Installing Nimsoft Web Service..... 125

Installing the Mobile Solution Services	125
Installing Nimsoft Web Access	125
Installing Nimsoft Dashboard Viewer	125
Chapter 6: Upgrading Client applications	131
Upgrade description	131
Chapter 7: Installing Nimsoft in an active/passive Microsoft Cluster	135
Installing Nimsoft in an active/passive Microsoft Cluster	135
Preparations	137
Installing and configuring	137
Reinstalling Nimsoft in an active/passive Microsoft Cluster	144
Chapter 8: LDAP Configuration	145
Configuring your login Hub	145
Connecting Access Control Lists to LDAP users	146
Verification	149
Advanced LDAP Configuration	149
Chapter 9: SSL – Encrypting network traffic	151
Troubleshooting	153
Chapter 10: Launching Nimsoft applications	154
Launching Infrastructure Manager, Enterprise Console or Service Level Manager	154
Chapter 11: Accessing ACL protected dashboards	156
Dashboards	158
Consoles	158
Reports	159
Chapter 12: Accessing Nimsoft Online Support	161
Chapter 13: Launching Dynamic Reports	163
Introduction	163
The Reports	164
Preparing for Dynamic Reports	166
Enabling Dynamic Reports	167
Report_engine not installed on the same server as the main hub?	174

Chapter 14: Launching Dynamic Dashboards 176

Introduction..... 176
The Dashboards..... 177
Preparing for Dynamic Dashboards..... 180
Enabling Dynamic Reports..... 180
Report_engine not installed on the same server as the main hub?..... 188

Chapter 15: NMS Connect 190

nws_api 190
numa_importer 191
 Probe Configuration 191
Configure Profile..... 193
 Setup 193
 QOS..... 194
 SLA..... 194
 Creating User, Account and ACL..... 195

Appendix 196

My SQL Installation Guide 196
 Summary 196
Physical/Virtual machine considerations 196
 Operating systems..... 196
 Licensing options 196
 Logging 196
 Hardware considerations 197
 Network..... 197
Backup and Restore..... 197
Monitoring..... 197
Configuration and Tuning..... 198
 Scope and Objectives 198
 Assumptions and Prerequisites..... 198
 *nix installation 199
 Windows Installation..... 201
Basic tuning configuration changes..... 202
Deployment statistics and estimations 204
Schema and data management..... 204

Index 208

Chapter 1: Nimsoft Server Introduction

Nimsoft Server, introduced in Nimsoft Server Release 3.10, is a package containing the Nimsoft Software for *Infrastructure, Availability, Service level Management* and *Discovery ACE Components*.

You can download and install Nimsoft Server from the Nimsoft download site (see the section [Nimsoft Server First-time Installation](#)).

The Nimsoft Server provides you the tool for managing your Nimsoft infrastructure. It gives you the opportunity to add and remove Nimsoft components through a web-interface.

It also holds shortcuts to the various consoles that may benefit you in your daily work.

This document

This document covers Nimsoft Server 5.00.

During this installation, you will be asked what you want to install:

- Infrastructure components (Robot, Hub, Distribution Server, Alarm Server)
- Nimsoft Availability Server
- SLM Server
- Nimsoft Discovery ACE Components

Use this module to automatically create monitoring profiles for devices detected on the network you want to monitor. Otherwise, you have to manually distribute probes and create monitoring profiles for the devices.

The devices found by the discovery process can later be found under the Dynamic Views node in the Enterprise Console (and the Service Delivery Portal, provided that you install it afterwards), but they will NOT be monitored and NOT send QoS values before you set them to Managed in the NIS Manager!

The installation consists of three steps:

1. Files are copied to your computer, and the Infrastructure is installed and initialized.
2. This step only applies if you select to install the SLM Server (see above).

The SLM installation is started; configuring SLM and setting up the database connection on your computer, and prepares for SLM client installations.

NOTE:

If this is a first time installation, or you are installing onto a new Domain, you will be prompted with the New User dialog. The user name is set to Administrator, and you have to select a password for domain login.

Nimsoft Discovery ACE is dependent on a SLM Server Installation and cannot be installed without SLM Server.

3. When the Nimsoft Server installation is completed, Nimsoft Server will automatically be opened in a web browser, provided that the Start Nimsoft Server window option was checked in the last dialog in the setup. Here you can start installing Nimsoft client software on your computer. Further, using the web browser, you can access Nimsoft Server from other computers on your network and install Nimsoft Client software.

As mentioned above, Nimsoft Server will, when installed on your server, 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 on your clients
- View your Nimsoft Dashboards and reports
- Access the Nimsoft Server on-line documentation.

Chapter 2: Nimsoft Server Installation

Introduction

To avoid unwanted access to your dashboards, Nimsoft installations etc. from the web, you should not install Nimsoft Server in a DMZ.

Prerequisites

NMS Server can be installed on the 32-bit and 64-bit versions of the following operating systems.

Microsoft Windows platform

- Microsoft Windows XP
- Microsoft Windows 2003
- Microsoft Windows Vista
- Microsoft Windows 2008
- Microsoft Windows 7

Note:

Administrator privileges are required both to install Nimsoft Server components and to run Infrastructure Manager on Microsoft Windows Vista, Microsoft Windows 2008 or Windows 7.

Microsoft Windows Vista and later specific:

On Windows Vista, you need to be logged in as a user with administrator privileges both to install and run Nimsoft Server.

Dragging & Dropping zip-packages from e.g. a Windows Explorer to the Infrastructure Manager archive is not allowed by Windows Vista security policy (Nimsoft is running with administration privileges).

You must copy the zip-file to any folder but the **Program Files\Nimsoft\archive** folder.

Then go to the archive in the Infrastructure Manager, find the probe, right-click it, select 'import' and browse to the folder to which you copied the zip-file.

This applies when User Account Control (UAC) is turned on. UAC is by default turned on after the installation of Windows Vista. You can solve the problem by turning UAC off. This can be done under **Control Panel > User Accounts > User Accounts > Turn User Account Control on or off**.

Note: The purpose of the UAC is to prevent against unauthorized modifications of the computer, and it is recommended to keep UAC turned on.

- OS Minor is listed as Windows and not Windows Vista.

Linux platform

- Red Hat Enterprise Linux (RHEL) 4 and 5
- SUSE Linux Enterprise Server (SLES) 10 and 11

Solaris platform

- Solaris 10 (SPARC and Intel)

The installation contains four main components:

1. Nimsoft Infrastructure components (Robot, Hub, Distribution Server, Alarm Server)
2. Nimsoft Availability Server
3. Nimsoft SLM Server
4. Nimsoft Discovery ACE Components

During the Setup Wizard, you have the option to install one or more of them.

You also need to ensure access to a database such as MS-SQL Server or MySQL or Oracle database.

Please refer to the chapter [Preparing a database for a SLM installation](#) for more details.

Note: You must use a case INSENSITIVE database.

If you want to install the Service Level Manager component on Microsoft Windows 2000 computers, you also need MDAC 2.8 or newer installed.

Java Requirements

- Java Runtime Environment 1.6 is a prerequisite for installation.
- Ensure that a Sun Microsystems JVM is used.
- The path to the Sun JVM should be set in the PATH environment of the terminal used for starting the installer. The Sun JVM should be found prior to any other java virtual machine.

Installation requirements

Installing on one or two machines?

When installing a small system, you may install the components involved on one machine, otherwise we recommend installing on two servers.

As a rule, if your Nimsoft installation shall handle more than 1000 QoS messages per minute, we recommend to install on two servers.

Installing on a virtual machine?

When installing the NMS on a VMware ESX Server, please review VMware's document "*Java in Virtual Machines on VMware ESX: Best Practices*"

The document is available at the following URL:

http://www.vmware.com/files/pdf/Java_in_Virtual_Machines_on_ESX-FINAL-Jan-15-2009.pdf

Installing one or more Hubs?

It is recommended that at least two Hubs should be installed on the same Domain and network to avoid loss of user/security data, such as Nimsoft user definitions ACLs etc., in case your Hub crashes. With more than one Hub, this information is mirrored between the Hubs.

System requirements

Large Network

Database Server:

- 2 CPUs
- 3+ GHz Processor
- 2-4 GB RAM
- Raid 10 disk system 100+ GB *

Nimsoft Server:

- 1 CPU
- 3+ GHz Processor
- 1 GB RAM
- 100 GB Disk *

Medium-size network

Nimsoft Server and Database Server:

- 1 CPU
- 3+ GHz Processor
- 1 GB RAM
- 100 GB Disk *

* Recommended disk configuration:

- Operating system on a separate disk
- Transaction log on a separate disk
- Data on a separate disk (or Raid 10)

Preparing a database for a SLM installation

The SLM product needs to store data in a database. If you want to install the SLM Server component during the Nimsoft Server installation, you must decide which database to use.

The NMS Server supports the following databases:

- Microsoft SQL Server
- MySQL
- Oracle

NOTE: The database must be case INSENSITIVE!

The modifications described below (depending on which database you are going to use) should be performed **before** starting the Nimsoft Server installation wizard.

Utilizing an existing database?

If you intend to utilize an existing database for a new installation or an upgrade of Nimsoft version 3.35 / 3.35 SR1 or earlier, please make sure that you make a backup of your database. The Nimsoft Server 4.3 contains a **non-reversible upgrade script** that changes the database structure of some tables.

The database upgrade may take a long time to finish if the database contains many QoS objects. It is difficult to estimate the duration of an upgrade, since the duration depends on a number of different factors. A database upgrade with 5000+ tables with a size of 25 GB may consume 5-6 hours. A database upgrade with the same amount of data, but with less than 1000 tables may consume only 30-45 minutes.

Another example from a site with a database of size 120GB with approximately 20000 QoS objects showed that the database upgrade were running approximately 8 hours.

If you have a database similar to the first example, you may consider upgrading during a weekend and stop the probes *sla_engine* and *report_engine* during the upgrade.

MS-SQL Server

You can use Microsoft SQL Server or Microsoft SQL Express.

For a production system, we recommend you to use Microsoft SQL Server, with database authentication or Windows authentication.

The following versions of MS-SQL Server are supported:

- MS-SQL Server 2005
- MS-SQL Server 2008

You may also use Microsoft SQL Server Express if you are planning to install an evaluation/demo system.

During the Nimsoft Server installation, a dialog will ask you to select one of the following three options:

- Using a SQL Server with database authentication
- Using a SQL Server with windows authentication
- Using SQL Server Express

Necessary modifications, depending on which database you are going to use, are described below:

4. Using a SQL Server with database authentication

No further configuration is needed.

5. Using SQL Server with windows authentication

The user running the SLM part of the Wizard must have administrative rights on the machine running the SQL Server. The *data_engine* probe must have administrative rights both on the local computer as well as on the SQL Server machine. This can be achieved by changing the Watcher service to run as an appropriate user.

6. Using SQL Server Express

In order to use SQL Server Express, you must specify the following options to the SQL Server Express setup program:

```
SAPWD=<password>
SECURITYMODE=SQL
DISABLENETWORKPROTOCOLS=0
```


Notes:

- When specifying the server name, you must use the format <server name>\SQLEXPRESS
- If you also later want to install the Nimsoft Service Delivery Portal (SDP), the “SQL Server Browser” service must be started on the computer after installation of SQL Express. Otherwise you will get a database error when logging in to the SDP.

MySQL

The following versions of MySQL are supported:

- MySQL 5.1

Please note that NMS requires the following configuration settings for MySQL server:

- lower_case_table_names=1
- local-infile=1

The second option is required to support data_engine’s use of ‘load data local infile’.

In order to use MySQL as the SLM database, you must specify the following options:

- **Database:** Specify the schema name (referred to as <DBname>) for SLM database. For example, *Nimsoft-SLM*
- **MySQL Host Address:** Specify the server name or IP address of the machine on which MySQL database is being hosted
- **Username:** Enter the login name for the user having administrative rights on the MySQL database. Usually this is *root*
- **Password:** Enter the password (referred to as <password>) for the above username. Ensure that the password does not contain any special characters (such as “;”).
- **Port:** Specify the port number at which database connection will be established with the MySQL database. Usually this port number is *3306*.

For further information on My SQL installation, please refer [Appendix](#) section in this document.

Oracle

The following versions of Oracle database are supported:

- Oracle 11g

Provide the following details while configuring the Oracle database.

- **Database Server Name or IP:** Specify the server name or IP address of the machine on which the Oracle database is being hosted.
- **Database port:** Specify the port number at which database connection will be established with the Oracle database. By default, this port number is *1521*
- **SYS user name:** Enter the login name for the user having administrative rights on the Oracle database.
- SYS user password
- Service Name for Oracle

NOTE

When installing Nimsoft Server 5.0 using Oracle database, the following point should be noted with reference to the “locale” settings.

The installation works fine with locale set as **en_US.UTF-8**.

If you use any other locale (for example, Norwegian), you may see the following error message:

"The database does not exist or could not be created"

To resolve this, please ensure to make the following changes:

```
shell# export LC_ALL=[your_Locale]
```

For example:

```
# export LC_ALL=norwegian
# locale
LANG=norwegian
LC_CTYPE="norwegian"
LC_NUMERIC="norwegian"
LC_TIME="norwegian"
LC_COLLATE="norwegian"
LC_MONETARY="norwegian"
LC_MESSAGES="norwegian"
LC_PAPER="norwegian"
LC_NAME="norwegian"
LC_ADDRESS="norwegian"
LC_TELEPHONE="norwegian"
LC_MEASUREMENT="norwegian"
LC_IDENTIFICATION="norwegian"
LC_ALL=norwegian
```

Modifications made on computers when Nimsoft is installed

This section describes the modifications made on computers when Nimsoft is installed, such as:

- New folders
- Updated DLLs
- Registry entries

Modifications made when Nimsoft Server or Nimsoft Infrastructure is installed (Windows 2000/XP/2003/ Vista/2008/Windows 7)

When installing the Nimsoft Server or Nimsoft 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

msvbvm60.dll

oleaut32.dll

olepro32.dll

Only updated if nonexistent or the existing version is old. These dll's are also registered.

<registered>

... \Nimsoft\lib\Nimbus.dll

This DLL is registered.

Modifications made when Robot is installed (Windows 2000/XP/2003/Vista/2008/Windows 7)

.../Nimsoft

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

Normally this is C:\Program Files\Nimsoft Monitoring

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_MACHINE\Software\Nimsoft Software

HKEY_LOCAL_MACHINE\Software\Nimsoft Software AS

HKEY_LOCAL_MACHINE\Software\Nimsoft Corporation

Stores some variables internally used by Nimsoft.

Start Menu\Programs\Nimsoft Monitoring

A common menu choice to start the *Service Controller*.

<services>

A service called '*Nimsoft Watcher*'. The service can be managed with the service controller. The complete service can be removed with the command

... \Nimsoft\bin\Nimsoft -remove

Nimsoft Licenses

Downloading and installing Nimsoft Server offers you a 30 days trial license for the Nimsoft products and some of the most common probes.

After the trial period of 30 days, you are welcome to contact us at www.nimsoft.com for valid permanent licenses.

The Nimsoft Server Installation Wizard

Nimsoft Server First-time Installation

1. Go to the Nimsoft Customer Support Centre site (which you will find [here](#)). Log in and start the installation by double-clicking Nimsoft Server xxx Full Distribution.

Note that this description applies to a first-time installation of Nimsoft Server software.

2. Setup starts extracting files. Wait for the *Welcome* dialog to appear and click the *Next* button to continue.
3. The *License Agreement* dialog appears. Read the license agreement carefully and click *Yes* to continue if you accept the terms, otherwise click *No* to exit.
4. The next dialog asks you to enter the password for your domain administrator. Enter the password and click the *Next* button.
5. A dialog containing important installation information pops up. Read this information before clicking the *Next* button to continue.
6. The next dialog enables you to select which components to install: *Nimsoft Availability Server* and/or *Nimsoft SLM Server* and/or *Nimsoft Discovery ACE Components*.

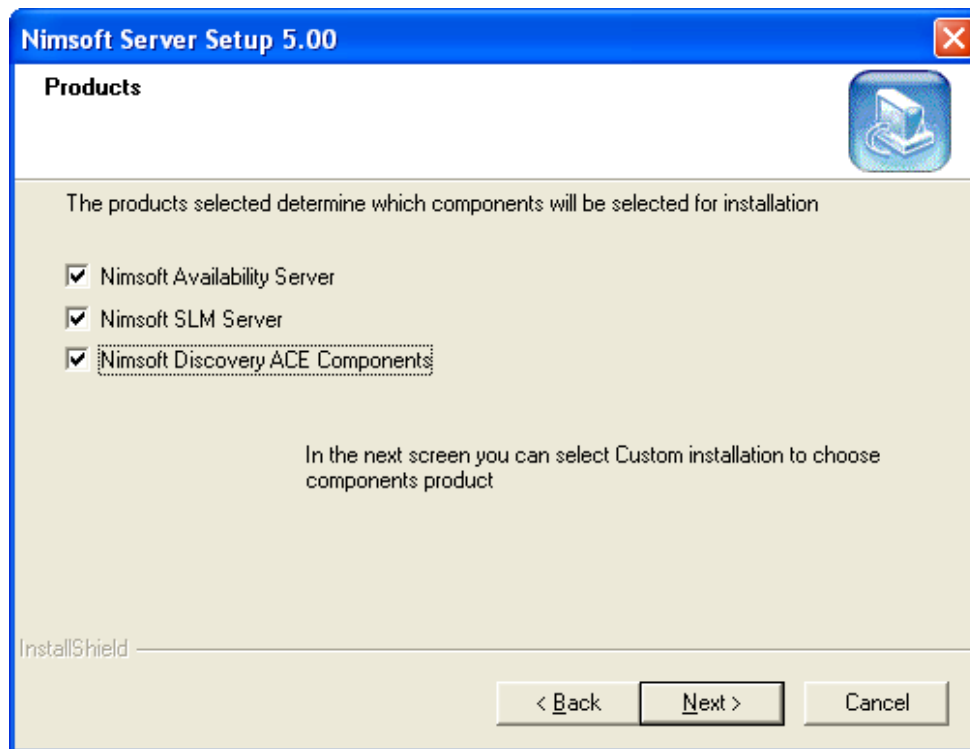
Ensure that the component(s) you want to install are checked.

NOTE:

If you select the Nimsoft Discovery ACE Component, the SLM Server will also automatically be installed.

The SLM component requires a database that must be case INSENSITIVE!

Click the Next button.

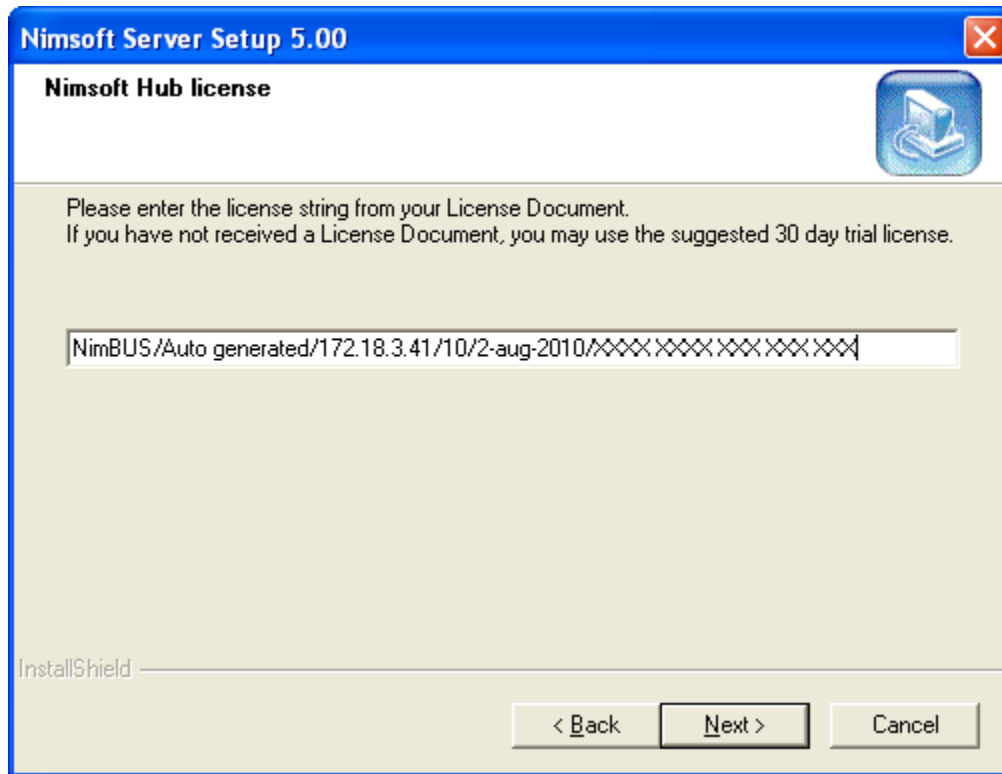


7. The next dialog lets you choose between Typical and Custom installation.

Typical searches for existing Nimsoft components on your computer and installs the necessary software. Custom offers you the option of selecting Nimsoft components to be installed. Make your choice and click the Next button to continue.
8. The next dialog displays the settings selected so far in the installation process. Click the *Back* button if you want to change something or click the *Next* button to continue. The next dialog confirms your selections so far
9. The next dialog prompts you for a *Domain* name (to which the *Hub*, which will be installed in the next step, will belong). Specify a name and click the *Next* button to continue.
10. This dialog prompts you for a *Hub* name. Specify a name and click the *Next* button to continue (if no name is specified, the name of your computer will be used).

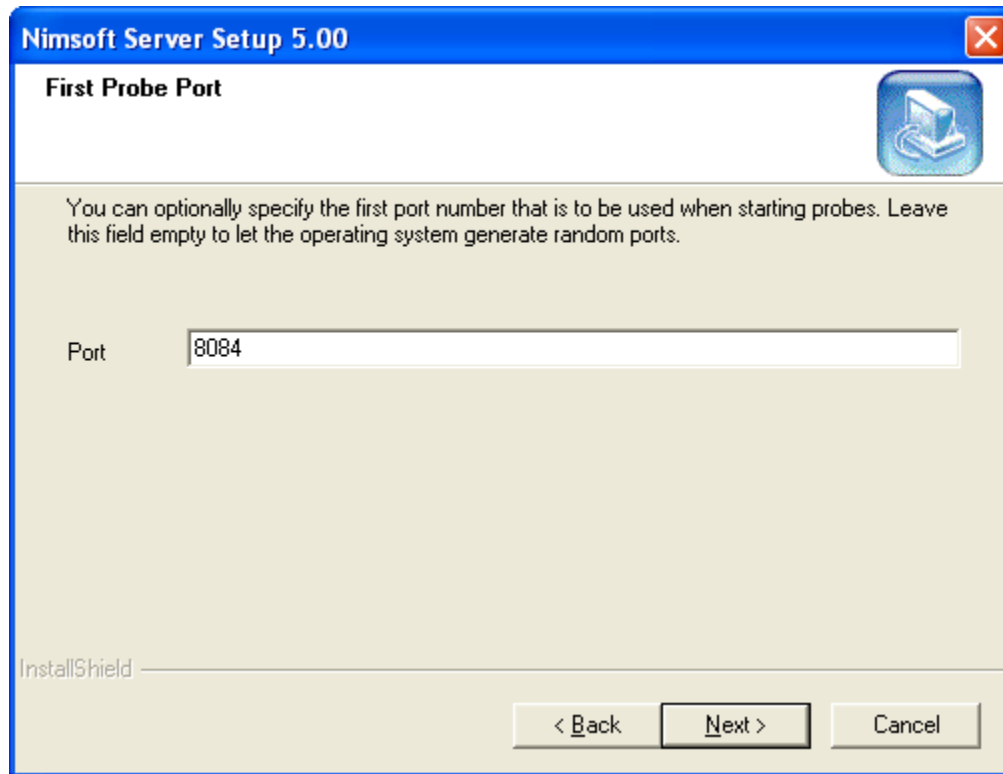
Note: It is recommended that at least two Hubs should be installed on the same Domain and network to ensure you have a backup of the user/security data. See the [Client Installations](#) for instructions on how to install another Hub after this wizard is finished.
11. The Hub License dialog prompts you for a Hub license. On an initial installation, the license field contains an evaluation license string, valid for 30 days.

If it is an upgrade, you will have the option of selecting your existing license, or to use the evaluation license.



Click the Next button to continue.

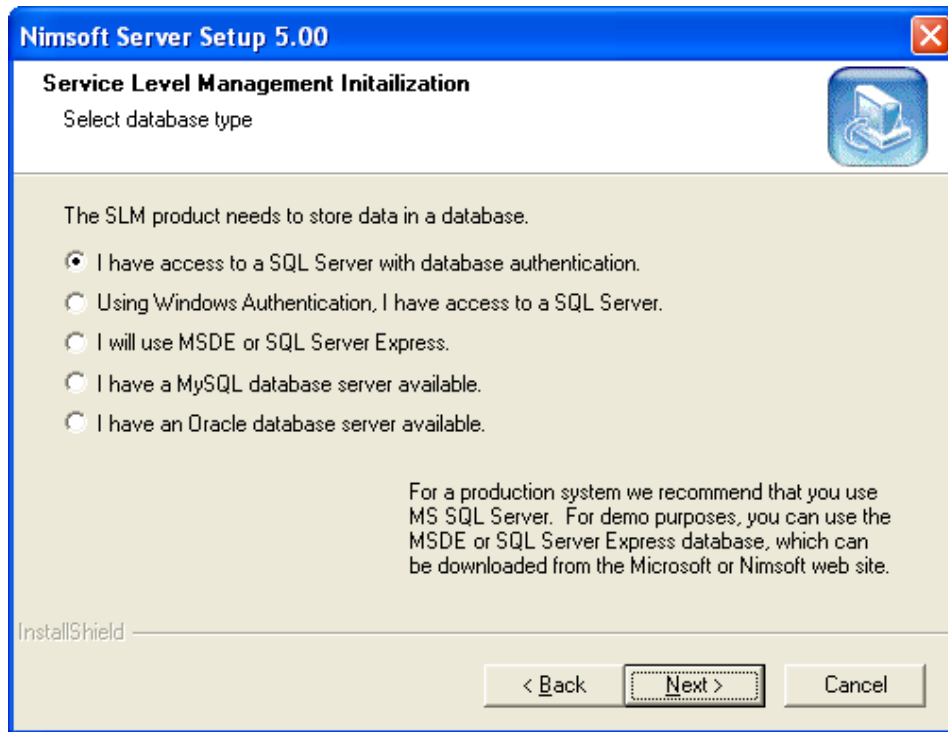
12. First Probe Port dialog appears. You can specify a port number to be used when starting the probes, or leave this field blank if you wish the operating system to generate a random port number. Click the Next button to continue.



13. At this point in the installation, and provided that you selected to install the SLA Server component in step 6, a dialog appears, asking what kind of database you are using.

Please use a login with sysadmin privileges when installing or upgrading:

- a. If using an existing database, make sure that the login used for installation/upgrade maps to the database's dbo.
- b. If database is created by the Nimsoft Server installation, the database's dbo will automatically be mapped to the login used in the installation.
- c. If you did NOT select to install the SLA Server component in step 6, clicking the Next button brings you to step 21.



If selecting the option "I have access to a SQL Server with database authentication", clicking the Next button brings you to step 14.

If selecting the option "Using Windows authentication, I have access to a SQL Server", clicking the Next button brings you to step 15.

If selecting the option "I will use MSDE or SQL Server Express", clicking the Next button brings you to step 16.

14. You have selected the option "I have access to a SQL Server with database authentication" in step 13.

Click the Next button and proceed with step 17.

15. You have selected the option "Using Windows authentication, I have access to a SQL Server" in step 13.

If you have prepared the database as described in this dialog before you started this wizard (see also), you click the Next button and proceed with step 17.

If the database was not prepared as described in this dialog before you started the wizard, you should now read the instructions in this dialog, and then click the Cancel button to finish the setup. Follow the instructions given in the dialog, and note that you must run the wizard again to install the SLM component.

16. You have selected the option "I will use MSDE or SQL Express" in step 13.

If you have prepared the database as described in this dialog before you started this wizard, you click the Next button and proceed with step 17.

If the database was not prepared as described in this dialog before you started the wizard, you should now read the instructions in this dialog, and then click the Cancel button to finish the setup. Follow the instructions given in the dialog, and note that you must run the wizard again to install the SLM component.

The installation procedure is a bit awkward if you want to use SQL Server Express with the command line parameters depicted above. This is due to the fact that the program SQLEXPRESS.EXE extracts the real Setup files to a directory and then invokes the Setup.exe program (see [http://msdn2.microsoft.com/en-us/library/ms143793\(SQL.90\).aspx](http://msdn2.microsoft.com/en-us/library/ms143793(SQL.90).aspx)).

It is the Setup.exe program that recognizes the command line parameters SAPWD etc.

e.g.:

```
setup.exe SAPWD="<password>" SECURITYMODE=SQL  
DISABLENETWORKPROTOCOLS=0
```

17. In the next step, you must connect to a database server, using a valid server name, database user name and password.
Note that the server name must be prepended with \SQLEXPRESS if you are using SQL Server Express, e.g. fluffy\SQLEXPRESS.
Click the Next button to continue.

Nimsoft Server Setup 5.00

SLM Database Access

Service Level Management requires the use of a database.

Server:

User:

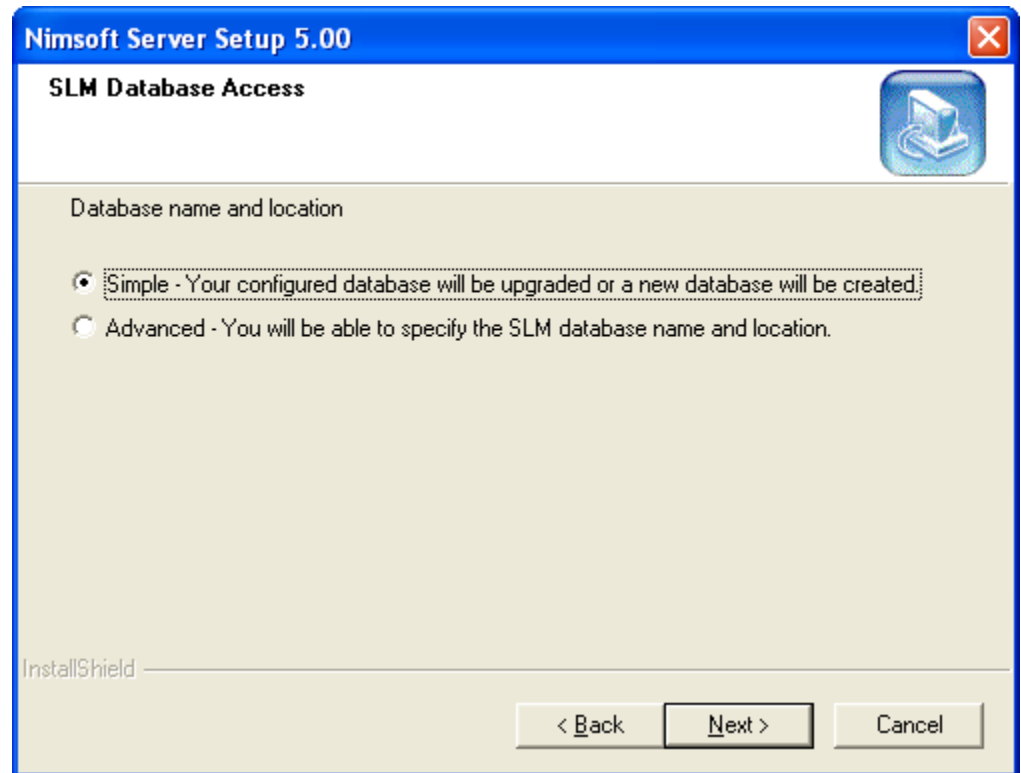
Password:

InstallShield

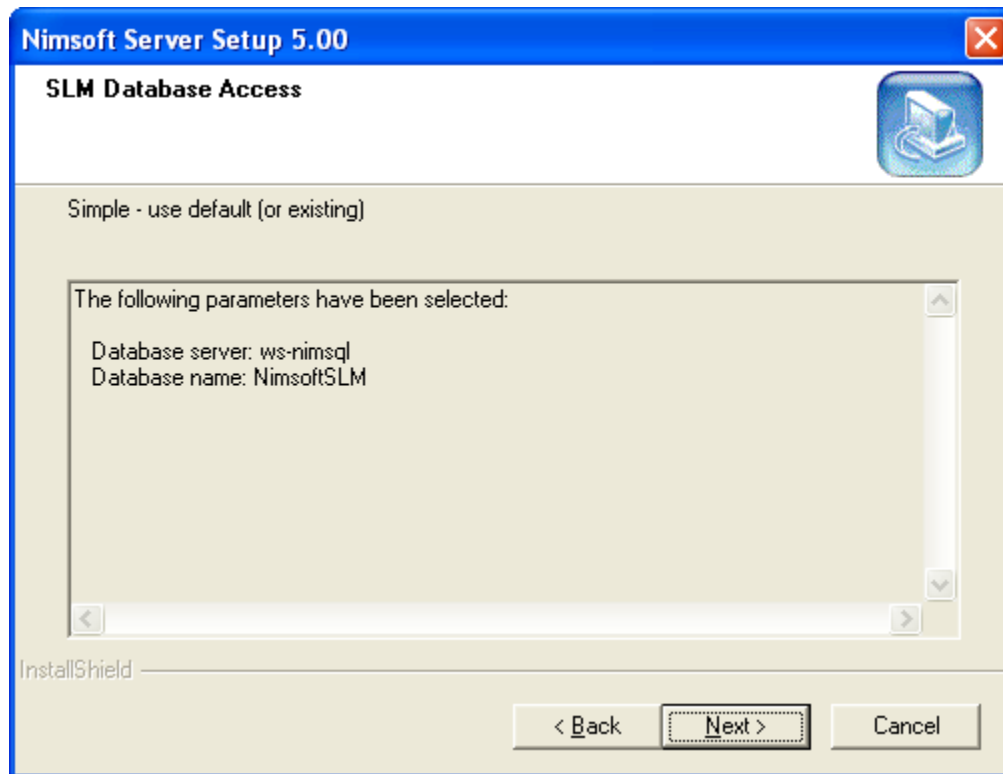
< Back **Next >** Cancel

18. In this step you select the SLM database. Clicking Simple, you select to use the default database which will be created if it does not exist). A new dialog appears, confirming the selected database settings. Click the Next button to continue. You will then proceed with step 20.

Clicking Advanced, you are allowed to select a database from the list. You will then proceed with step 19.



19. Clicking Advanced in step 18, this dialog pops up, allowing you to select a database from the list (or create a new one). Make your choice and click the Next button.
20. Give the new database a name and click the Next button.
21. A new dialog appears, confirming the selected database settings. Note that if you are running a Custom installation, a dialog appears where you must select one of the databases listed. Click the Next button to continue.



22. At this point in the installation, and provided that you selected to install the Discovery ACE Components component in step 6, a dialog appears. This lets you select the network (or discovery scope) to be scanned for computer systems to be monitored.

Note:

The dialogs in step 21-26 will be presented only once for each database, so if you use an existing database, these steps will be skipped. The Discovery Agent needs to know which discovery scope (IP range) to explore and search for computer systems. This information must be specified here and can further be modified using the NIS Manager. The discovery scope is the sum of specified IP-ranges and excludes.

Specify a network as an IP address/mask, IP Address Range or specific IP address. Optionally you may specify an exclude IP range, excluding parts of the network from the discovery.

Specify the network and click Next to proceed.

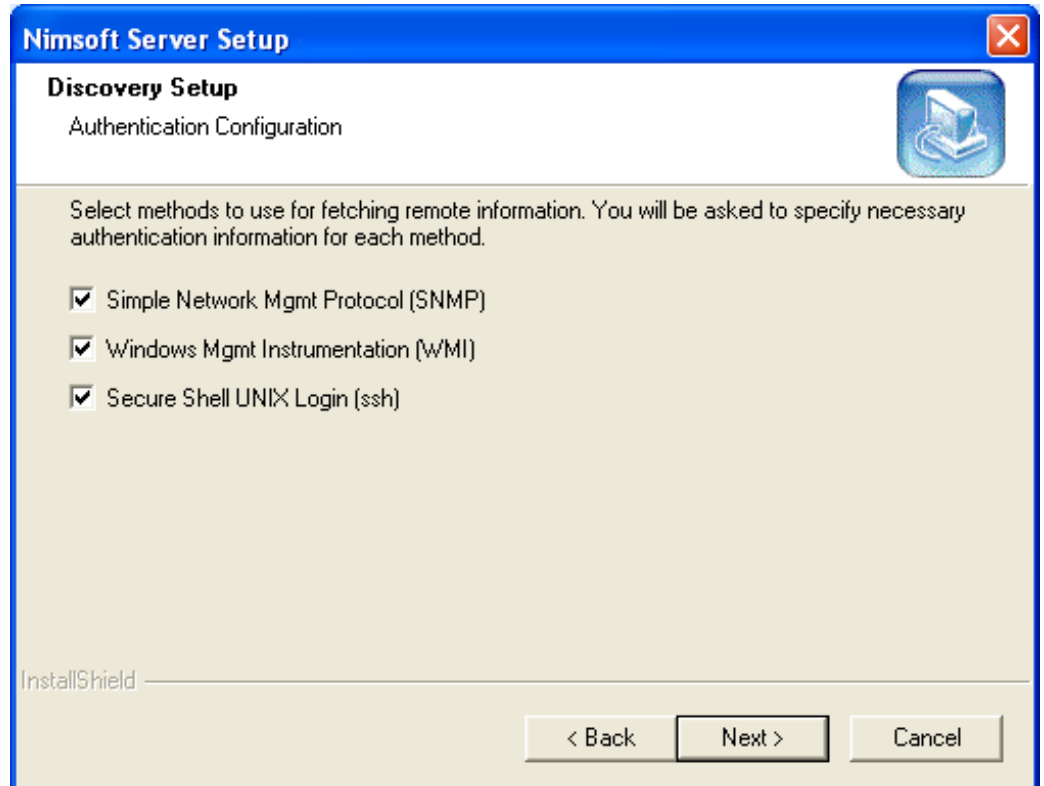
Note that you may later modify the network specification in the NIS Manager.

23. The devices found by the discovery process can later be found under the Dynamic Views node in the Enterprise Console (and the Service Delivery Portal, provided that you install it afterwards), but they will NOT be monitored and NOT send QoS values before you set them to Managed in the NIS Manager!

This dialog lets you select the network authentication protocols to be used to communicate with the computer systems in the network specified.

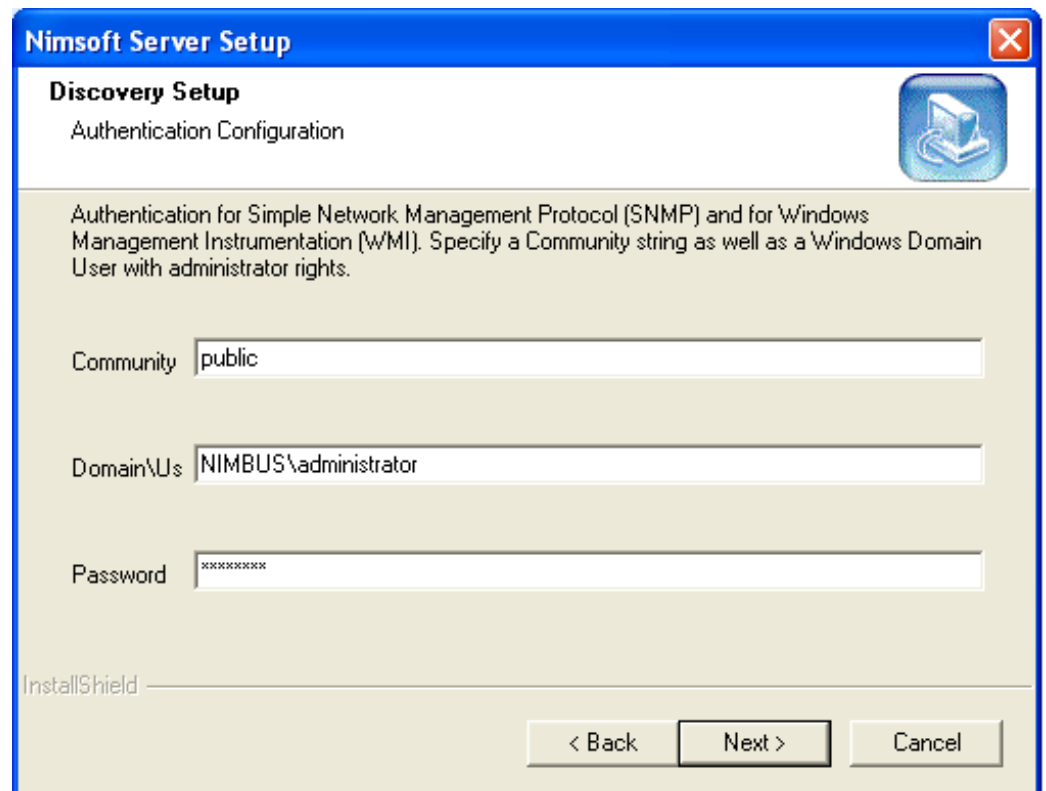
Valid options are Windows Management Instrumentation (WMI) and Simple Network Management Protocol (SNMP).

Make your selection and click Next to proceed



24. Specify the community for SNMP authentication and a user name (Domain\username) and password the WMI authentication. Click Next to proceed.

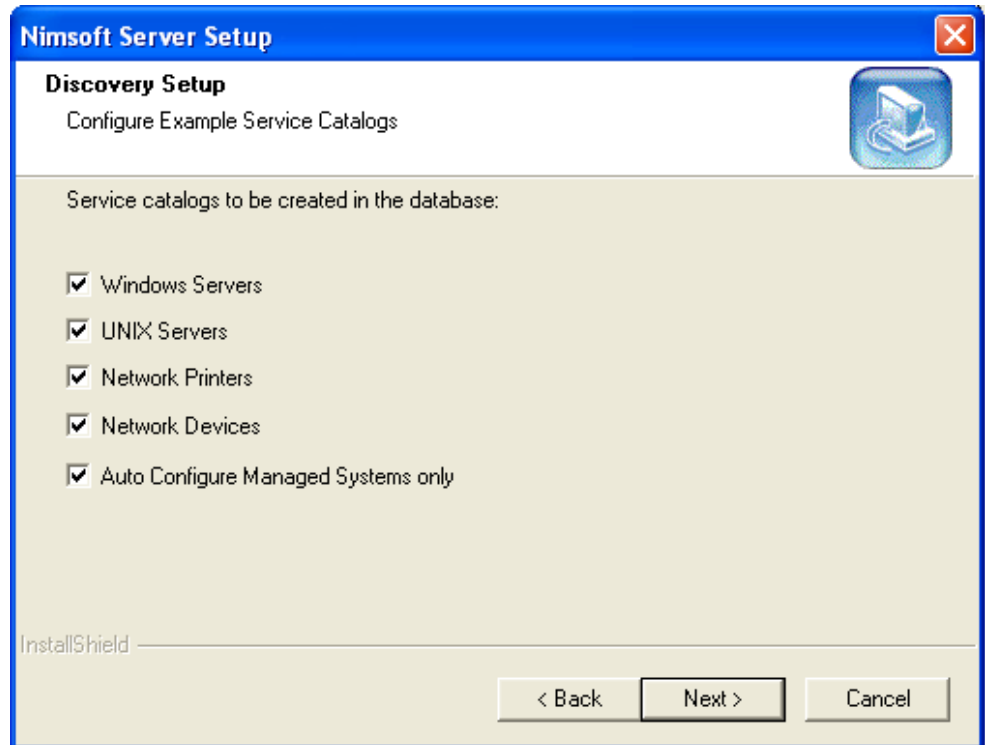
Note that you may later modify these settings in the NIS Manager.



25. Specify authentication parameters for Secure Shell UNIX Login (ssh). Click Next to proceed.
26. Now a dialog appears, enabling you to select one or more Service Catalogs to be created in the database. Note that you may later add and delete Service Catalogs in the NiS Manager. The different computer systems discovered on the network will be grouped into Service Catalogs, depending on type of computer system. Pre-defined filters define which kind of computer systems to be placed in the different Service Catalogs. These filters can be modified in the NiS Manager. You can filter on a lot of parameters, such as IP-range, OS etc.

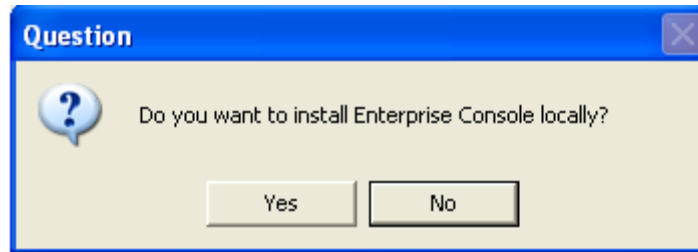
Selecting the “Auto Configure Managed Systems only” option, a pre-defined configuration profile will be used for all computer systems set to Managed state in the NiS Manager. The Managed state must be set manually for each of the system in the NiS Manager.

If this option is **not** set, the pre-defined configuration profile will be used for all computer systems, independent of state set in the NiS Manager.



27. The next dialog shows the Discovery parameters chosen. If you want to modify these parameters, click the Back button and make your changes, and then proceed the wizard. Otherwise click the Next button to continue.
28. Setup starts copying files.
29. The Setup will now check if one or more of the Nimsoft user interfaces already are installed on your computer:
 - a. Infrastructure Manager
 - b. Service Level Manager
 - c. Enterprise Console

If any of these are found with older version than the current version (included in this installation package), the current version will now automatically be installed.
If NOT found, you will be asked if you want to install it.



Note

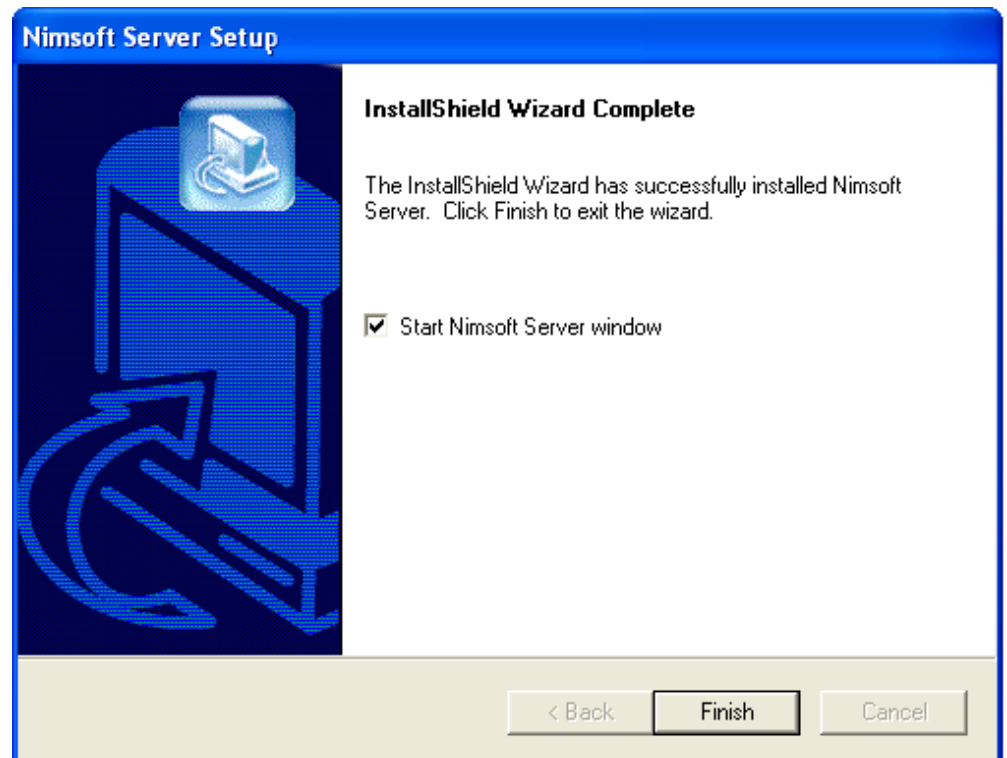
After each of these consoles has been successfully installed, you may be asked if you want to restart your computer. We recommend answering No and rather manually restarting your computer after the Nimsoft Server installation is completed.

30. When finished, the following dialog appears. Note the checkbox Start Nimsoft Server window.

When checked, the Start Nimsoft Server window will be launched when you have clicked the Finish button in this dialog.

Otherwise you will have to launch it by clicking the Nimsoft Server icon that will be added to your desktop.

Click the Finish button to exit.



Nimsoft Server Upgrade

This chapter describes how to upgrade Nimsoft Server 4.3 installation to Nimsoft Server 5.0

Before you begin with the upgrade, ensure that Nimsoft robot is running on your computer.

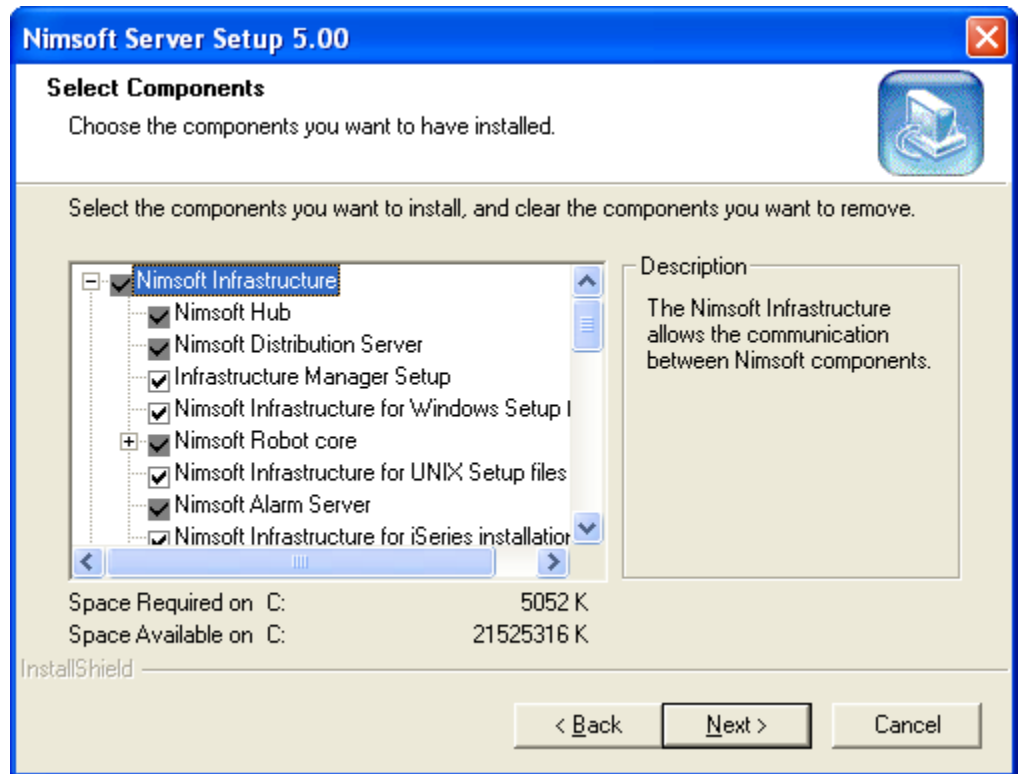
1. Go to the Nimsoft Customer Support Centre site (which you will find [here](#)). Log in and start the installation by double-clicking Nimsoft Server xxx Full Distribution.

Note that this description applies to a re-installation of the Nimsoft Server software.

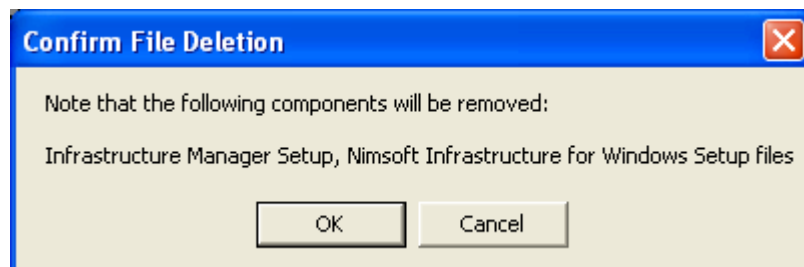
2. Setup starts extracting the files necessary for the installation. Wait for the Welcome dialog.
3. When the Welcome dialog appears; select Modify if you want to add new components or select Remove if you want to remove all installed components. In this example we use Modify. Click the Next button to continue.
4. The next dialog asks you to enter the password for your domain administrator. Enter the password and click the Verify button. On successful verification the Verify button changes to Success. Then click the Next button.
5. Choose the components you want to have installed on your computer.

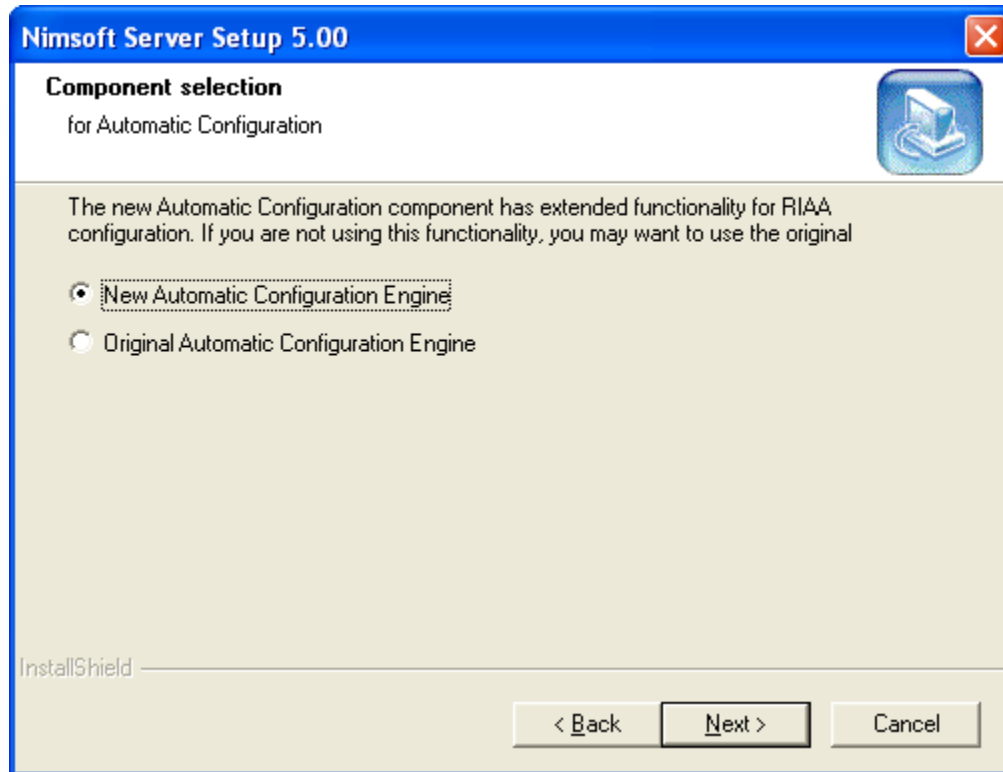
Note only the components selected will be installed and present on the computer after the installation, all unselected components will be removed from the computer.

Click the Next button to continue.



Note if you have deselected a component in the dialog above that is currently installed on your computer (e.g. the SLA Server component), you will be asked if you really want to remove it.

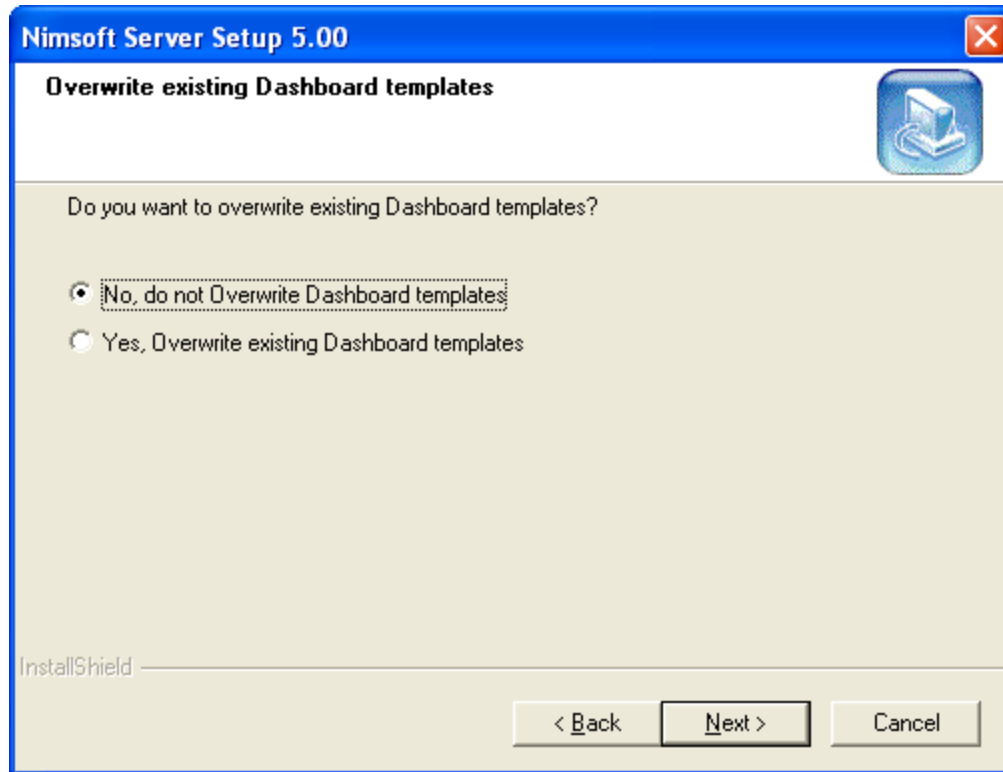




6. If you have a distributed SLM system and re-install the SLM SLA Server component, the wizard will automatically find where your current SLM components are located and install the new ones on the same location.

Choose the option for Automatic Configuration from the given two option:

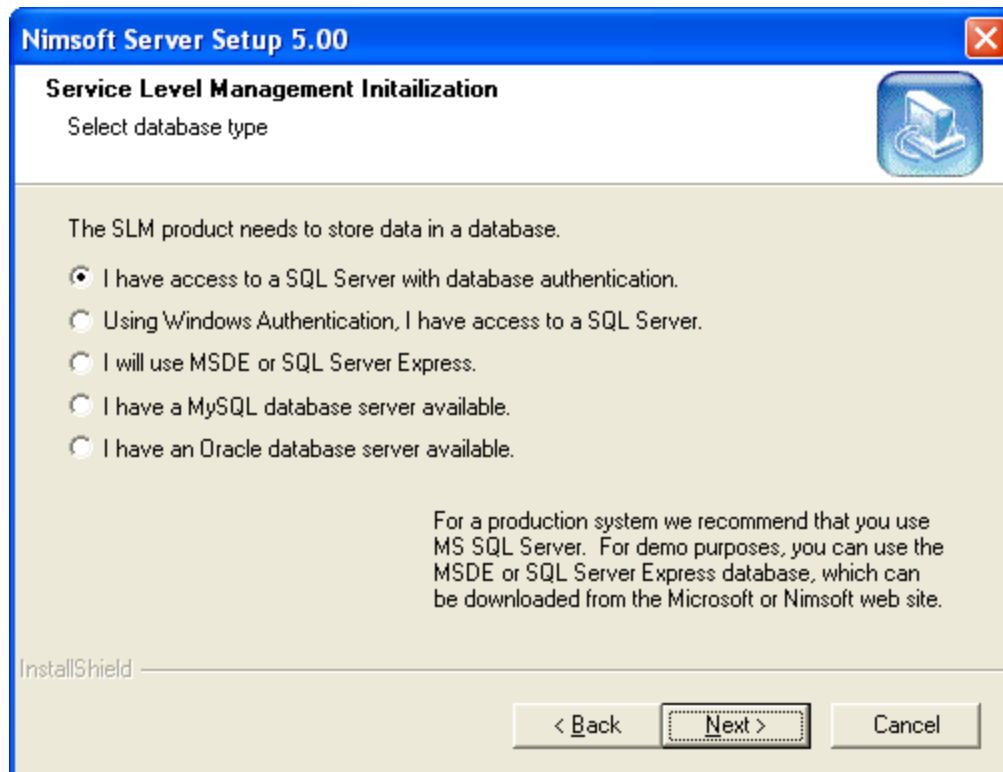
- a. New Automatic Configuration Engine
 - b. Original Automatic Configuration Engine
7. Setup will now look for and suggest a hub license. Click the Next button to continue.



9. First Probe Port dialog appears, asking you to specify a port on which the first probe will start. You can leave this field if you wish the operating system to generate random ports.
10. At this point in the installation, and provided that you selected to install the SLA Server component in step 5, a dialog appears, asking what kind of database you are using.

Please use a login with sysadmin privileges when installing or upgrading to Nimsoft Server 4:

- a. If using an existing database, make sure that the login used for installation/upgrade maps to the database's dbo.
- b. If database is created by the Nimsoft Server installation, the database's dbo will automatically be mapped to the login used in the installation.



If selecting the option "I have access to a SQL Server with database authentication", clicking the Next button brings you to step 10.

If selecting the option "Using Windows authentication, I have access to a SQL Server", clicking the Next button brings you to step 11.

If selecting the option "I will use MSDE or SQL Express", clicking the Next button brings you to step 12.

11. You have selected the option "I have access to a SQL Server with database authentication" in step 9.

Click the Next button and proceed with step 13.

12. You have selected the option "Using Windows authentication, I have access to a SQL Server" in step 9.

If you have prepared the database as described in this dialog before you started this wizard, you click the Next button and proceed with step 13.

If the database was not prepared as described in this dialog before you started the wizard, you should now read the instructions in this dialog, and then click the Cancel button to finish the setup. Follow the instructions given in the dialog, and note that you must run the wizard again to install the SLM component.

13. You have selected the option "I will use MSDE or SQL Express" in step 9.

If you have prepared the database as described in this dialog before you started this wizard, you click the Next button and proceed with step 13.

If the database was not prepared as described in this dialog before you started the wizard, you should now read the instructions in this dialog, and then click the Cancel button to finish the setup. Follow the instructions given in the dialog, and note that you must run the wizard again to install the SLM component.

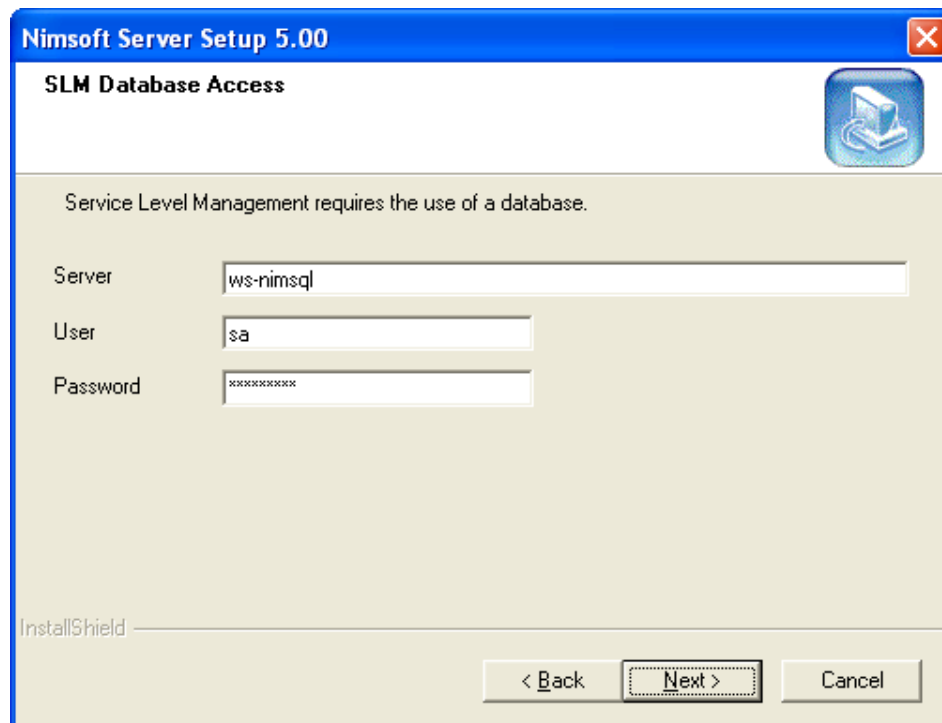
The installation procedure is a bit awkward if you want to use SQL Server Express with the command line parameters depicted above. This is due to the fact that the program SQLEXPRESS.EXE extracts the real Setup files to a directory and then invokes the Setup.exe program (see [http://msdn2.microsoft.com/en-us/library/ms143793\(SQL.90\).aspx](http://msdn2.microsoft.com/en-us/library/ms143793(SQL.90).aspx)).

It is the Setup.exe program that recognizes the command line parameters SAPWD etc.

e.g.:

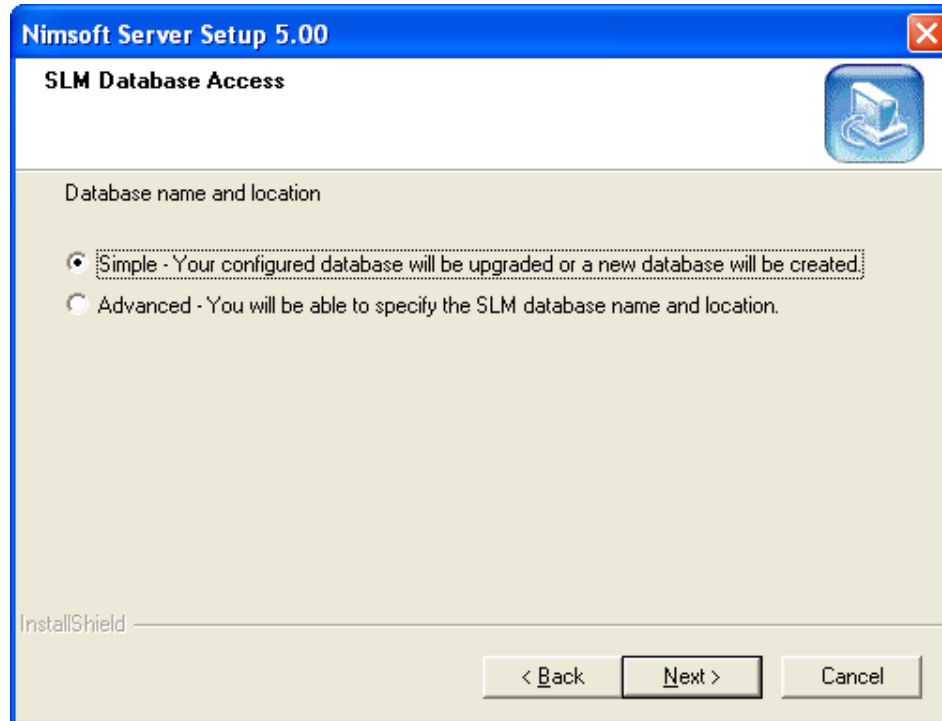
```
setup.exe SAPWD="<password>" SECURITYMODE=SQL  
DISABLENETWORKPROTOCOLS=0
```

14. In the next step, you must connect to a database server, using a valid server name, database user name and password.
Note that the server name must be prepended with \SQLEXPRESS if you are using SQL Server Express, e.g. fluffy\SQLEXPRESS.
Click the Next button to continue.



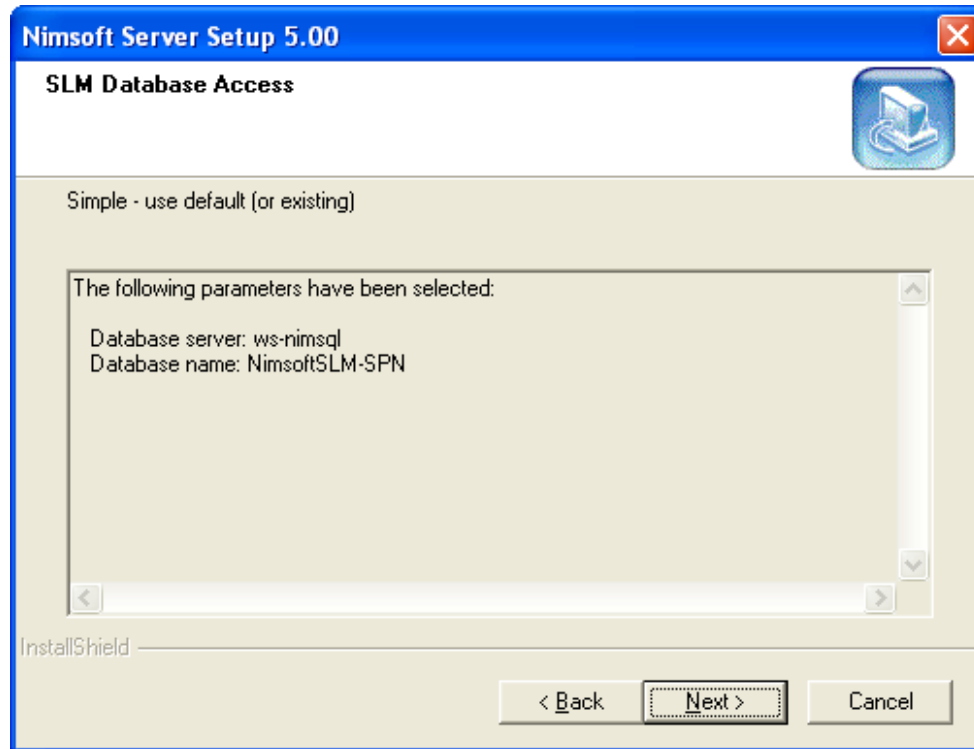
The screenshot shows a Windows-style dialog box titled "Nimsoft Server Setup 5.00" with a sub-title "SLM Database Access". The dialog contains the text "Service Level Management requires the use of a database." and three input fields: "Server" with the value "ws-nimsql", "User" with the value "sa", and "Password" with masked characters "*****". At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

15. In this step you select the SLM database.
Clicking Simple, you select to use the default database which will be created if it does not exist. A new dialog appears, confirming the selected database settings. Click the Next button to continue. You will then proceed with step 16.



Clicking Advanced, you are allowed to select a database from the list. You will then proceed with step 15.

16. Select a database name from the list or create a new one. Click the Next button to continue.
17. If you selected to create a new database, please specify the name and location of the database. Click the Next button to continue.
18. A new dialog appears, confirming the selected database settings. Note that if you are running a Custom installation, a dialog appears where you must select one of the databases listed. Click the Next button to continue.



19. Provided that you selected to install the Discovery ACE Components component in step 5, a dialog appears.

Note:

The dialogs in step 18-23 will be presented only once for each database, so if you use an existing database, these steps will be skipped.

This lets you select the network (or discovery scope) to be scanned for computer systems to be monitored. The Discovery Agent needs to know which discovery scope (IP range) to explore and search for computer systems. This information must be specified here and can further be modified using the NIS Manager. The discovery scope is the sum of specified IP-ranges and excludes.

Specify a network as an IP address/mask, IP Address Range or specific IP address. Optionally you may specify an exclude IP range, excluding parts of the network from the discovery.

Specify the network and click Next to proceed.

Note that you may later modify the network specification in the NIS Manager.

20. This dialog lets you select the network authentication protocols to be used to communicate with the computer systems in the network specified.

Valid options are Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI) and Secure Shell UNIX Login (ssh).

Make your selection and click **Next** to proceed.

21. Specify the community for SNMP authentication and a user name (Domain\username) and password the WMI authentication. Click Next to proceed.
Note that you may later modify these settings in the NiS Manager.
22. Specify authentication parameters for Secure Shell UNIX Login (ssh). Click Next to proceed.
23. Now a dialog appears, enabling you to select one or more Service Catalogs to be created in the database. Note that you may later add and delete Service Catalogs in the NiS Manager.

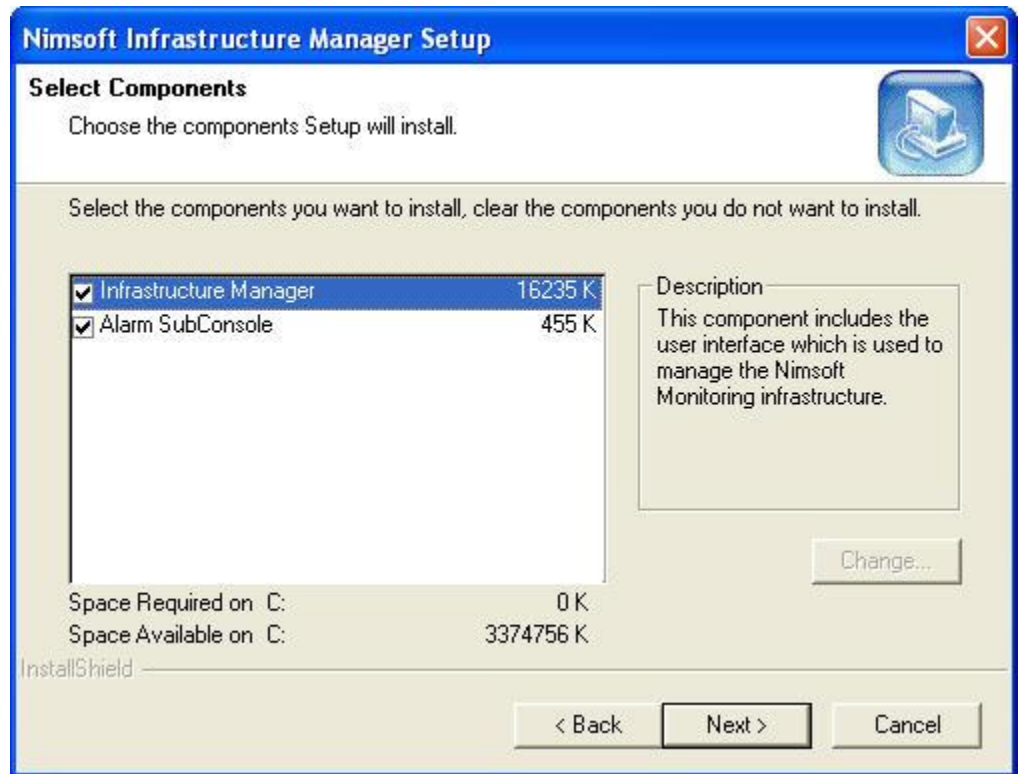
The different computer systems discovered on the network will be grouped into Service Catalogs, depending on type of computer system. Pre-filters define which kind of computer systems to be placed in that Service Catalog. These filters can be modified in the NiS Manager. You can filter on a lot of parameters, such as IP-range, OS etc.

Selecting this option, a pre-defined configuration profile will be used for all computer systems set to Managed state in the NiS Manager. This state must be set manually in the NiS Manager.

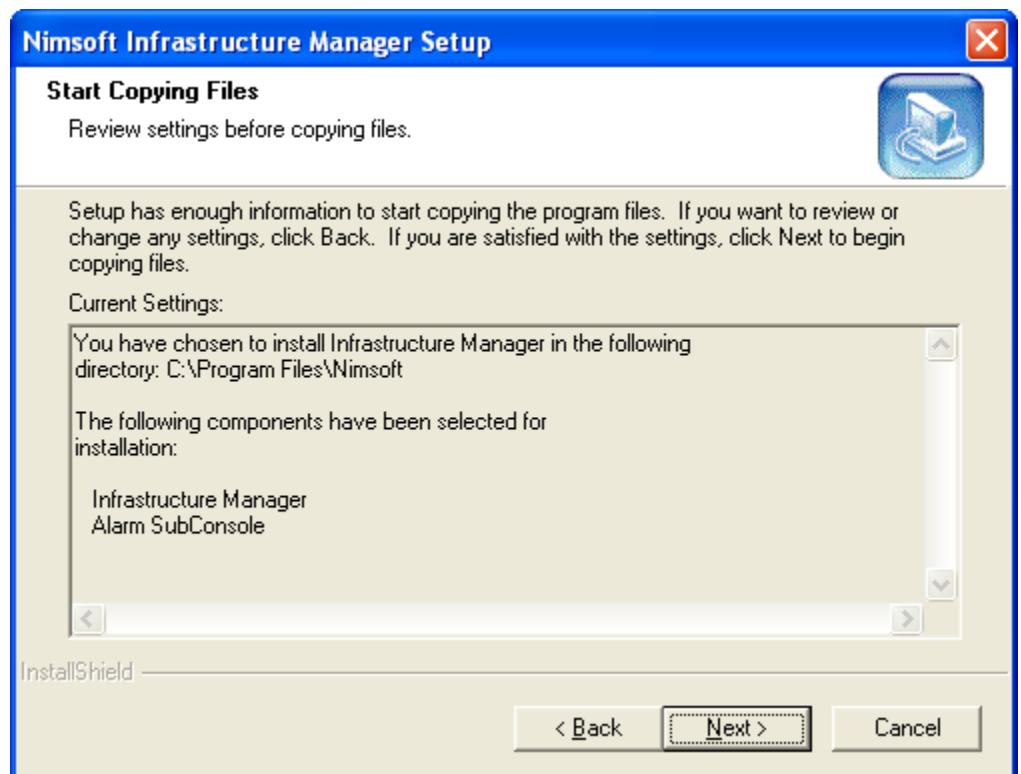
24. The next dialog shows the Discovery parameters chosen. If you want to modify these parameters, click the Back button and make your changes, and then proceed the wizard.
Otherwise click the Next button to continue.
25. Setup starts copying files.
26. The Setup will now check if one or more of the Nimsoft user interfaces already are installed on your computer:
 - Infrastructure Manager
 - Service Level Manager
 - Enterprise Console

If any of these are found with older version than the current version (included in this installation package), the current version will now automatically be installed.

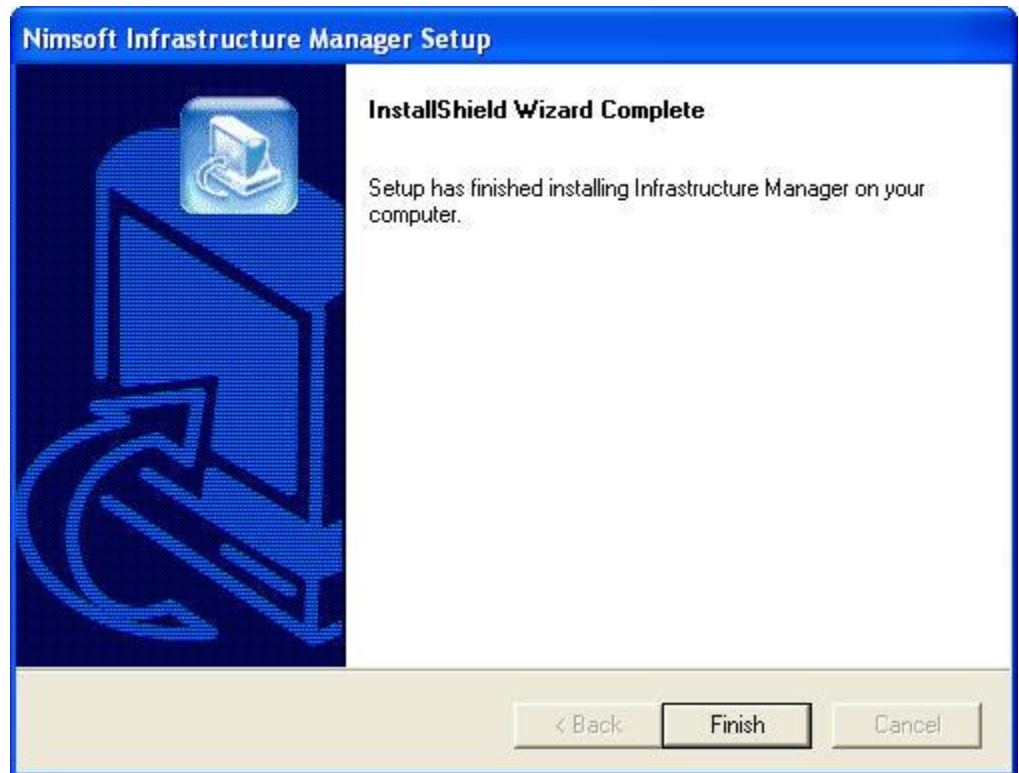
If NOT found, you will be asked if you want to install it.
27. In the Infrastructure Manager dialog, click the Next button to continue.
28. Setup Type dialog appears. Select the Upgrade/Reinstall option, and click the Next button.
29. In the License Agreement dialog, click the Yes button to continue.
30. In the Select Components dialog, select the components you want to install.



31. Start Copying files dialog appears, which displays all the settings you have selected so far. After reviewing and confirming the settings, click the Next button.



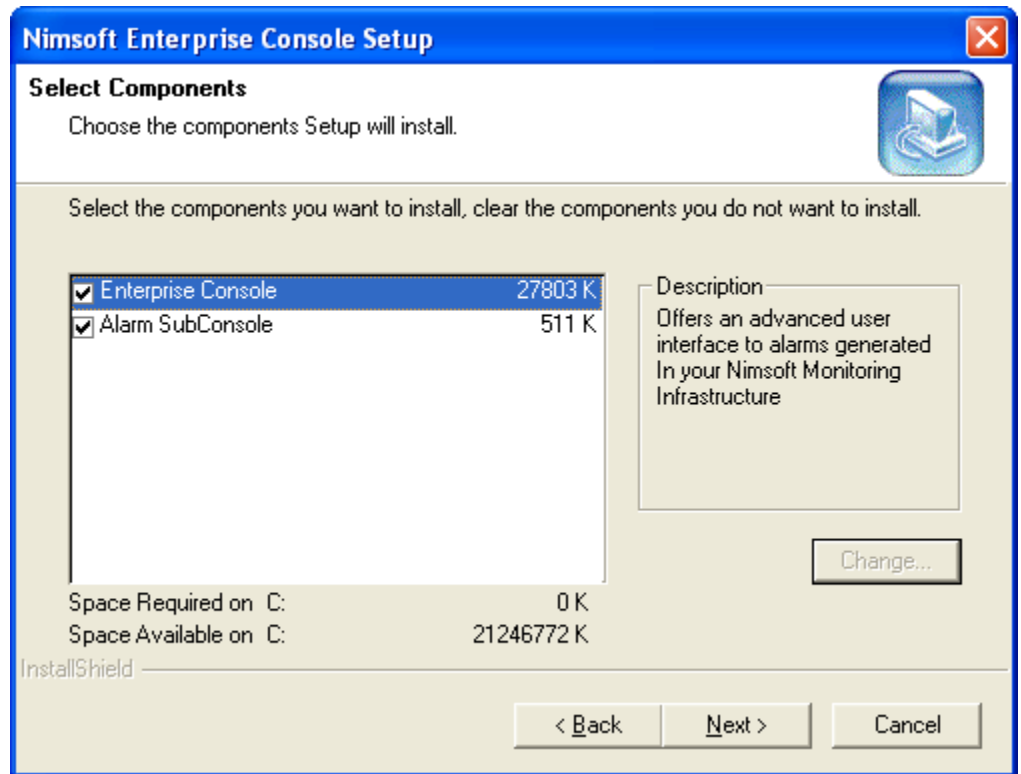
32. Setup Status dialog appears.
33. After installation is complete, the following dialog appears. Click the Finish button.



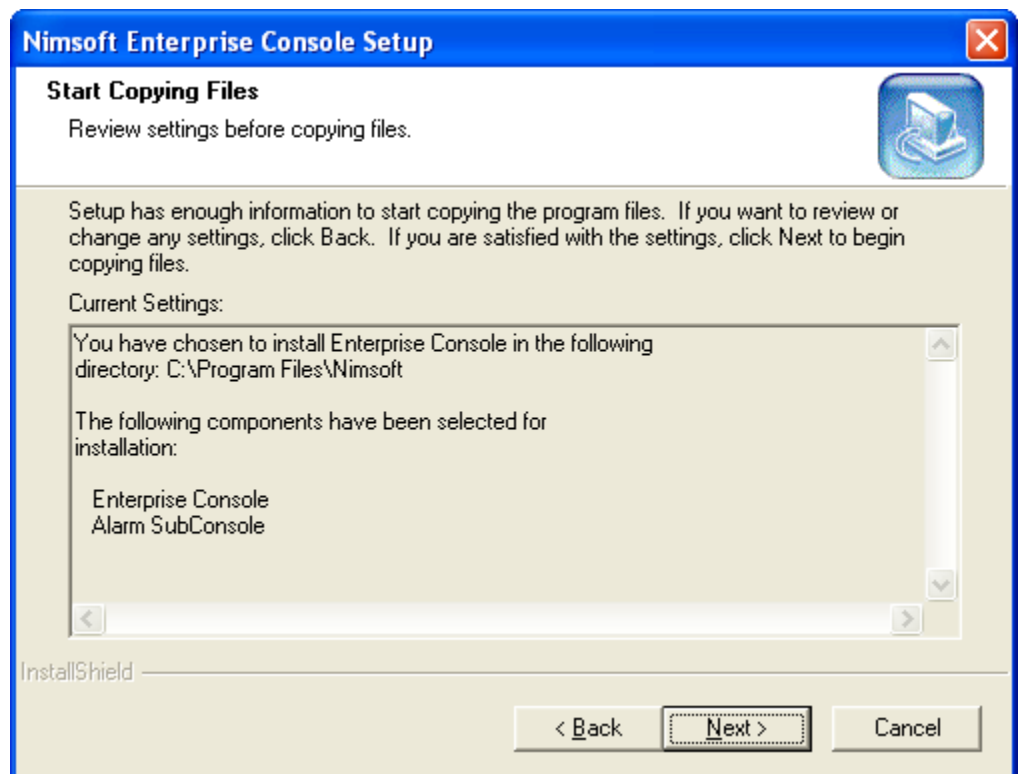
Note

After each of these consoles has been successfully installed, you may be asked if you want to restart your computer. We recommend answering No and rather manually restarting your computer after the Nimsoft Server installation is completed

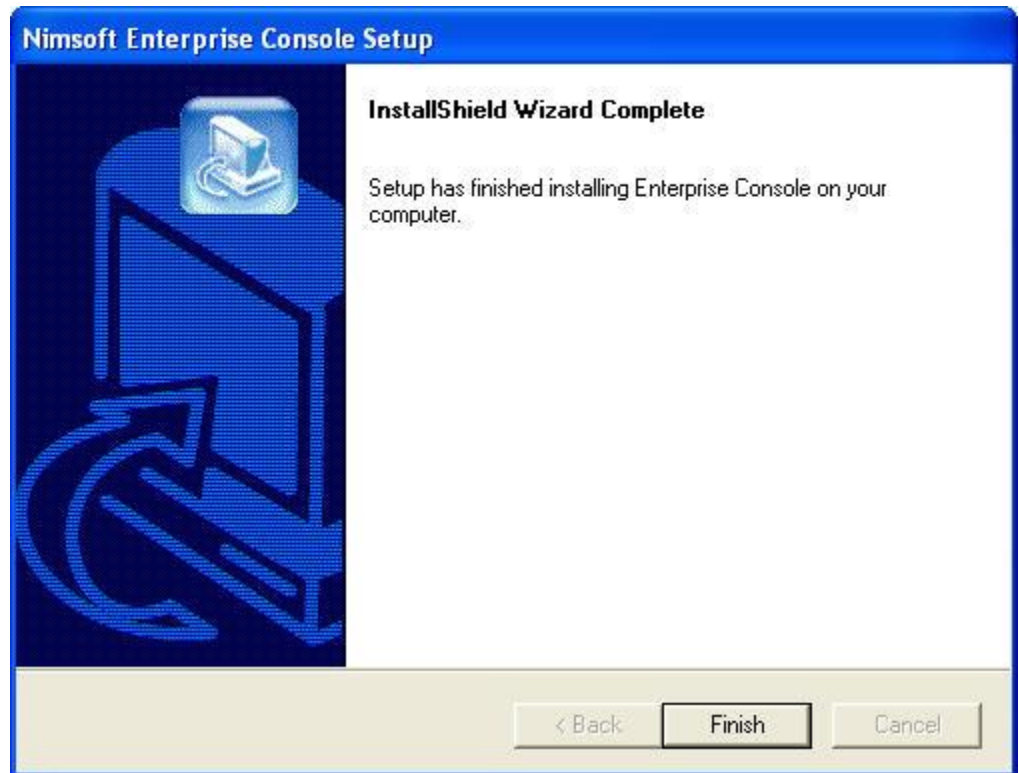
34. In the Nimsoft Enterprise Console maintenance dialog, click the Next button to continue.
35. Setup Type dialog appears. Select the Upgrade/Reinstall option, and click the Next button.
36. In the License Agreement dialog, click the Yes button to continue.
37. In the Select Components dialog, select the components you want to install.



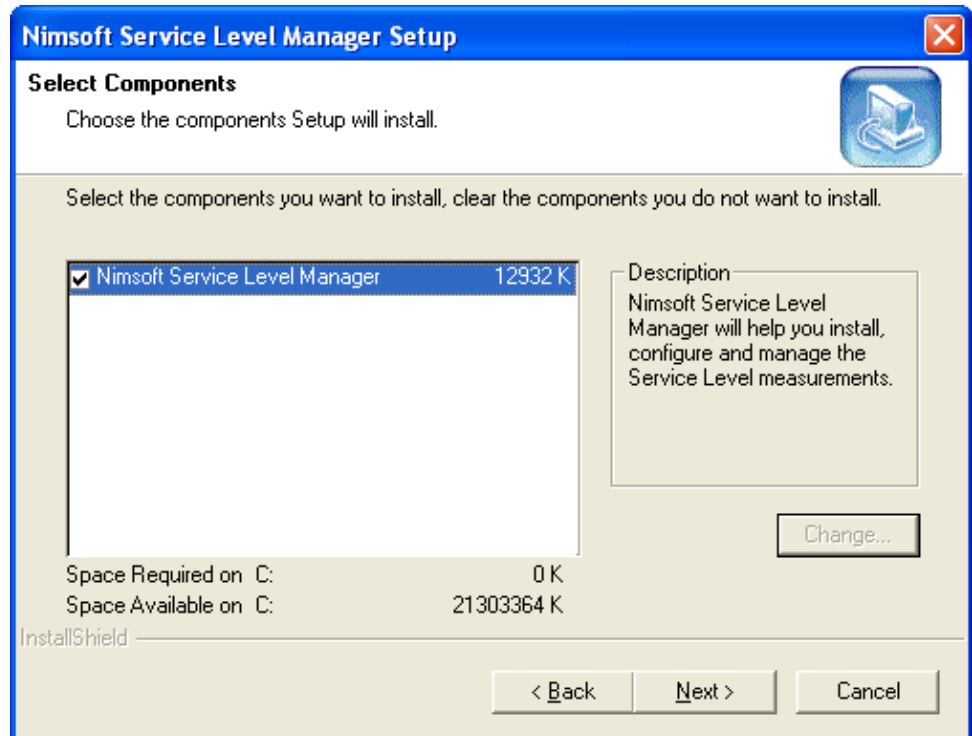
38. Start Copying files dialog appears, which displays all the settings you have selected so far. After reviewing and confirming the settings, click the Next button.



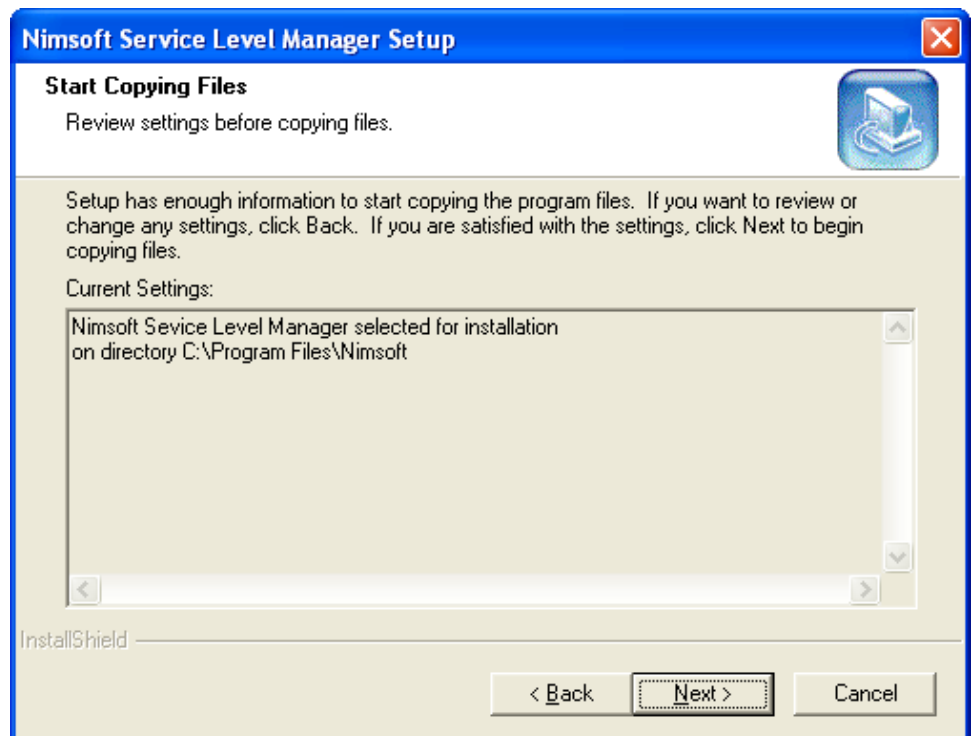
39. Setup Status dialog appears.
40. After installation is complete, the following dialog appears. Click the Finish button.



41. In the Nimsoft Service Level Manager maintenance dialog, click the Next button to continue.
42. Setup Type dialog appears. Select the Upgrade/Reinstall option, and click the Next button.
43. In the License Agreement dialog, click the Yes button to continue.
44. The Select Components dialog, select the components you want to install.

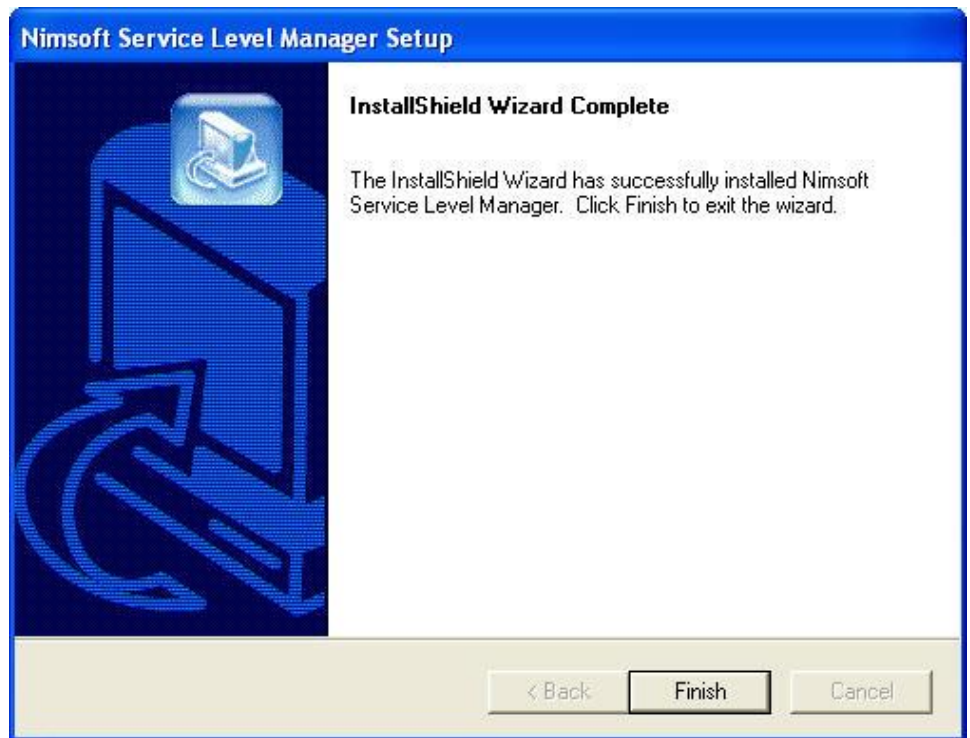


45. Start Copying files dialog appears, which displays all the settings you have selected so far. After reviewing and confirming the settings, click the Next button.

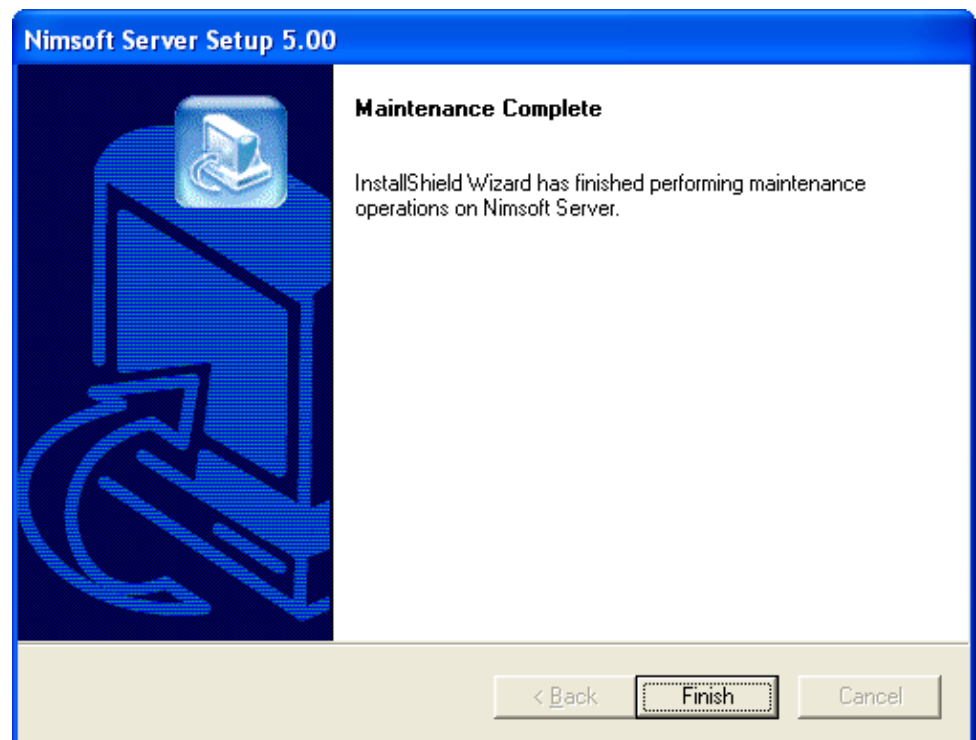


46. Setup Status dialog appears.

47. After installation is complete, the following dialog appears. Click the Finish button.



48. When finished, the following dialog appears. Click the Finish button to exit.



49. You can launch the newly installed Nimsoft Server by clicking the Nimsoft Server icon that will be added to your desktop.

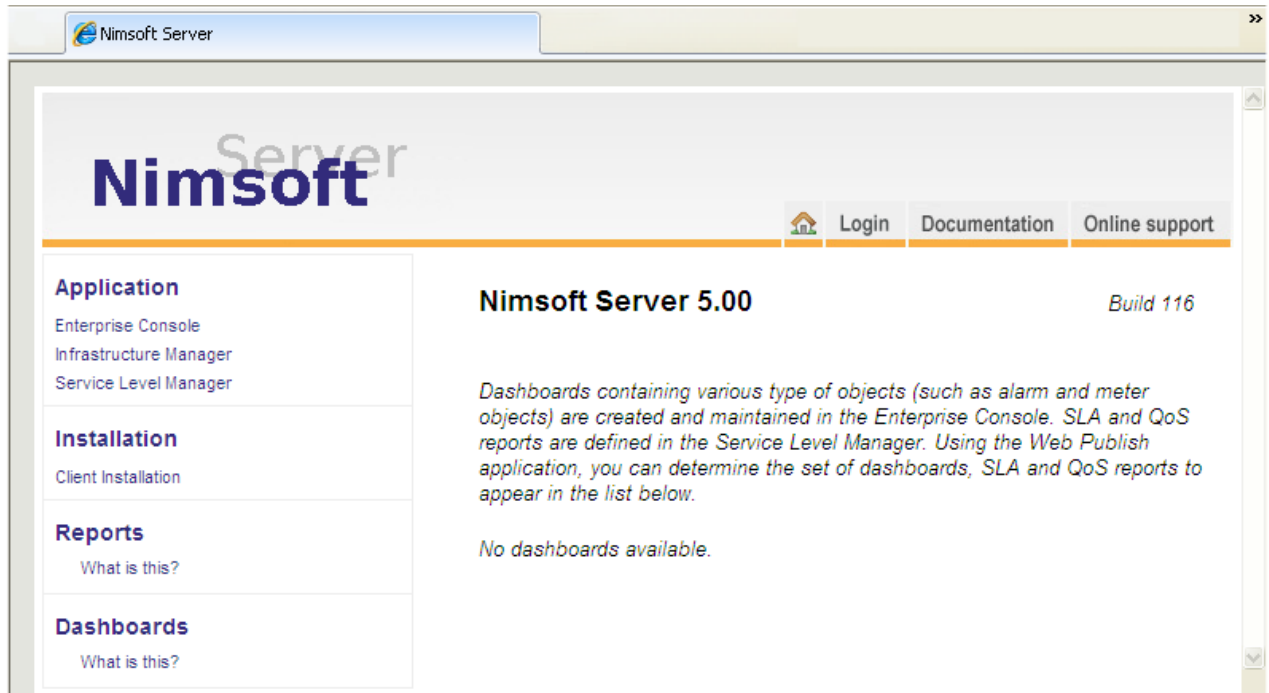
Chapter 3: Accessing Nimsoft Server

Introduction

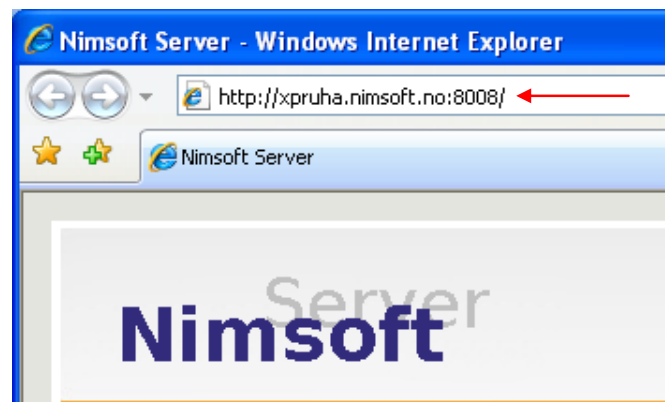
When the Nimsoft Server installation is completed, you may start it by clicking



the icon created on your desktop.



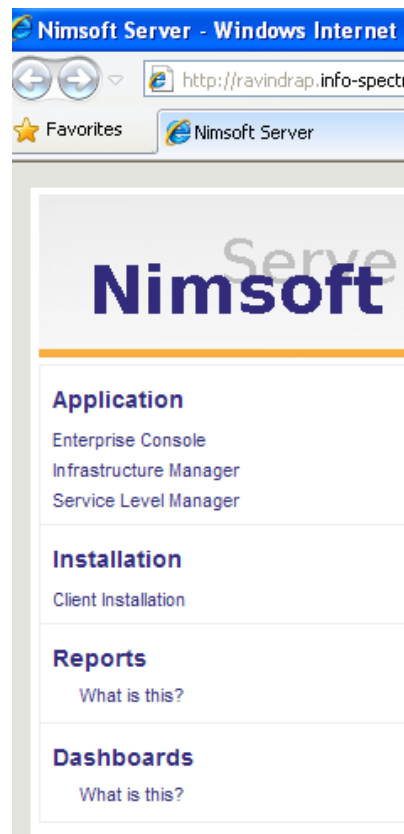
Note the address in the browser's address field. Use this address in the address field of the web browser when accessing *Nimsoft Server* from your other computers.



Using a web browser, you may access the Nimsoft Server from ANY computer on your network.

From this page, you may now perform a lot of tasks:

The menu bar located in the left part of the window:



- Launch Nimsoft applications.
 - Infrastructure Manager
 - Enterprise Console
 - Service Level Manager
- Install Nimsoft Software on clients.
- Launch Dynamic Reports, generated (as an option) by the Report Engine probe.
- Launch Dynamic Views dashboards, gathered from the Enterprise Console. These dashboards are populated with QoS data organized by the new Group Server probe.
- Access Nimsoft Documentation.

The main window:

- Access html files that are links to Nimsoft consoles, dashboards, SLA reports and QoS Reports, made accessible using the Web Publish application, using target ACL Default (ACL = Access Control List). These are listed in the main window.

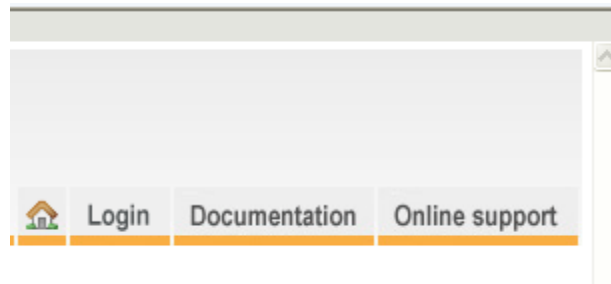
If you are not already logged on, you will be prompted for a valid Nimsoft user name and password when attempting to access one of the dashboards or reports.

Note:

When publishing dashboards and consoles, it is also possible to specify default login parameters. These parameters will appear in the login dialog when logging on.

When published (from the Web Publish application), consoles, dashboards and reports are organized in a way that gives different users different access privileges. That means that some files (those not published using target ACL Default) are hidden from the first page. In order to access these files, you have to click the User login link (see the section [Accessing ACL protected dashboards](#)).

The tool bar in the upper right corner:

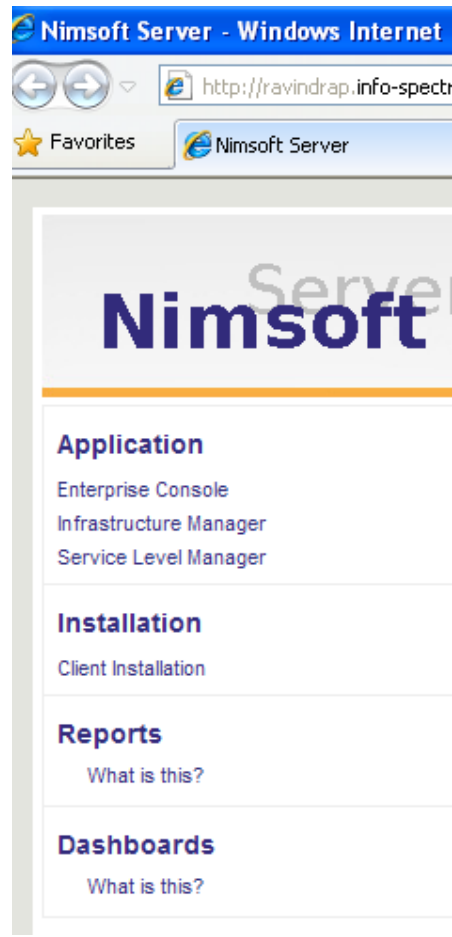


- A Home button, taking you back to the initial home page as it appears at application start-up.
- A documentation link, opening the Nimsoft Server on-line help documentation in a separate window.
- A link to the Nimsoft Online support. Clicking this button opens the Nimsoft Technical support site in a separate window.

Modifying the layout of the menu bar

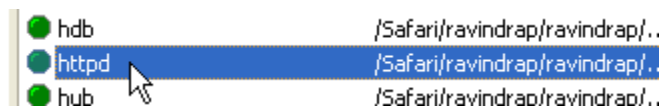
The menu bar located in the left part of the window by default contains four sections:

- Application
- Installation
- Reports
- Dashboards

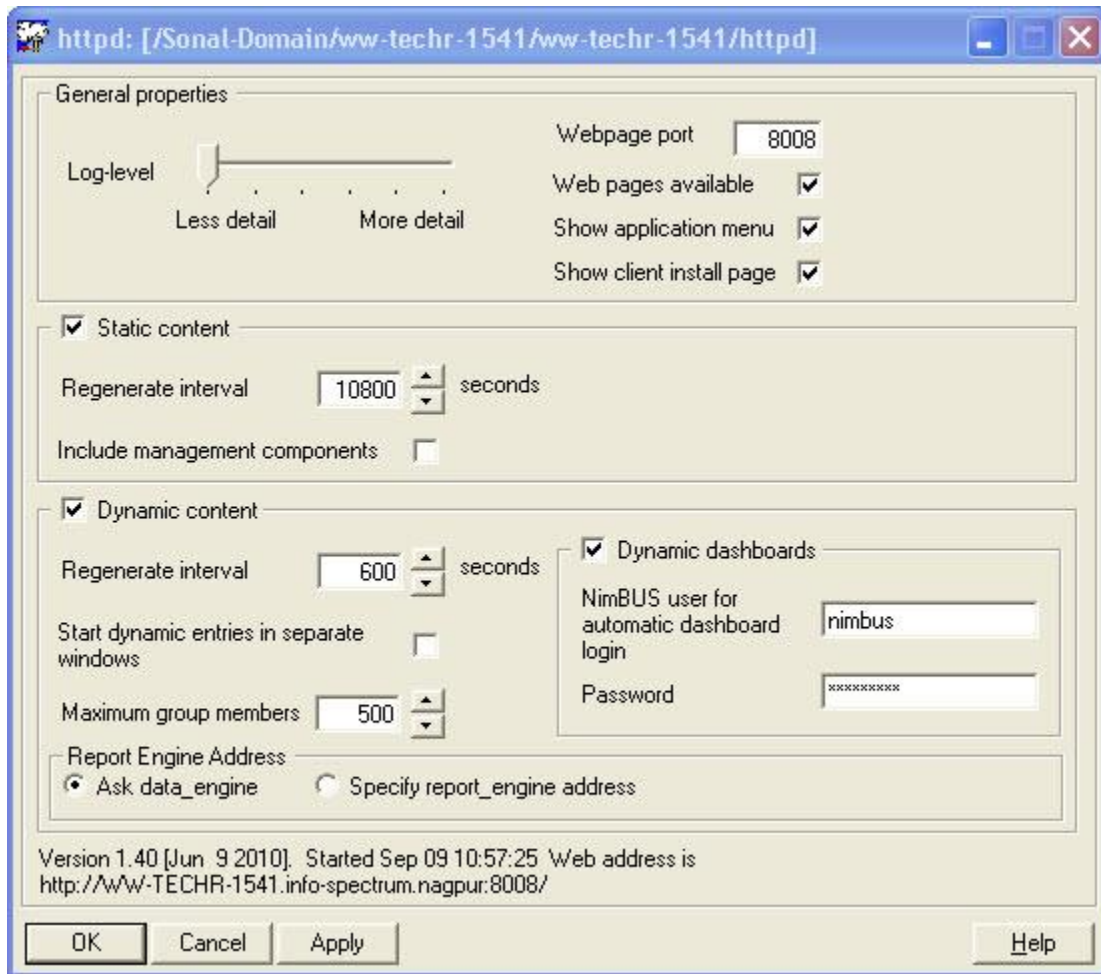


You may hide one or more of these sections from the menu by configuring httpd probe on the computer running the Nimsoft Server software.

With the Nimsoft Server application window opened in your web browser, double-click the httpd probe in Infrastructure Manager on the computer running the Nimsoft Server software.

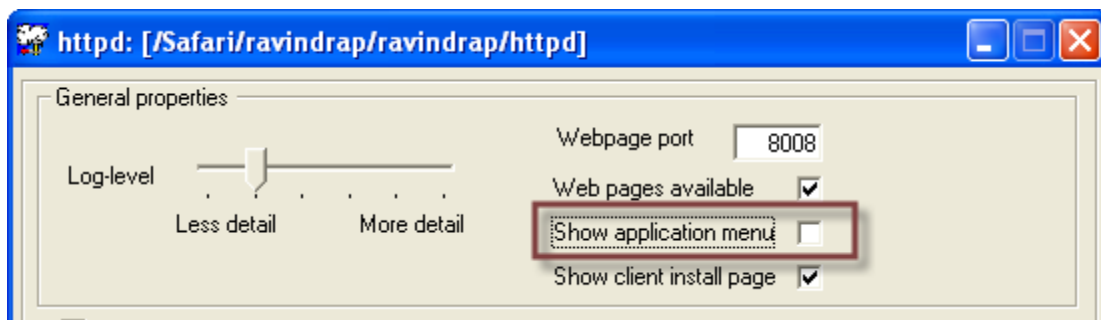


This brings the configuration tool for the probe.



Removing the *Application* section from the menu:

Deselect the *Show application menu* option and click the *Apply* button.

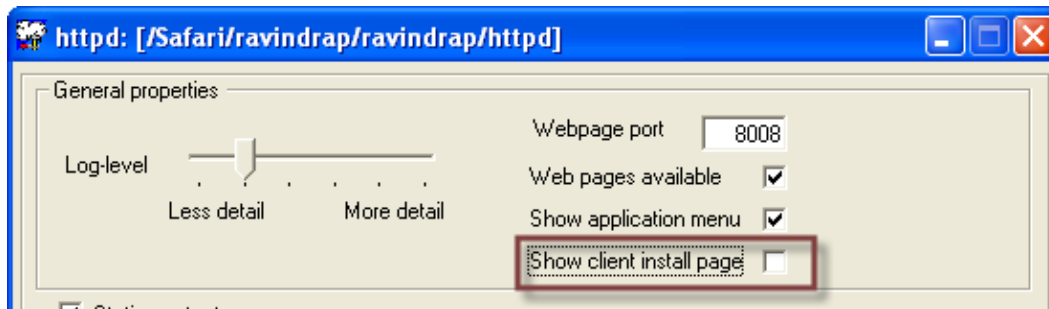


Now click the *Refresh* button in your browser and verify that the *Application* section is hidden from the menu.

Select the option again if you want the section to be shown again.

Removing the *Installation* section from the menu:

Deselect the *Show client install page* option and click the *Apply* button.

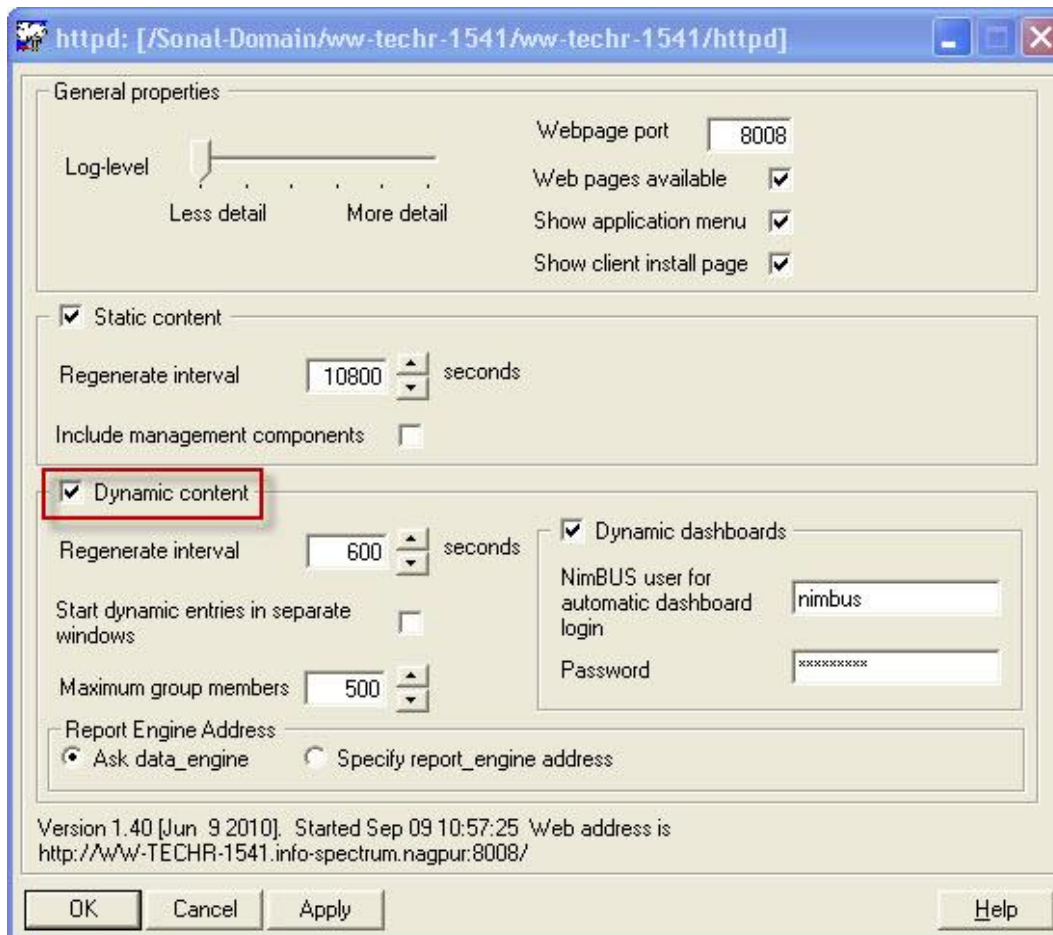


Now click the *Refresh* button in your browser and verify that the section is hidden from the menu.

Select the option again if you want the section to be shown again.

Removing the *Reports* and *Dashboards* sections from the menu:

Deselect the *Dynamic content* option and click the *Apply* button.

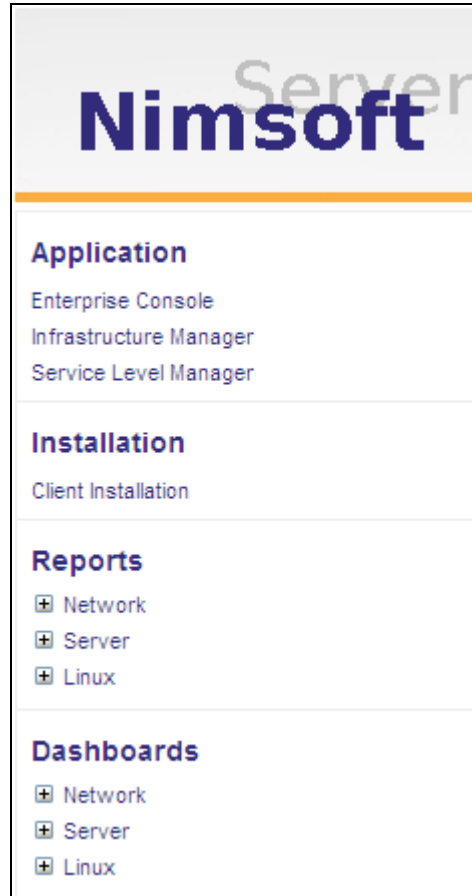


Now click the *Refresh* button in your browser and verify that the section is hidden from the menu.

Select the option again if you want the section to be shown again.

Browser Setup

Depending on the browser on the computer, it may be necessary to do some configuration in the browser setup to be able to activate the options in the left pane of the Nimsoft Server window.



If nothing happens when left-clicking these options, you should do as described below:

1. Select the Tools > Internet Options Menu item in your browser.
2. Enter the Security Tab and select Trusted sites.
3. Click the Sites button and add the URL you found in the first step. Uncheck the https requirement and click OK.
4. Verify that the security level for Trusted sites is set to Low.

Chapter 4: Planning your installation

Introduction

This chapter contains a brief introduction to the Nimsoft Infrastructure. For further information, see the User Guide sections in the on-line documentation for:

- Infrastructure Manager
- Enterprise Console

This documentation will be available when installing the Enterprise Console and Infrastructure Manager.

Planning and Establishing your Infrastructure

Defining your goals

The Nimsoft concept reduces the technical challenges of installing the Nimsoft products and making your computers communicate to a minimum. Your challenge is to create a setup which is useful in your organization. Nimsoft products are designed to grow, and the product itself puts no limits to how the solution evolves. And, even if strategies are changed and the Nimsoft Domain has to be completely redesigned, it's far less work than with most of the other competing products. However, as always when designing a complex system: a good strategy from the start helps you keep in control, even when things start evolving and growing fast. You should ask yourselves these questions:

- What are your short- and long-term goals? Will your Nimsoft installation be an enterprise-wide, strategic infrastructure, or will it be a narrow solution for just one application on a few systems? If narrow at the start, do you want to plan for the possibility that it will grow in the future?
- Understand the applications you plan to use. Some applications can easily co-exist in one common infrastructure, while others will be better off with a complete infrastructure on its own.
- What computers should the Nimsoft product be installed on? Check that you have enough licenses and that all platforms are supported with Robots and the probes you need for the solution.
- What other messaging environments should your Nimsoft Infrastructure be integrated with? Does Nimsoft provide a suitable gateway, or should you have one developed?

- How critical is it that the Nimsoft messages can be delivered at all times, even in periods with network problems? Do you need a fault-tolerant configuration?
- Who will need to be trained in Nimsoft Architecture issues, the application's you will be using, and (possibly) probe development? What GUI tools will these users need and what computers will they need them installed on?

What domains do you need?

In most sites, this answer is simple: You need one Domain, and we recommend that you name it after your company. The picture can be more complicated, though:

- If you use Nimsoft products in an outsourcing context where you manage systems in many companies from one workstation, it will be more logical to define one Domain per company.
- If you have more than one Nimsoft-based application installed and you feel that they should be treated as two different "worlds", either because they are managed by different operators, managing entirely different computers, or, simply because you feel it "feels more right".
- Even if you have only one application, but still have two different organizational units managing different areas (for example: a Alarm site in a big corporation with dedicated IT operations staff within each department or subsidiary), it may be a good idea to group the robots or hubs in one Domain per organizational unit.

As you may understand, there is no definitely "right" way of doing this: it is more a question of what gives the most logical grouping for the users. In later versions of Nimsoft, it will be possible to set security restrictions on the Domain level, so you might also keep that in mind when selecting the Domain structure. Anyway: a good, descriptive (but not too long) name is essential!

Where do you need hubs?

A Hub represents a connection point for a group of robots, and in the addressing scheme it represents the second level in the hierarchy after the Domain. In a small site with one LAN, just a few robots and no special need for fault-tolerance, the answer is simple: you need one Hub, installed on the machine which is least likely to go down. In a larger environment, things get trickier.

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.

Things to consider when deciding the Hub configuration in a large site are:

- In a WAN, we recommend that you have at least one Hub per LAN, or per subnet if the LANS are sub netted. This is not mandatory, but there is more network traffic between the Hub and the robots connected to it than between Hub's. The connections between Hub's are also more configurable in terms of controlling the network bandwidth consumption. It therefore makes sense using the Wan links for Hub-Hub connections only.
- If the subnets are separated by firewalls, having one Hub in each subnet reduces the number of nodes which must be accessible for traffic within the secured zone to one, reducing the security risk and the complexity of the firewall configuration to a minimum.
- If you have different Nimsoft-based applications in your network, you may want to have different hubs for different applications. This is a good idea if you need different administrators to administer each application. Otherwise, it is probably better to set up one common infrastructure for all applications.
- If you have many robots in the same LAN, it may also be wise to divide them between different Hub's, for example based on the department the users work in. This can also be a good idea if you need to limit the access to the robots based on organizational boundaries, for example to have different Nimsoft administrators in different departments.

The Hub should get a name reflecting the choices you have made above. It is usually not a good idea to use the node name of the computer where the Hub is installed as the Hub name. The reason for that is that the Robot is automatically assigned the node name. Thus, you may confuse the Hub and the Robot unless you choose another name for the Hub.

Planning and Establishing your ALARM Installation

Defining your goals

Nimsoft Alarm is an application for informing the right person in the organization about symptoms to error situations on the critical computers in a network. So, the first thing to do is to get to know the organization: who is "the right person", what do you regard as "error situations" and "critical computer?" Ask yourselves these questions:

- Who are the right persons to inform about problems?
For example, does the organization have a help-desk which is always manned, or should you direct the alarms to one or more "personal" PCs in the network?
- How would they like the alarms delivered?
As list items in a Windows GUI or WEB page, as SMS messages to a GSM phone or an E-mail?
- Very often, the answer to the above question is "all of the above, depending on the type of error, time of day, day of the week etc." If so: what are the exact rules to program into the solution?
- What other management solutions should the Nimsoft product be integrated with? Does your organization use a management framework such as CA Unicentre or HP Openview?
- What computers need to be monitored, and for what types of errors? Does Nimsoft (or your vendor) provide standard product covering all these needs, or should you consider developing your own probes?
- Are alerts presented in a MS Windows console application enough for your needs, or do you need forwarding mechanisms to other technologies, such as pagers, WEB-pages, E-mail or mobile phones? If so, do you need any kind of filtering of what alerts are forwarded when and where?
- How important is it that your Domain keeps working in case of a network failure? Do you need to implement alternative routes and fail-over solutions?

Planning the Infrastructure

Planning an infrastructure for Nimsoft Alarm is not very different from planning an infrastructure for any other Nimsoft-based application. This is covered in the section [Planning and Establishing your Infrastructure](#). The only additional concern on the infrastructure level is the Alarm Server probe(s).

Where do you need nas probes?

Each nas contains a database of received alarms. When a console application is opened, it connects to one nas and displays the contents of the database found there. Therefore, the answer to this question is:

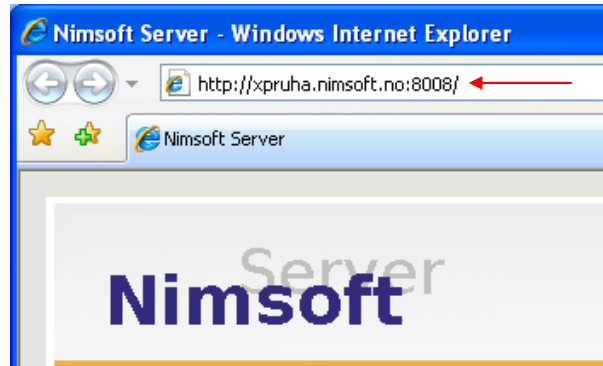
- If you want all users to see all alarms, it is best to have only one nas. If you want to feed different alarms to different users, you need a configuration with one nas per group of identically treated users.

The nas is always installed on the same computer as a Hub.

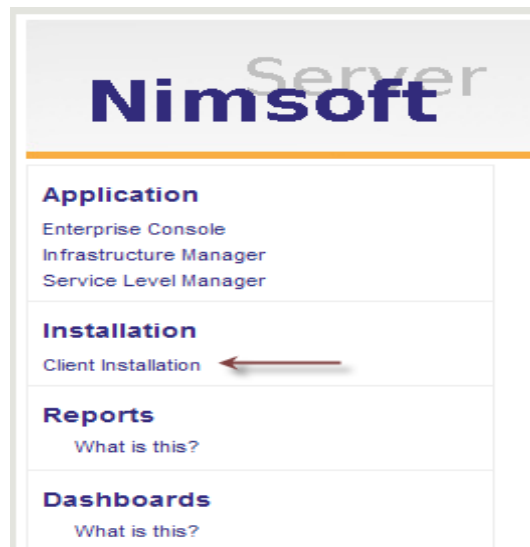
Chapter 5: Client Installations

Introduction

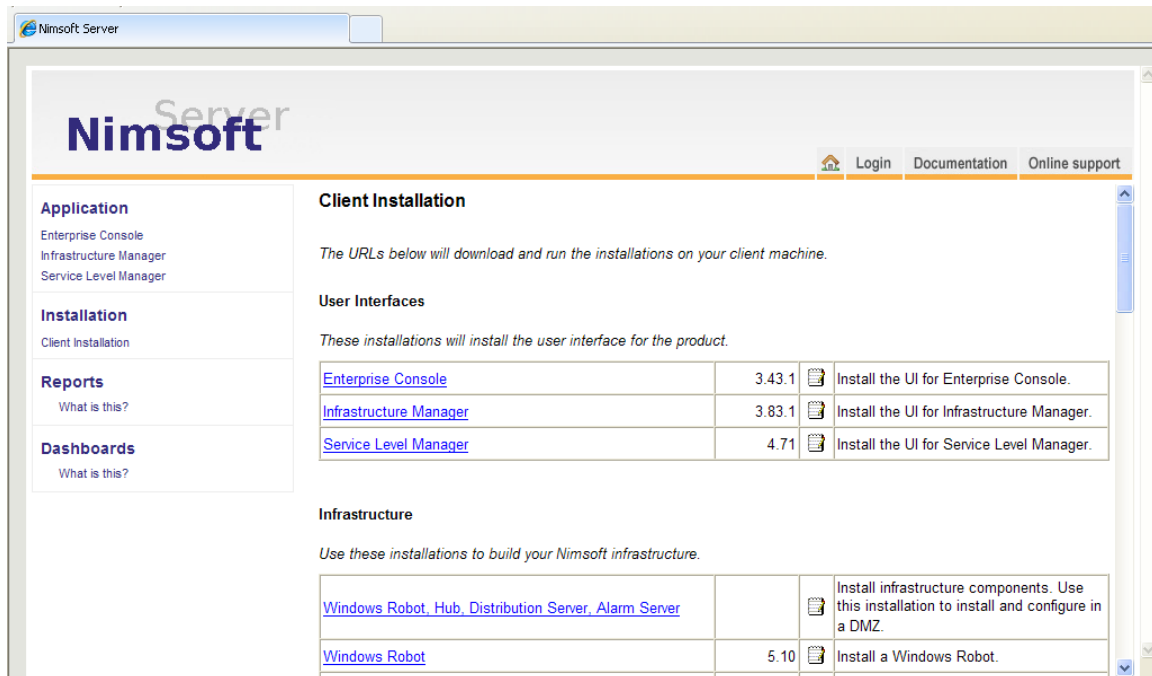
To install Nimsoft Software on a client computer, you access Nimsoft Server from the client computer by entering the address in the browser's address field.



Click the *Client Installation* icon in the left pane of the window.



The *Client Installation* section will be launched in the main window, enabling to select the product you want to install.



The products are divided into four groups:

- **User Interfaces**

The user interfaces are:

- **Enterprise Console**

An advanced user interface to alarms generated by Probes in your IT infrastructure.

You can also create and view complex graphical Dashboards to get the best possible hierarchical overview of the current alarm status.

Installation dependencies:

The Enterprise Console may be installed and run stand-alone on any windows-based computer in your network, but as you have to log onto a Hub at application start-up, Nimsoft Infrastructure must be installed on the same computer or another windows-based computer in your network.

- **Infrastructure Manager**

The Infrastructure Manager user interface manages the Nimsoft Infrastructure and provides monitoring and management solutions for systems, applications and networks.

Installation dependencies:

The Infrastructure Manager may be installed and run stand-alone on any windows-based computer in your network, but as you have to log onto a Hub at application start-up, Nimsoft Infrastructure must be installed on the same computer or another windows-based computer in your network.

- **Service Level Manager**

The Service Level Manager enables administrators to quickly define Service Level Agreements between the client and the service-provider and to generate QoS and reports.

Installation dependencies:

The Service Level Manager may be installed and run stand-alone on any windows-based computer in your network.

Nimsoft Infrastructure must be installed on the same computer or another windows-based computer in your network

- **Nimsoft Infrastructure**

The Nimsoft Infrastructure is divided into several parts:

- ***A package containing Nimsoft Infrastructure components:***

This package consists of the following products: Windows Robot, Hub, Distribution Server and Alarm Server.

The package also contains the DMZ wizard component. This wizard sets up a tunnel between the intranet behind the firewall and the DMZ server.

Installation dependencies:

Nimsoft User interfaces must be able to connect to the Nimsoft Infrastructure. The Nimsoft Infrastructure package must therefore be installed on the same computer as the Nimsoft User interface(s), or on another windows-based computer on the same network.

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.

- ***Windows Robot***

Installation dependencies:

The Windows Robot must be installed on all windows-based computers where you want to distribute Probes.

Nimsoft Infrastructure (nimldr) for all UNIX platforms.

Here you can download the nimldr, which contains the Robot software for UNIX-based computers.

- **Nimsoft Web Service**

The section contains the following two products:

- Microsoft .NET Framework ver. 2.0. This run time ***framework*** is a prerequisite to the web service installations.
- The WebService API, containing methods to retrieve data from and to perform a set of operations.

Installation Dependencies:

These installation packages integrate with a web-server, and need to be installed there.

- **Nimsoft Mobile Panels**

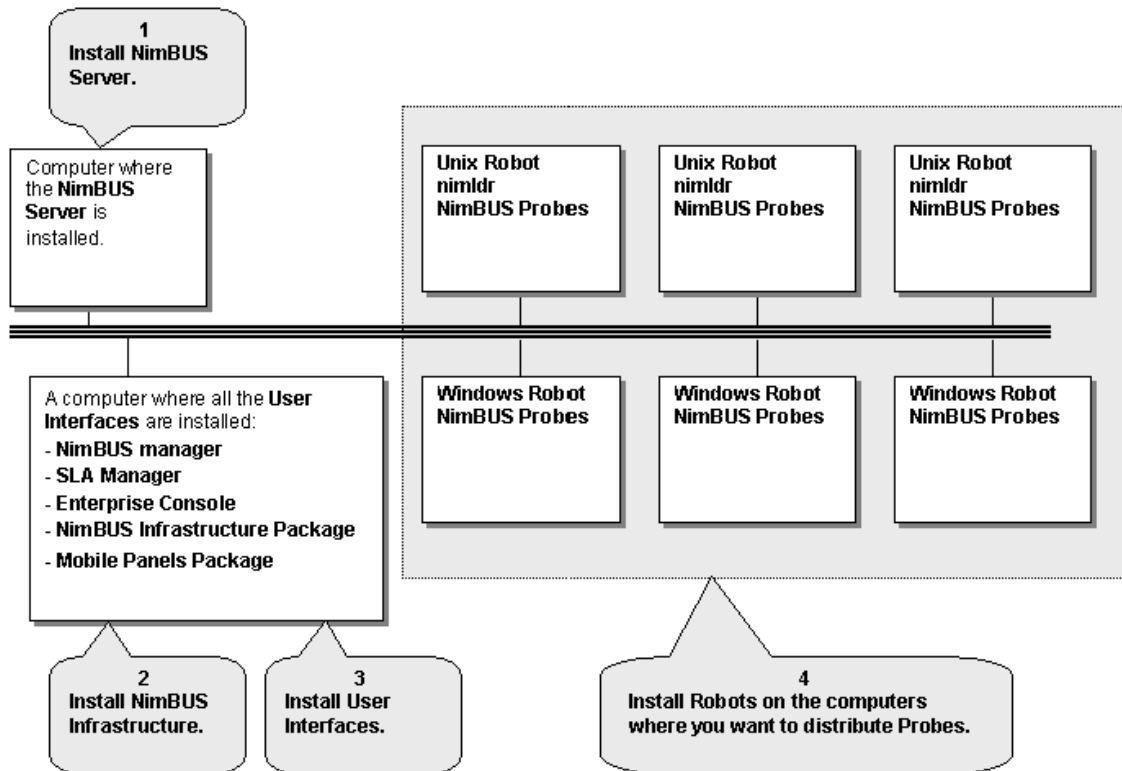
This section contains the 3 following modules:

- Microsoft .NET Framework ver. 1.1.
- Nimsoft Webservice for the Mobile solution.
- Mobile Panel Client

Installation Dependencies:

These installation packages integrate with a web-server, and need to be installed there.

Installation Example:



Installation in a firewalled environment

Introduction

This section describes the installation of Nimsoft components in a firewalled environment.

Note that if you are not required to set up an internet solution within a **demilitarized zone (DMZ)**, you may rather use internet solution with direct QoS Access. That means an open configuration with direct QoS data access will provide the best performance.

See the section [Rather use an open Internet solution with Direct QoS Access.](#)

Using the tunnel mechanism provided by the hubs, a secure connection can be set up between hubs located in the DMZ and hubs residing in the secure zone inside the DMZ firewall.

Computers in the DMZ can then be managed and supervised from inside the firewall. The Mobile Panels solution have provided a possibility to access the DMZ from the outside world, using mobile phones and gaining information about alarms and quality of service data from inside the firewall, using the secure tunnel connection.

This same mechanism is also the basis for setting up web dashboards in the DMZ. By opening a selected few ports in the outer firewall from the DMZ to the Internet, fully functional dashboards can be viewed in ActiveX supported web browsers.

Installing Nimsoft components in a DMZ

The installation of Nimsoft components in a DMZ is described in the sections [Installing Windows Robot, Hub, Distribution Server and Alarm Server](#) and [Installing Nimsoft Infrastructure on a Unix computer in a DMZ](#).

Rather use an open Internet solution with Direct QoS Access?

From a performance point of view, the most efficient way to access the QoS data is to process the database queries directly from the various dashboards and not through the use of tunnels. However, this solution requires you to open your port access to your SQL server and a number of other ports as well. The SQL server port is typically 1433, and the ports required to be opened are typically found within the range 48000 to 48020. Remember to configure the 'First Probe Port Number' parameter in the controller to ensure that Nimsoft components will be assigned port numbers beginning just after 48000. The Nimsoft components the open intranet/internet solution needs access to are the hub, controller, distsrv and nas.

What is a DMZ

The term DMZ comes from military use and is short for **demilitarized zone**.

In computer networks, a DMZ is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

Requests from the inside:

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Requests from the outside:

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data.

What is a tunnel

Most 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 is separated by a Firewall. The Tunnel sets up a VPN-like (**V**irtual **P**riate **N**etwork) connection between the two Hubs and enables all 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.

NOTE:

Do not use Static Hubs when setting up a tunnel!

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 spans 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.

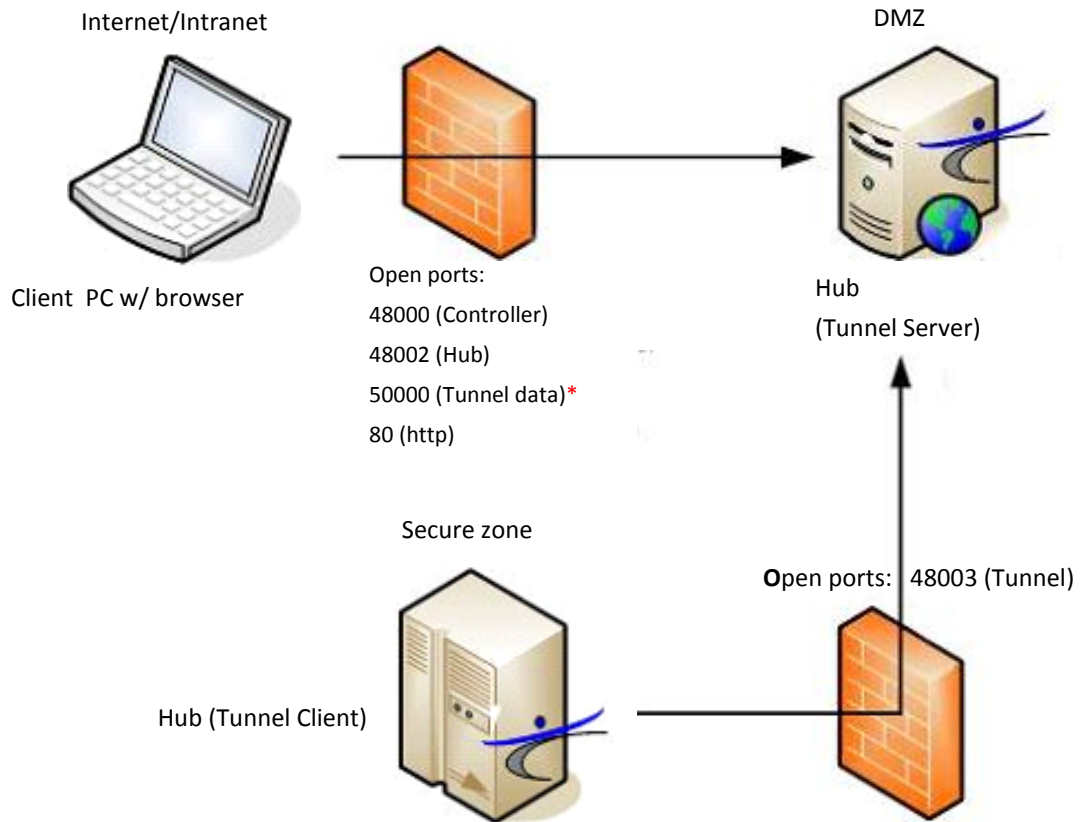
Installing Nimsoft in a firewalled environment requires that installation happen in a given order. There is also the issue of which ports to open in the different firewalls to allow users to access Dashboards and view web reports.

Installation order

The installation of Nimsoft components in a DMZ is described in the sections [Installing Nimsoft Infrastructure on Windows](#) and [Installing Nimsoft Infrastructure on a Unix computer in a DMZ](#).

The picture below shows the different components installed and the ports that need to be opened in the firewall.

Installation order can be as follows:



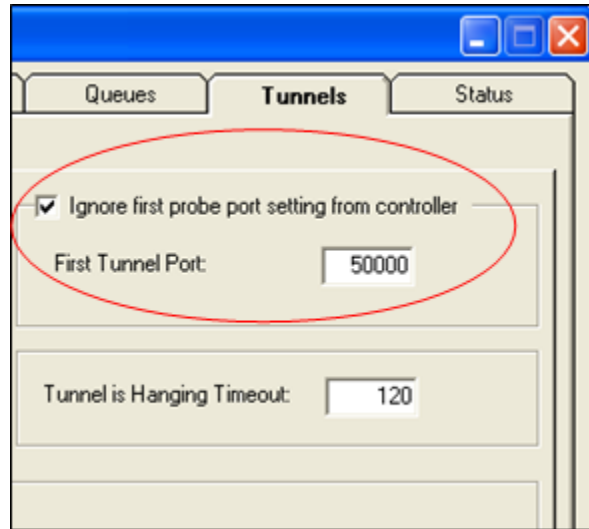
*) Port 50000 (Tunnel data) is the port the client connects to when attempting to send/receive data through the tunnel from the outside. In a default installation this port is randomly assigned by the OS. To control your tunnel data port range (if you want to send/receive data through the tunnels from the outside), you should set this port to e.g. 50000. This is done by setting the *First Tunnel port* to 50000 on the *Tunnels > Advanced* tab on the HUB GUI (see screenshot below).

Note that also the option *Ignore first probe port setting from controller* on the HUB GUI must be checked, even the first probe port not is set on the Controller probe.

Note

Logging on a HUB through a NAT'ed address is not supported in the Nimsoft consoles.

The HUB GUI, Tunnels > Advanced tab:



1. Secure zone

Nimsoft Server can be installed first. If you already have a running Nimsoft installation, this is already in place.

2. Firewall between Secure zone and DMZ

The Hub in the secure zone needs to be able to access the Hub in the DMZ on configured tunnel server port (default port 48003). How this is set up in the firewall is of course firewall dependant, and you should check your firewalls documentation on how to open a connection between the two systems.

3. DMZ

When installing Nimsoft components in a DMZ, you are given the option of installing in DMZ mode, as described in the sections [Installing Nimsoft Infrastructure on Windows](#) and [Installing Nimsoft Infrastructure on a Unix computer in a DMZ](#).

Once that is set up, you can generate a Client certificate for the Hub in the secure zone.

NOTE:

The hub in the DMZ must have a public IP address, if you want to access it from the Internet.

You now have an access point into Nimsoft installed in the DMZ. To allow people to connect to Nimsoft through this Hub you must allow traffic to some ports on the Hub computer in the DMZ.

Port 80 (http) is required if you want to give people access to web components like SLA reports and Dashboards. A web server like IIS or Apache can be used.

If you are allowing Dashboards to be accessed, you must in addition open port 48000 (Controller), 48002 (Hub) and 50000 (Tunnel data).

50000 is not a fixed port, you can set any port you want to use. Set up this port by setting the *First Tunnel port* to e.g. 50000 on the Tunnels > Advanced tab on the HUB GUI (see screenshot above). **Note:** Make sure the port selected is not in the same range as the port configured as *first probe port number* on the controller probe.

Note that also the option *Ignore first probe port setting from controller* on the HUB GUI must be checked, even if the first probe port not is set on the Controller.

Finally, after you have opened the external firewall for the listed ports, you must make Dashboards and SLA reports available on the DMZ system. This can be accomplished using the WebExport utility for Dashboards and by setting up an FTP profile in the SLA system.

Please note that users still have to log in to Nimsoft unless you specify user/password information in the Dashboard (in which case you should use an extremely limited user!).

Users should now be able to access Nimsoft content from the Internet or Intranet depending on how you set the system up.

Deploying dashboards to the DMZ web server

Use the Web Publish application to configure the html file containing the dashboard reference and also to deploy the files involved to the web server in the DMZ. Unlike the Nimsoft Server portal where dashboards appear automatically once they have been published from the Web Publish application, you need to determine where to put the dashboard related files on the web server and to also make sure you refer to them properly.

Note:

When using the Web Publish application to configure the html file containing the dashboard reference, note the *Quality of Service / Service Level Agreement* section in the properties dialog for the html file.

The screenshot shows the 'New Page' dialog box with the following configuration:

- Type: Dashboard Viewer
- Login: User, Password, Hub IP (empty); Encrypt:
- General: Dashboard: Example; Alarm Server: <default>; Dashboard Server: <none>; Archive Server: <default>
- Quality of Service/Service Level Agreement: Direct Database Access; Server Access; None; Data Engine: /HubTest/xprone/xprone/data_engine; QoS/SLA Server: /Development/mkilde/xpmoki/variable_server; Use default time zone for QoS graphs; Adjust for local time zone
- Appearance: Show Scrollbar; Show Statusbar
- Published Window Attributes: Width: 650; Height: 600; Always On Top

Select the *Server Access* option if you are going to deploy the html file to a web server in a DMZ.

From the *QoS/SLA Server* drop-down menu, select the *variable_server* on the Hub at the end of the tunnel (in the secure zone).

Next, set up an ftp site on the web server. Once this is done, exporting from the Web Publish will be a piece of cake. In the Web Publish, create a new Export Target referring to the ftp site on the web server.

Now drop the dashboard html definition you want to be accessible from the web server at the ftp export target node in the navigation tree. A dialog will prompt you for cab URL. You need to enter here the URL (absolute URL path or relative to the html file) where the necessary cab files are located on the web server. For instance, if the cab files are located in the dashboard\cab directory under Inetpub\wwwroot at the Nimsoft web server, the cab URL would be <http://www.nimsoft.com/dashboard/cab>.

From the destination ftp site on the web server, copy the html files to e.g. the Inetpub\wwwroot\dashboard directory and the cab files to the Inetpub\wwwroot\dashboard\cab directory.

To access the dashboards from the Internet, you will need to open some additional ports in the DMZ outer firewall (48000-48002). Once an Internet client accesses the html file, cab files from the web server will be downloaded to the client machine. Once installed the, Login pop-up box will appear, and you can log onto the domain that the DMZ hub is configured to be in. The hub tunnel through to the inner firewall will enable the retrieval of the dashboard archive package and also to update the dashboard properly once installed on client machine.

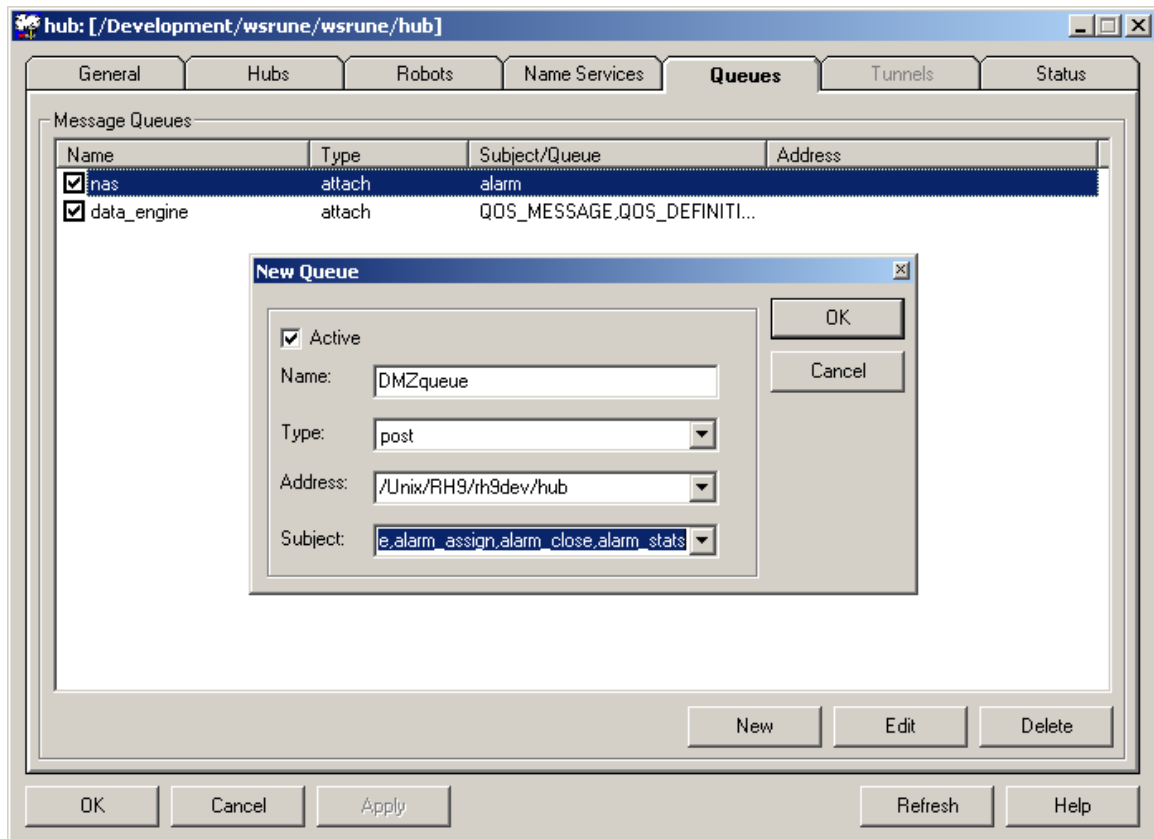
Enabling Dashboards in the DMZ to receive alarm events from the outside

To ensure that Dashboards made available in the DMZ system receive correct events from the outside, it is necessary to set up a *post queue* on the hub computer inside the firewall (on the computer where the tunnel ends).

This is done by opening the *hub configuration tool* from the Infrastructure Manager and selecting the *Queues* tab. Click the *New* button, and the Queue dialog pops up.

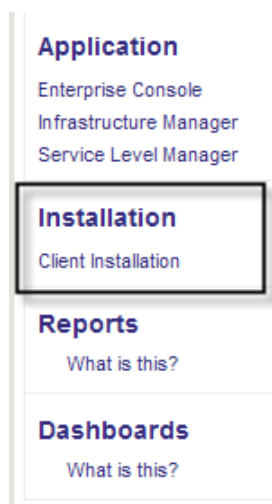
- Queue type:
Post
- Address:
The address of the DMZ hub (on the other side of the tunnel)
- Subjects:
alarm_new, alarm_update, alarm_assign, alarm_close, alarm_stats

Client Installations






Installing Enterprise Console

1. Start the installation procedure from the Nimsoft Server by clicking the Client Installation icon. The Client Installation section will be launched in the main window. Click the Enterprise Console link in the Client Installation section.



User Interfaces

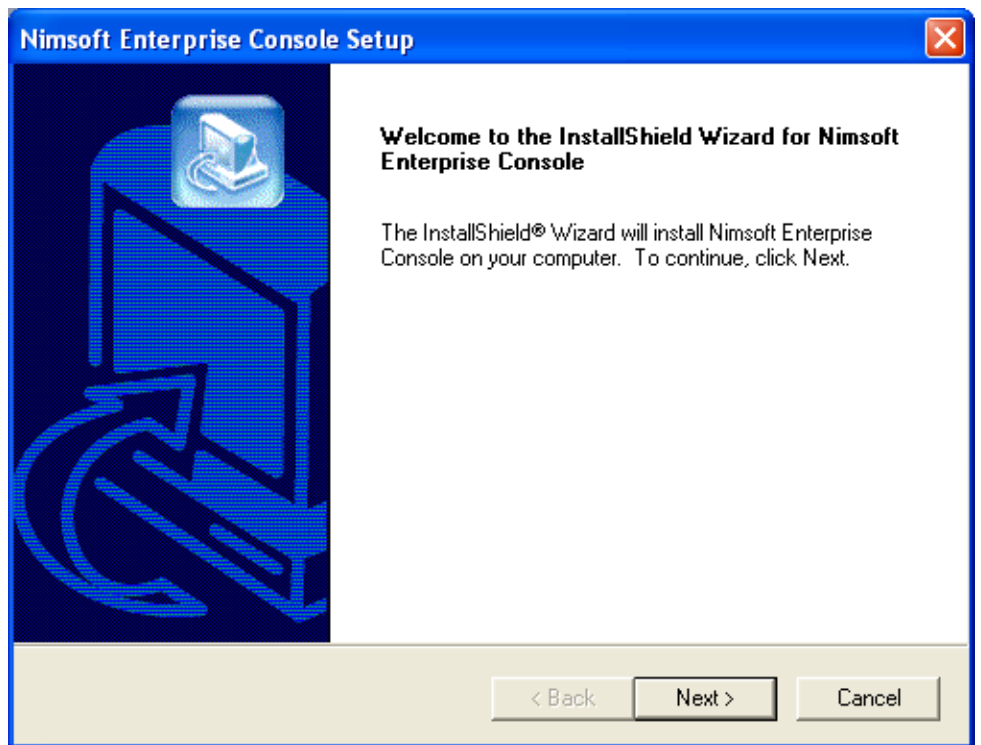
These installations will install the user interface for the product.

Enterprise Console	3.43.1		Install the UI for Enterprise Console.
Infrastructure Manager	3.83.1		Install the UI for Infrastructure Manager.
Service Level Manager	4.71		Install the UI for Service Level Manager.

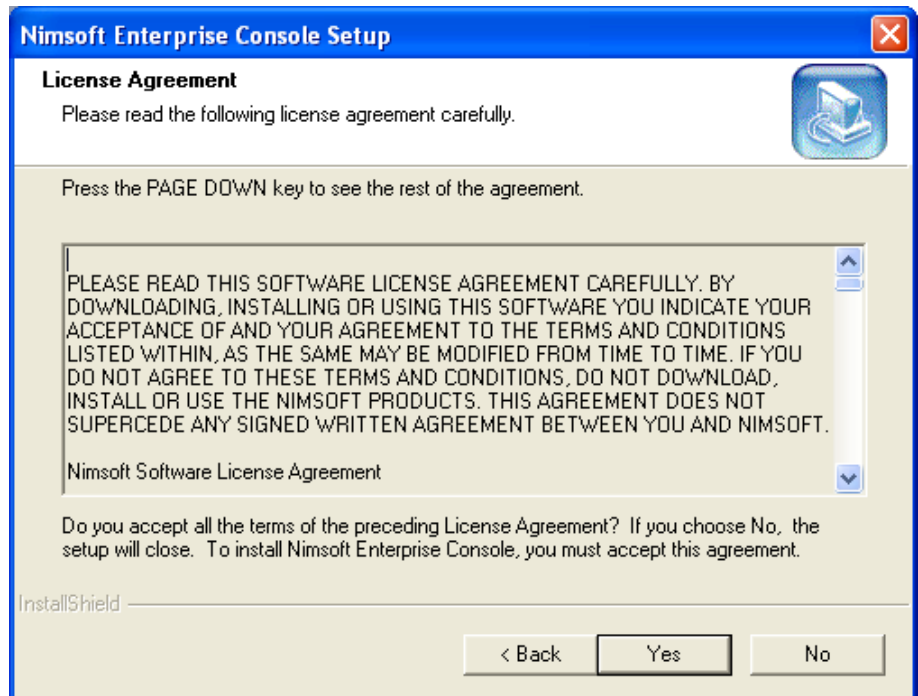
2. The download dialog pops up. Select Run to start the installation immediately (note that you may select Save if you want to save the EnterpriseConsole.exe file to disk and run the installation later).

The files are copied from the Nimsoft Server to your computer, and the wizard starts extracting the files.

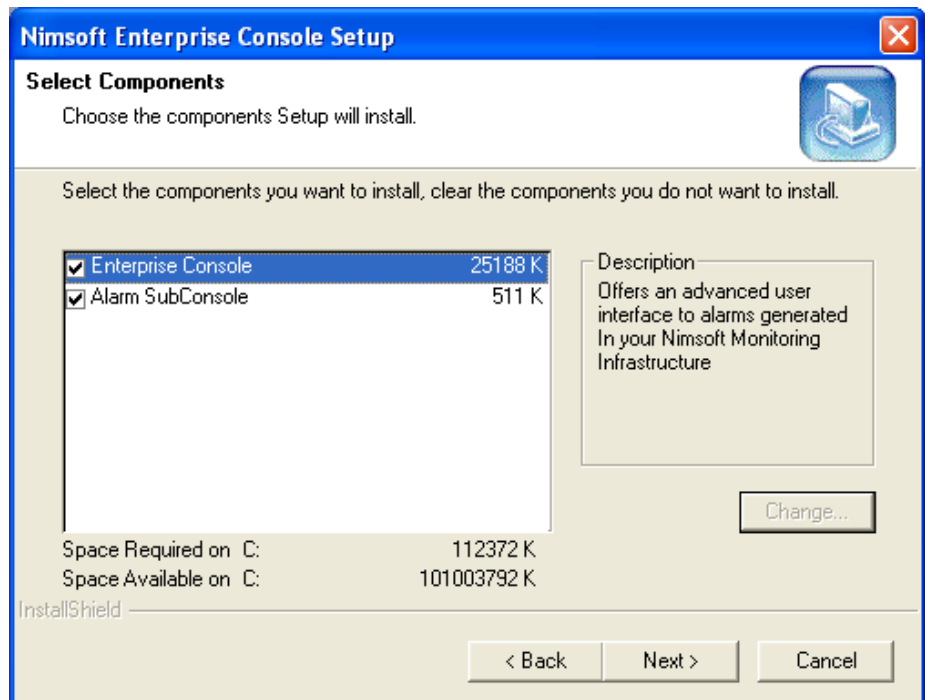
3. Wait for the following dialog to appear and click the Next button.



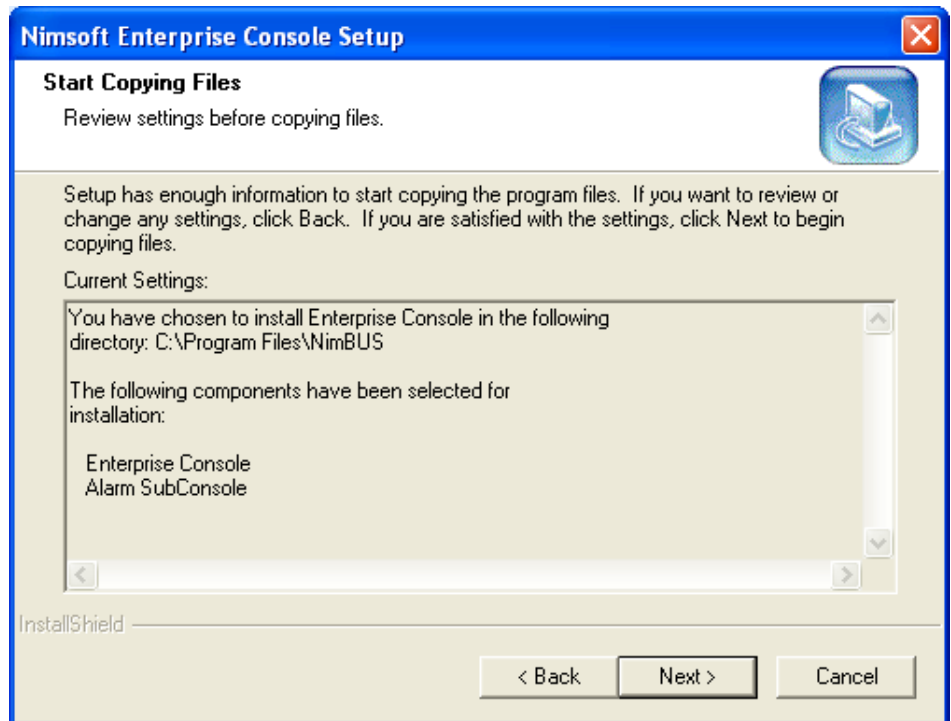
4. The License Agreement dialog appears. Read the license agreement carefully and click Yes to continue if you accept the terms, otherwise click No to exit.



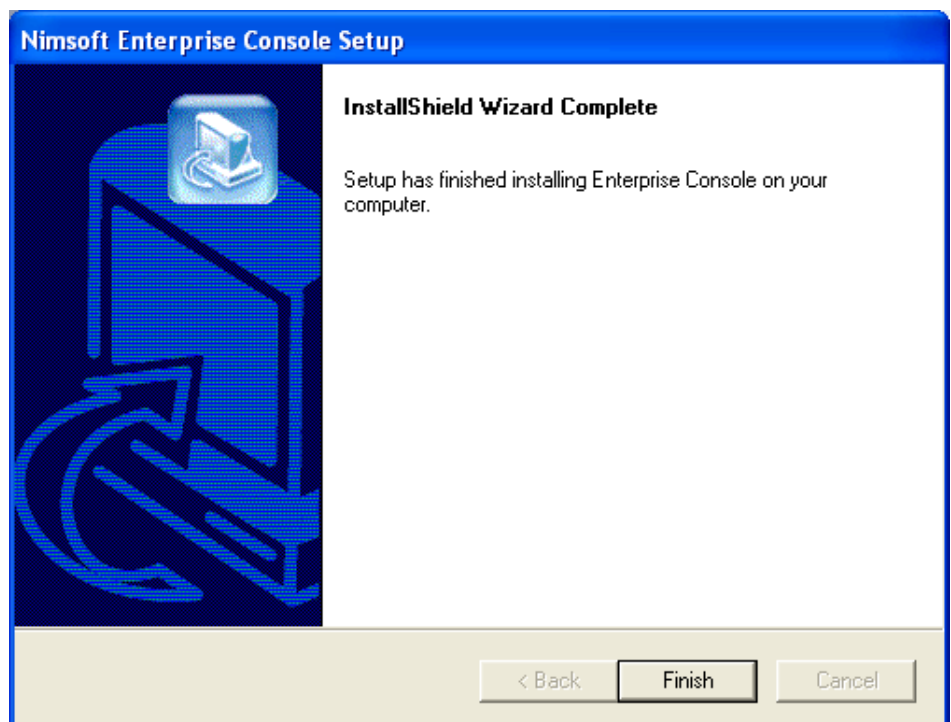
5. The next dialog enables you to select which components to install: The Enterprise Console and/or the Alarm SubConsole. Normally both should be installed. Ensure that the components you want to install are checked and click the Next button.



6. The next dialog displays the settings you have selected so far in the installation process. Click the Back button if you want to change something or click the Next button to start copying files.



7. A window appears, showing you the installation progress. Wait until the following dialog appears, confirming that the installation process is complete. Click the Finish button to exit Setup.






8. Verify that the installation was successful by launching the application (Start > Programs > Nimsoft Monitoring > Enterprise Console).

Installing Infrastructure Manager

1. Start the installation procedure from the Nimsoft Server by clicking the Client Installation icon. The Client Installation section will be launched in the main window. Then click the Infrastructure Manager link.

User Interfaces

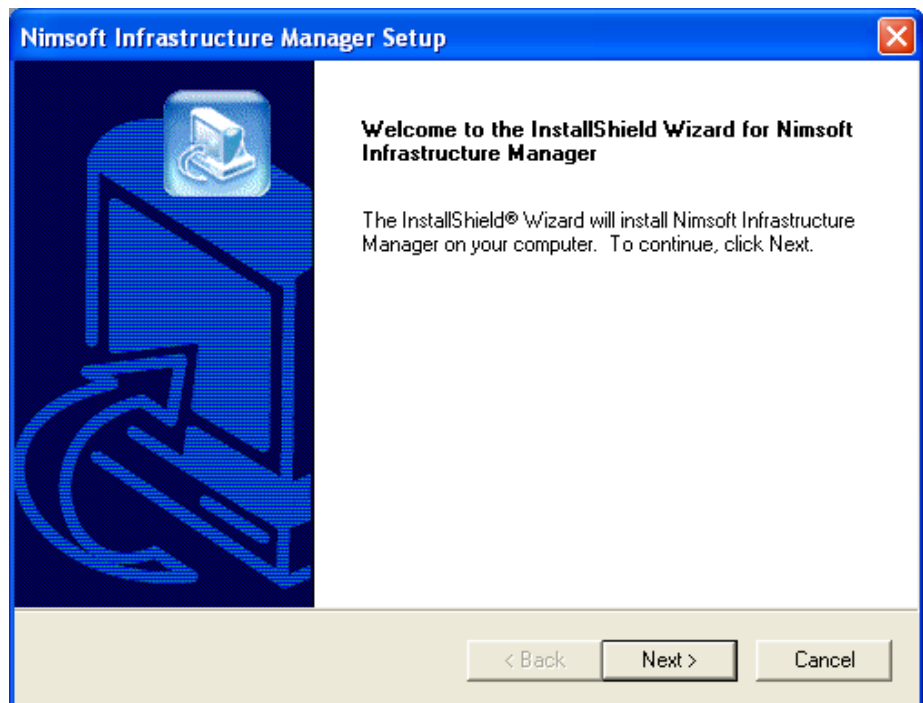
These installations will install the user interface for the product.

Enterprise Console	3.35.1		Install the UI for Enterprise Console.
Infrastructure Manager	3.75.1		Install the UI for Infrastructure Manager.
Service Level Manager	4.40		Install the UI for Service Level Manager.

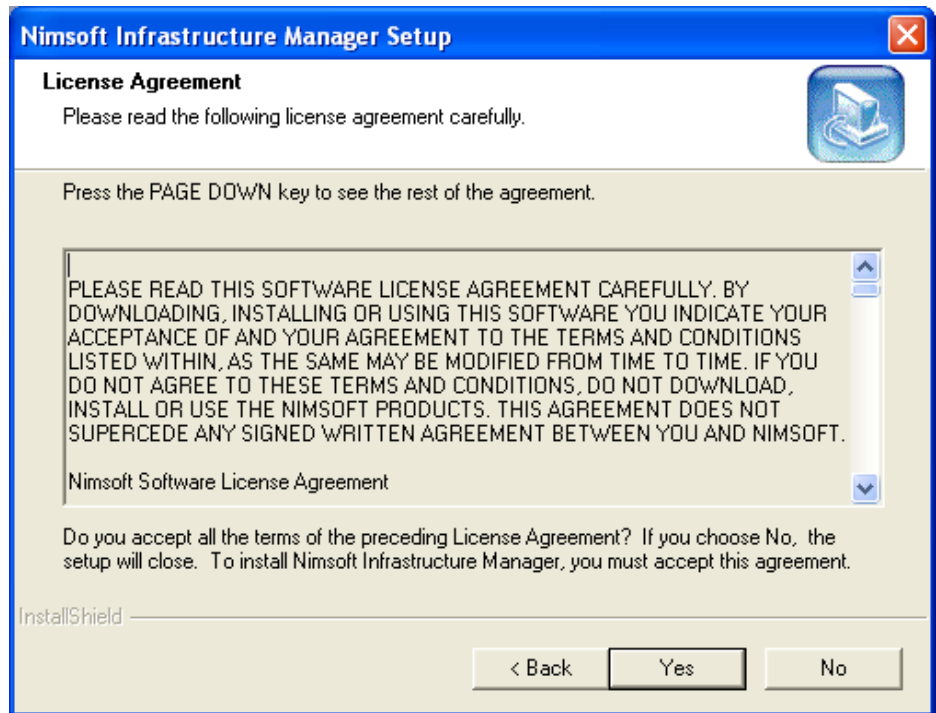
2. The Download dialog pops up. Select Run to start the installation immediately (note that you may select Save if you want to save the Infrastructure Manager.exe file to disk if you want to run the installation later).

The files are copied from the Nimsoft Server to your computer, and the wizard starts extracting the files.

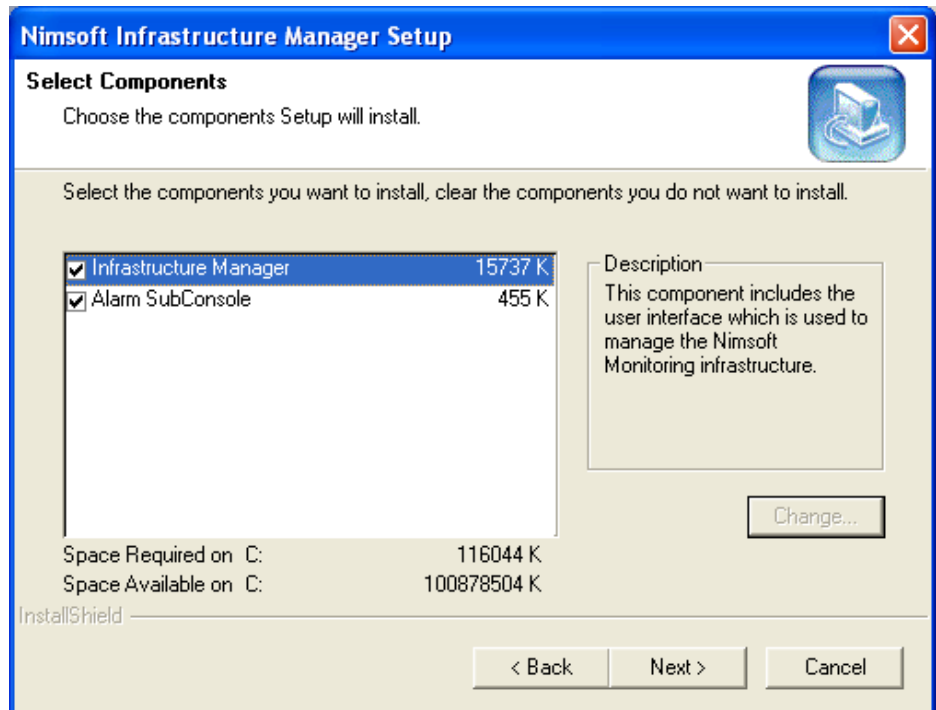
3. Wait for the following dialog to appear and click the Next button.



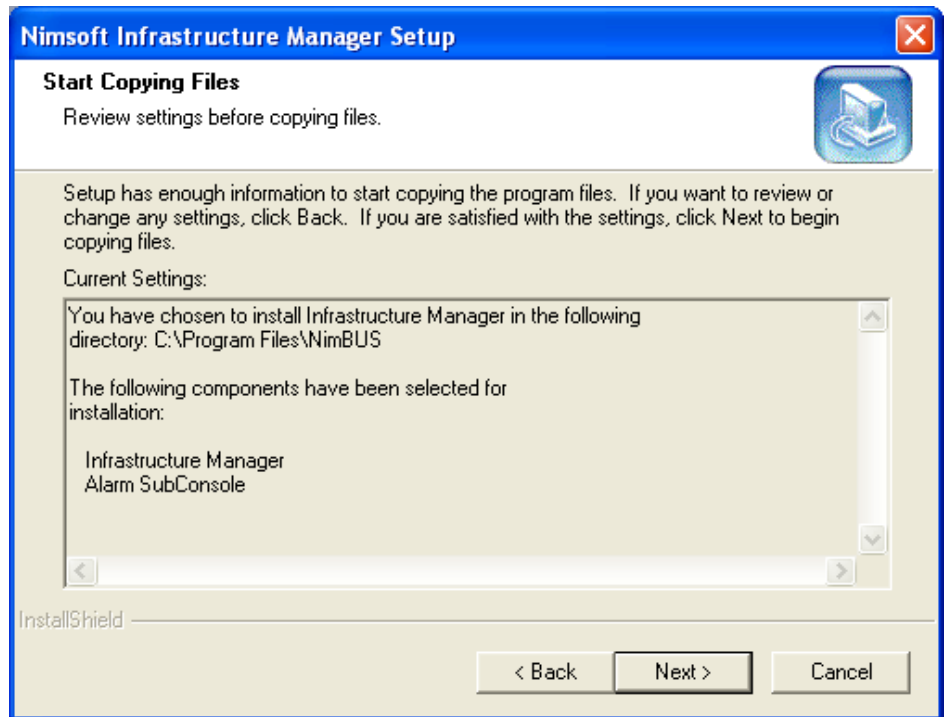
4. The License Agreement dialog appears. Read the license agreement carefully and click Yes to continue if you accept the terms, otherwise click No to exit.



5. The next dialog enables you to select which components to install: The Infrastructure Manager and/or the Alarm SubConsole. Normally both should be installed. Ensure that the components you want to install are checked and click the Next button.



6. The next dialog displays the settings you have selected so far in the installation process. Click the Back button if you want to change something or click the Next button to start copying files.



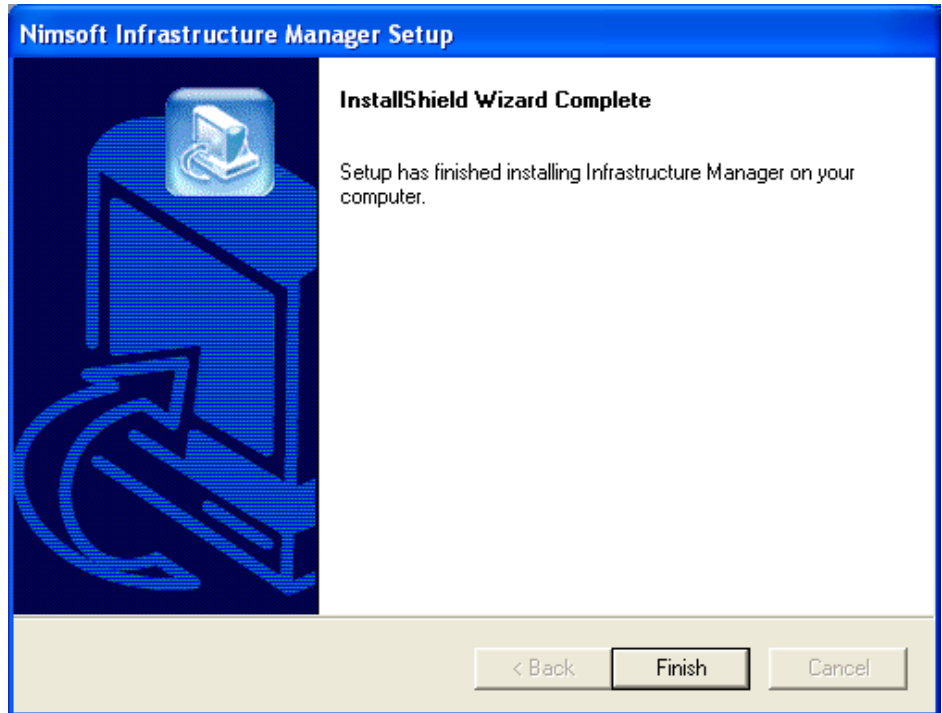
7. A window appears, showing you the installation progress. Wait until the following dialog appears, confirming that the installation progress is finished.

Infrastructure Manager requires the Microsoft SOAP Toolkit 3.0 to be installed on your computer.

If not already installed, you are asked if you want to install it.

Click the Yes button to launch the Microsoft SOAP Toolkit 3.0 Setup wizard. The wizard will guide you through the installation.

Finally, when the SOAP wizard is finished, click the Finish button to exit Infrastructure Manager Setup.






8. Verify that the installation was successful by launching the application (Start > Programs > Nimsoft Monitoring > Infrastructure Manager).

Installing Service Level Manager

1. Start the installation procedure from the Nimsoft Server by clicking the Client Installation icon. The Client Installation section will be launched in the main window. Then click the Service Level Manager link.

User Interfaces

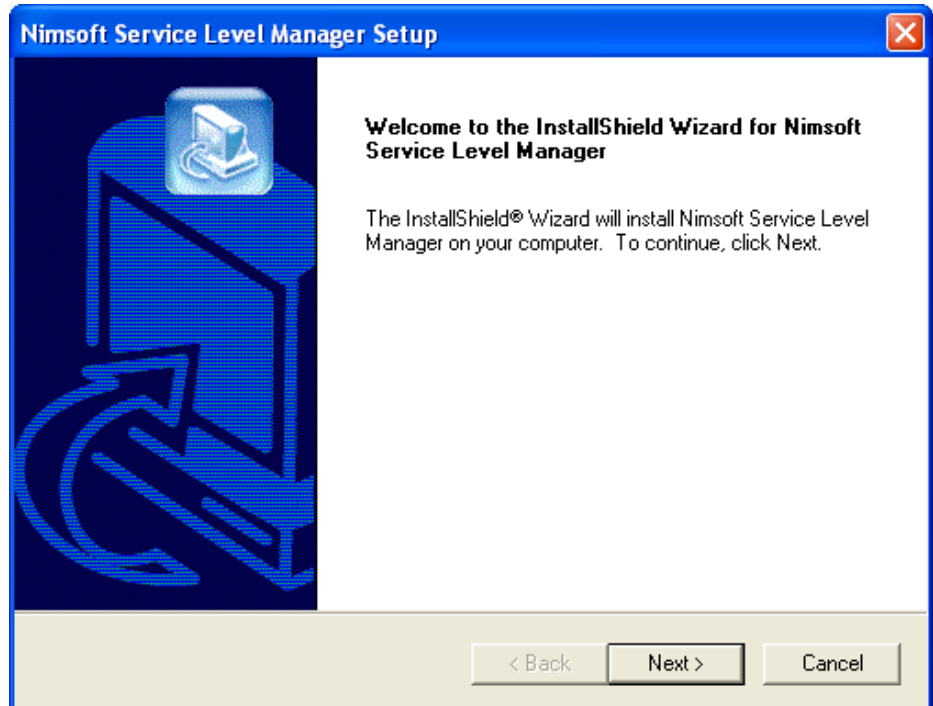
These installations will install the user interface for the product.

Enterprise Console	3.35.1		Install the UI for Enterprise Console.
Infrastructure Manager	3.75.1		Install the UI for Infrastructure Manager.
Service Level Manager	4.40		Install the UI for Service Level Manager.

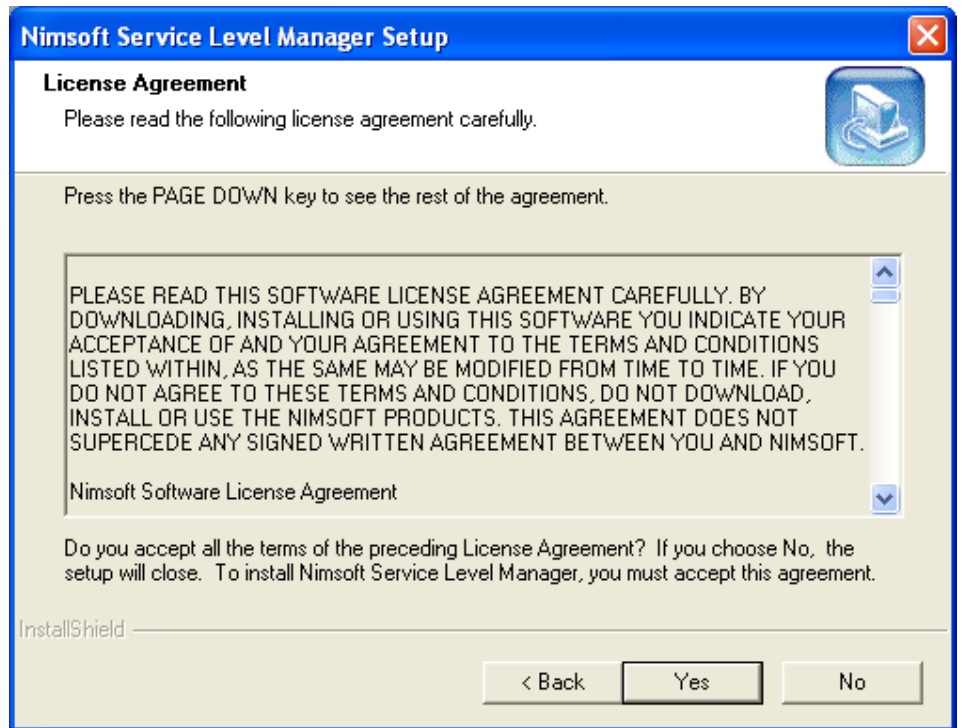
2. The Download dialog pops up. Select Run to start the installation immediately (note that you may select Save if you want to save the SLM.exe file to disk if you want to run the installation later).

The files are copied from the Nimsoft Server to your computer, and the wizard starts extracting the files.

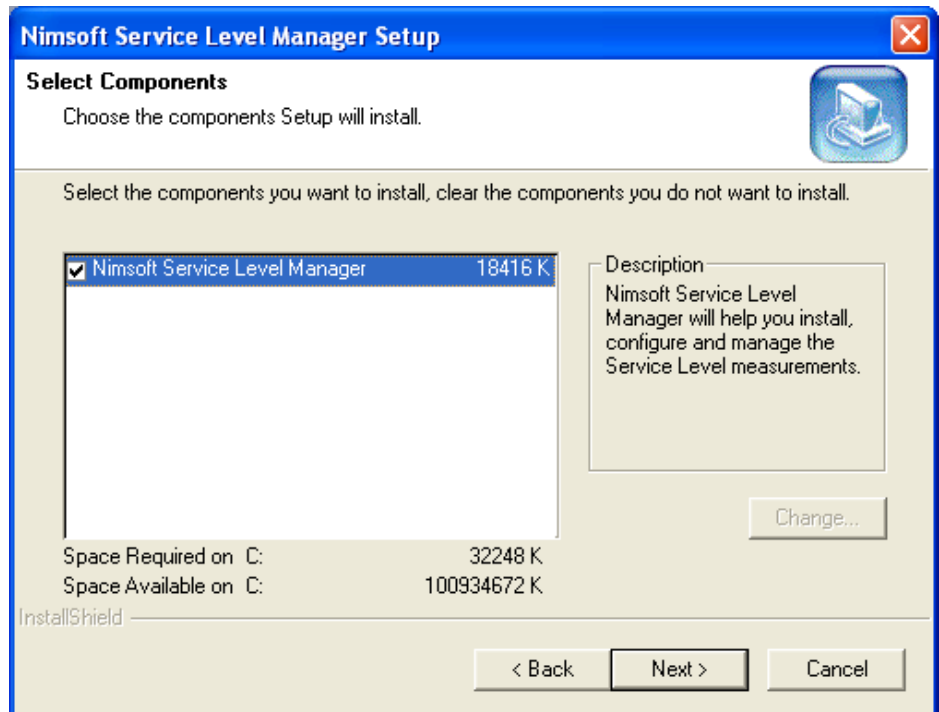
3. Wait for the following dialog to appear and click the Next button.



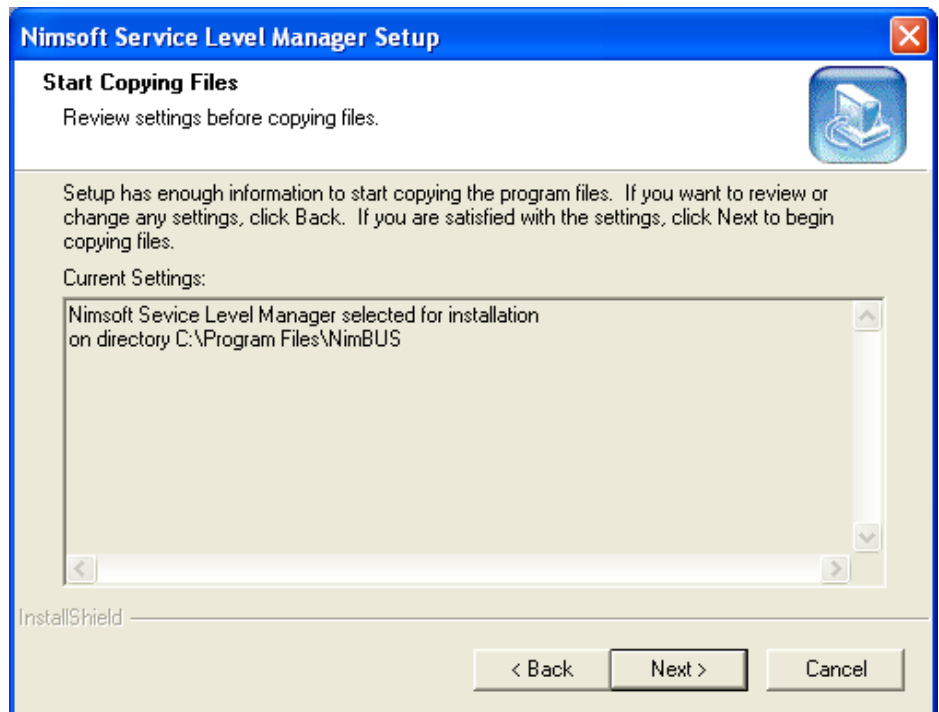
4. The License Agreement dialog appears. Read the license agreement carefully and click Yes to continue if you accept the terms, otherwise click No to exit.



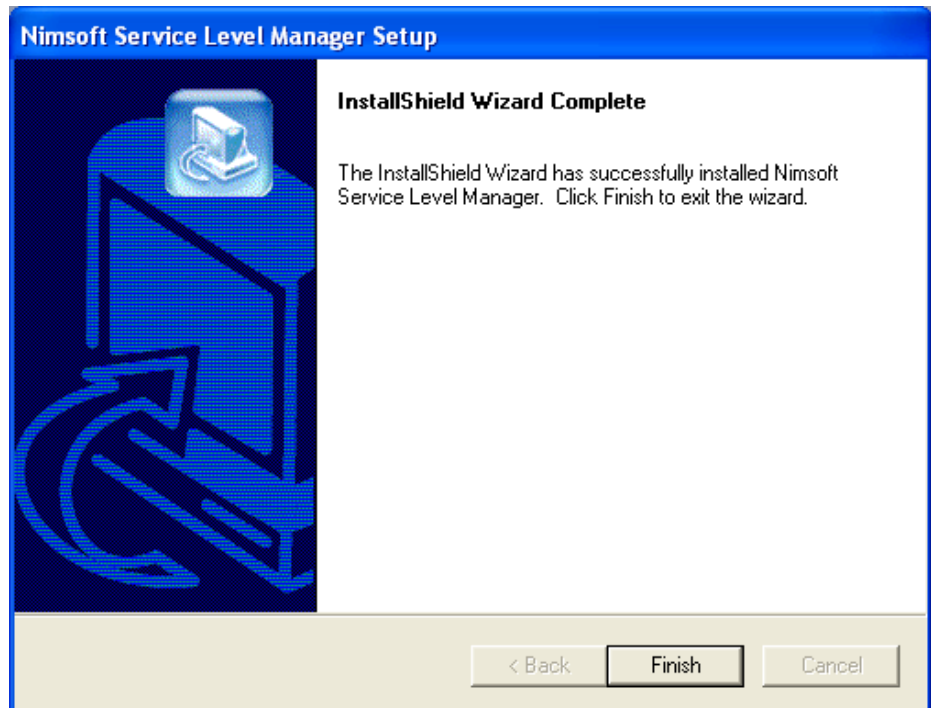
- The next dialog enables you to select which component(s) to install. Ensure that the Service Level Manager component is checked and click the Next button.



- The next dialog displays the settings you have selected so far in the installation process. Click the Back button if you want to change something or click the Next button to start copying files.



7. A window appears, showing you the installation progress. Wait until the following dialog appears, confirming that the installation progress is finished. Click the Finish button to exit Setup.



8. Verify that the installation was successful by launching the application (Start > Programs > Nimsoft Monitoring > Service Level Manager).

Installing Nimsoft Infrastructure on Windows

This section describes two different cases:

- Installing a Robot on a Windows computer.
- Installing the Infrastructure package (Robot, Hub, Distribution Server and Alarm Server) on a Windows computer.
Note that this package contains the DMZ wizard component, used when installing Nimsoft on a DMZ in a firewalled environment.

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.

Installing a Windows Robot

1. On the computer where you want to install the Robot:
Launch the Nimsoft Server portal in a web browser. Start the installation procedure from the Nimsoft Server by clicking the Client Installation icon. Then click the Robot link in the Client Installation window.

[Windows Robot, Hub, Distribution Server, Alarm Server](#)

[Windows Robot](#)

[UNIX installation utility \(*nimldr*\) for all platforms](#)

[Installation archive for AIX 5](#)

[Installation archive for 64bit AIX 5](#)

[Installation archive for HP-UX 11](#)

[Installation archive for 64bit HP-UX 11](#)

[Installation archive for 64bit Itanium HP-UX 11](#)

[Installation archive for LINUX with Glibc 2.3](#)

[Installation archive for 64bit LINUX with Glibc 2.3](#)

[Installation archive for 64bit PowerPC LINUX with Glibc 2.3](#)

[Installation archive for SOLARIS 8 \(sparc\)](#)

[Installation archive for 64bit SOLARIS 8 \(sparcv9\)](#)

[Installation archive for 64bit SOLARIS 10 \(amd64\)](#)

[Installation archive for SOLARIS 10 \(i386\)](#)

[Installation archive for TRU64](#)

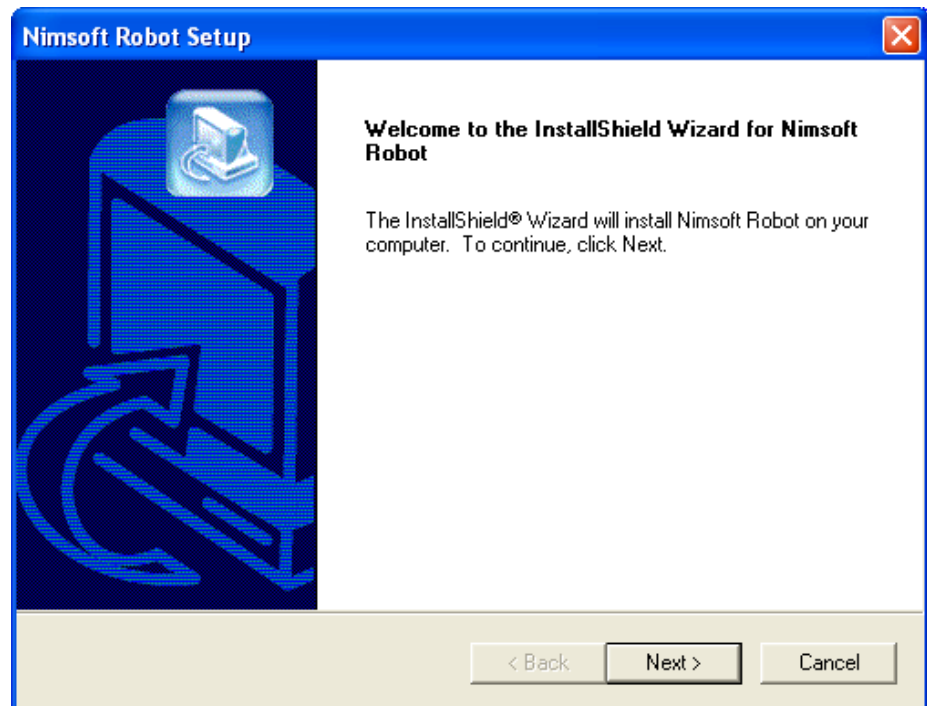
[iSeries Robot Program Files](#)

[iSeries Robot File Structure](#)

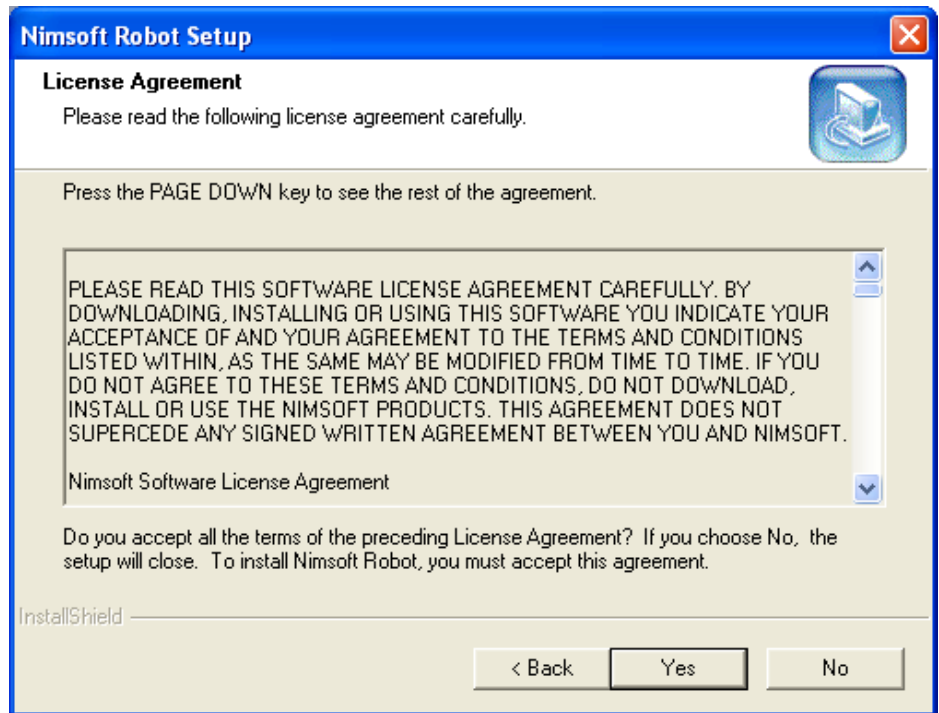
2. The Download dialog pops up. Select Run to start the installation immediately. Note that you may select Save if you want to save the Infrastructure.exe file to disk if you want to run the installation later.

The files are copied from the Nimsoft Server to your computer, and the wizard starts extracting the files.

3. Wait for the following dialog to appear and click the Next button.



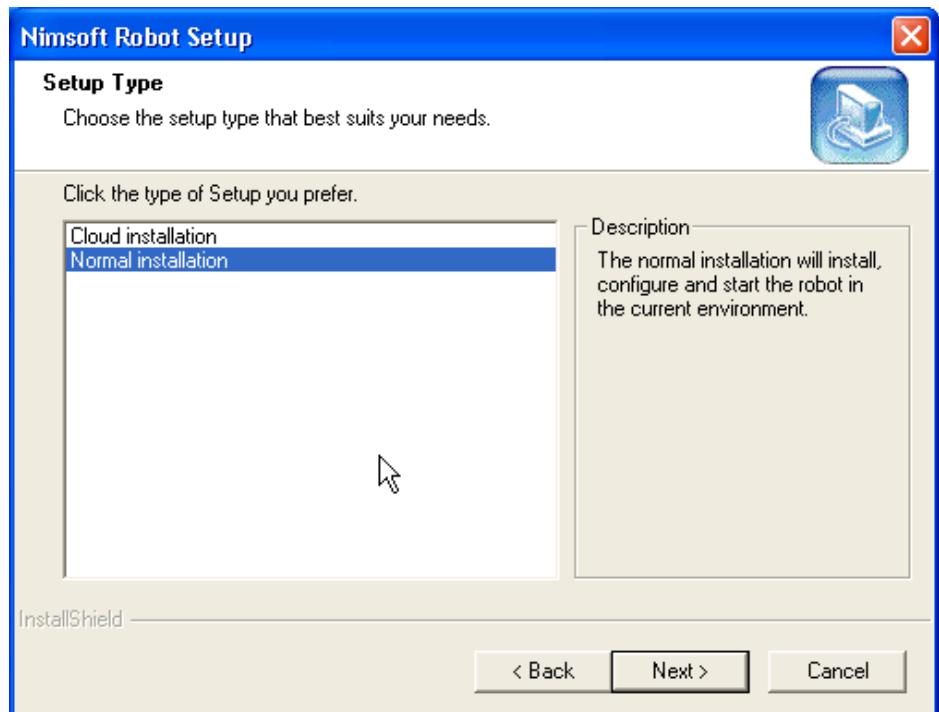
4. The License Agreement dialog appears. Read the license agreement carefully and click Yes to continue if you accept the terms, otherwise click No to exit the setup.



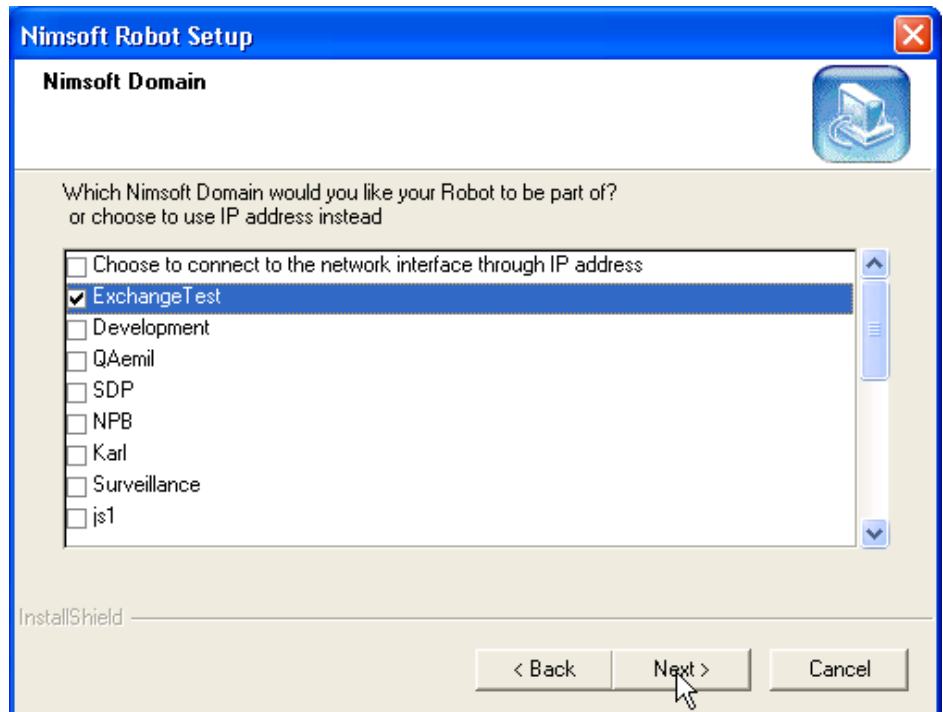
5. The Setup Type dialog appears. It shows two options: Cloud installation and Normal installation.

Normal installation

1. In the Setup Type dialog, select the Normal installation option. Click Next.



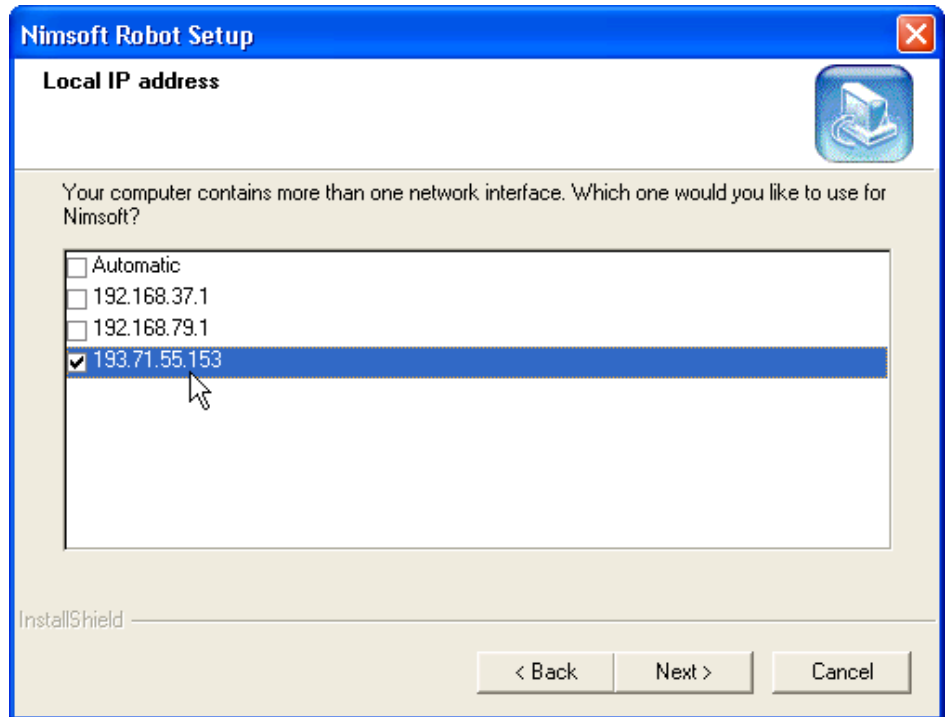
2. If more than one domain exists, the next dialog asks you to select which Domain you want the Robot to be part of. Check one of the Domains and click the Next button.



3. Selecting the option **Choose to connect to the network interface through IP address**, you may select to attach the robot to a specific Hub. Click **Next**.
4. The **Local IP address** dialog appears where you will then be asked to specify the IP address of the hub computer you are installing on.

Note:

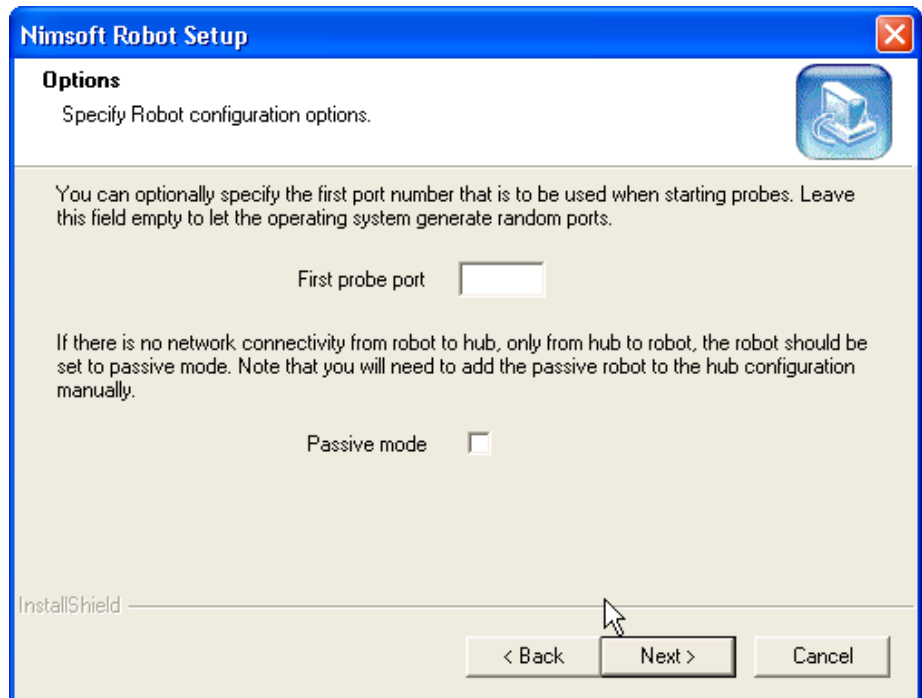
The Local IP Address dialog will only be shown when the computer has multiple network interfaces.



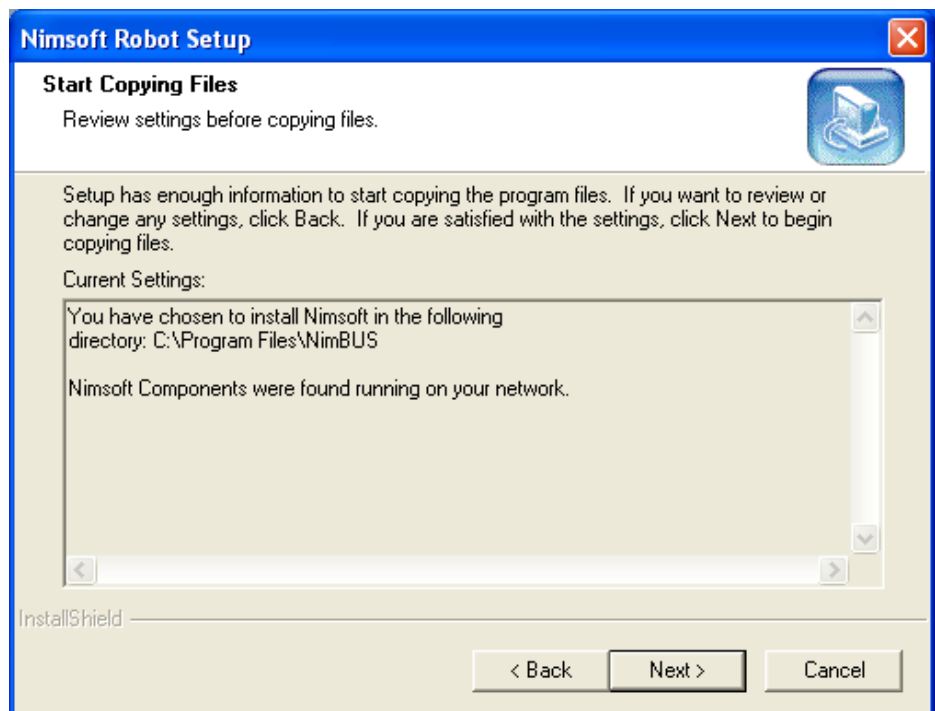
5. Select IP address and click **Next**.
6. **Options** screen appears. In the **First probe port** you can specify the first port to be used to start probes. Leave this field blank to generate port numbers randomly.

Select the **Passive mode** checkbox if you wish to set the hub as passive. By default this checkbox is not selected.

Click **Next**.



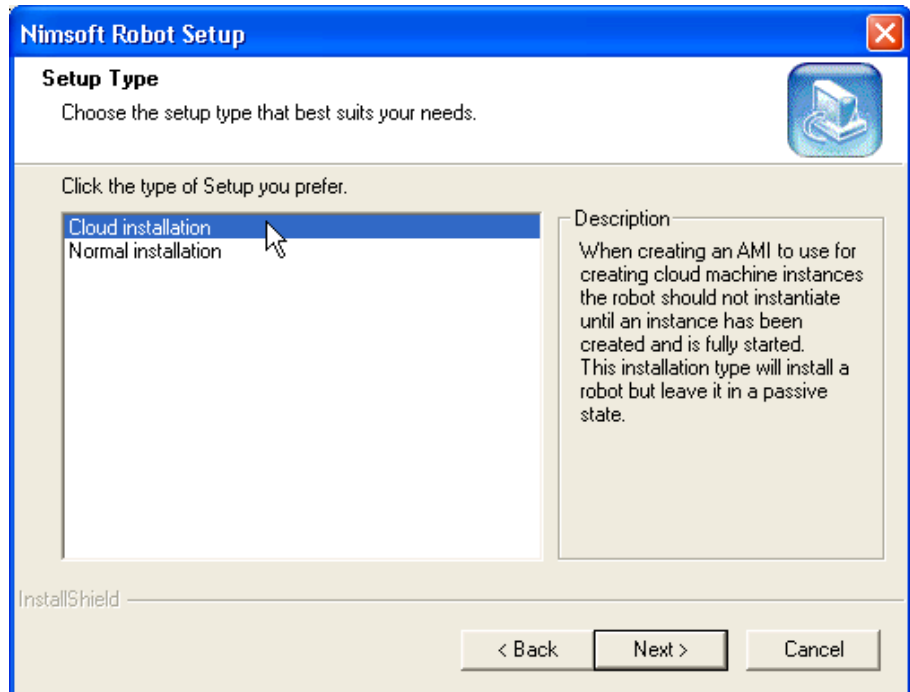
7. Next dialog displays the settings selected in the installation process. Click the Back button to change something or click the Next button to start copying files.



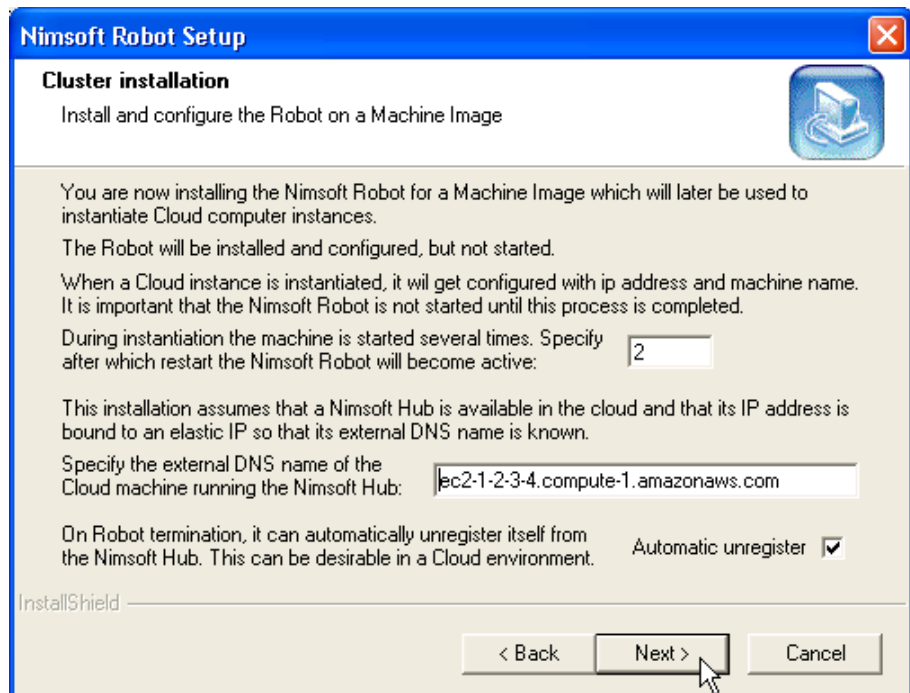
8. A window appears, showing you the installation progress. Wait until the following dialog appears, confirming that the installation progress is finished. Click the Finish button to exit setup.

For Cloud setup

1. In the **Setup Type** dialog, select the Cloud installation option. Click Next.



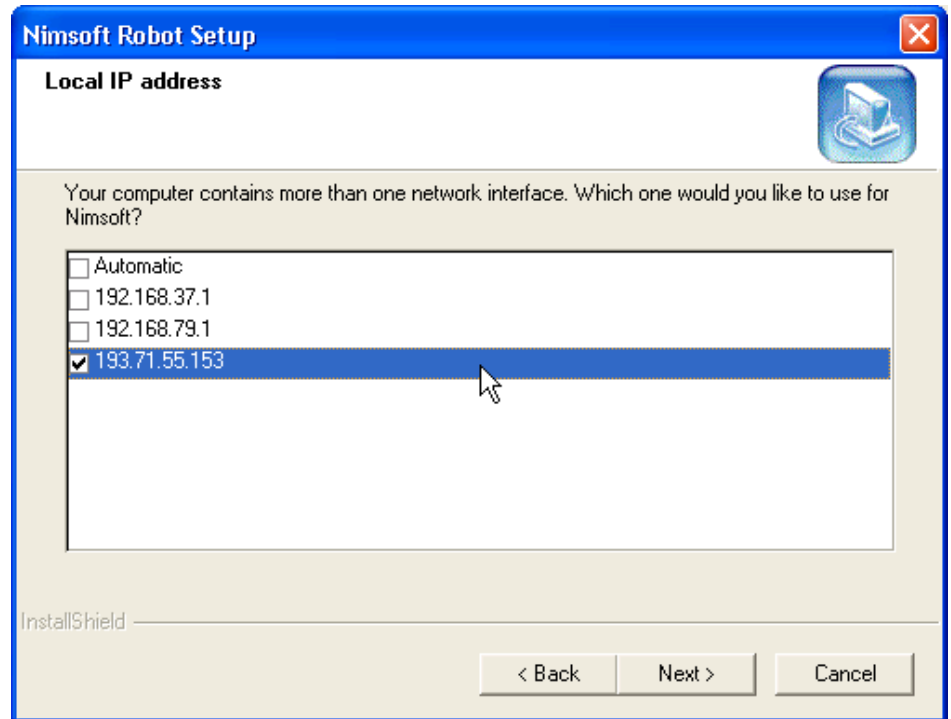
2. **Cluster installation** dialog appears. Note that a hub on a cloud instance is assumed. If a hub external to the cloud is used, the robot will need to be configured with **robotip_alias** = <external IP of cloud instance> after the cloud instance is created.



The **Local IP** address dialog appears where you will then be asked to specify the IP address of the hub computer you are installing on.

Note:

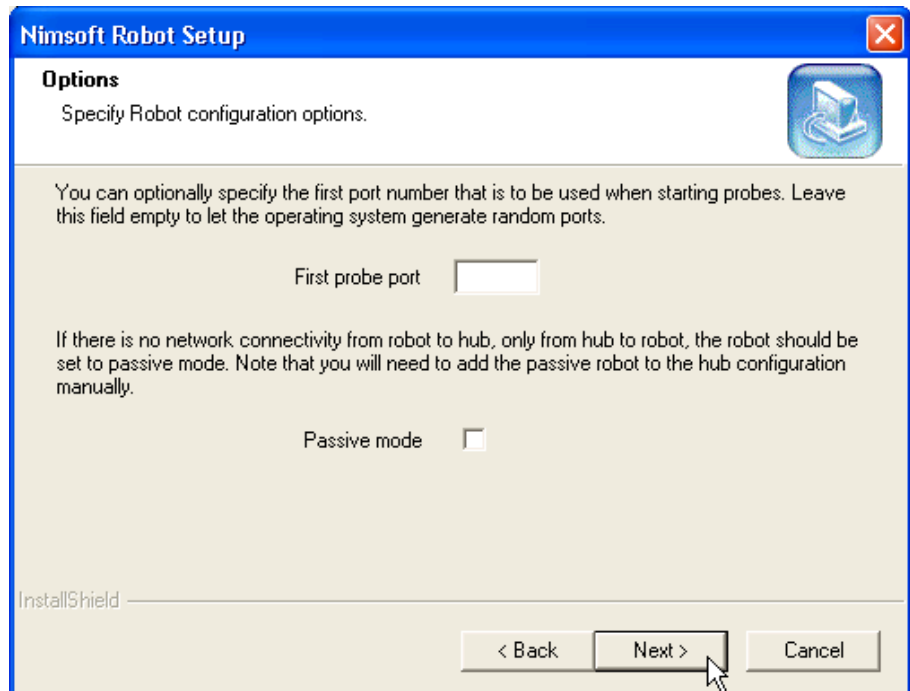
The Local IP Address dialog will only be shown when the computer has multiple network interfaces.



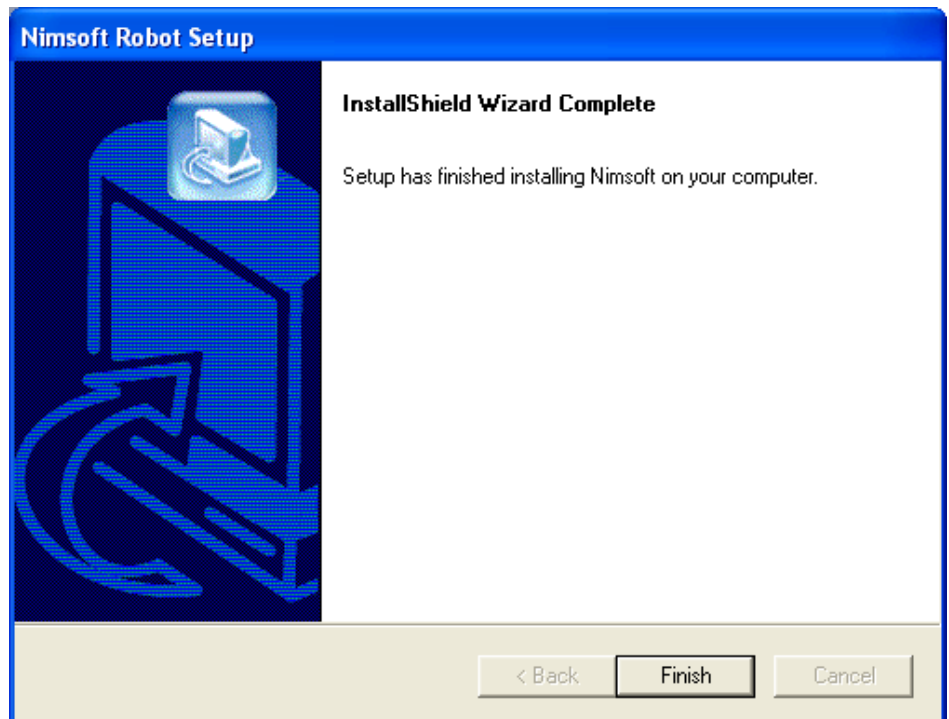
3. Select IP address and click **Next**.
4. **Options** screen appears. In the **First probe port** you can specify the first port to be used to start probes. Leave this field blank to generate port numbers randomly.

Select the **Passive mode** checkbox if you wish to set the hub as passive. By default this checkbox is not selected.

Click **Next**.



5. The next dialog displays the settings you have selected so far in the installation process. Click the **Back** button if you want to change something or click the **Next** button to start copying files.
6. A window appears, showing you the installation progress. Wait until the following dialog appears, confirming that the installation progress is finished. Click the **Finish** button to exit setup.



Installing Windows Robot, Hub, Distribution Server and Alarm Server

NOTES

This package contains the DMZ wizard component, used when installing Nimsoft on a DMZ computer in a firewalled environment. This wizard sets up a tunnel between the intranet in the secure zone and the DMZ server.

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.

If you plan to run the DMZ wizard, you should determine in which direction you want to set up the tunnel.

- If you want the DMZ hub to be the server side of the tunnel:
 - First run the wizard described below, selecting Server setup, on the DMZ computer. A client certificate will then be generated. You will need this when setting up the client on the other side of the tunnel.
 - Then go to the hub in the secure zone and set it up as a tunnel client, using the hub configurator (see description in the Hub section of the Probes online documentation, made available by selecting Help > Probes from the menu in Infrastructure Manager). Note that you need the certificate and password generated in the previous step.
 - If you want the hub in the secure zone to be the server side of the tunnel:
 - First set up the hub in the secure zone as a tunnel server, using the hub configurator (see description in the Hub section of the Nimsoft Probes online documentation, made available by selecting Help > Probes from the menu in Infrastructure Manager).
 - Then go to the hub computer in the DMZ and run the wizard described below, selecting Client setup. Note that you need the certificate and password generated in the previous step.
-
1. Start the installation procedure from the Nimsoft Server by clicking the Client Installation icon. The Client Installation section will be launched in the main window. Then click the Infrastructure package link (Windows Robot, Hub, Distribution server, Alarm Server).

[Windows Robot, Hub, Distribution Server, Alarm Server](#)

[Windows Robot](#)

[UNIX installation utility \(*nimldr*\) for all platforms](#)

[Installation archive for AIX 5](#)

[Installation archive for 64bit AIX 5](#)

[Installation archive for HP-UX 11](#)

[Installation archive for 64bit HP-UX 11](#)

[Installation archive for 64bit Itanium HP-UX 11](#)

[Installation archive for LINUX with Glibc 2.3](#)

[Installation archive for 64bit LINUX with Glibc 2.3](#)

[Installation archive for 64bit PowerPC LINUX with Glibc 2.3](#)

[Installation archive for SOLARIS 8 \(sparc\)](#)

[Installation archive for 64bit SOLARIS 8 \(sparcv9\)](#)

[Installation archive for 64bit SOLARIS 10 \(amd64\)](#)

[Installation archive for SOLARIS 10 \(i386\)](#)

[Installation archive for TRU64](#)

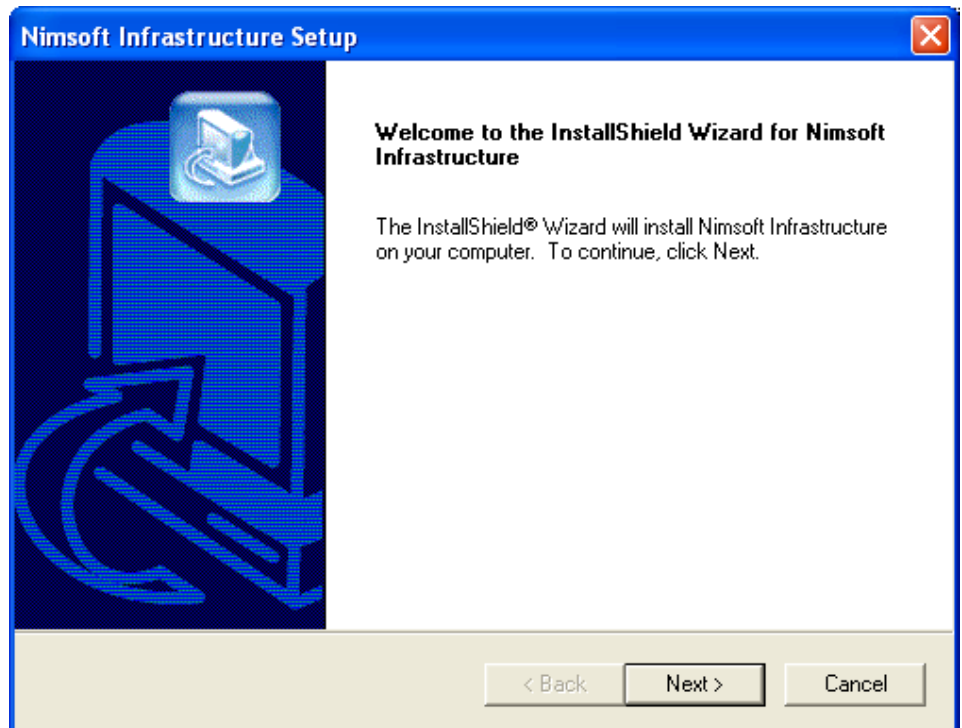
[iSeries Robot Program Files](#)

[iSeries Robot File Structure](#)

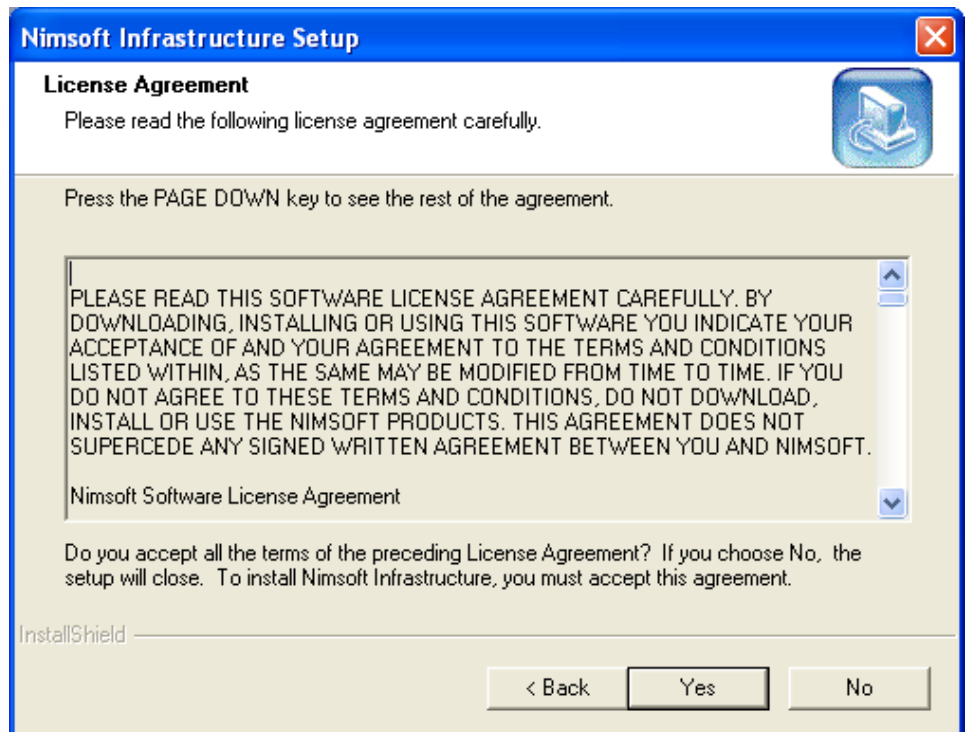
2. The Download dialog pops up. Select Run to start the installation immediately (note that you may select Save if you want to save the Infrastructure.exe file to disk if you want to run the installation later).

The files are copied from the Nimsoft Server to your computer, and the wizard starts extracting the files.

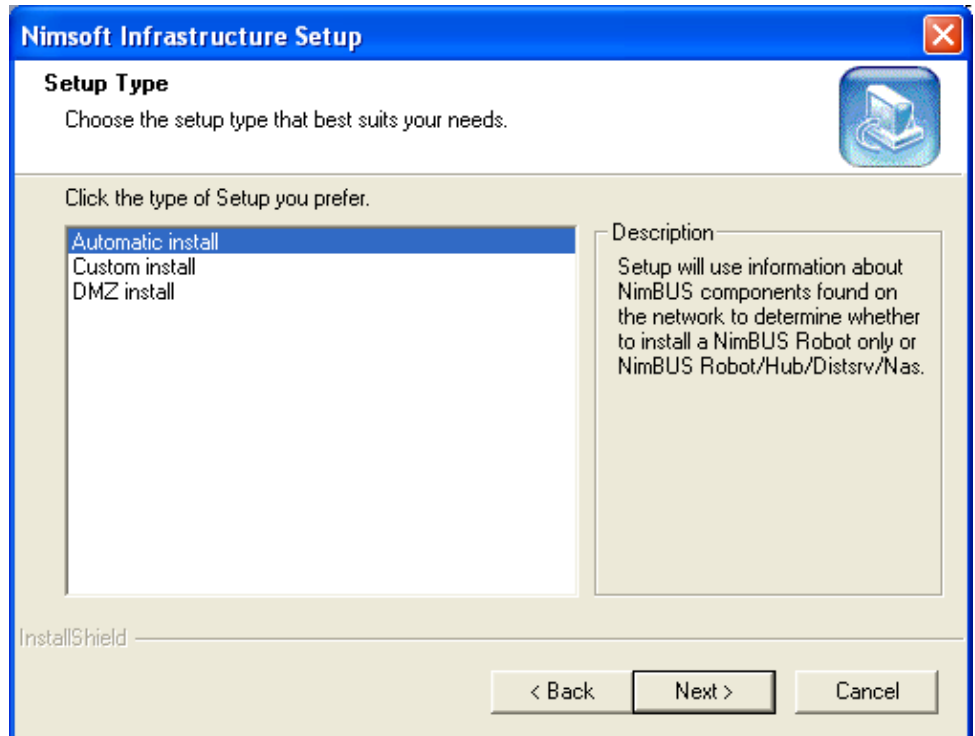
3. Wait for the following dialog to appear and click the Next button.



4. The License Agreement dialog appears. Read the license agreement carefully and click Yes to continue if you accept the terms, otherwise click No to exit.



5. The next dialog enables you to select setup type:
 - **Automatic Install**
 - Detects if Hubs found.
 - If found:
 - Installs Robot + Hub + nas + distsrv
 - If not found:
 - Installs the Robot only, and also reinstalls a Hub (if already present on the computer).
 - **Custom Install**
 - Letting you select which Nimsoft components to install:
 - - Robot
 - - Hub
 - - Alarm Server
 - - Distribution Server
 - - Probe Runtime libraries (needed to create your own Probes).
 - - DMZ Wizard
 - **DMZ Install**
 - This installation must be run on the DMZ host. The necessary components (Hub and Robot) will be installed on the DMZ host, and the wizard for configuring the tunnel through the firewall will be launched.
- Make your choice and click the Next button.



6. The next dialogs depend on what type of setup you selected in the previous dialog:
 - *Automatic install:*
 - Lists the settings you have selected so far in the installation process.

 - If setup detects that a Hub needs to be installed:
 - Depending on which components you selected, you have to specify parameters such as Domain name and Hub name.
 - Setup suggests a license.
 - Starts copying files.
 - The Finish dialog appears, indicating that the Nimsoft Infrastructure Setup is finished.
 - *Custom Install:*
 - You are asked to specify which components to install.
 - Depending on which components you selected, you have to specify parameters such as Domain name and Hub name.
 - Setup suggests a license.
 - Lists the settings you have selected so far in the installation process.
 - Starts copying files.

- The Finish dialog appears, indicating that the Nimsoft Infrastructure Setup is finished.

NOTE:

If the DMZ Wizard component was selected, the setup will also launch the DMZ wizard.

- *DMZ Install:*

- You will be prompted for a Domain name and a Hub name. The DMZ wizard will be launched.

7. DMZ installation

NOTE:

The hub in the DMZ must have a public IP address, if you want to access it from the Internet.

The DMZ installation consists of two parts:

- ◆ First you must configure a tunnel server
- ◆ Second you must configure a tunnel client.

Before running the DMZ wizard, you should determine in which direction you want to set up the tunnel.

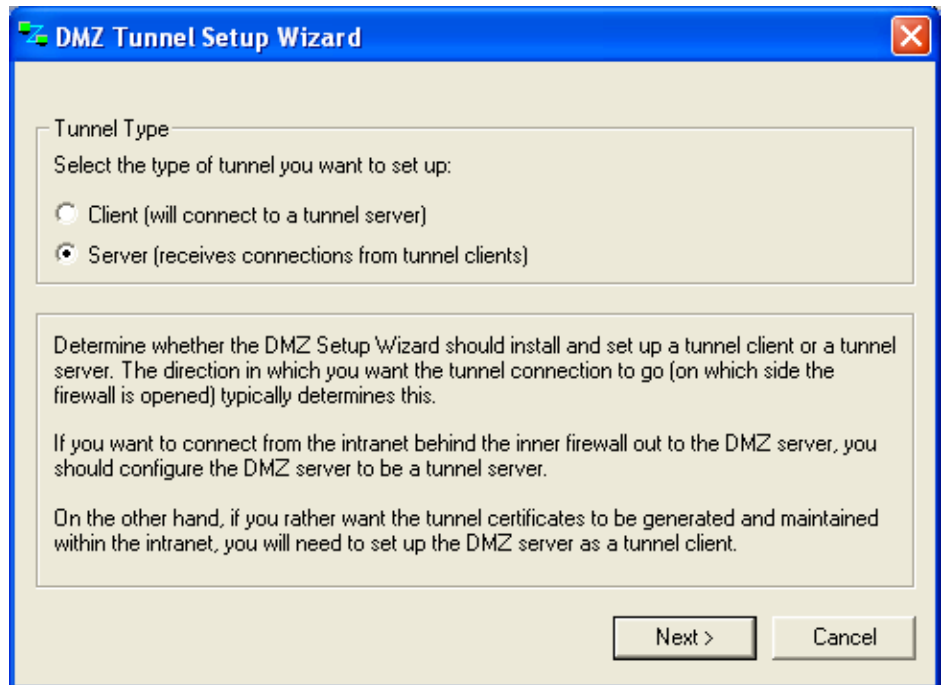
Read the instructions in the dialog carefully and make your choice. Also see the note at the start of this section.

The DMZ wizard is launched, asking to select the type of tunnel you want to set up:

- ◆ Client - will connect to a tunnel server)
- ◆ Server - receives connections from tunnel clients).
When setting up the server, a client certificate will be generated (you will need this when setting up the client).

Run the DMZ wizard on the computer you have selected to be the server and select Server in the initial dialog.

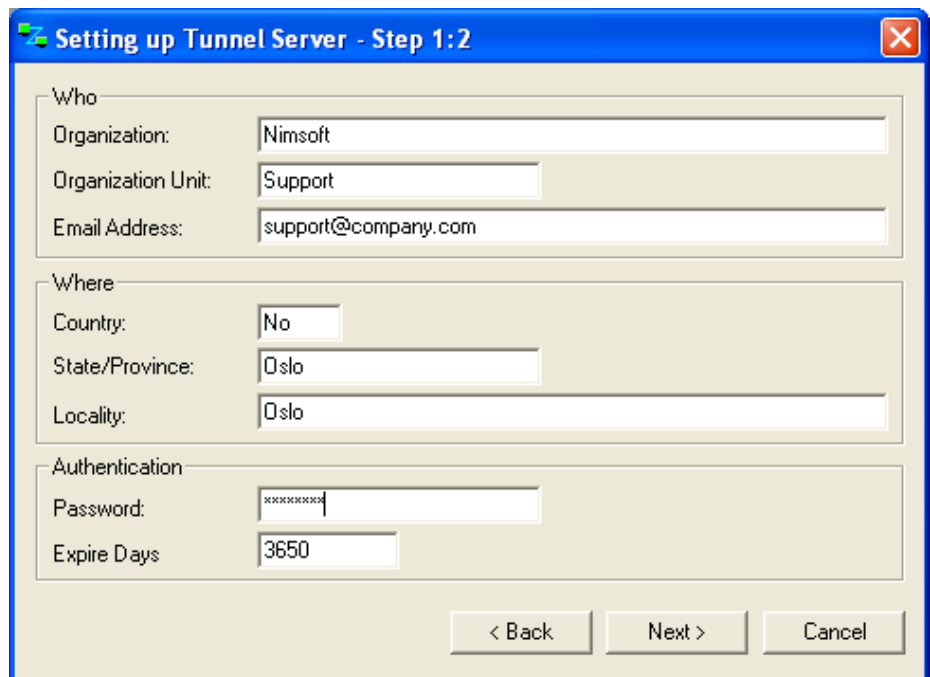
Click the Next button to continue.



8. Configure the Server:

The following dialog appears.

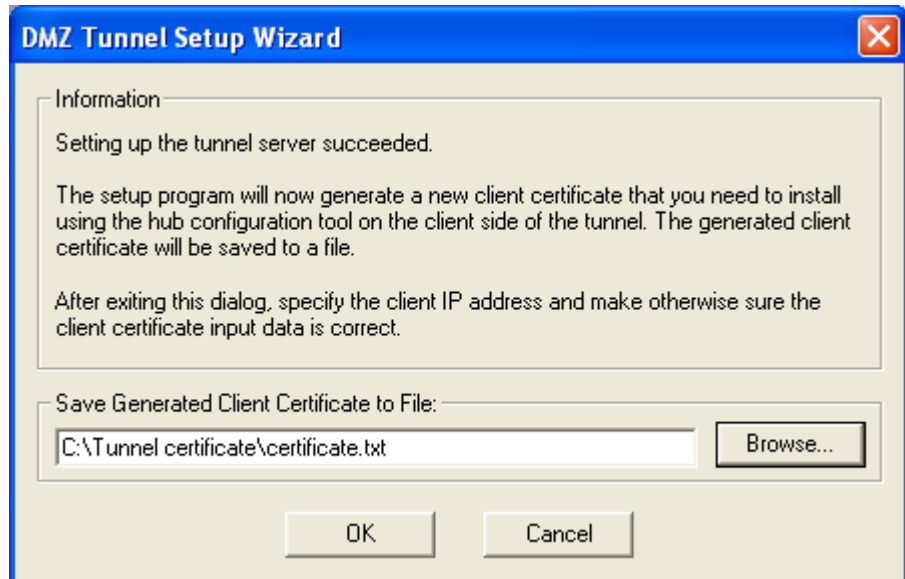
- Fill in organization and address information.
- Specify a password in the Password field.
- Note that you need this password when configuring the client.
- Click the Next button.



9. The following dialog appears, telling that the tunnel setup succeeded.

Specify a file name and location for storing the client certificate to be generated in the next step.

Click the **Next** button to continue.

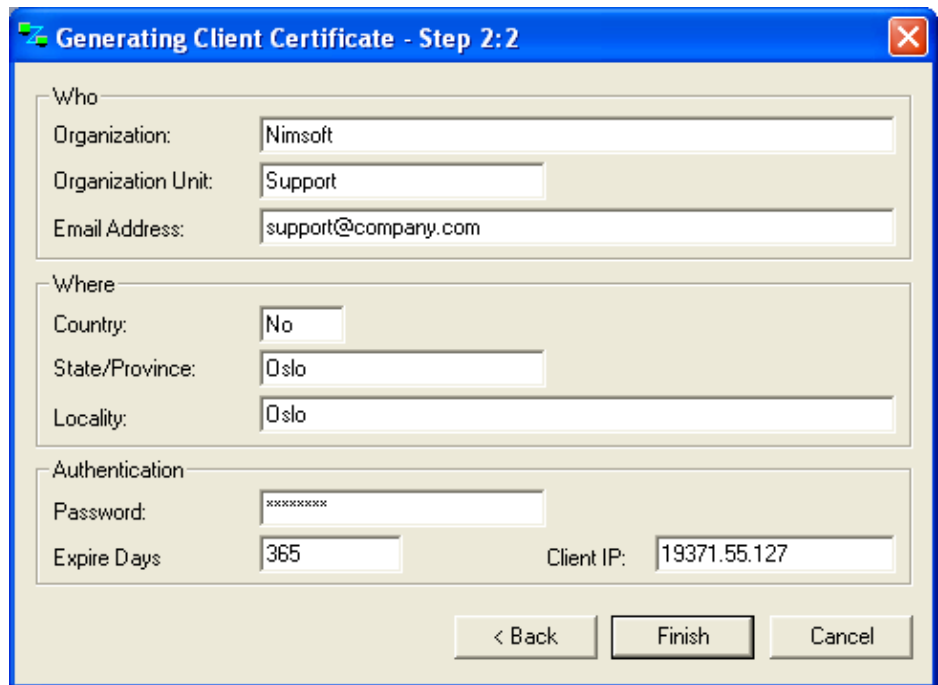


10. The dialog shown below appears. Type the IP address of the client (for which you want to generate the certificate) in the Client IP field. The certificate will be generated and saved to the file specified in the previous step.

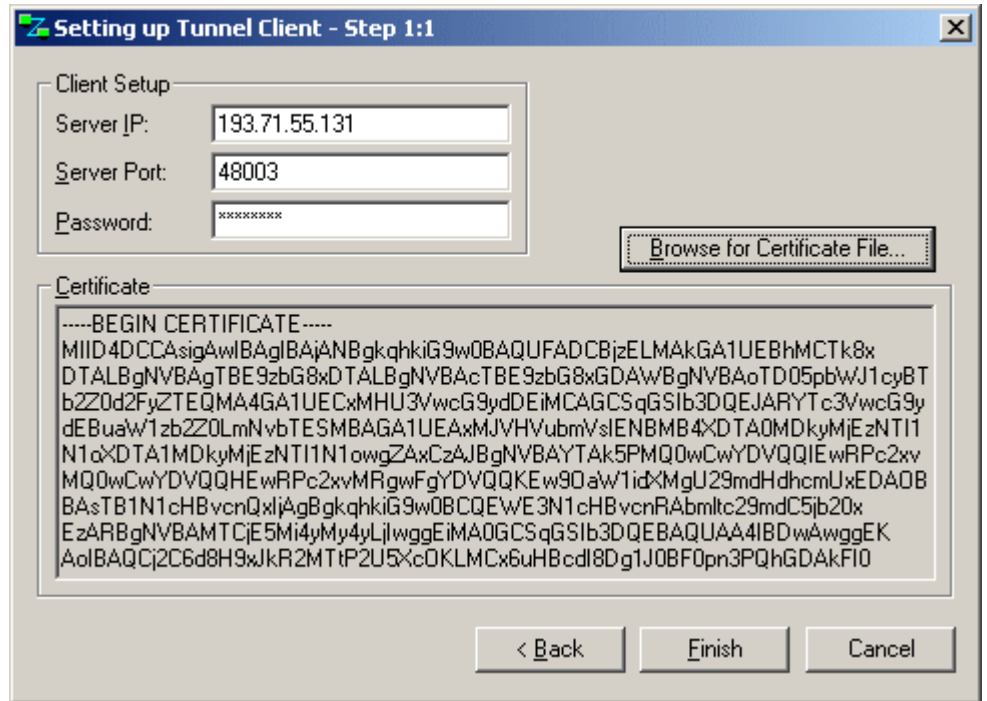
Note: You will need this file when setting up the client, so it is advisable to copy it to e.g. a floppy.

Click the **Finish** button.

You will return to the Finish dialog in the Nimsoft Infrastructure Setup.



11. **Configure the Client:**
If configuring the client on a hub in the secure zone, you must set up the client as described in the Hub section of the Nimsoft Probes online documentation, made available by selecting Help > Probes from the menu in Infrastructure Manager.
12. When configuring a tunnel (client or server) on a computer in the secure zone, we use the hub configurator. If configuring the client on a hub in the DMZ, you must run the DMZ setup on the DMZ computer and select Client in the initial dialog. The following dialog appears.

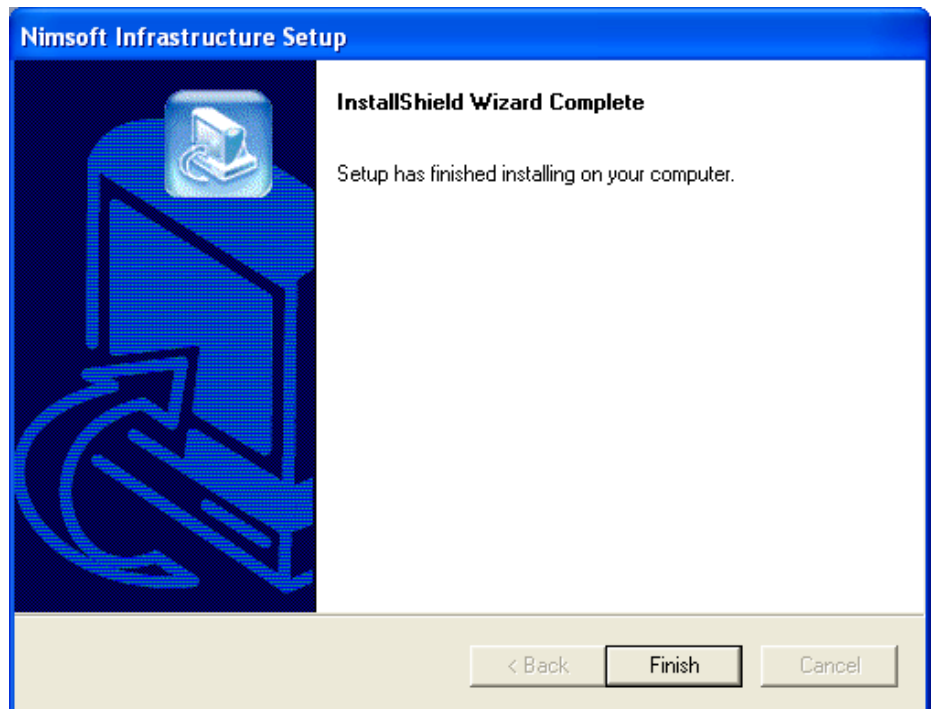


Specify the IP of the server you configured as the tunnel server and fill in the password you specified when you generated the client certificate.

Click the Browse... button to find the client certificate file. When the file is found, the certificate text will appear in the dialog window.

Click the **Finish** button to finish the DMZ wizard.

13. The following dialog appears, confirming that the Nimsoft infrastructure Setup is finished. Click the Finish button to exit.



Installing Nimsoft Infrastructure on Unix

This section will describe two scenarios:

- Installing Nimsoft Infrastructure on a Unix computer on your internal network.
- Installing Nimsoft Infrastructure on a Unix computer in a DMZ.

NOTES:

- It is recommended that at least two Nimsoft Hubs should be installed on the same Domain and network to ensure you have a backup of the user/security data.
- In case of Linux, if you install Nimsoft server with command-line mode (that is, using `./installNMS_linux.bin -i console`), and then try to uninstall it with graphical interfaces (that is, using `./installNMS_linux.bin`), then the un-installation will fail.
- If the server is installed using the command-line mode, it is necessary that command-line mode is used for un-installation as well.
- If Nimsoft already is installed and running on the system, you should perform the following commands prior to the installation:
`/opt/Nimsoft/bin/niminit stop`
`/opt/Nimsoft/bin/inst_init.sh remove`

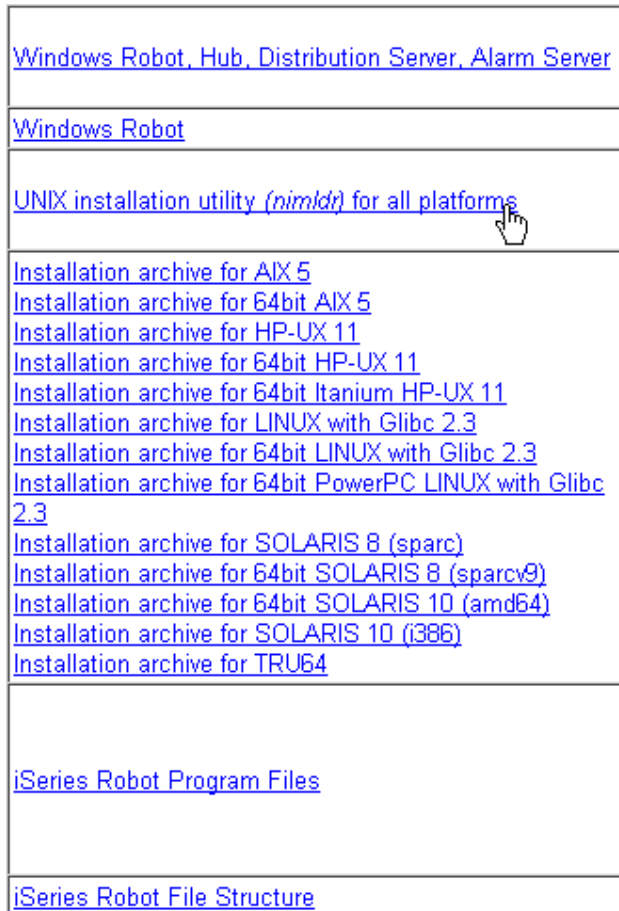
Installing Nimsoft Infrastructure on a Unix computer on your internal network

1. On the computer where you want to install the Nimsoft Infrastructure: Launch the Nimsoft Server portal in a web browser.

NOTE:

If you cannot access a browser on your UNIX computer, you must perform Step 1 and Step 2 in this procedure on a Windows computer, and then copy the nimldr.tar.Z file to the UNIX computer, using ftp.

Start the installation procedure from the Nimsoft Server by clicking the Client Installation icon. The Client Installation section will be launched in the main window. Then click the nimldr for all Unix platforms link in the Client Installation window.



2. The Download dialog pops up. Select Open to start the installation immediately (note that you may select Save if you want to save the nimldr.tar.Z file to disk if you want to run the installation later). The file will be saved on your disk.

Note:

Some browsers (notably some versions of Internet Explorer) have problems saving the file with the correct name and extension. The name of the file is nimldr.tar.Z, and the capital Z is important because Unix is case sensitive.

3. Uncompress the file:

uncompress nimldr.tar.Z

4. Extract nimldr.tar (this makes a directory on your disk with tree-structure, where you can access the different UNIX platforms):

tar xf nimldr.tar

Enter the sub-directory to which your UNIX platform was copied (e.g. LINUX) and run nimldr.

If the UNIX system is on the same network segment as the Nimsoft Server computer:

use # ./nimldr

If the UNIX system is on a different network segment:

Use # ./nimldr -I <ip-address to Nimsoft Server computer>.

Unix Installation Utility (nimldr) usage

```
[root@unixbuilder stian]# ./nimldr -?
Usage: ./nimldr [flags]

Common flags:
-d <debuglevel 0-5>
  default=0
-l <installation logfile>
  default=nimldr.log
-t <path to use for temporary files during installation>
  default=/opt/nimsoft/tmp
-D <NimBUS Domain name>
-H <NimBUS Hub name>
-N <Override Robot name>
-p <NimBUS installation path>
  default=/opt/nimsoft
-f <Override package file name>
  default installation file is detected by the program
  NOTE: Case sensitive, and without the .zip extension
-u install as current user, not as root
  NOTE: This is NOT recommended!
-o <first probe port>
-R <IP address for this robot>
  This is mostly useful for systems with multiple network cards
-a set the automatic unregister flag
  default = 'no'
-s set the robot to passive mode
-v prints version of ./nimldr
```

-h prints this help text

Installation file on local machine:

-F <directory containing installation file>

Installation file on a NimBUS Distribution Server:

-I <IP address of NimBUS Hub running a Distribution Server>

NOTE: This will override the -H option

-V <package version>

get the specified version of the package, not the latest one

Installation modes:

-r install Robot only (default mode)

-i install Infrastructure (Robot, Hub, Nas and Distsrv)

-E express installation (uses defaults or supplied flags)

-X silent express installation (fails instead of going to interactive mode)

Cloud installation:

-C <number of restarts until Robot should become active>

-M <DNS name of the machine running the Hub>

Copyright(c) 1998-2010, Nimsoft Corp.

Take note of the following:

- For the flag “-f”, make sure you do not include the “.zip” extension in the file name. Also note that the file name is case sensitive.
- The “-E” and “-X” flags require that the install file is saved on your local computer.

Robot installation from the Nimsoft Archive

```
linux-jvrz:/tmp # ./nimldr
```

This program will help you install NimBUS on the current system.

You will be given a series of questions, default answers are in brackets:

query? ==>[default]

Pressing Enter directly will use the default value, otherwise you should type in the requested information.

If express installation is specified, the default value will be used automatically.

A log of the installation is found in the file: nimldr.log

WARNING: The temporary files directory is removed after installation!

Where should nimldr store temporary files?

==>[/opt/nimsoft/tmp]

Beginning Robot installation:

Is this a Cloud installation?

==>[no]

```
Do we have the installation file locally?
==>[no]

Is there a host running a NimBUS Hub we can query for the installation file?
==>[yes]

What is the IP address of the host running a NimBUS Hub?
==>[] 193.71.55.147

Preparing to search for Archives:

What is the NimBUS Domain called (*=search)?
==>[Development]

What is the NimBUS Hub called (*=search)?
==>[w7stian]

What is the installation file called?
==>[install_LINUX_23]

Searching for Archives:
 1 /Development/w7stian/unixbuilder/distsrv
 2 /Development/w7stian/w7stian/distsrv

Which of these archives would you like to connect to?
==>[1] 2

We need to log in to NimBUS to query the Archive
Enter NimBUS username and password...
  Username: administrator
  Password:
Beginning download of install_LINUX_23
\
Done!

What are we installing? (1=Robot,2=Infrastructure)
==>[1]
Extracting files from archive /opt/nimsoft/tmp//install_LINUX_23.zip to temp directory
/opt/nimsoft/tmp/

Where should NimBUS be installed?
==>[/opt/nimsoft]

Automatically unregister Robot from Hub on termination?
==>[yes]

Should this Robot run in passive mode?
==>[no]

What is this NimBUS Domain called?
==>[Development]

Which NimBUS Hub should this Robot connect to?
==>[w7stian]
```

What is that NimBUS Hub's IP address?

==>[] 193.71.55.147

Starting NimBUS:

Cleaning up temporary files

Finished Robot installation!

linux-jvrz:/tmp #

Infrastructure installation from local file

linux-jvrz:/tmp # ./nimldr

This program will help you install NimBUS on the current system.

You will be given a series of questions, default answers are in brackets:

query? ==>[default]

Pressing Enter directly will use the default value, otherwise you should type in the requested information.

If express installation is specified, the default value will be used automatically.

A log of the installation is found in the file: nimldr.log

WARNING: The temporary files directory is removed after installation!

Where should nimldr store temporary files?

==>[/opt/nimsoft/tmp]

Beginning Robot installation:

Is this a Cloud installation?

==>[no]

Do we have the installation file locally?

==>[no] yes

Where do we have the installation file(s)?

==>[] /tmp

What are we installing? (1=Robot,2=Infrastructure)

==>[1] 2

A NimBUS Robot and Hub will be installed.

Would you like to install the NimBUS Alarm Server (nas)?

==>[yes]

Would you like to install the Distribution Server (distsrv)?

==>[yes]

Extracting files from archive /tmp/install_LINUX_23 to temp directory /opt/nimsoft/tmp/

Where should NimBUS be installed?

==>[/opt/nimsoft]


```
Automatically unregister Robot from Hub on termination?
==>[yes]

Should this Robot run in passive mode?
==>[no]

What is this NimBUS Domain called?
==>[] Development

What is this NimBUS Hub called?
==>[linux-jvrz]

What is this NimBUS Hubs IP address?
==>[193.71.55.62]
Starting NimBUS:

Waiting for Hub to start...

Are you setting up a NimBUS Tunnel between this Hub and another Hub?
==>[no]

Would you like to initialize the security settings on this Hub?
==>[yes]

Please specify the administrator user password:
  Type password:
  Retype password:
Initializing security for this Hub...Security initialized!
Cleaning up temporary files
Finished Robot installation!
linux-jvrz:/tmp #
```

Installing Nimsoft Infrastructure on a Unix computer in a DMZ

In this case you have to copy the following files from the Nimsoft Web Server application and bring them to the DMZ host (e.g. using a CD or ftp):

nimldr for all Unix platforms (to install Nimsoft infrastructure components and DMZ on the DMZ host.

- Installation archive for your Unix type.

Windows Robot, Hub, Distribution Server, Alarm Server
Windows Robot
UNIX installation utility (<i>nimldr</i>) for all platforms
Installation archive for AIX 5 Installation archive for 64bit AIX 5 Installation archive for HP-UX 11 Installation archive for 64bit HP-UX 11 Installation archive for 64bit Itanium HP-UX 11 Installation archive for LINUX with Glibc 2.3 Installation archive for 64bit LINUX with Glibc 2.3 Installation archive for 64bit PowerPC LINUX with Glibc 2.3 Installation archive for SOLARIS 8 (sparc) Installation archive for 64bit SOLARIS 8 (sparcv9) Installation archive for 64bit SOLARIS 10 (amd64) Installation archive for SOLARIS 10 (i386) Installation archive for TRU64
iSeries Robot Program Files
iSeries Robot File Structure



- Copy the files into a folder on the DMZ host.
Note the name of the file is `nimldr.tar.Z`: the capital Z is important because Unix is case sensitive.

Procedure:

1. Uncompress the file:

```
# uncompress nimldr.tar.Z
```

2. Extract nimldr.tar (this makes a directory on your disk with tree-structure, where you can access the different UNIX platforms):
tar xf nimldr.tar
3. Enter the sub-directory to which your UNIX platform was copied (e.g. Linux) and run nimldr.

Further action, as described in the sections Infrastructure installation, Tunnel Server and Infrastructure installation, Tunnel Client, depends on the direction of the tunnel (see below).

Decide the direction of the tunnel through the firewall.

NOTE:

The hub in the DMZ must have a public IP address if you want to access it from the Internet.

Opening the tunnel from the DMZ:

If you are opening the tunnel through the firewall from the DMZ, you should first run the procedure described in the section [Infrastructure installation, Tunnel Server](#) on the DMZ computer.

Make a note of the password and save the client certificate file.

You should then go to the hub in the secure zone and configure the tunnel client as described in the section [Infrastructure installation, Tunnel Client](#).

Opening the tunnel from the secure zone:

If you want to open the tunnel through the firewall from the secure zone, you should first configure the hub in the secure zone as tunnel server as described in the section [Infrastructure installation, Tunnel Server](#).

Bring the client certificate file (and password) to the DMZ computer and run the procedure described in the section [Infrastructure installation, Tunnel Client](#) to install the tunnel client component.

For details, see the section [Installation in a firewalled environment](#).

Infrastructure installation, Tunnel Server

This section applies to an installation where you install the tunnel server component on the DMZ host, and then bring the client certificate file (and password) to the hub on the outside and install the tunnel client component there.

```
linux-jvrz:/tmp # ./nimldr
```

This program will help you install NimBUS on the current system.
You will be given a series of questions, default answers are in brackets:

```
query? ==>[default]
```

Pressing Enter directly will use the default value, otherwise you should type in the requested information.

If express installation is specified, the default value will be used automatically.

A log of the installation is found in the file: nimldr.log

WARNING: The temporary files directory is removed after installation!

Where should nimldr store temporary files?

```
==>[/opt/nimsoft/tmp]
```

Beginning Robot installation:

Is this a Cloud installation?

```
==>[no]
```

Do we have the installation file locally?

```
==>[no] yes
```

Where do we have the installation file(s)?

```
==>[] /tmp
```

What are we installing? (1=Robot,2=Infrastructure)

```
==>[1] 2
```

A NimBUS Robot and Hub will be installed.

Would you like to install the NimBUS Alarm Server (nas)?

```
==>[yes]
```

Would you like to install the Distribution Server (distsrv)?

```
==>[yes]
```

Extracting files from archive /tmp/install_LINUX_23 to temp directory /opt/nimsoft/tmp/

Where should NimBUS be installed?

```
==>[/opt/nimsoft]
```

Automatically unregister Robot from Hub on termination?

```
==>[yes]
```

Should this Robot run in passive mode?

```
==>[no]
```

```
What is this NimBUS Domain called?
==>[] Development

What is this NimBUS Hub called?
==>[linux-jvrz]

What is this NimBUS Hubs IP address?
==>[193.71.55.62]
Starting NimBUS:

Waiting for Hub to start...

Are you setting up a Nimsoft Tunnel between this Hub and another Hub?
==>[no] yes

We need to login to Nimsoft to set Tunnel options
Enter Nimsoft username and password...
  Username: administrator
  Password:

Is this Hub going to be a Tunnel Server?
==>[no]

Setting up the Server:

The Server needs to generate a CA certificate
This certificate will be used to sign Client certificates

What is the name of your orgainzation?
==>[My Company Inc.] Nimsoft Corp

What is the name of the organizational unit?
==>[SysAdmin] Development

What is the administrator email address?
==>[sysadmin@my.company.com] developers@nimsoft.com
What password should we use for the Server certificate?
  Type password:
  Retype password:
Generating CA certificate - this may take a few moments...
Done generating CA certificate!

Creating a Client Certificate:

The Client will need this certificate to connect to this Server

What is the IP address of the Client Hub?
==>[] 10.1.1.1

What is the name of your orgainzation?
==>[Nimsoft Corp]
```

```
What is the name of the organizational unit?
==>[Development] DMZ

What is the administrator email address?
==>[developers@nimsoft.com]
What password should we use for this certificate?
Type password: Comment: Type and retype a password
of your own choice here.
Retype password:

What file should the certificate be written to (full path)?
==>[/opt/nimsoft/client.txt]

Generating Client certificate - this may take a few moments...
Done creating Client certificate /opt/Nimsoft/client.txt
Cleaning up temporary files
Finished Robot installation!
```

NOTE:

Copy the file /opt/nimsoft/client.txt to removable medium or transfer electronically to the client Hub and set up Tunnel Client there. Communication will be possible between the two systems on port 48003/tcp.

Infrastructure installation, Tunnel Client

This section applies to an installation where you install the tunnel client component. Note that you will need the client certificate file that was generated when you installed the tunnel server component, and also the password you used.

Copy the certificate file (client.txt) to e.g. the /tmp directory.

```
linux-jvz:/tmp # ./nimldr
```

```
This program will help you install NimBUS on the current system.
You will be given a series of questions, default answers are in brackets:
query? ==>[default]
Pressing Enter directly will use the default value, otherwise you should
type in the requested information.
```

```
If express installation is specified, the default value will be used
automatically.
```

```
A log of the installation is found in the file: nimldr.log
WARNING: The temporary files directory is removed after installation!
```

```
Where should nimldr store temporary files?
==>[/opt/nimsoft/tmp]
Beginning Robot installation:
```

```
Is this a Cloud installation?
==>[no]

Do we have the installation file locally?
==>[no] yes

Where do we have the installation file(s)?
==>[] /tmp

What are we installing? (1=Robot,2=Infrastructure)
==>[1] 2
A NimBUS Robot and Hub will be installed.

Would you like to install the NimBUS Alarm Server (nas)?
==>[yes]

Would you like to install the Distribution Server (distsrv)?
==>[yes]
Extracting files from archive /tmp/install_LINUX_23 to temp directory /opt/nimsoft/tmp/

Where should NimBUS be installed?
==>[/opt/nimsoft]

Automatically unregister Robot from Hub on termination?
==>[yes]

Should this Robot run in passive mode?
==>[no]

What is this NimBUS Domain called?
==>[] Development

What is this NimBUS Hub called?
==>[linux-jvrz]

What is this NimBUS Hubs IP address?
==>[193.71.55.62]
Starting NimBUS:

Waiting for Hub to start...

Are you setting up a Nimsoft Tunnel between this Hub and another Hub?
==>[no] yes

We need to login to Nimsoft to set Tunnel options
Enter Nimsoft username and password...
  Username: administrator
  Password:

Is this Hub going to be a Tunnel Server?
==>[no]
```

```
Is this Hub going to be a Tunnel Server?
==>[no]

Is this Hub going to be a Tunnel Client?
==>[yes]

What is the IP address of the Tunnel Server Hub?
==>[] 10.1.1.6

What port is the Server listening on?
==>[48003]

What password was used to generate this certificate?
  Type password: Comment: Type and retype a password the password here.
  Retype password:

What file is the client certificate in (full path)?
==>[/opt/nimsoft/tmp/client.txt] /tmp/client.txt
Done setting up Client
Cleaning up temporary files
Finished Robot installation!
linux-jvz:/tmp #
```



Installing the robot on AS400

Launch the Nimsoft Server portal in a web browser on a workstation on your network.

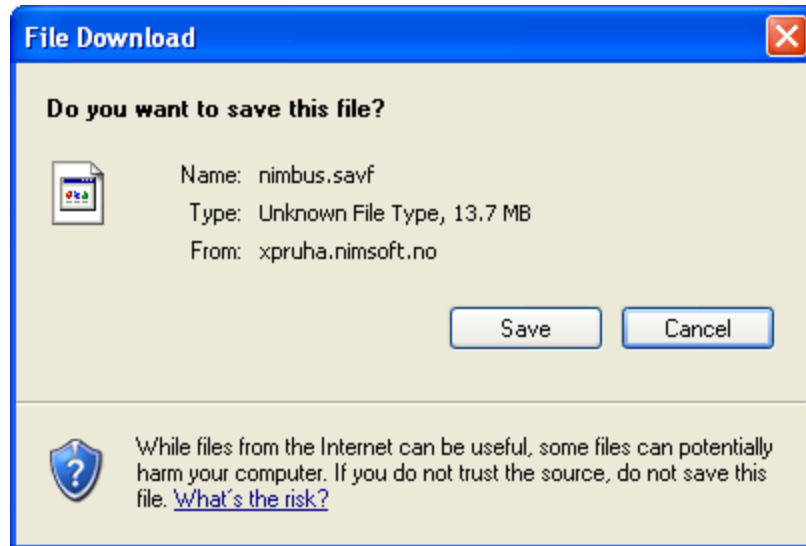
Start the installation procedure from the Nimsoft Server by clicking the *Client Installation* icon.

You must now copy the two files *NimBUS.savf* and *NIMSOFT.savf* to your workstation:

First click the *iSeries Robot Program Files* link in the Client Installation window.

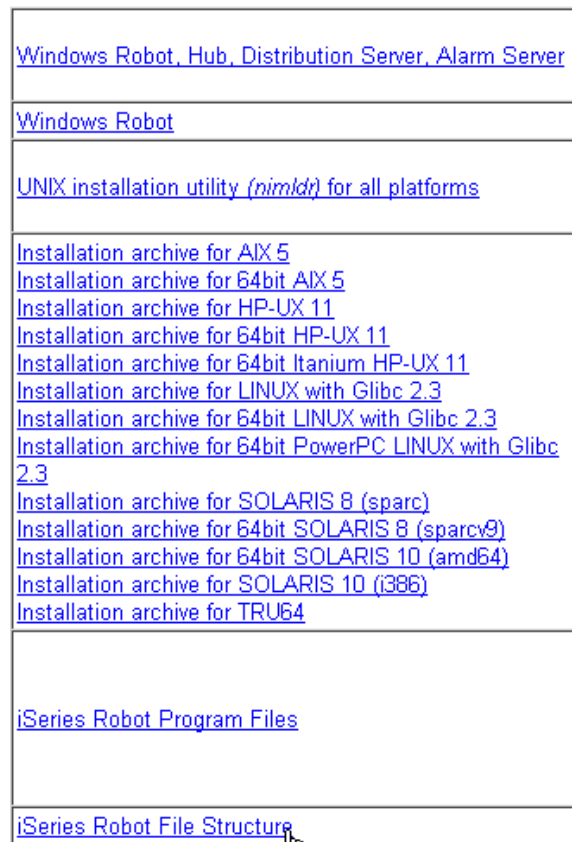
Windows Robot, Hub, Distribution Server, Alarm Server
Windows Robot
UNIX installation utility (<i>nim/dr</i>) for all platforms
Installation archive for AIX 5 Installation archive for 64bit AIX 5 Installation archive for HP-UX 11 Installation archive for 64bit HP-UX 11 Installation archive for 64bit Itanium HP-UX 11 Installation archive for LINUX with Glibc 2.3 Installation archive for 64bit LINUX with Glibc 2.3 Installation archive for 64bit PowerPC LINUX with Glibc 2.3 Installation archive for SOLARIS 8 (sparc) Installation archive for 64bit SOLARIS 8 (sparcv9) Installation archive for 64bit SOLARIS 10 (amd64) Installation archive for SOLARIS 10 (i386) Installation archive for TRU64
iSeries Robot Program Files 
iSeries Robot File Structure

The dialog popping up asks you if you want to save the *NimBUS.savf* file. This save file contains the program files for the iSeries Robot.

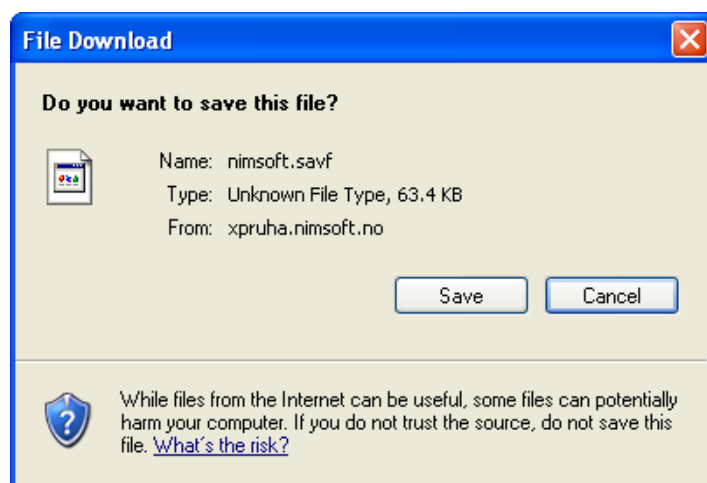


Click the Save button to continue. You will be asked where you want to save the file. Choose a location and click the Save button.

Next you must click the *iSeries Robot File Structure* link in the Client Installation window.



The dialog popping up asks you if you want to save the *nimsoft.savf* file. This save file contains the file structure for the iSeries Robot together with some configuration files.



Click the *Save* button to continue. You will be asked where you want to save the file. Choose a location and click the *Save* button.

Continue with the procedure described below:

Installation procedure

On the AS400

Create the user NIMBUS:

```
CRTUSRPRF USRPRF(NIMBUS) PASSWORD()  
USRCLS(*SECOFR) TEXT('Nimbus User for  
Nimsoft Management')
```

Create temporary files for the 'save files':

```
CRTSAVF <<LIBRARY>>/NIMBUS TEXT('Savf of Nimsoft LIB')  
CRTSAVF <<LIBRARY>>/NIMSOFT TEXT('Savf of  
Nimbus_Software')
```

On the workstation on the network

In this step you are going to copy the two files you saved during the Client Installation section above (NIMBUS.savf and NIMSOFT.savf) to the AS400 :

```
ftp <<AS/400>>
```

Log on the AS400

```
LCD <<the folder where savefiles are located on the
workstation>>
CD <<LIBRARY where the temporary save files were created
on AS400>>
BIN
PUT NIMBUS.savf
PUT NIMSOFTE.savf
Quit
```

On the AS400

Restore /qsys.lib/Nimbus.lib

```
RSTLIB SAVLIB (NIMBUS) DEV (*SAVF) SAVF (<<LIBRARY>>/NIMBUS)
```

Restore /Nimbus_Software/NimBUS file-tree

```
QSYS/CRTDIR DIR ('/Nimbus_Software')
QSYS/CRTDIR DIR ('/Nimbus_Software/NimBUS/')
QSYS/RST DEV ('/QSYS.lib/<<LIBRARY>>.lib/NIMSOFTE.file')
OBJ ((' /Nimbus_Software/NimBUS/*')
```

Edit the configuration file `/Nimbus_Software/NimBUS/robot.cfg` according to the example below. The fields with bold text in the example below must be modified according to your system configuration.

Note that `robotip` and `contip` should both be the local computer's ip-address.

```
EDTF STMF ('/Nimbus_Software/NimBUS/robot/robot.cfg')
```

Example

```
<controller>
  domain = Nimsoft
  hub = Development
  hubrobotname = src1
  hubip = 193.71.55.11
  robotname = server3
  robotip = 193.71.55.103
</controller>
<remote>
  contip = 193.71.55.103
</remote>
```

Start the robot with the command

```
STRSBS NIMBUS/NIMBUS
```

The robot can be stopped with the command

```
ENDSBS NIMBUS
```

NOTE

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 jobscde as described in the example below (stop time 01.00.00 and start time 07.00.00, every day):

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

If you later want to change the schedules, use WRKJOBSCDE.

Installing Nimsoft Web Service

The support for Nimsoft Web Service has been discontinued. Please refer to the Wasp Web Service documentation for more details.

Installing the Mobile Solution Services

The support for Nimsoft Web Service and Mobile Panels has been discontinued.

Installing Nimsoft Web Access



Note that the Nimsoft Web Access product is for web access purpose only. Do not install Dashboard Viewer on machines that have Enterprise Console or Infrastructure Manager installed.

The Installation of the Nimsoft Web Access product involves two steps:

- Installing the Microsoft .NET Framework Ver 2.0 (if not already installed)
- Installing the Nimsoft Dashboard Viewer (see Installing Nimsoft Dashboard Viewer)

Installing Nimsoft Dashboard Viewer

1. Start the installation procedure from the Nimsoft Server by clicking the Client Installation icon. The Client Installation section will be launched in the main window. Click the Nimsoft Dashboard Viewer link in the Client Installation section.

Microsoft .NET Framework (x86) Microsoft .NET Framework (x64)	2.0	
Dashboard Viewer	1.30	

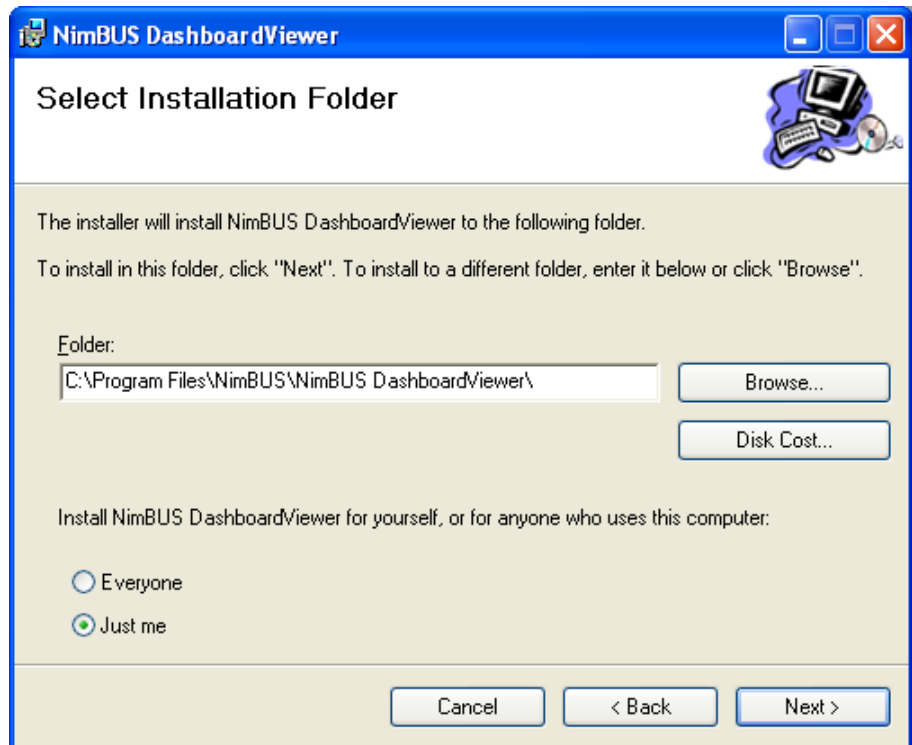
2. The download dialog pops up. Select Run to start the installation immediately (note that you may select Save if you want to save the Nimsoft DashboardViewer.exe file to disk and run the installation later).

The files are copied from the Nimsoft Server to your computer, and the wizard starts extracting the files.

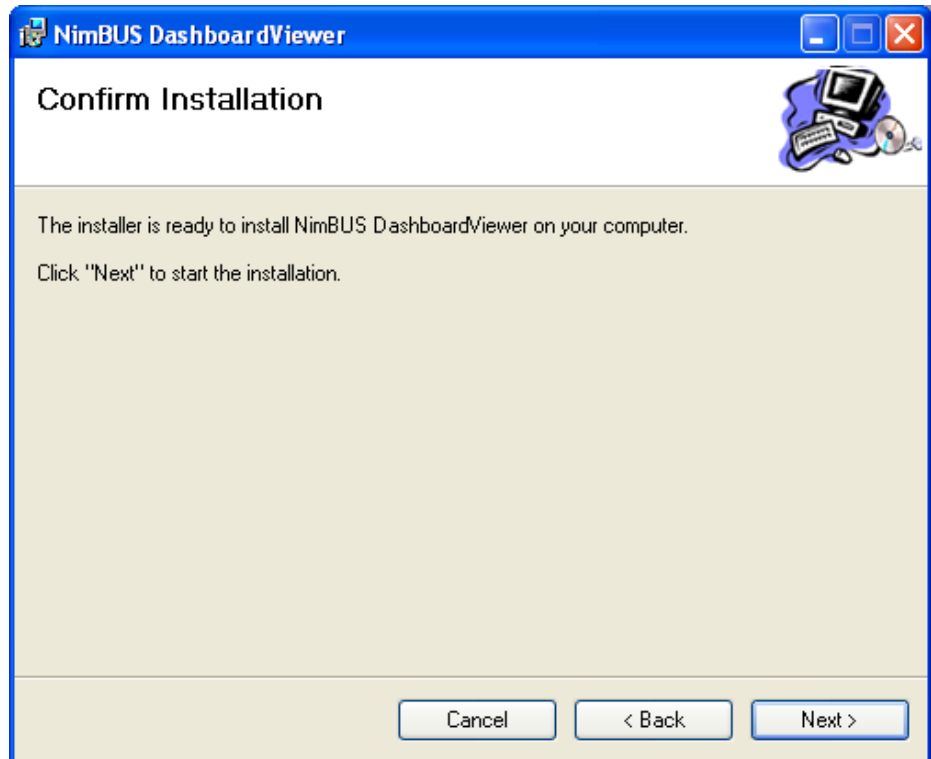
3. Wait for the following dialog to appear and click the Next button.



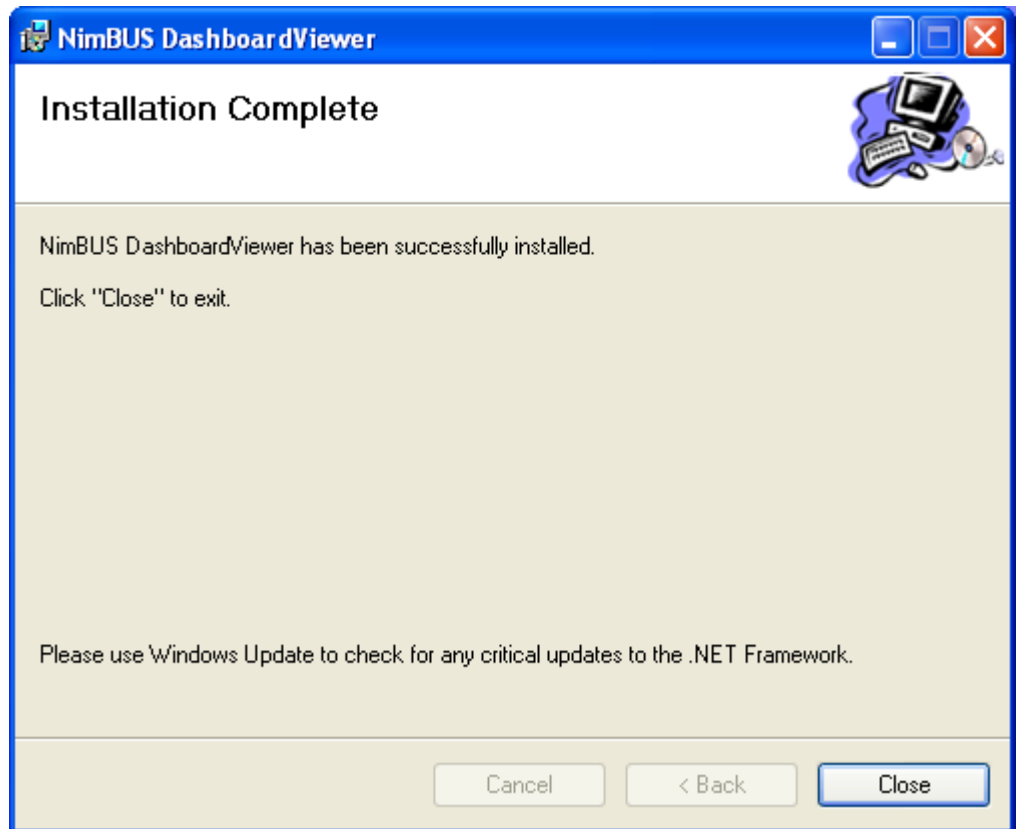
4. The Installation Folder dialog appears, informing you that the default destination folder (where Setup will install the files) is C:\Program Files\Nimsoft Monitoring. Click the Next button to accept, or click the Browse button to select another folder.



5. The next dialog asks you to confirm the installation parameters entered. Click the Next button to accept.



6. A window appears, showing you the installation progress. Wait until the following dialog appears, confirming that the installation process is complete. Click the Close button to exit Setup.



7. Verify that the installation was successful by launching the application (Start > Programs > Nimsoft Monitoring > DashboardViewer).

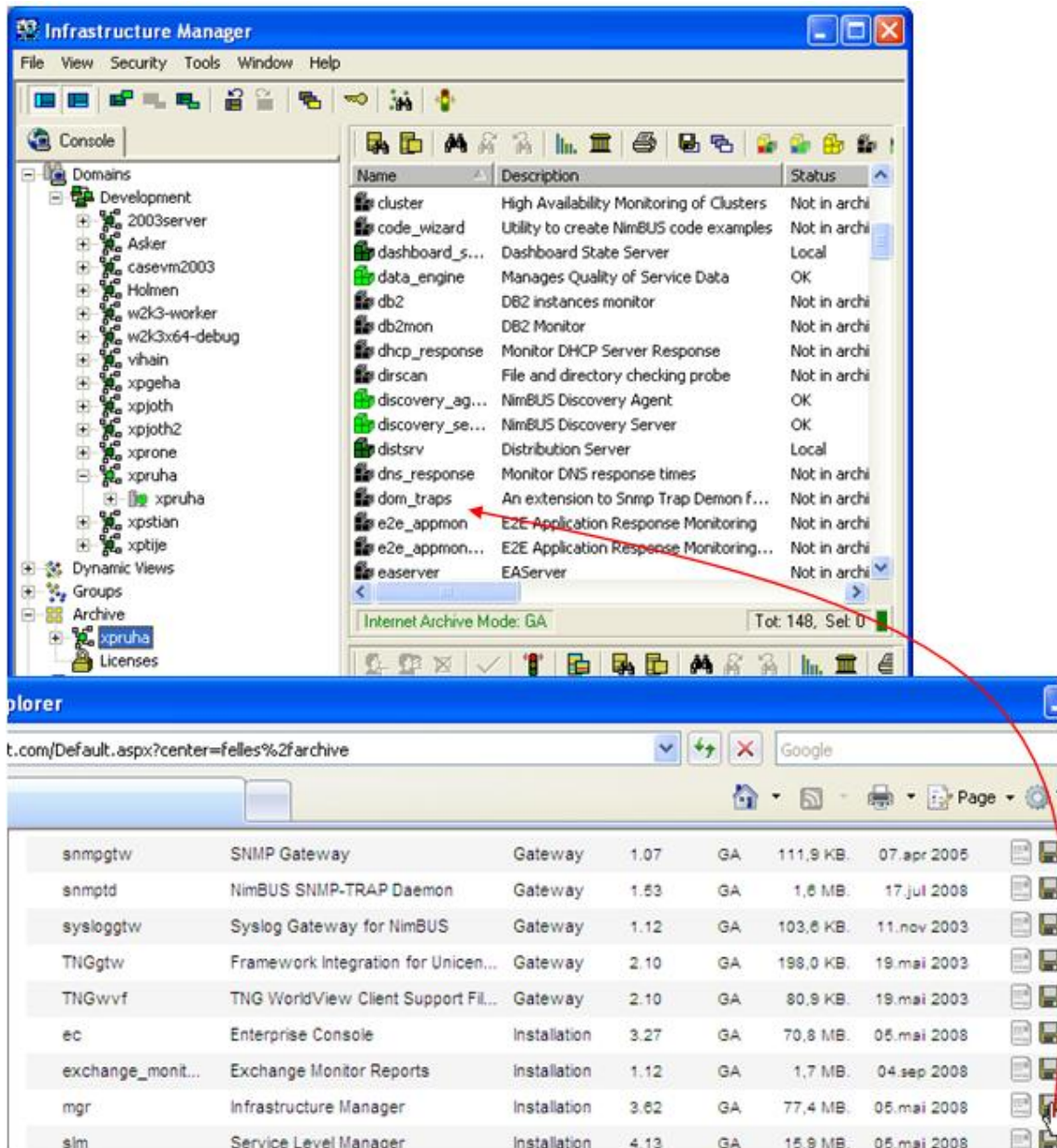
Chapter 6: Upgrading Client applications

Upgrade description

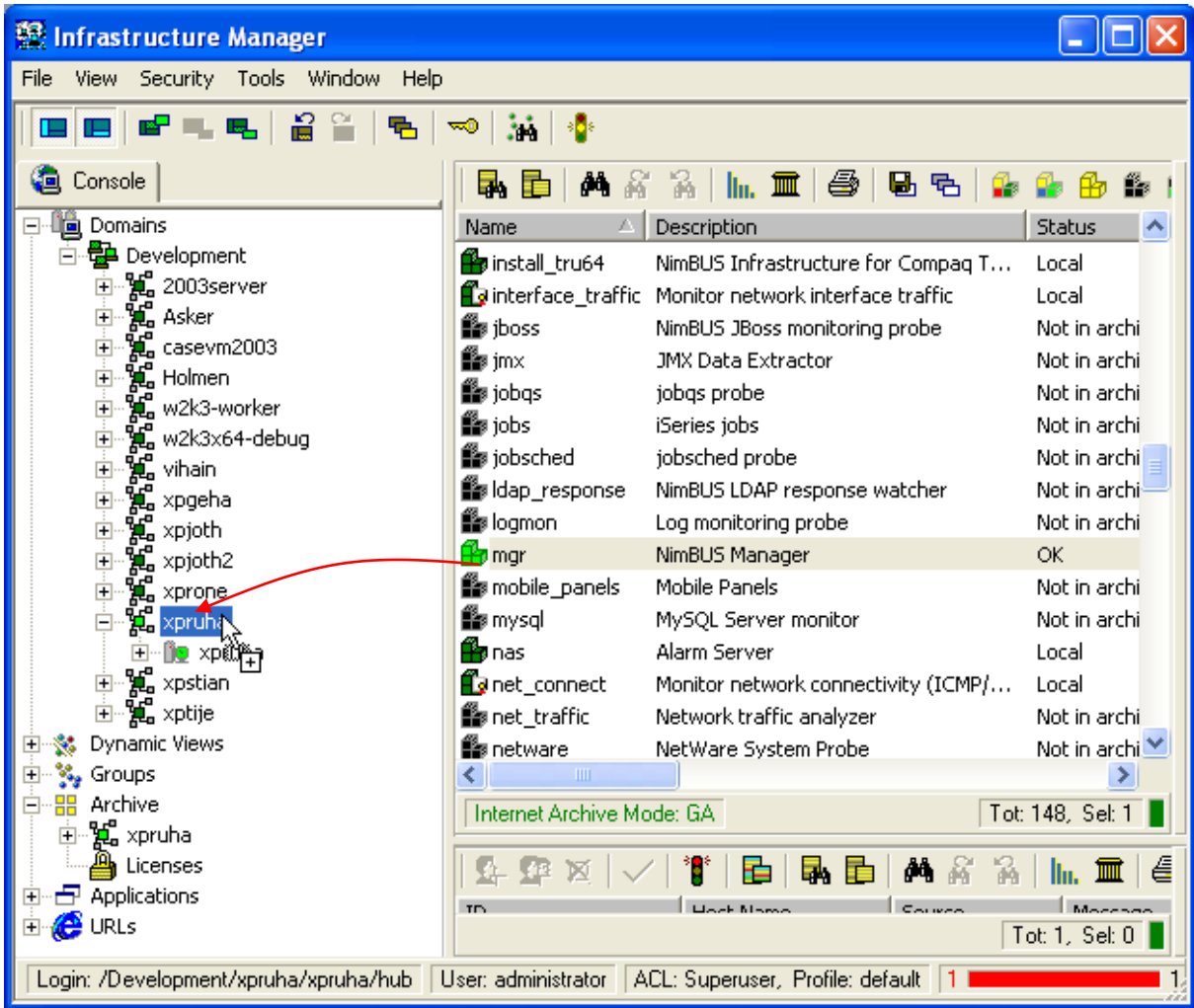
Nimsoft Server is the tool for downloading and installing Nimsoft Software products.

A simple procedure to upgrade a client application is described below. The example describes how to upgrade Infrastructure Manager:

1. Open the Nimsoft Web Archive. Under the Installation section, you will find the files to download (in this case the zip file for Infrastructure Manager).
2. Open the local package archive located under the Archive node in the Navigation Pane in Infrastructure Manager.
3. Drag the zip file (e.g. mgr) from the Nimsoft Internet Archive and drop it in your local package archive in Infrastructure Manager.



4. In Infrastructure Manager, distribute the package from your local archive to the computer where Nimsoft Server is installed, using drag and drop.



- To upgrade the client application in your environment:
From the client machine you want to upgrade, open a browser and address your Nimsoft Server page (for example: wsrune.nimsoft.no). Start the installation procedure from the Nimsoft Server by clicking the Client Install icon and then clicking the Infrastructure Manager link in the Client Installation window.

User Interfaces

These installations will install the user interface for the product.

Enterprise Console
Infrastructure Manager
Service Level Manager

6. The Download dialog pops up. Select Open to start the installation immediately (note that you may select Save if you want to save the Infrastructure Manager.exe file to disk if you want to run the installation later).

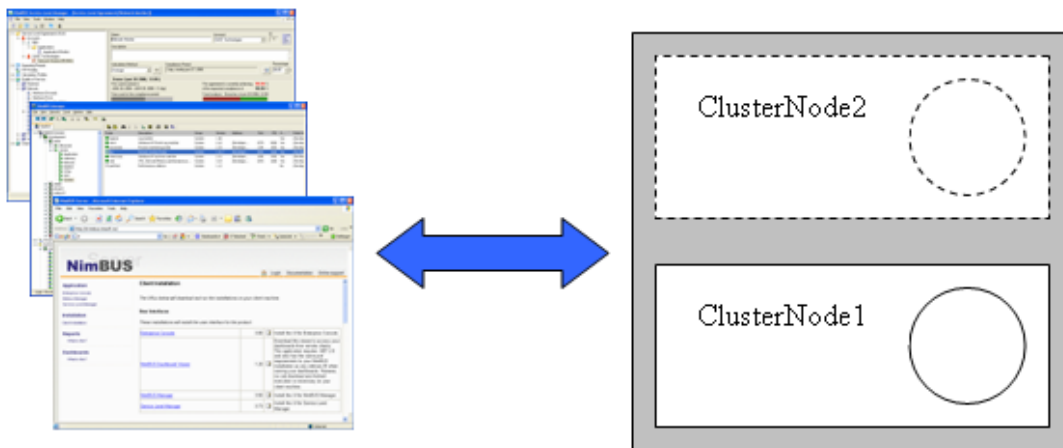
The files are copied from the Nimsoft Server to your computer, and the wizard starts extracting the files.

7. Follow the steps in the wizard to complete the installation.

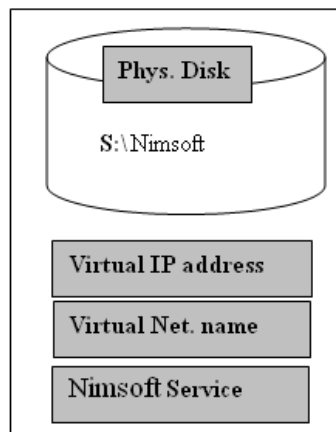
Chapter 7: Installing Nimsoft in an active/passive Microsoft Cluster

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 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.

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 installing the Nimsoft Consoles (Infrastructure Manager, Enterprise Console and Service Level Manager) on the cluster nodes, but rather installing 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).

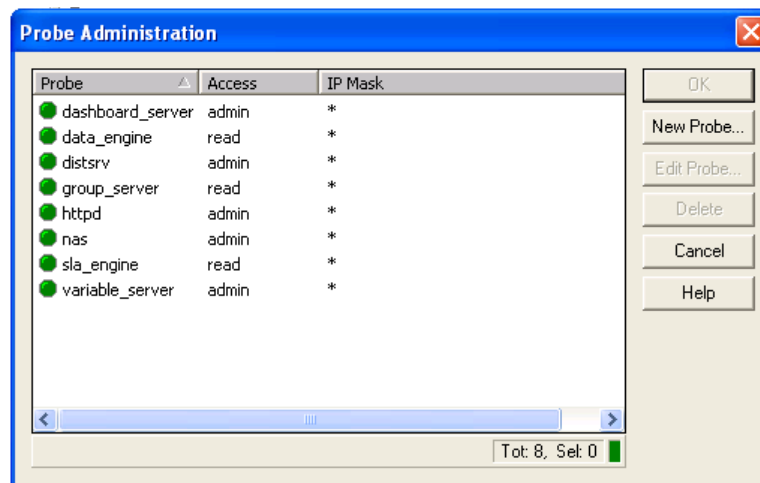
Test whether the above configuration works by moving it from one cluster node to the other. Bring up a command shell from the Start/Run menu, and check that the virtual IP address is available using the ipconfig command, that you may access the disk resource by dir S:

6. Prepare to install the Nimsoft infrastructure component of your choice. We chose to install a complete Nimsoft Server.
7. Modify the install directory to e.g. S:\Nimsoft (the physical disk from step 5).
8. Give the hub a name, e.g. CL-NIMSOFT and complete the installation acc. to your needs. Do not install Nimsoft consoles.
9. The installation program will detect multiple network interfaces and will present them in a list. Choose "Automatic".
10. Log in with Infrastructure Manager from another machine.
11. 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).
12. 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.



13. 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-bits systems, it should look like this:

SOFTWARE\Wow6432Node\Nimbus Software\NimBUS Installation

14. Bring the Nimsoft Service resource to an online state in the Cluster Administrator using the action menu on the selected item.
15. 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.
16. Register Nimbus.dll on the other computer (the one you are NOT installing from).
Example:
`regsvr32 S:\Nimsoft\lib\Nimbus.dll`
17. Export the "Nimbus Watch Service" entry from under "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services" and import it on to cluster member.
18. Reboot the computer for the DLL registration and the service entry to take effect.

Complete the installation on the second cluster node

Installing Nimsoft in an active/passive Microsoft Cluster

19. 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.
20. Register Nimbus.dll on the other computer (the one you are NOT installing from).
Example:
regsvr32 S:\Nimsoft\lib\Nimbus.dll
21. Move the Nimsoft Cluster Groups between the nodes and verify that the Nimsoft probes come up on both nodes.

You should now have a Nimsoft running in your cluster.

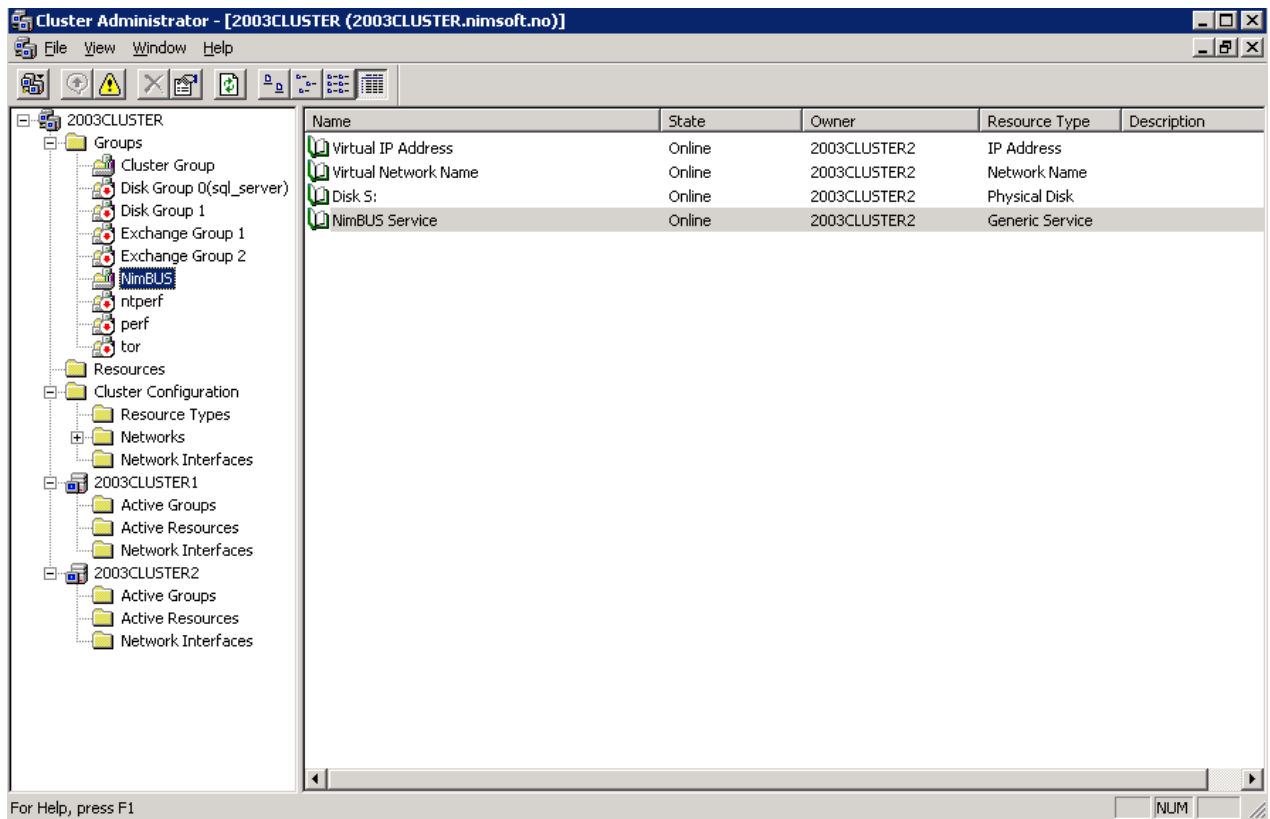


Fig. 1 – The Cluster Administrator

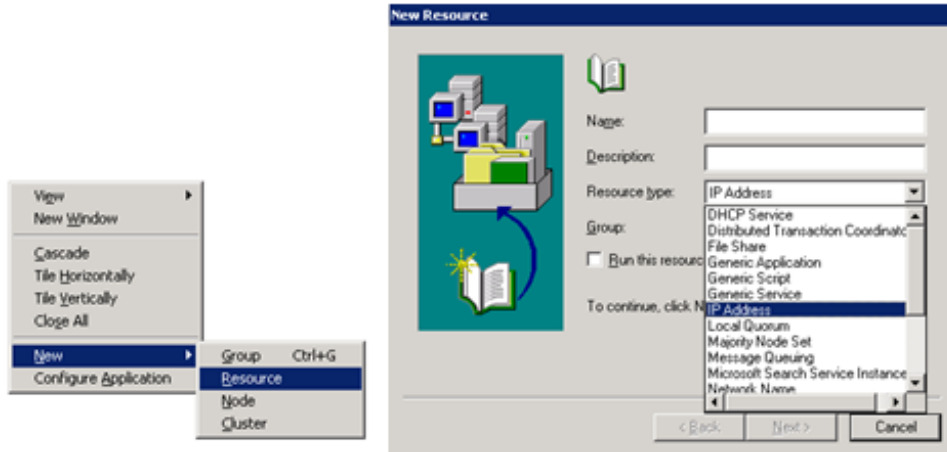


Fig.2 – Defining a new cluster resource

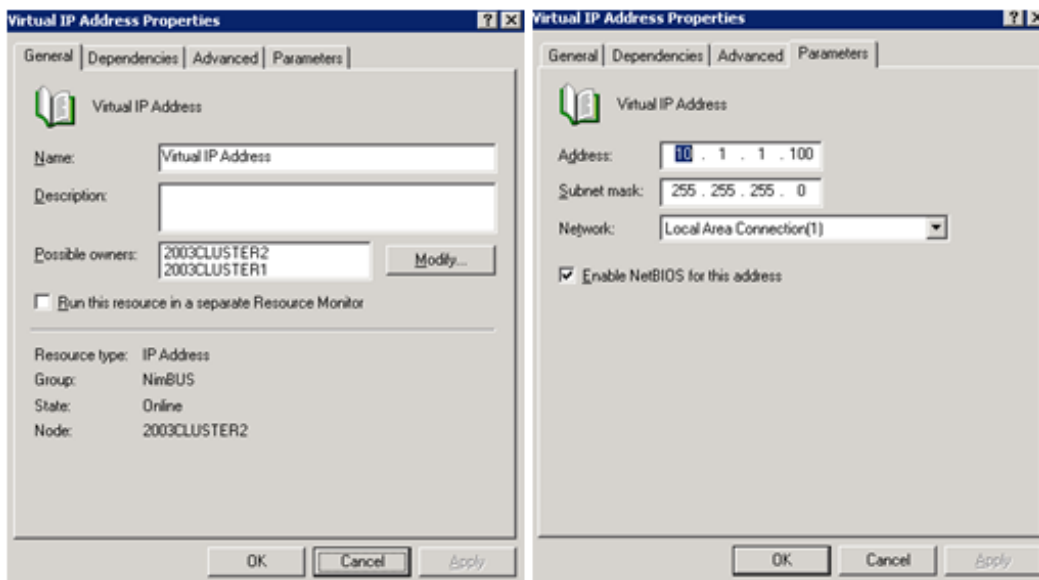


Fig. 3. – Defining a Virtual IP Address resource

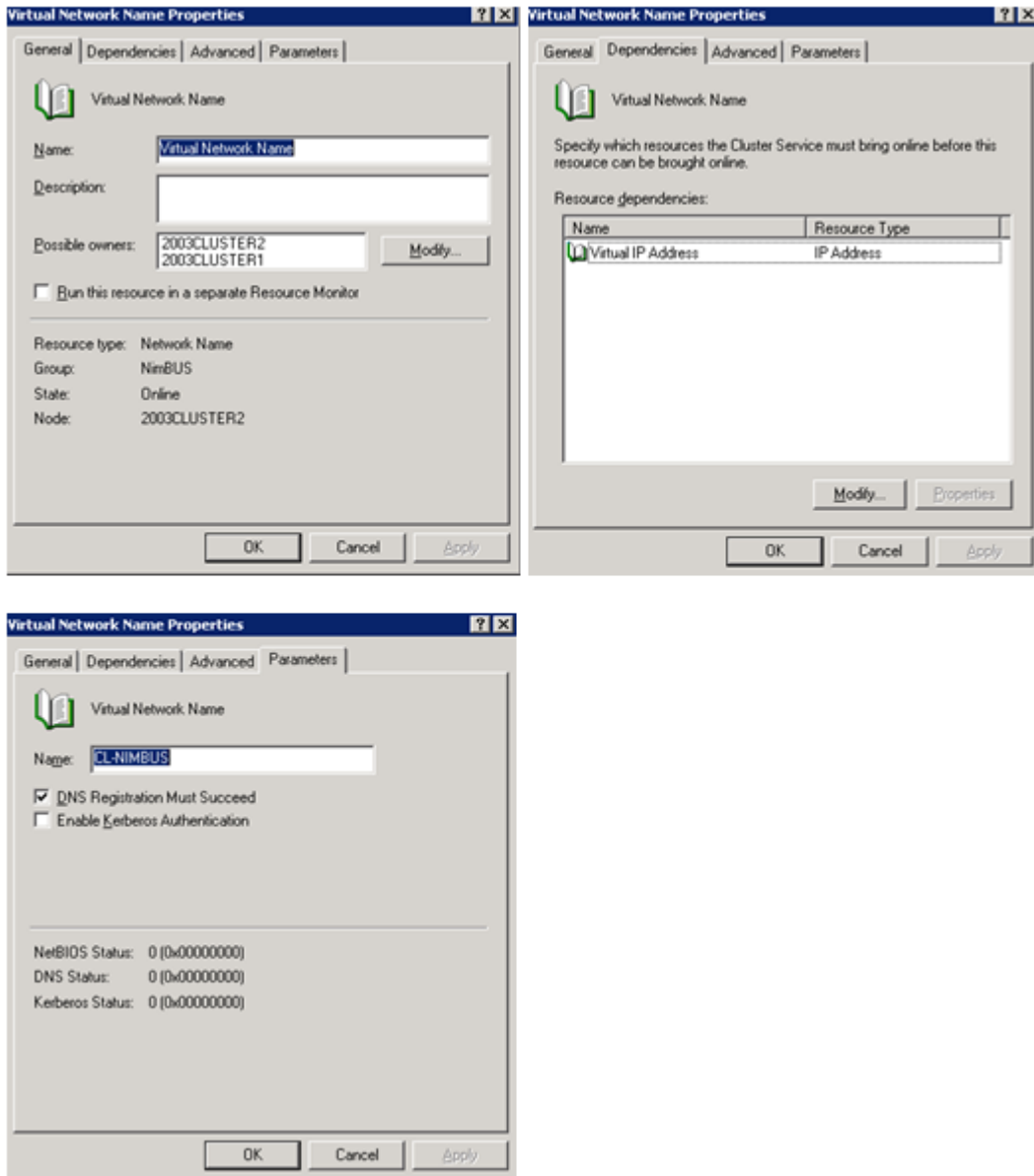


Fig. 4 – Defining a Network Name resource

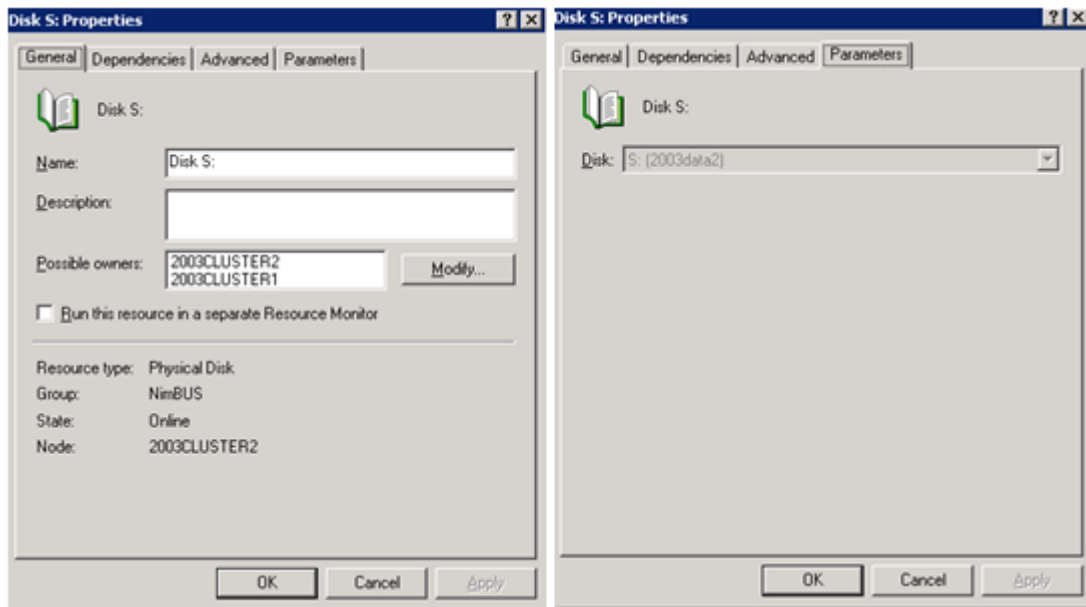
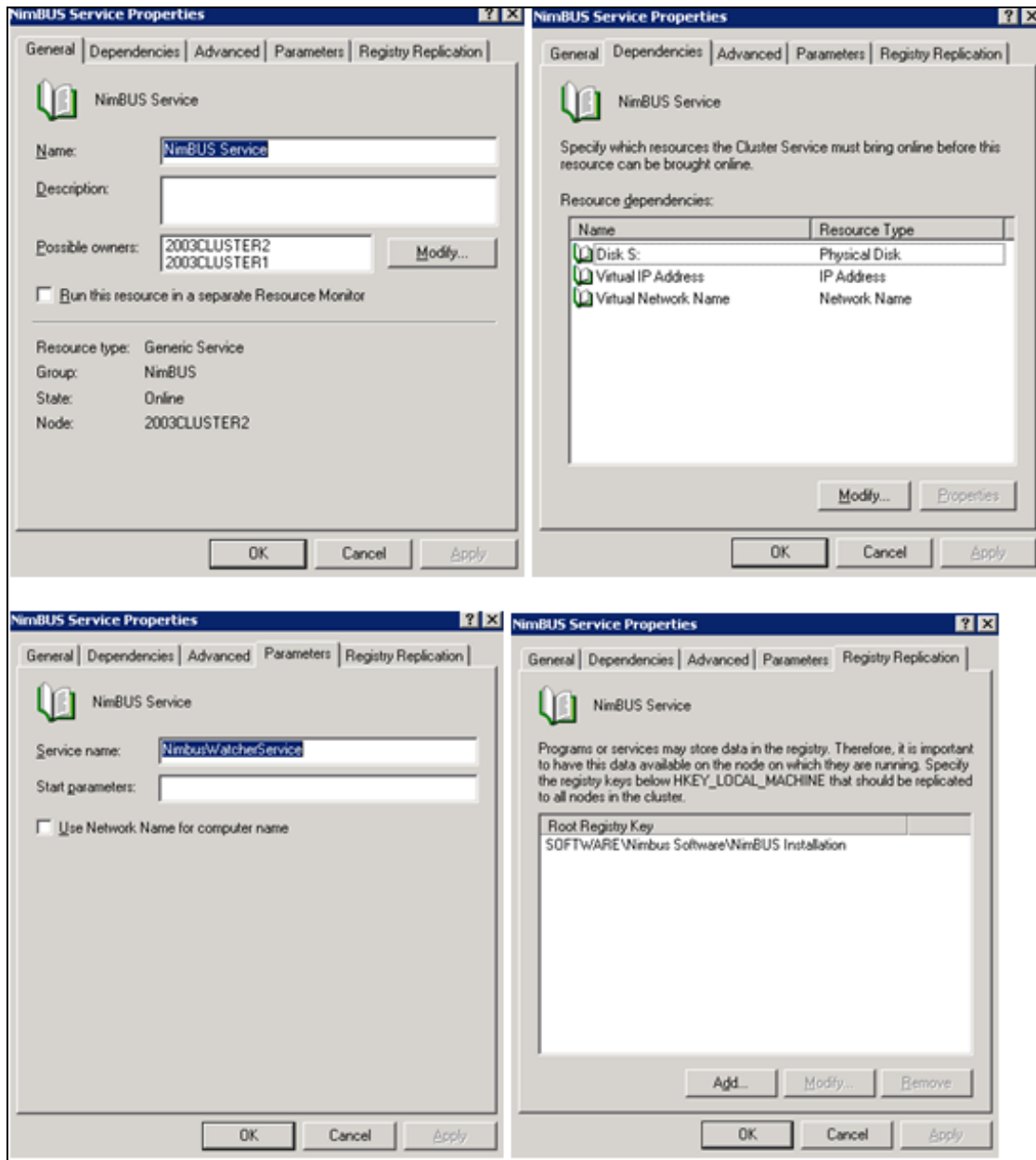
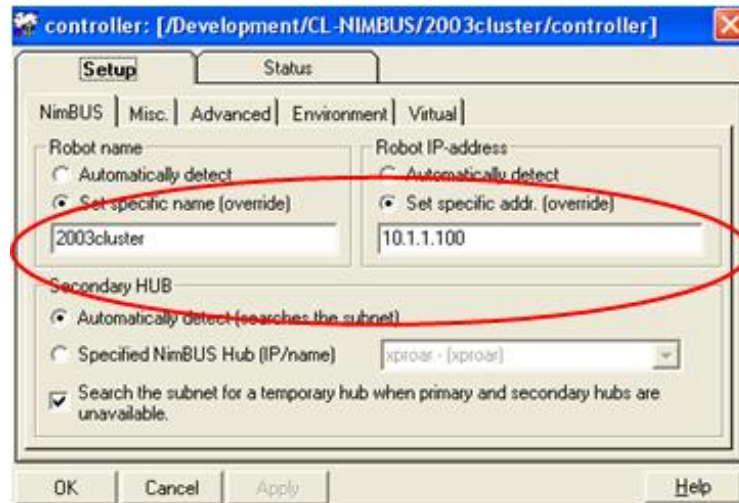


Fig. 5 - Defining a Disk resource





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 reinstallation.
Bring the Nimsoft Service online again in the Cluster Administrator.
- Log into Infrastructure Manager and activate the probes which are not running.
- If upgrading Nimsoft Server from an version older than Nimsoft Server 3.60:
Install the following files on the second cluster node:
vcredist_x64.exe
<http://www.microsoft.com/downloads/details.aspx?FamilyID=ba9257ca-337f-4b40-8c14-157cfdffee4e&DisplayLang=en>

vcredist_x86.exe
<http://www.microsoft.com/downloads/details.aspx?FamilyID=9b2da534-3e03-4391-8a4d-074b9f2bc1bf&DisplayLang=en>

Chapter 8: LDAP Configuration

The Nimsoft LDAP solution makes 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.

The screenshot shows the 'Hub Advanced Settings' dialog box. The 'LDAP Authentication' section is highlighted with a red border. The settings are as follows:

Section	Setting	Value
Broadcast On	Broadcast Address	255.255.255.255
	Hub Request Timeout	30
Queue Settings	Reconnect Interval	180
	Disconnect Passive Queues	180
Hub Settings	Hub Update Interval	600
	Post Reply Timeout	300
Origin	Origin	xpemce
SSL Settings	Mode	Off
	Cipher Type	DEFAULT
LDAP Authentication	LDAP Authentication	<input checked="" type="checkbox"/>
	Server Name	odin.nimsoft.no
	Server Type	Active Directory
	Use SSL	<input checked="" type="checkbox"/>
	User	administrator
	Group Container (DN)	DC=nimsoft,DC=no
LDAP Authentication	Group Container (DN)	DC=nimsoft,DC=no

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.

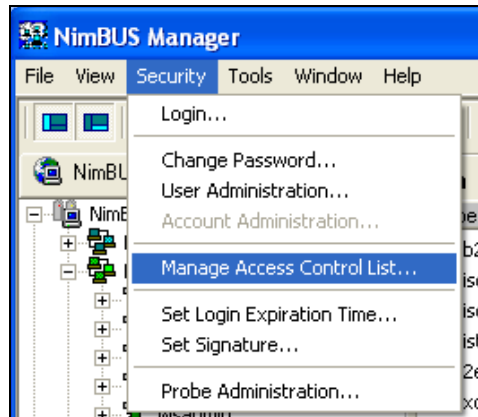
Connecting Access Control Lists to LDAP users

You can create Access Control Lists (ACLs) with belonging privileges. These ACLs can be associated with specific LDAP groups (when you attach the ACL to a LDAP group, the HUB will supply a list of groups from the container specified in the HUB). The users in the LDAP group will then be assigned the privileges for the associated ACL.

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.

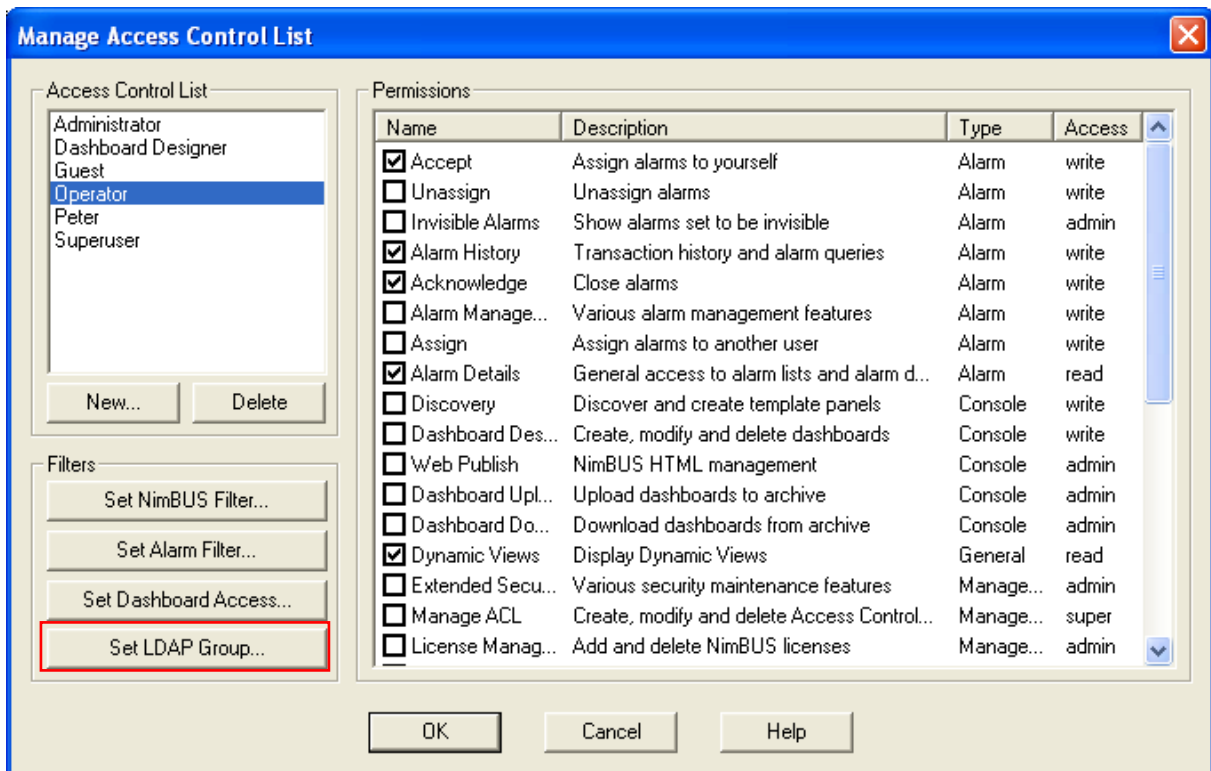
If the user belongs to multiple groups connected to ACLs, the user will be assigned the privileges from the ACL with the most extended privileges.

1. In Infrastructure Manager, open the Manage Access Control List dialog by selecting Security > Manage Access Control List from the menu bar.

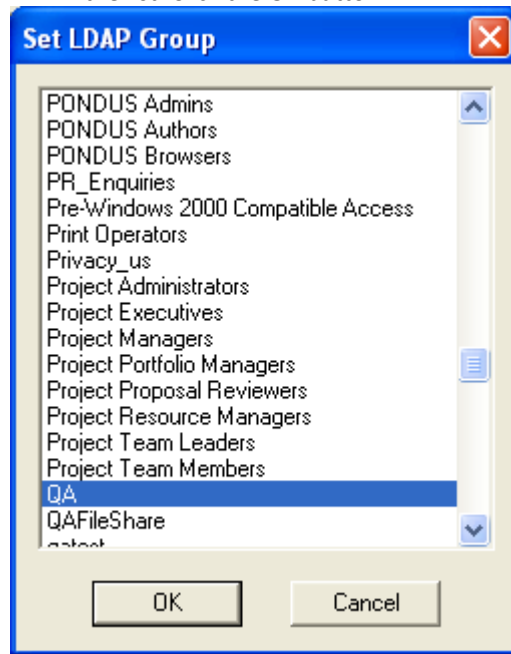


In this example we will assign the ACL called **Operator** to the users in a LDAP group called **QA**.

2. Select the ACL Operator and click the Set LDAP Group button.

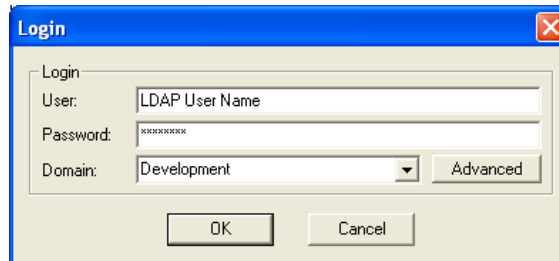


3. The Set LDAP Group dialog appears. Scroll to find and select the QA entry in the list. Click the OK button.



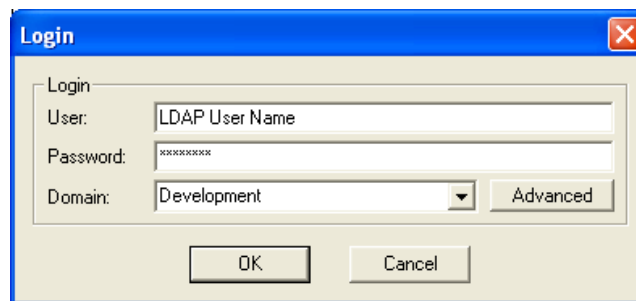
- Click the OK button in the Manage Access Control List dialog to exit and activate the new setting.

Test that the LDAP user login works by logging on Infrastructure Manager with a user in the LDAP group you selected in step 3.



Verification

Launch the Infrastructure Manager and log in as a LDAP user that does not exist as a Nimsoft user.



Verify that you can access the expected contents and have the privileges as described by the ACL which 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 do 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:

[http://msdn.microsoft.com/en-us/library/ms776446\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms776446(VS.85).aspx)

On Windows, the Hub LDAP library will use MultibyteToWideChar and WideCharToMultiByte functions to translate to and from ANSI/UTF-8. These functions take a codepage as a parameter.

On all other platforms, the Hub LDAP library will use iconv functions. Ref:

<http://www.gnu.org/software/libiconv/>

The codepage key is not shipped with the Hub configuration file.

The default value if none is specified is:

codepage value	OS	Description
28591	WINDOWS	ISO 8859-1 Latin 1; Western European (ISO)
ISO-8859-1	UNIX	ISO 8859-1 Latin 1; Western European (ISO)

On windows platforms, it's a numerical value, on Linux; it's a text string which can be passed into iconv_open function.

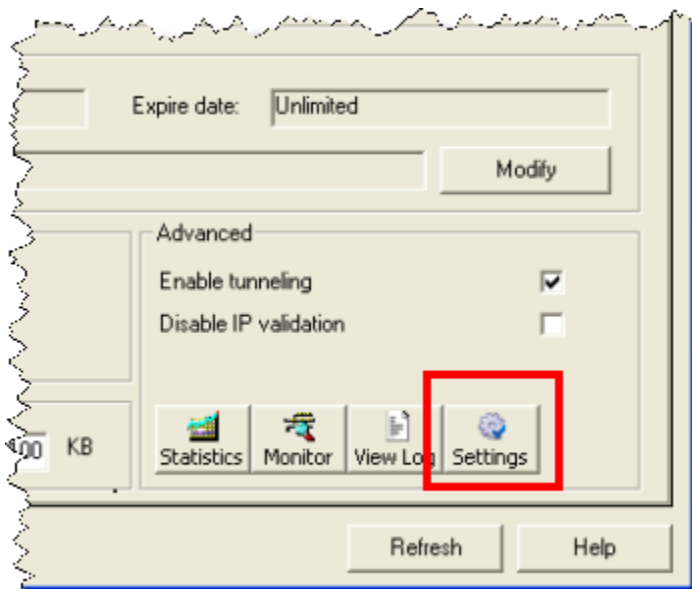
Chapter 9: SSL – Encrypting network traffic

Nimsoft Secure Communication gives you the option of SSL encrypted communication between all Nimsoft components. This feature also has a compatibility mode which allows you to use old and new components in the same environment (with and without SSL). The SSL feature only encrypts network traffic. It is not used for authentication.

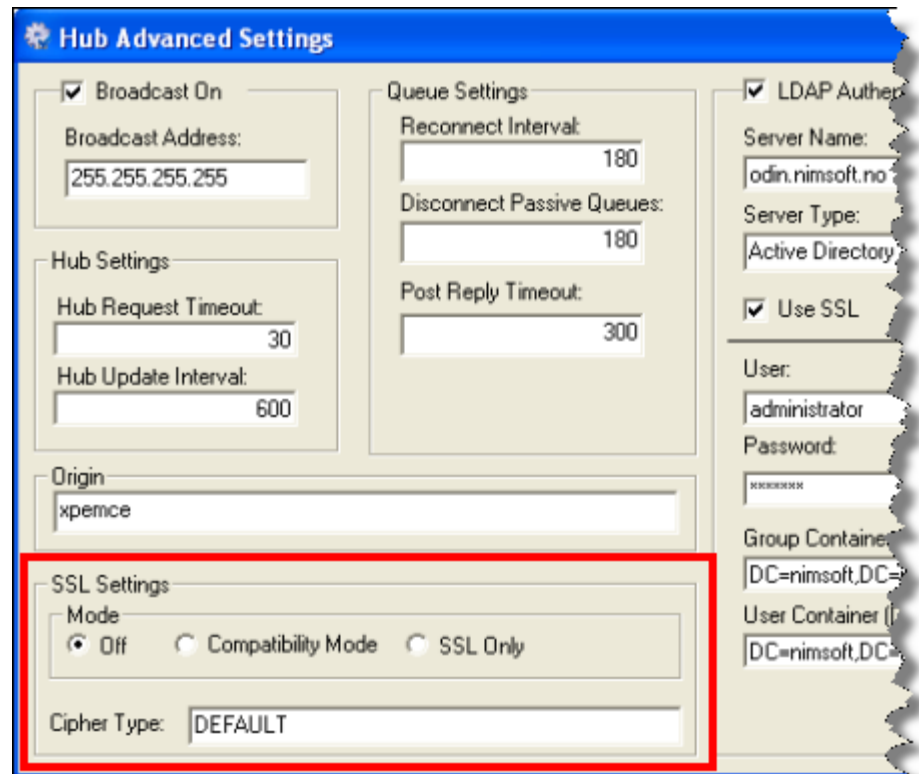
SSL settings are specific to each Hub, and you need to repeat the procedure below for every Hub requiring SSL.

Do as follows:

1. Navigate to the relevant Hub and double-click it. The General tab opens.



2. In the General tab, click the Settings button in the lower right corner. The Hub Advanced Settings dialog opens.



3. In the lower left corner, you can set the SSL Settings as follows:
 - Off – NimBUS only
 - Compatibility Mode (recommended!) – Mixed SSL/Nimbus mode. The system checks for SSL compatibility. If there is no SSL compatibility, the system uses NimBUS
 - SSL Only – the Hub will only communicate with components using SSL.
- We recommend that you use Compatibility Mode. In this mode all components will try SSL communication first, but will be able to switch to NimBUS communication for older components.
- Note! If one Hub in a domain is changed to SSL Only mode, all hubs in the same domain that have the Off mode will also be changed to SSL Only mode. (Hubs with Compatibility Mode will not be affected.) And since all Hubs exchange security and address information all the time, all systems will switch to use SSL Only after a time.
4. Click OK when you are finished. The Hub will propagate the SSL settings to the robots, which in turn propagate the settings to the probes.
 5. Repeat the procedure above for each Hub you want to set SSL for.

Troubleshooting

If you run a Hub in **SSL Only** mode the older components will not be able to talk to the new Nimbus components. So mixing different versions of NMS is not possible if you for some reason want to use the **SSL Only** mode.

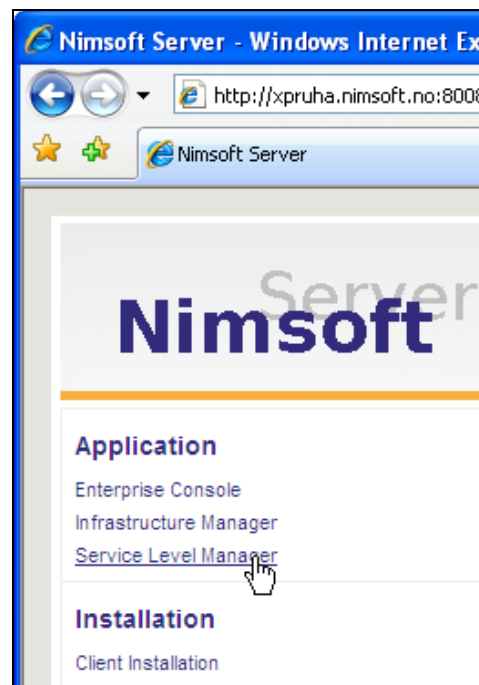
Chapter 10: Launching Nimsoft applications

Launching Infrastructure Manager, Enterprise Console or Service Level Manager

Via a web browser, you may launch the following Nimsoft applications from the Nimsoft Server portal from any computer on your network, provided that you selected to install them when downloading Nimsoft Server:

- Infrastructure Manager
- Enterprise Console
- Service Level Manager

Launch the application you prefer by clicking one of the icons in the left pane of the window:

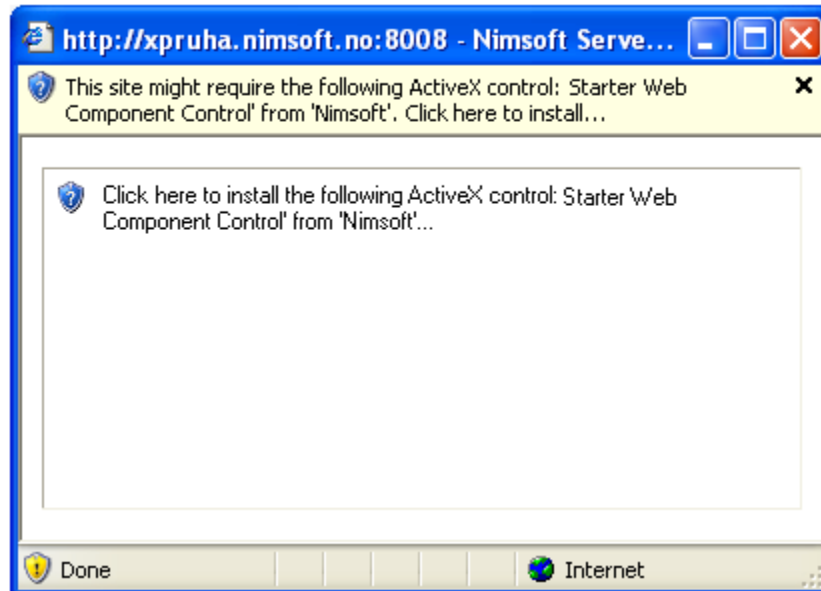


When launching the application, a check will be done to find if the application is installed on your computer.

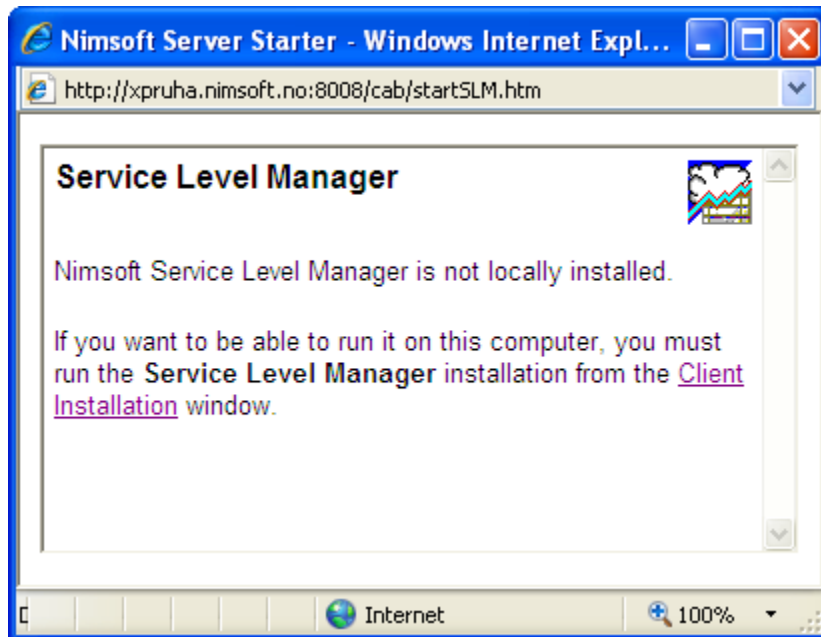
If the application is found, it will be launched.

Launching Nimsoft applications

Probably you need to install a specific ActiveX control required. If the following window pops up, just click inside the window to install the required *ActiveX control Nimsoft Starter Web Component Control*.



If it is not found, a small window opens, asking if you want to install the application.



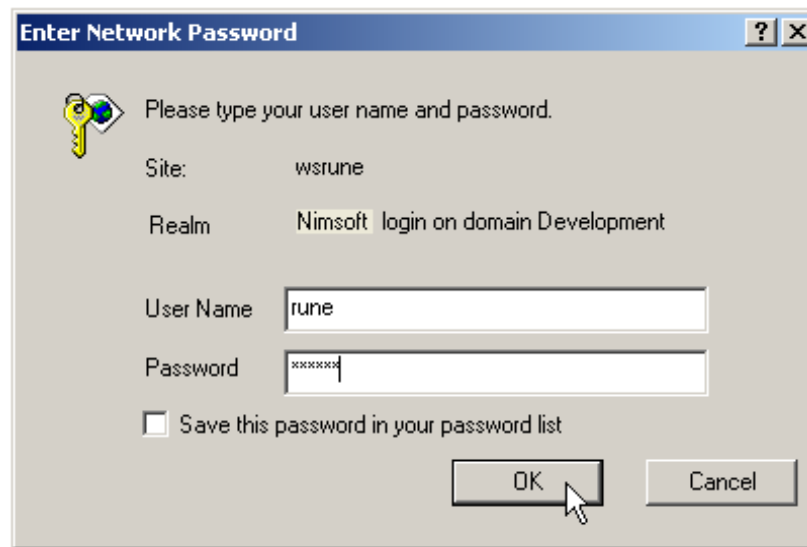
For further information, see the section [Client Installations](#).

Chapter 11: Accessing ACL protected dashboards

Using the *Web Publish* application (see the *Enterprise Console* on-line documentation), you can publish consoles, dashboards and reports. These published items will be listed in the main window of the home page in the Nimsoft Server application.

When publishing these items, you have the option to organize it in a way that gives different users different access privileges. **It means that some files (those not published using target ACL Default) are hidden from the home page. In order to access these files, you have to click the *User login* link.**

Logging on with a valid username and password, you will be able to access files published to the target ACL associated with this user.



Type the user name and password and click the *OK* button.

Note: When publishing dashboards and consoles, it is also possible to specify default login parameters. These parameters will appear in the login dialog when logging on.

Dashboards

 [Example](#)

Grouped Service Level Agreement Reports

 [Network Group](#)

 [Nimsoft Norway](#)

Service Level Agreement Reports

 [Demo](#)

 [nimsoft-gtw](#)

 [Nimsoft Network Infrastructure](#)

 [Nimsoft Web Page Monitor](#)

 [Rone](#)

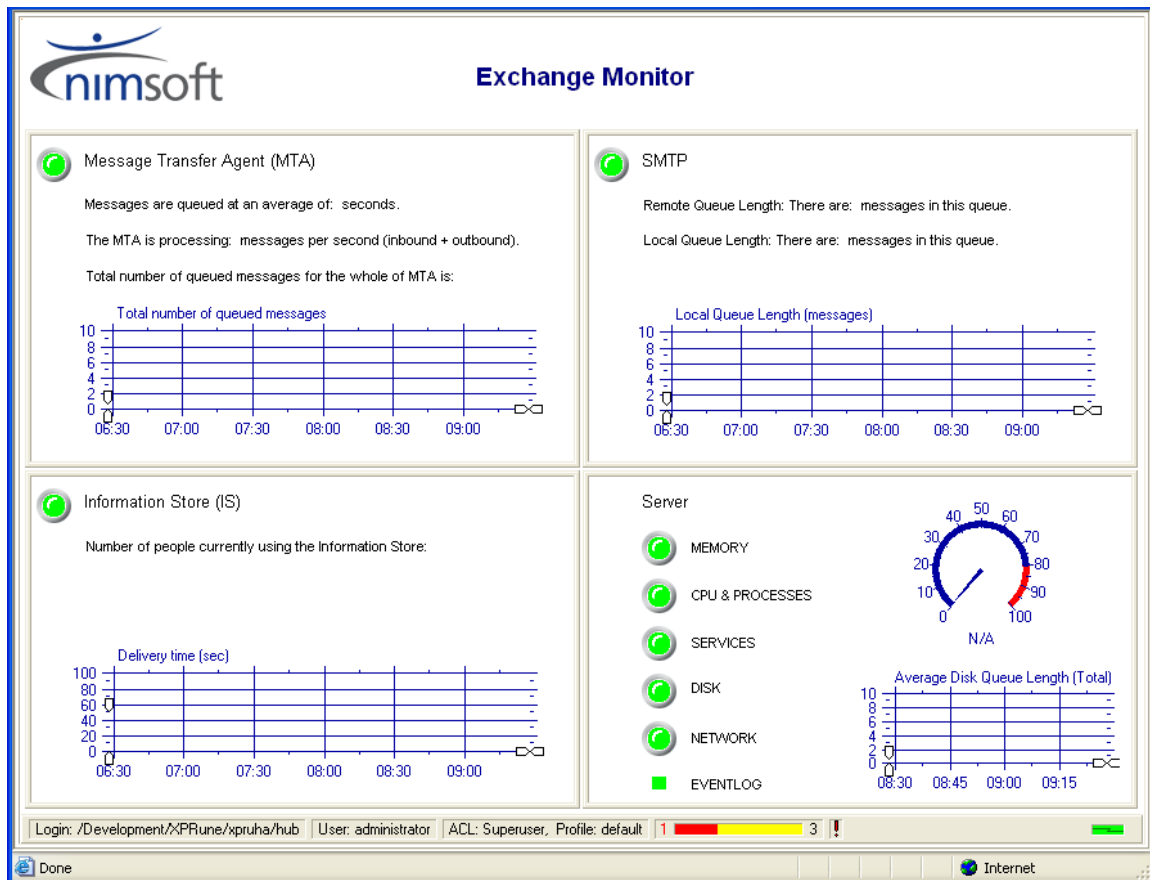
Quality of Service Reports

 [Example Report](#)

 [Jitter Test](#)

Dashboards

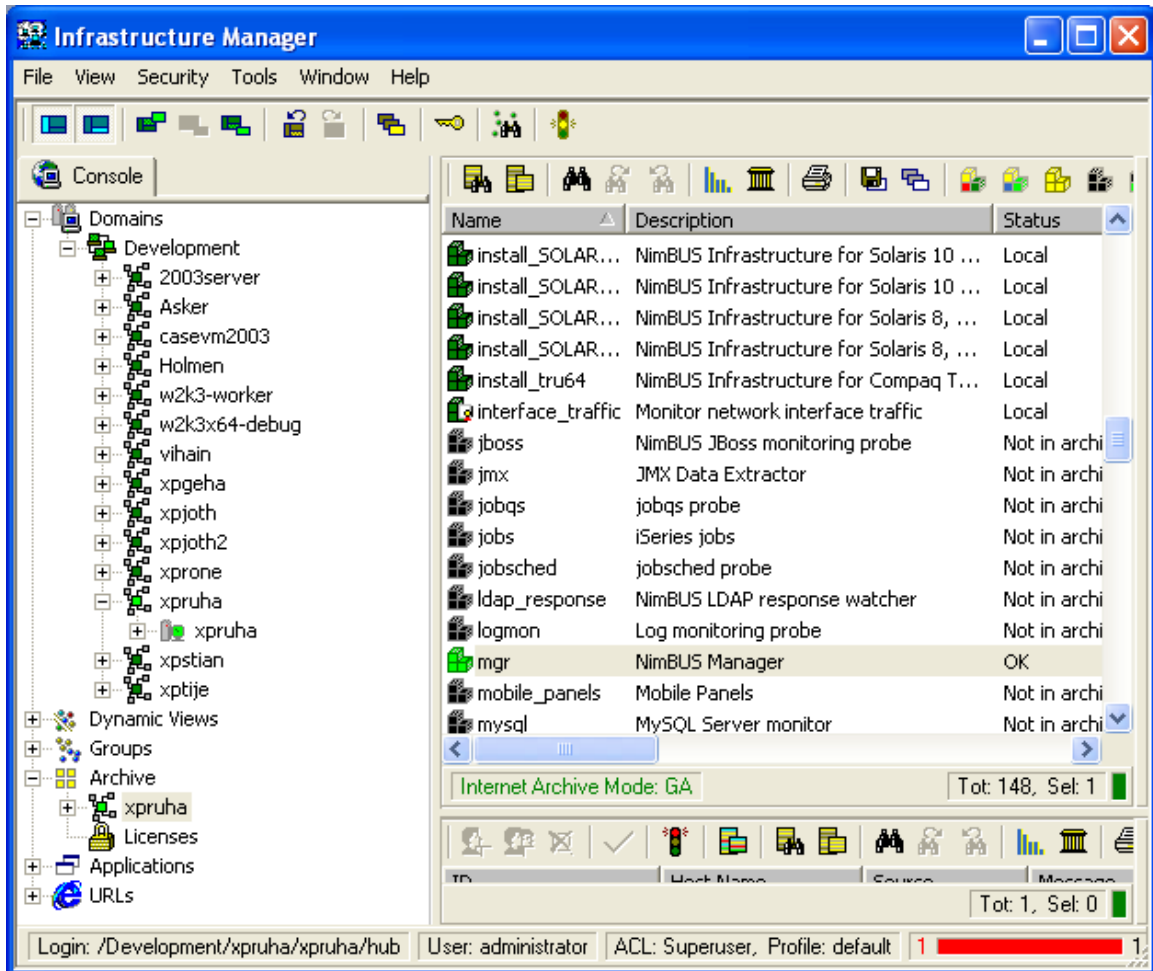
Clicking one of the dashboards will launch the dashboard in a separate window. You can view the selected Dashboard exactly the same way as in the Enterprise Console.



Consoles

Accessing ACL protected dashboards

If a console (for example the Infrastructure Manager) is published, clicking the link on this page will launch the Infrastructure Manager in a separate window. You may perform tasks such as configuring probes, distributing probe packages etc. just the same way as with the Infrastructure Manager application.



Reports

Clicking one of the reports will launch the report in a separate window. You can view the selected report exactly the same way as in the Service Level Manager.

nimsoft

Status History

Demo

hfhfhfh

This status is generated **June 12, 2006 00:05**.
The current period is **June 01, 2006 - July 01, 2006** (1 month)

Current compliance is 33.29%, the goal is 100.00%

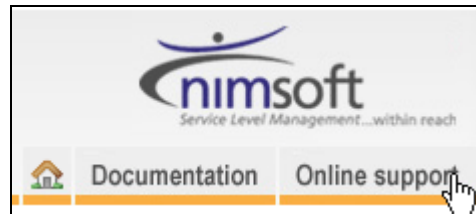
Trend Analysis: Breached at June 01 2006, 00:00

Service Level Objectives (Summary)
The following service level objectives are defined in this SLA. Each objective is listed with its weight and the percentage of fulfillment. The *fulfillment* is the relationship between the weight and the compliancy of the Quality of Service constraints defined within the SLO.

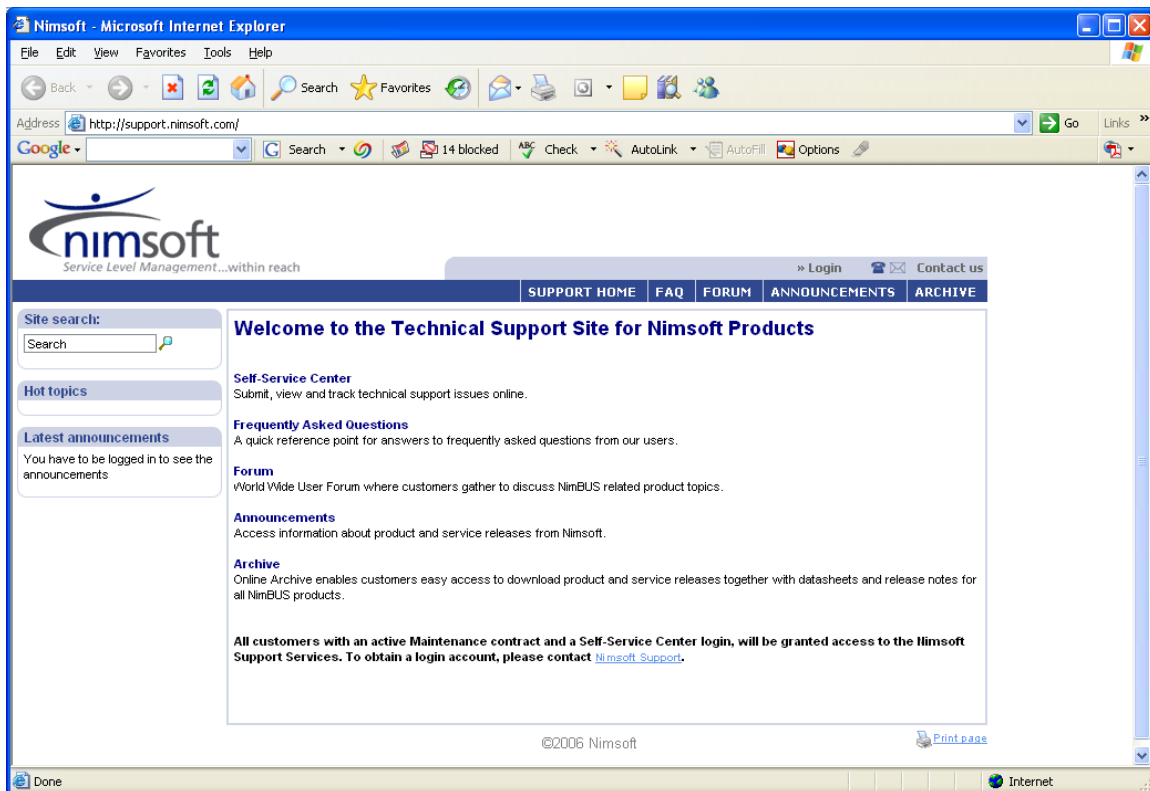
State	Objective	Description	Weight (%)	Achieved (%)	Expected (%)
🚩	E2E Målning fra Oslo		auto	33.29	100.00

Nimsoft Corp © 2006. The page was last updated Monday, June 12, 2006 00:05:25

Chapter 12: Accessing Nimsoft Online Support



In the upper right corner of the application window you will find the *Online Support* button. Clicking this button opens the Nimsoft Technical support site in a separate window.



The site offers the following services:

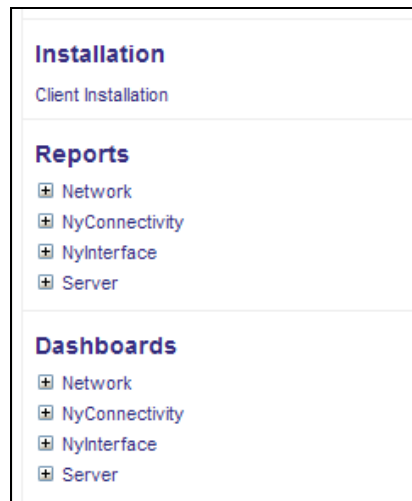
- Self-Service Center
Submit, view and track technical support issues online.
- Frequently Asked Questions
A quick reference point for answers to frequently asked questions from our users.

- Forum
World Wide User Forum where customers gather to discuss Nimsoft related product topics.
- Announcements
Access information about product and service releases from Nimsoft.
- Archive
Online Archive enables customers easy access to download product and service releases together with datasheets and release notes for all Nimsoft products.

Chapter 13: Launching Dynamic Reports

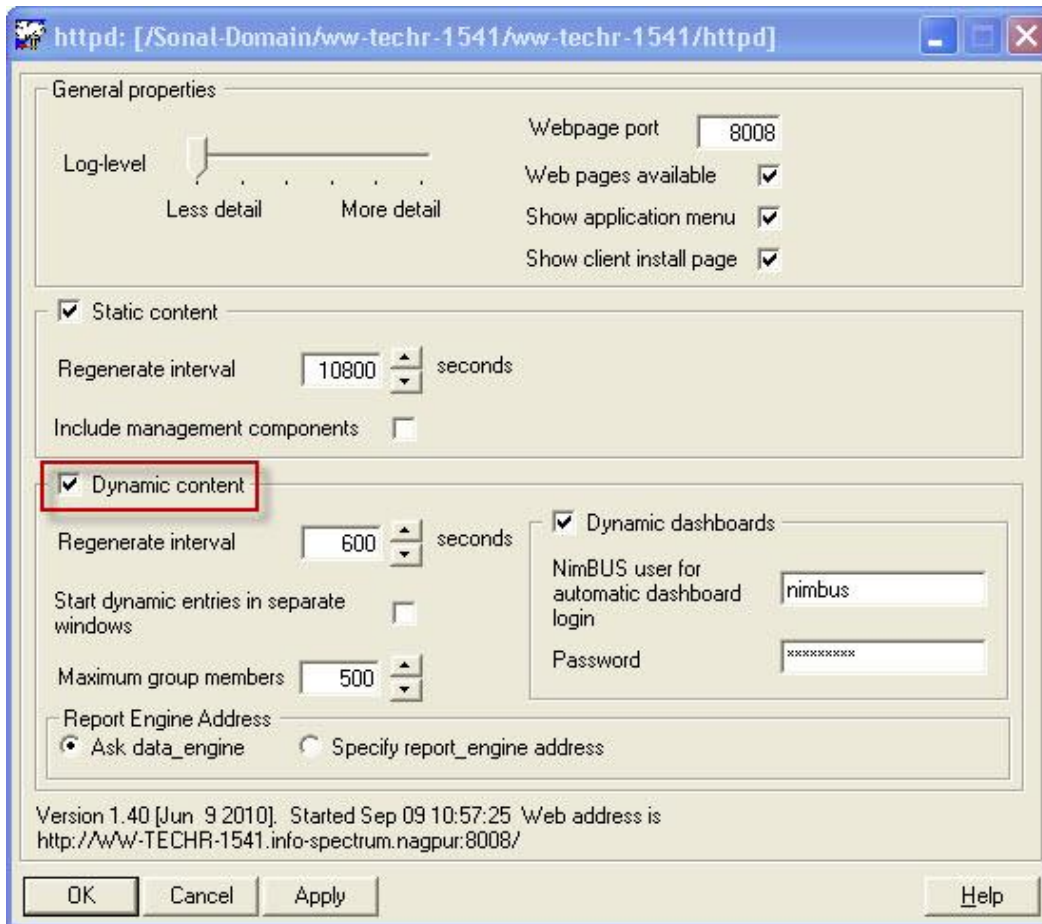
Introduction

Dynamic Dashboards and Reports can be launched from the Nimsoft Server application. The Navigation Pane of the Nimsoft Server application window by default contains the two nodes: Reports and Dashboards.



Note that you may hide these two nodes by re-configuring an option in the httpd probe.

Launch the httpd probe by double-clicking the probe in Infrastructure Manager. Turn the *Dynamic Content* option off (de-select it) and click the *Apply* button.



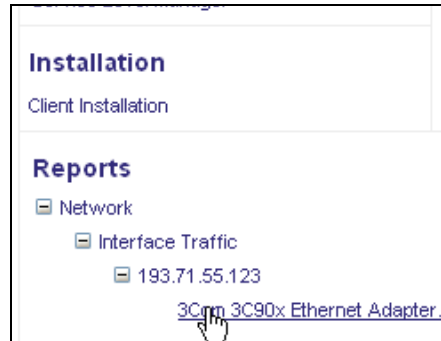
The Reports

The Dynamic Reports node lists Dynamic Reports generated by the Report Engine probe, provided that the option *Dynamic Reports* option in the Report Engine probe is activated.

Note that only devices delivering QoS data will be listed here. To achieve this, you must do as follows:

- If the Discovery module was selected during the installation of Nimsoft Server, you must set the devices you want to monitor to Managed, using the NIS Manager.
- If the Discovery module was NOT selected during the installation of Nimsoft Server, you configure the devices you want to monitor to deliver QoS data as described in the section Enabling Dynamic Reports.
- Clicking the end node will launch the Dashboard in the main window.

These Dashboards will be populated with context related data, organized by the Group Server probe.

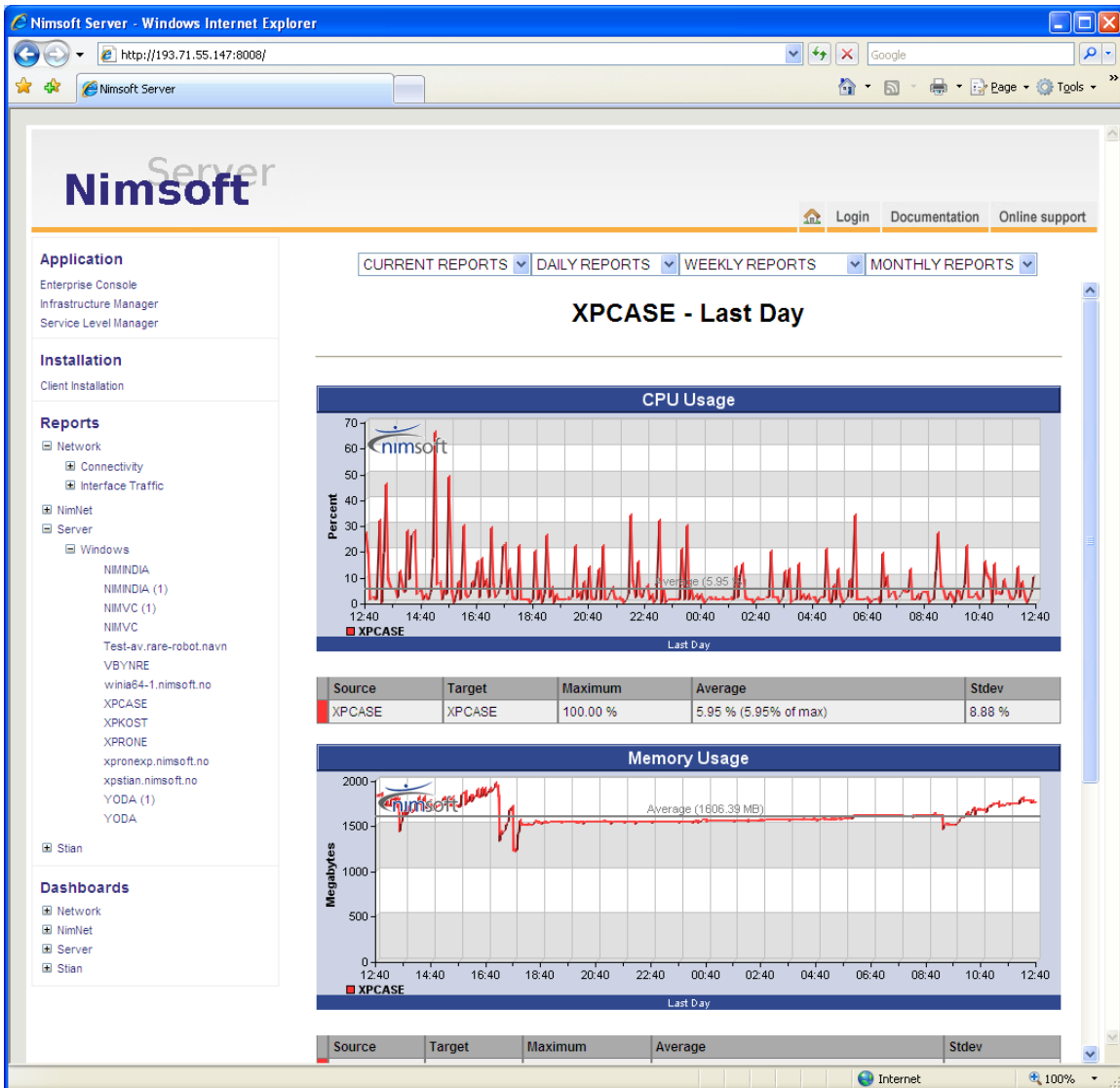


Initially after installation, you may experience that no reports are listed under the Reports Node.



Instead you will find the link *What is this*. Click this link and read the configuration instructions displayed in the main window, or read the instructions in the section [Preparing for Dynamic Reports](#).

When expanding the Reports node, you will find a set of child-nodes, representing different parts of your Nimsoft Infrastructure. The end-node will represent a Dynamic Report representing a device or host in your Nimsoft Infrastructure. Clicking the end node will launch the report in the main window. Note that option the Report Engine probe lets you choose between different report-layouts, using templates. You may also edit these templates to match your needs.



Drop-down menus in the reports let you choose between the following views:

- Current reports:
Last day (last 24 hours),
Last week report (last 7 days) and
Last month reports (last 30 days).
- Daily, Weekly, Monthly and Quarterly reports.
Note that the report_engine configuration tool lets you hide or show all or just some of these reports.

Preparing for Dynamic Reports

Initially after installation, you may experience that no reports are listed under the Reports Node.

If this is the case, you should check that the `report_engine` is correctly addressed and that Dynamic Reports are enabled on your system.

See the sections [Report engine not installed on the same server as the main hub?](#) and [Enabling Dynamic Reports](#)

Enabling Dynamic Reports

To enable reports, the following steps must be performed:

If "Discovery" WAS selected during the Nimsoft Server installation:

Set the devices to "Managed" in the NIS Manager.

Configure the **report_engine** and activate "Dynamic Reports" in the Setup window.

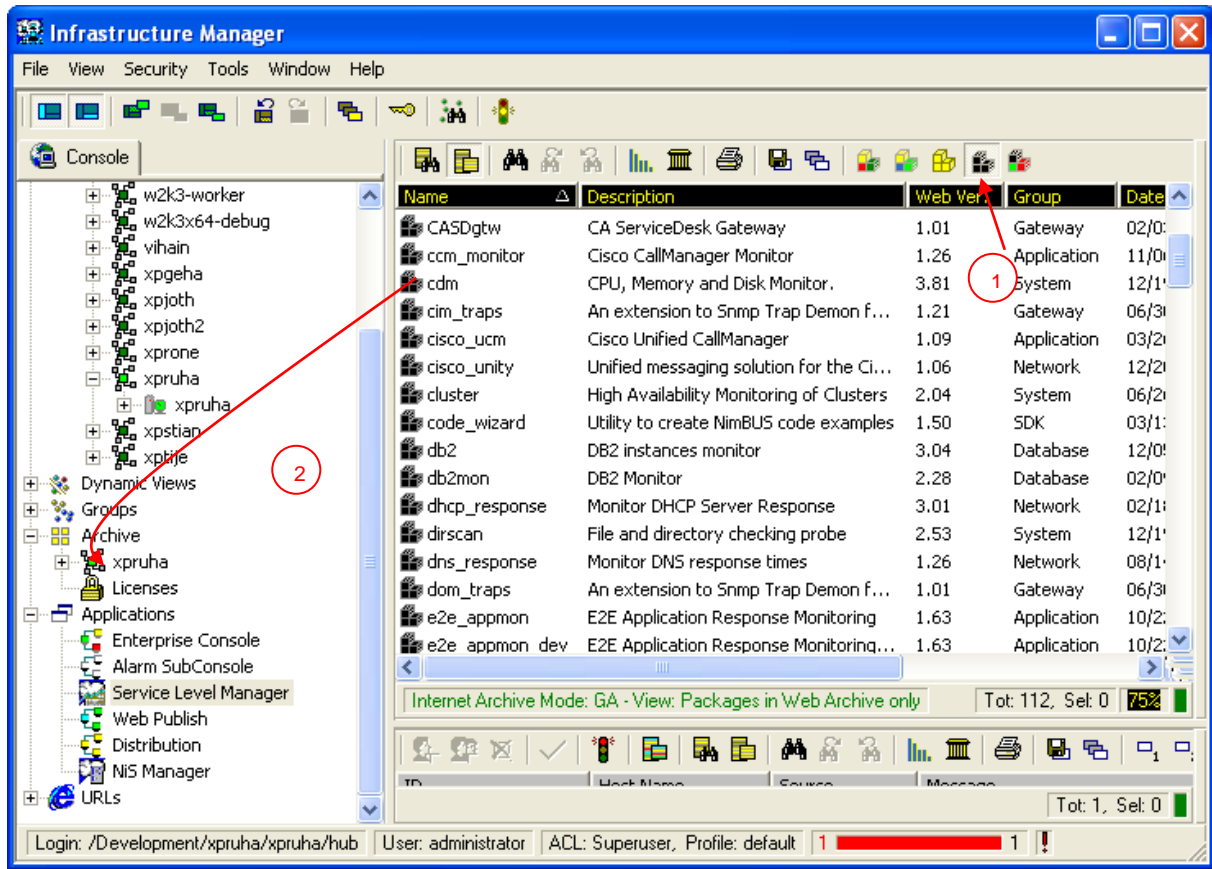
If "Discovery" WAS NOT selected during the Nimsoft Server installation:

1. Download `cdm`, `net_connect` and `interface_traffic` probes.

Ensure the Infrastructure Manager is installed. If not, install Infrastructure Manager as described in the section Installing Infrastructure Manager.

Launch the Infrastructure Manager. 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.

Click the "Packages in Web archive only" icon (1). Select the Probe package(s) you want to download. Drag and drop them onto your archive node (2).

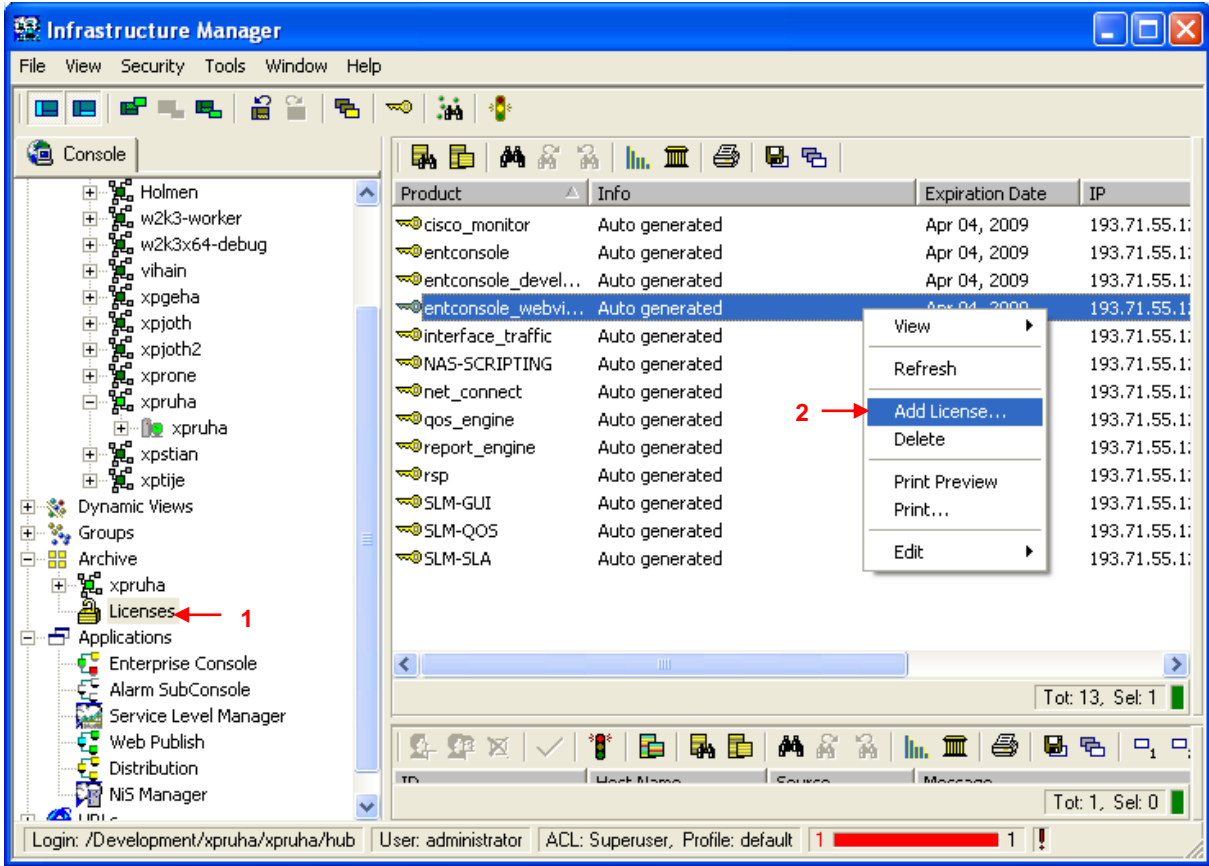


Note:

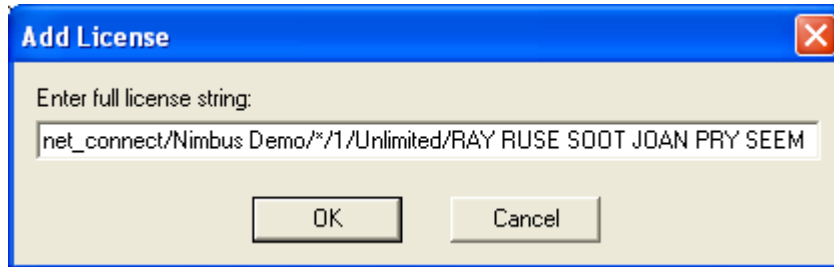
Unless you have checked the option Attempt Internet Archive integration with local archive, and filled in Salesforce Self-Service Center user credentials in the Tools > Options menu in Infrastructure Manager, you will be asked to enter Salesforce Self-Service Center user credentials to log in when you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

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

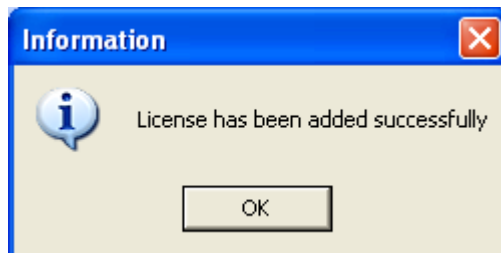
2. Install licenses for the net_connect and interface_traffic probes. Order licenses for the Probes by sending an email to support@nimsoft.com. You will then receive an e-mail, containing the licenses as a text strings. Do as described for both probes: With the Licenses icon under the Archive Node in the Navigation Pane selected (1), right-click in the main window pane and select Add license (2).



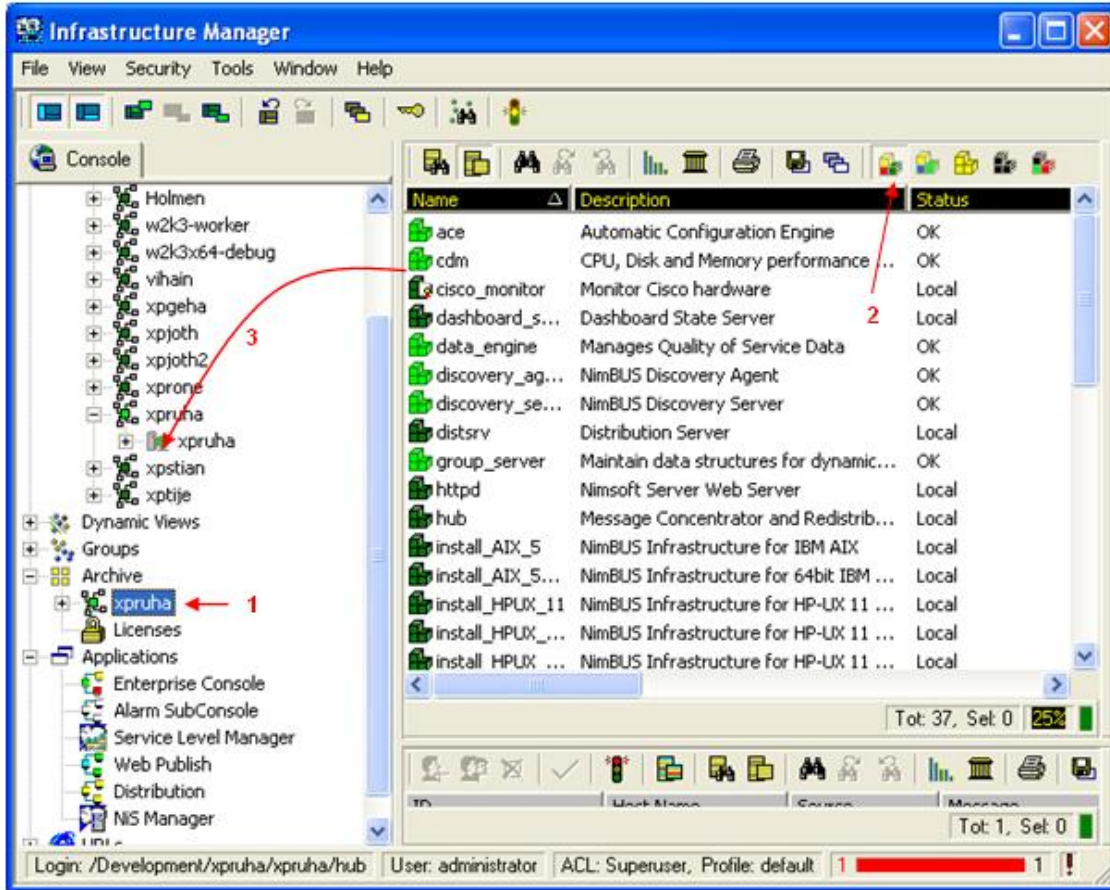
The following dialog appears. Paste or type the license text string into the text field of the dialog and click the OK button.



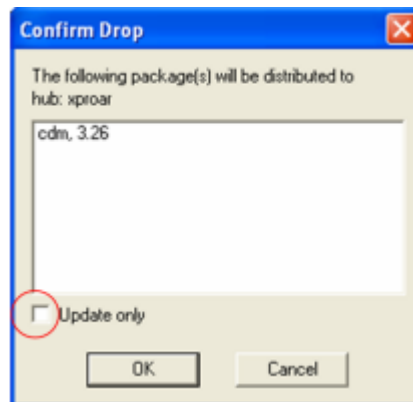
A message like the one shown below appears on the screen. Click the OK button.



3. Configure the net-connect and interface traffic probes with monitoring profiles for the devices you want to monitor. For information, see the Probes on-line documentation, made available by selecting Help > Probes from the menu bar in Infrastructure Manager.
4. Distribute the cdm probe to the servers to be monitored. Select the logon Hub icon under the Archive node in the Navigation Pane again (1). Click the “Packages in local archive only” icon (2). The Probe packages are listed in the Main Window. Drag the cdm probe package drop it on the servers to be monitored (3).
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.
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.



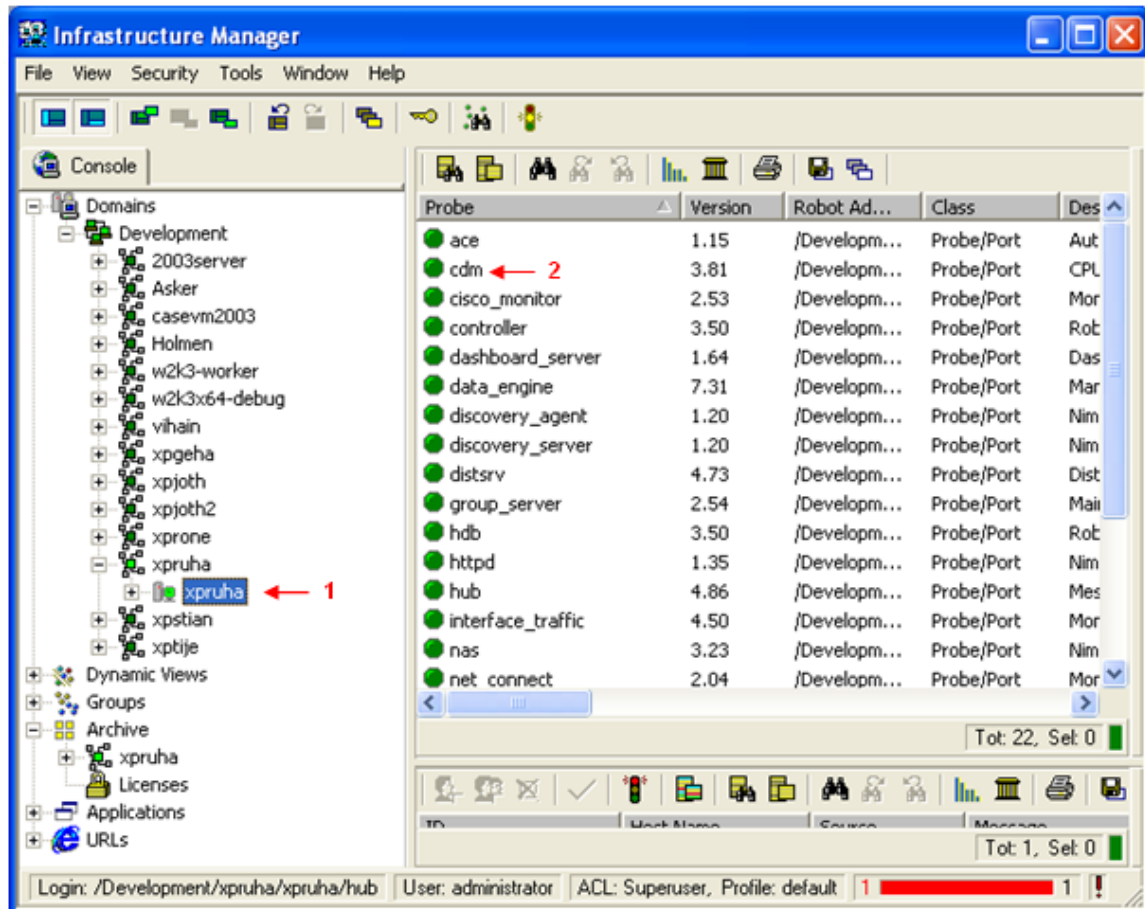
The following dialog appears. Note the Update only option. Uncheck this option (otherwise the probe packages will only be distributed to robots on which it already exists).



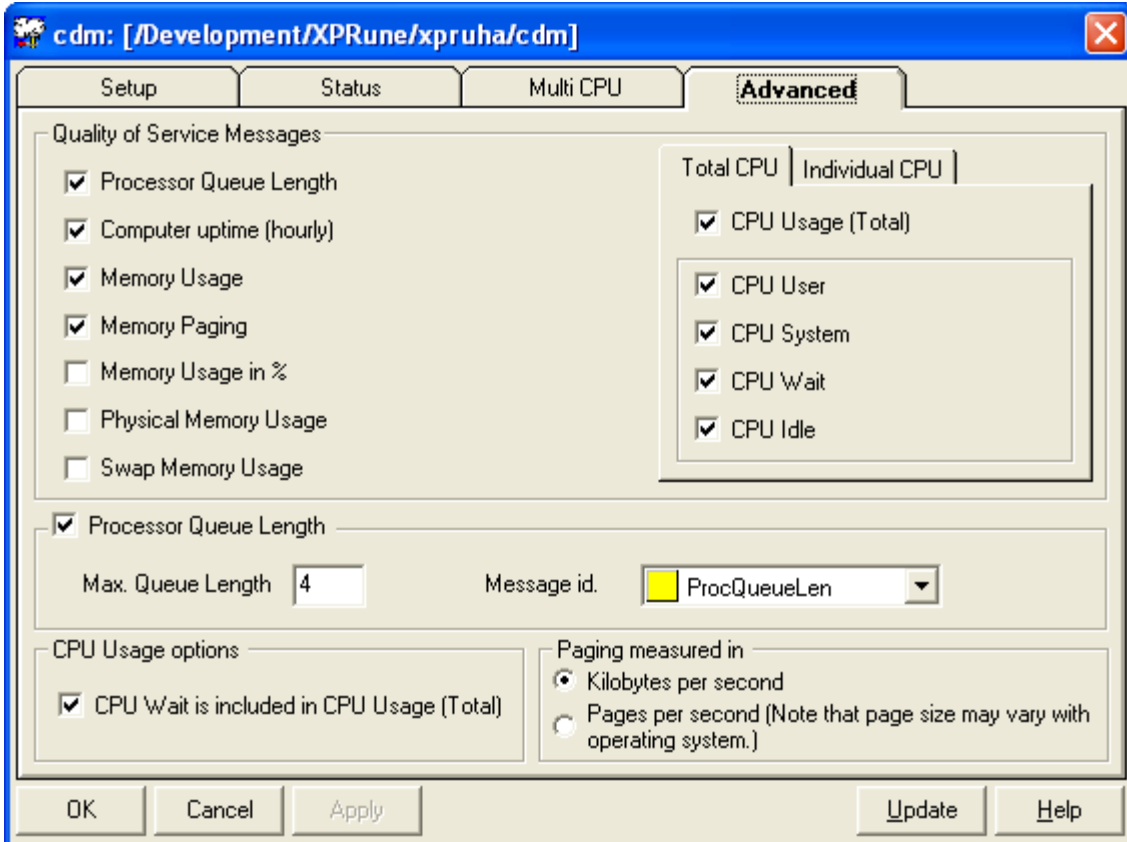
Click the OK button to continue.

5. Configure the cdm probes to collect Quality of Service data.

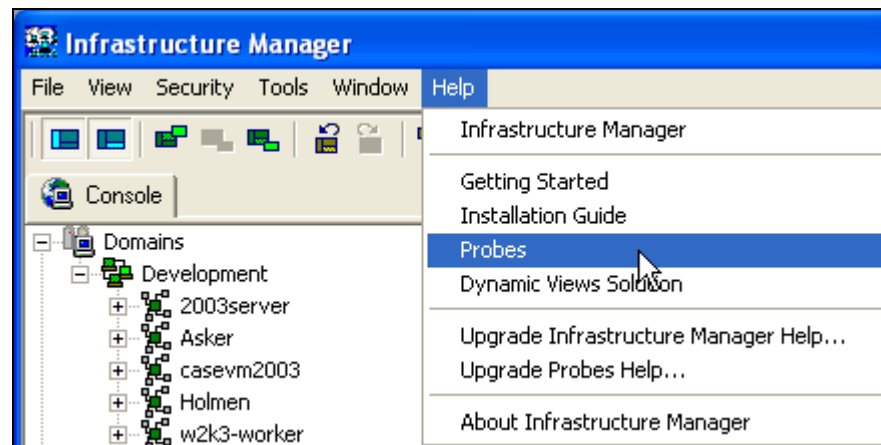
Do as described for all probes mentioned in step 1:
Select the Robot on which you want to configure the probe (1). All probes will be listed in the main window pane.
Double-click the probe to launch the probe GUI (2).



The probe GUI appears. Find the tab in the GUI where the QoS messages are selected. Select the QoS messages you want.

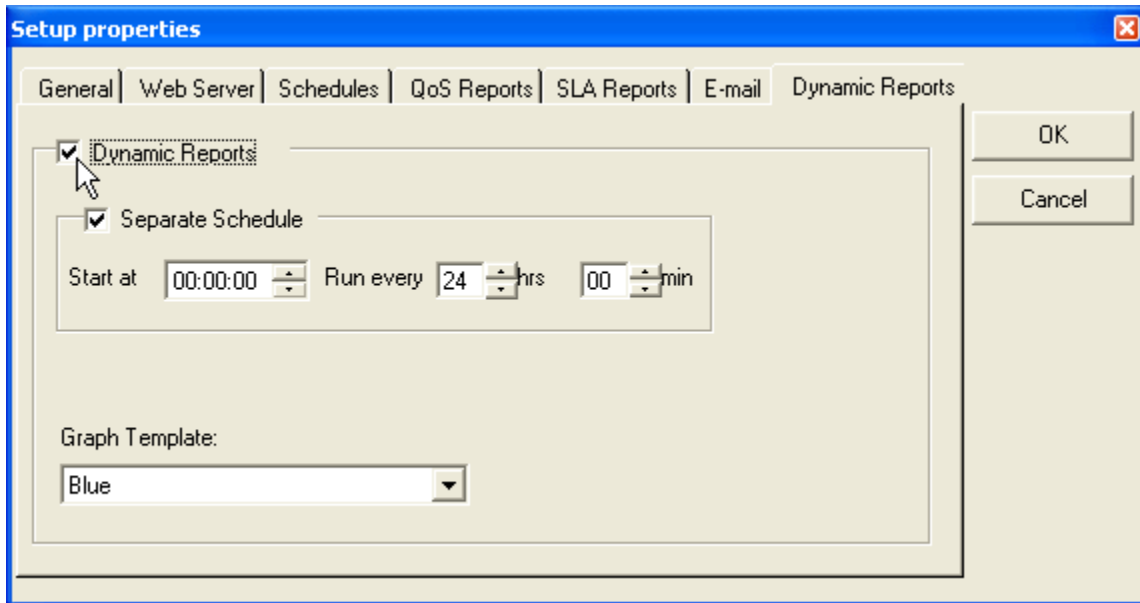


For information, see the Probes on-line documentation, made available by selecting Help > Probes from the menu bar in Infrastructure Manager.



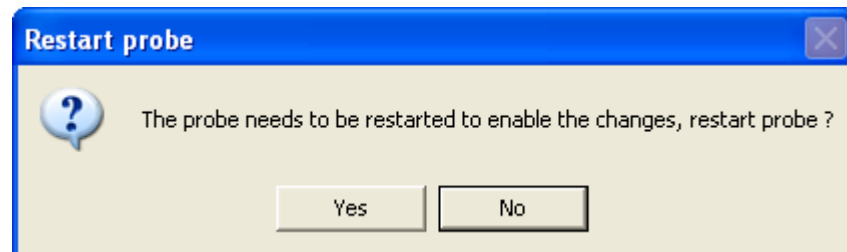
6. Configure the report_engine and activate "Dynamic Reports" in the Setup window.

As described in step 4, double-click the report_engine probe to open the GUI. Click the Setup button in the upper left corner of the GUI, and then select the Dynamic Reports tab.



Ensure that the Dynamic Reports option is selected and click the OK button to exit.

Click the Apply button in the probe GUI to confirm and exit the GUI. The following dialog appears. Click Yes to finish.



Note that you must wait about 10 minutes from the option Dynamic Reports is activated before you can view the reports in Nimsoft Server.

Report_engine not installed on the same server as the main hub?

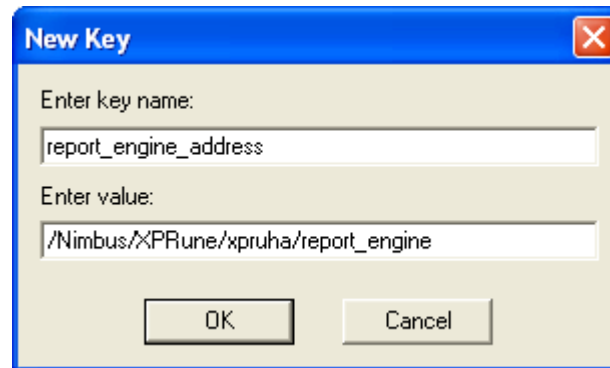
If the report_engine is not installed on the same server as the main hub and the httpd probe, you must configure the httpd server to see the report_engine. Otherwise you will not be able to see the Dynamic Reports.

Launching Dynamic Reports

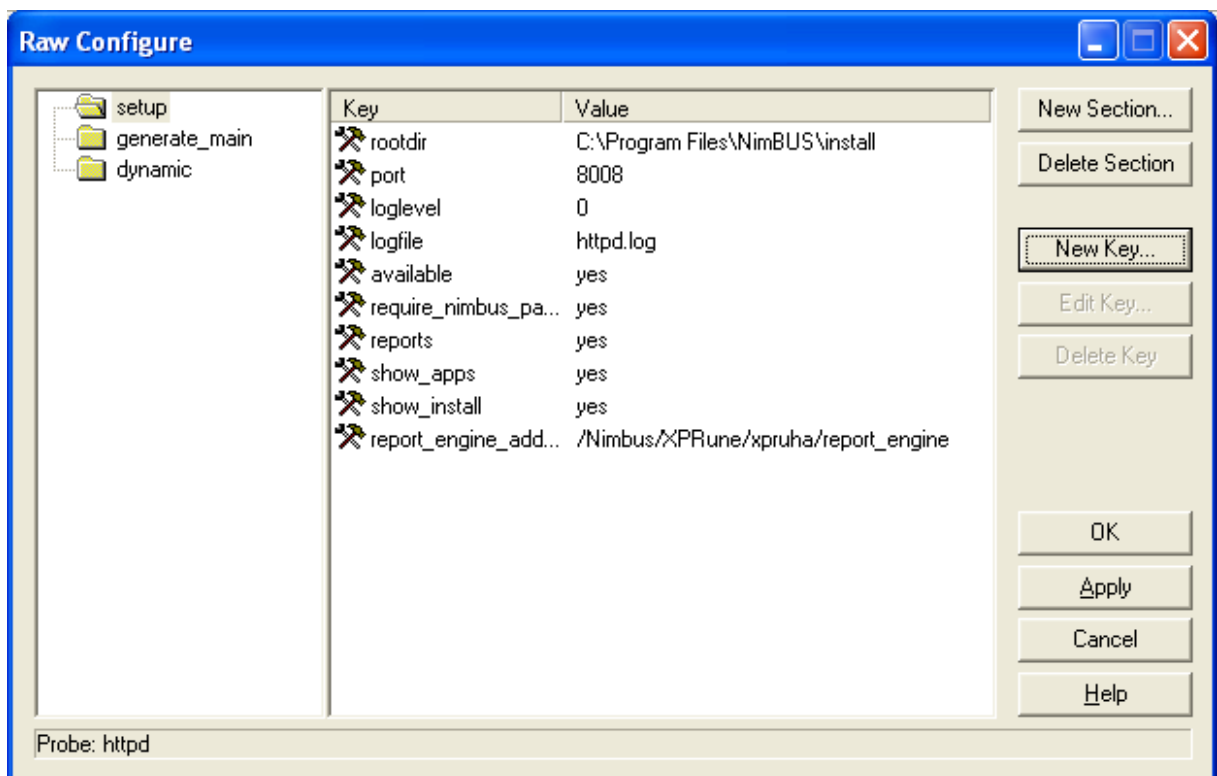
This is possible in version 1.21 of the httpd probe by configuring the address to the report_engine in the setup section.

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 /<Domain>/<hub>/<robot>/report_engine.

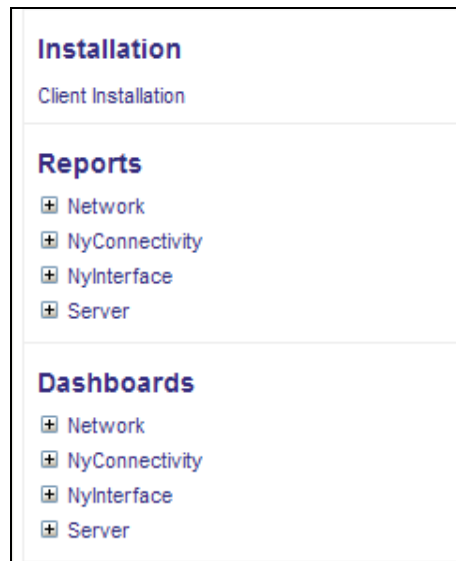


Click the Apply button to activate the new setting and exit the Raw configure dialog.

Chapter 14: Launching Dynamic Dashboards

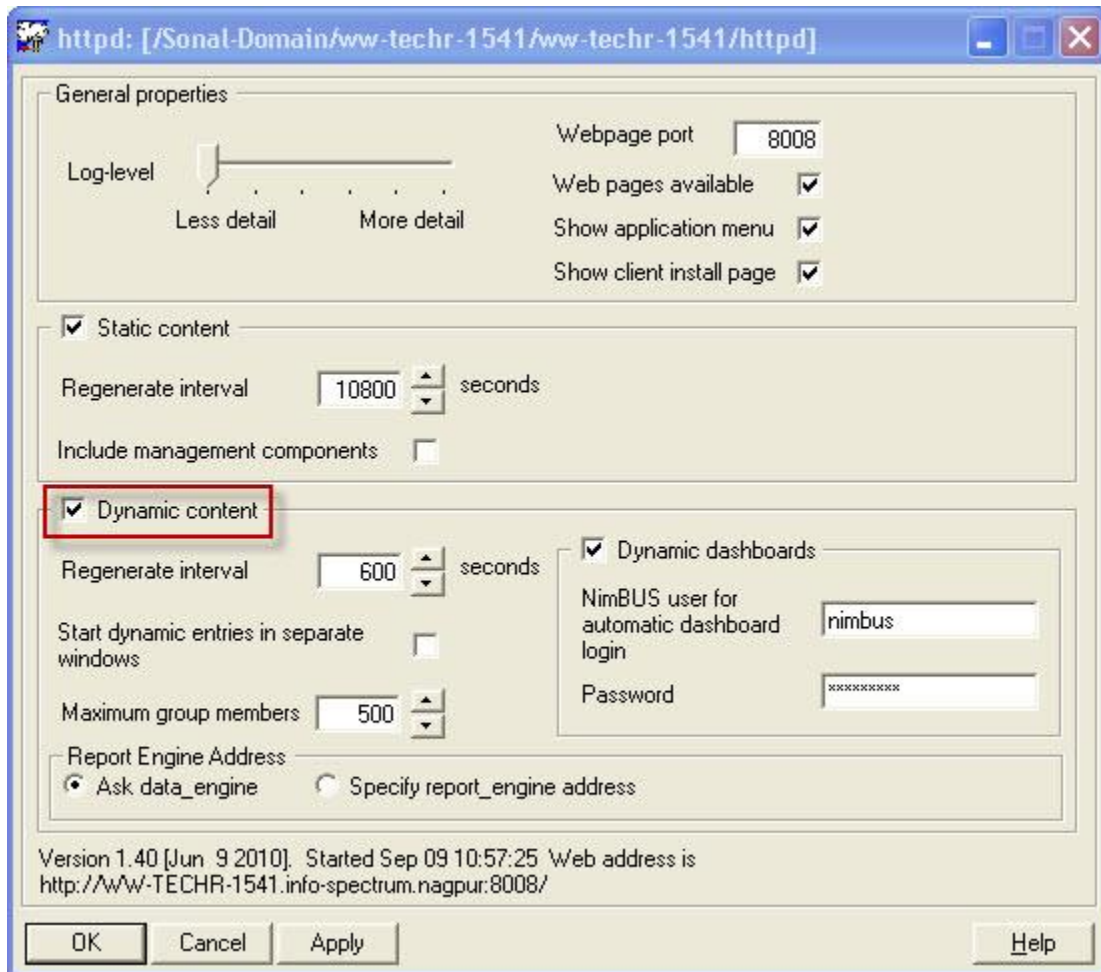
Introduction

Dynamic Dashboards and Reports can be launched from the Nimsoft Server application. The Navigation Pane of the Nimsoft Server application window by default contains the two nodes Reports and Dashboards.



Note that you may hide these two nodes by re-configuring an option in the httpd probe.

Launch the httpd probe by double-clicking the probe in Infrastructure Manager. Turn the *Dynamic Content* option off (de-select it) and click the *Apply* button.



The Dashboards

When expanding the Dashboards node, you will find a set of child-nodes representing different parts of your Nimsoft Infrastructure. The end-node will represent a Dynamic Dashboard representing a device or host in your Nimsoft Infrastructure.

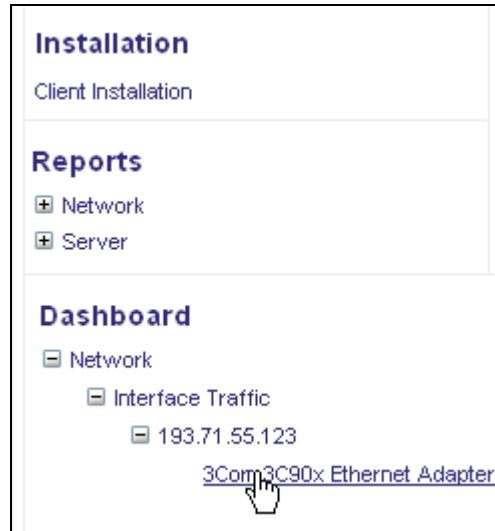
Note that only devices delivering QoS data will be listed here. To achieve this, you must do as follows:

- If the Discovery module was selected during the installation of Nimsoft Server, you must set the devices you want to monitor to Managed, using the NIS Manager.
- If the Discovery module was NOT selected during the installation of Nimsoft Server, you configure the devices you want to monitor to deliver QoS data as described in the section Preparing for Dynamic Dashboards.

Clicking the end node will launch the Dashboard in the main window.

These Dashboards will be populated with context related data, organized by the Group Server probe.

These are the same Dashboards as those found under the Dynamic Views Node in the Enterprise Console.



Initially after installation, you may experience that no dashboards are listed under the Dashboards Node.



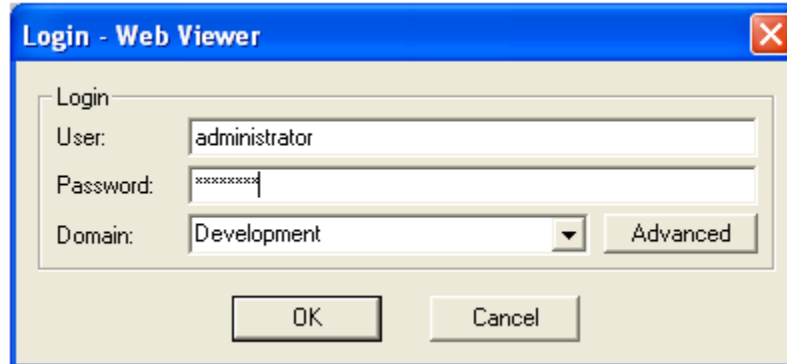
Instead you will find the link *What is this*. Click this link and read the configuration instructions displayed in the main window, or read the instructions in the section [Preparing for Dynamic Dashboards](#).

When expanding the Dashboards node, you will find a set of child-nodes, representing different parts of your Nimsoft Infrastructure. The end-node will be a link a Dashboard representing a device or host in your Nimsoft Infrastructure.

Provided that you are logged on, a dashboard representing the link will appear in the main window.

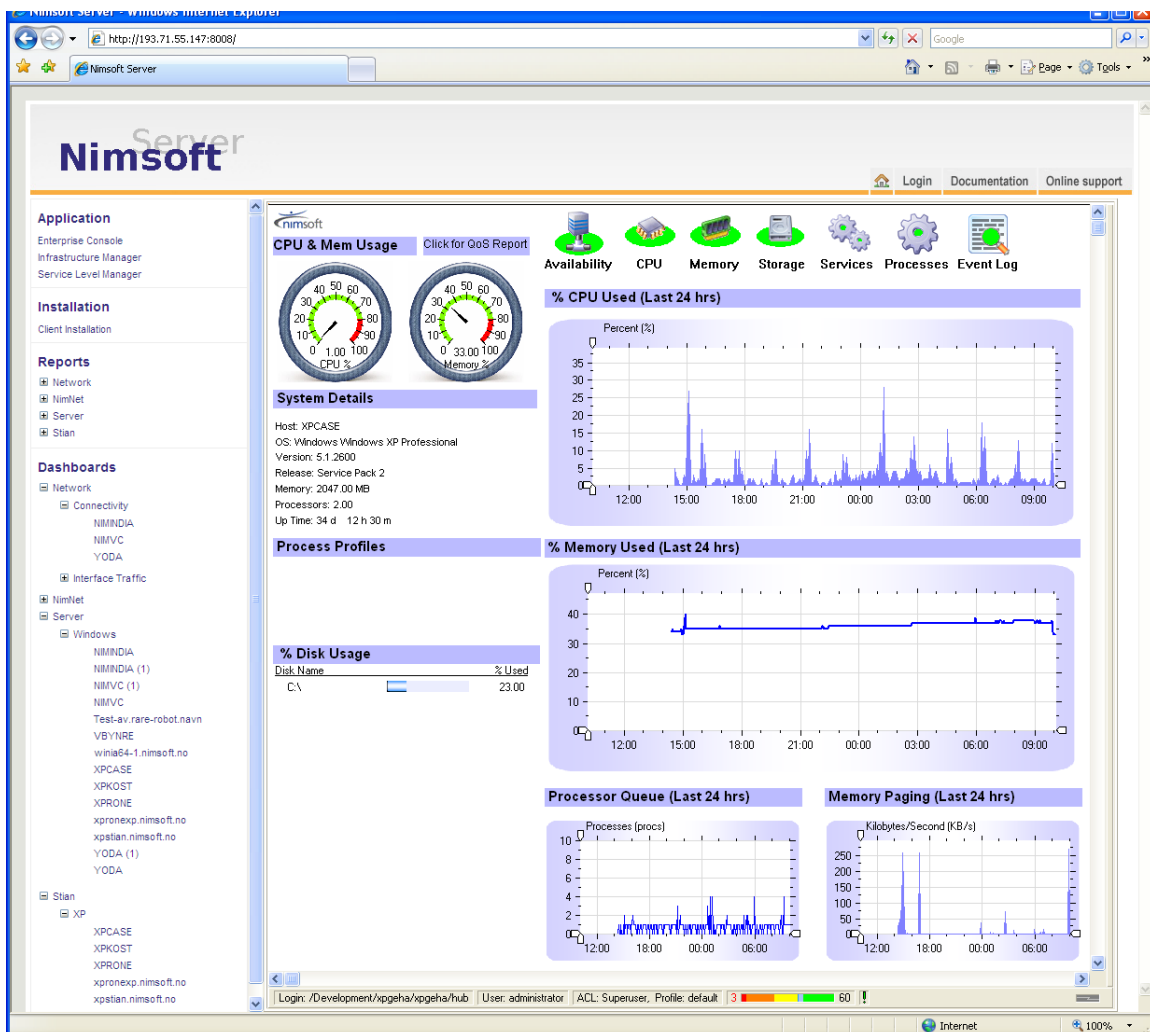
Otherwise, the login dialog for the Nimsoft Web Viewer application will pop up.

Launching Dynamic Dashboards



Log in, using a valid Nimsoft user name and password, and the dashboard representing the link will appear in the main window.

The below dashboard is just an example of a server type of dashboard being launched when clicking a server end-node.



Preparing for Dynamic Dashboards

Initially after installation, you may experience that no dashboards are listed under the Dashboards Node. If this is the case, you should check that the report_engine is correctly addressed and that Dynamic Dashboards are enabled on your system.

See the sections [Report engine not installed on the same server as the main hub?](#) .

If this is the case, you should check that the report_engine is correctly addressed and that Dynamic Reports are enabled on your system.

See the sections [Report engine not installed on the same server as the main hub?](#) and [Enabling Dynamic Reports](#)

Enabling Dynamic Reports

To enable reports, the following steps must be performed:

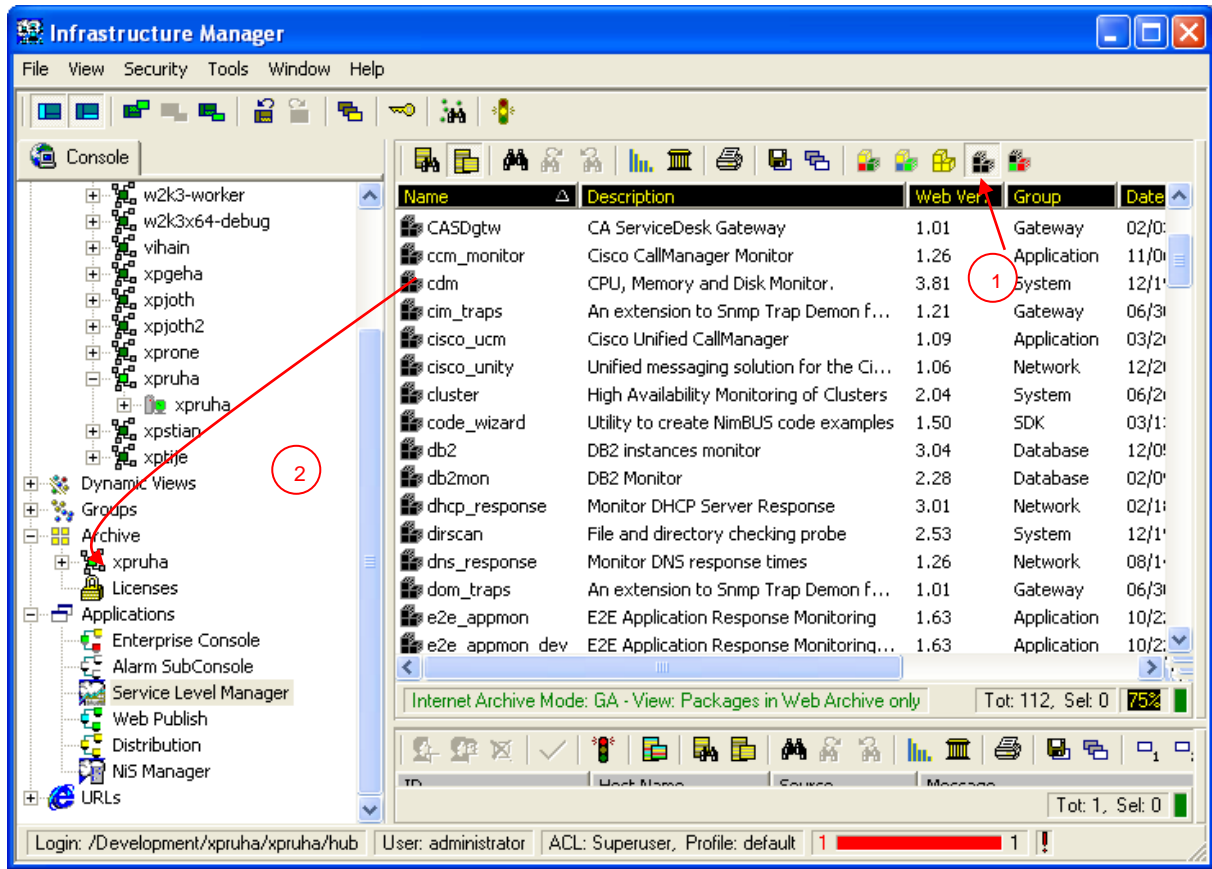
If "Discovery" WAS selected during the Nimsoft Server installation:

Set the devices to "Managed" in the NIS Manager.

Configure the **report_engine** and activate "Dynamic Reports" in the Setup window.

If "Discovery" WAS NOT selected during the Nimsoft Server installation:

1. Download cdm, net_connect and interface_traffic probes.
 - Ensure the Infrastructure Manager is installed. If not, install Infrastructure Manager as described in the section Installing Infrastructure Manager.
Launch the Infrastructure Manager. 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. Click the "Packages in Web archive only" icon (1). Select the Probe package(s) you want to download. Drag and drop them onto your archive node (2).



Note:

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

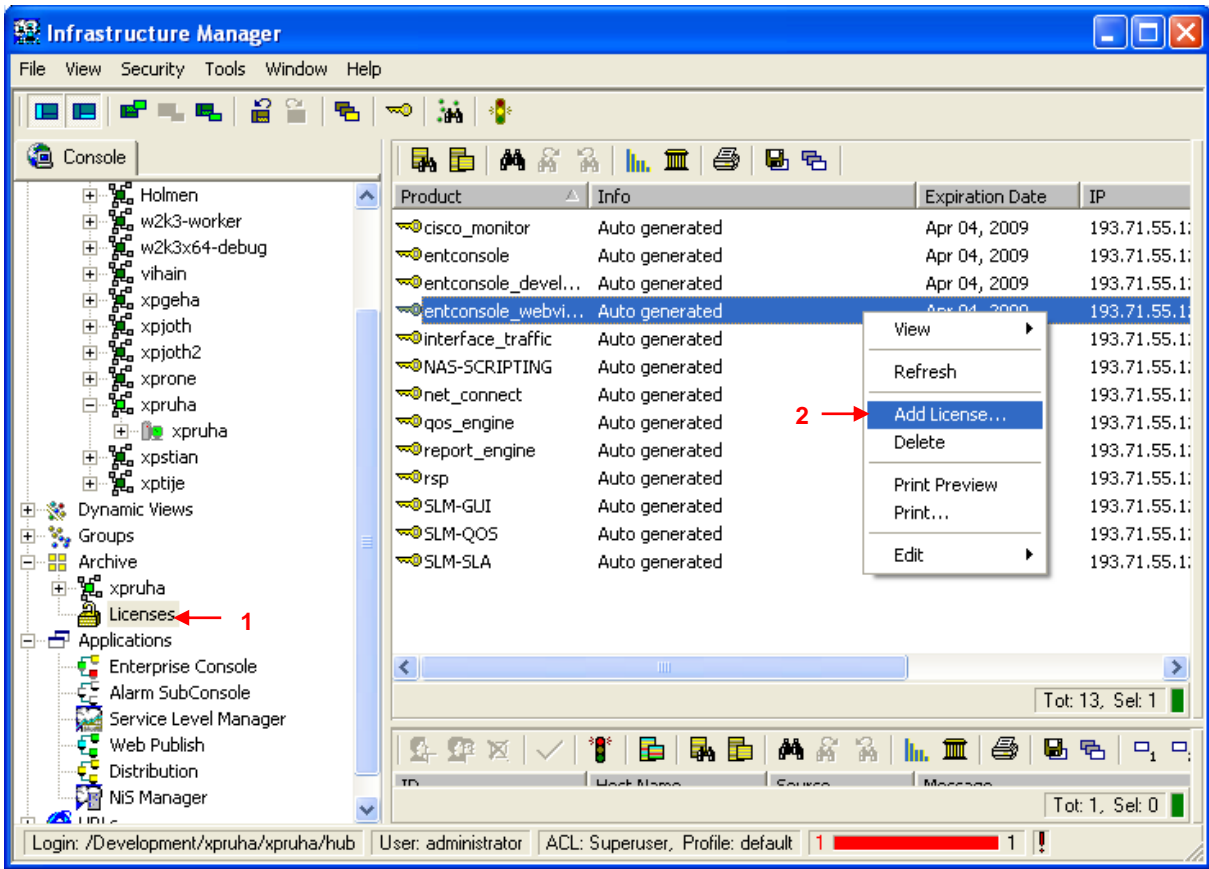
To obtain a login account, please contact support@nimsoft.com.

2. Install licenses for the net_connect and interface_traffic probes.

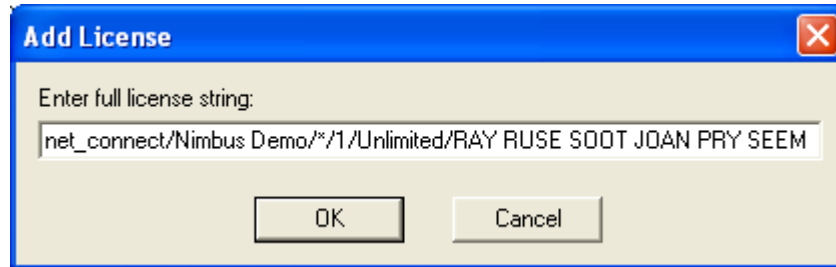
Order licenses for the Probes by sending an email to support@nimsoft.com. You will then receive an e-mail, containing the licenses as a text strings.

Do as described for both probes:

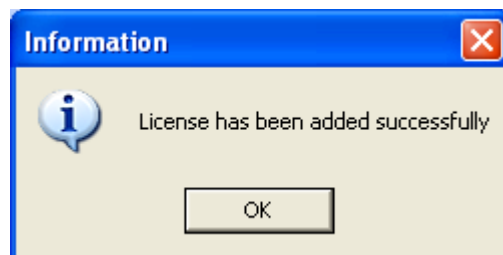
With the Licenses icon under the Archive Node in the Navigation Pane selected (1), right-click in the main window pane and select Add license (2).



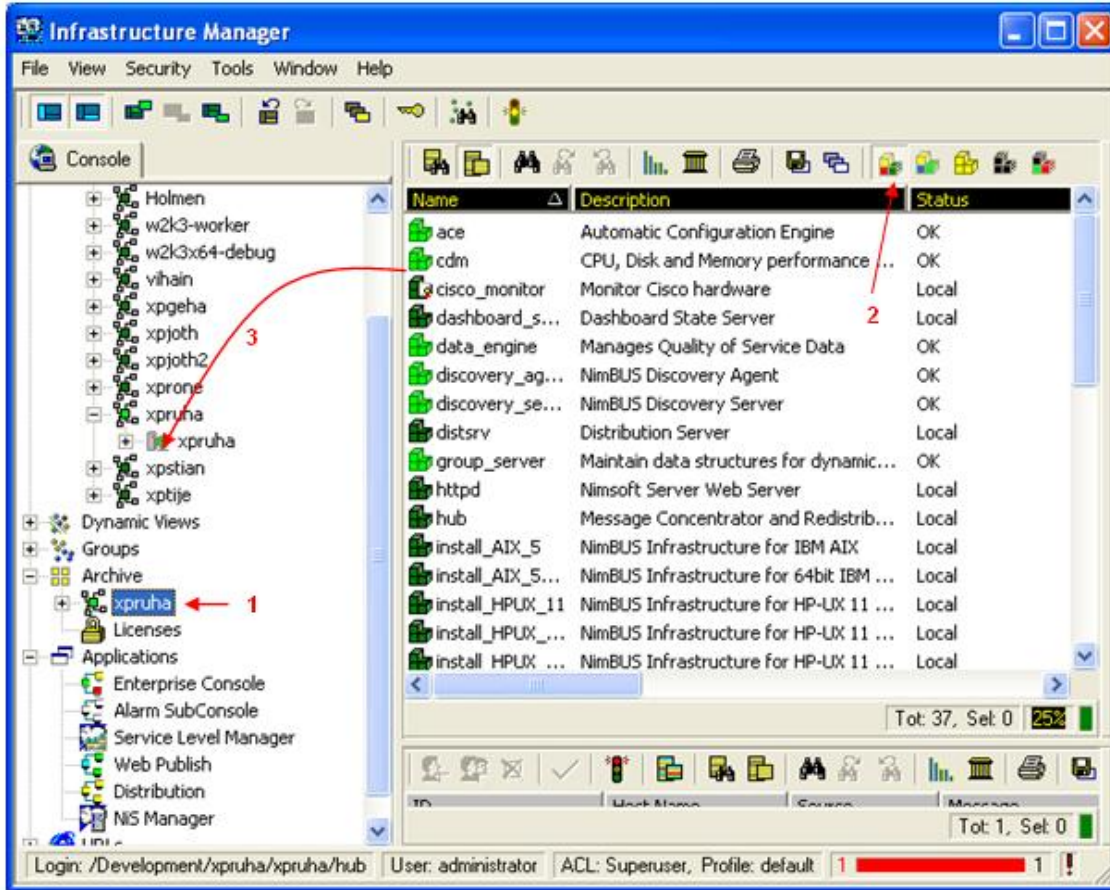
The following dialog appears. Paste or type the license text string into the text field of the dialog and click the OK button.



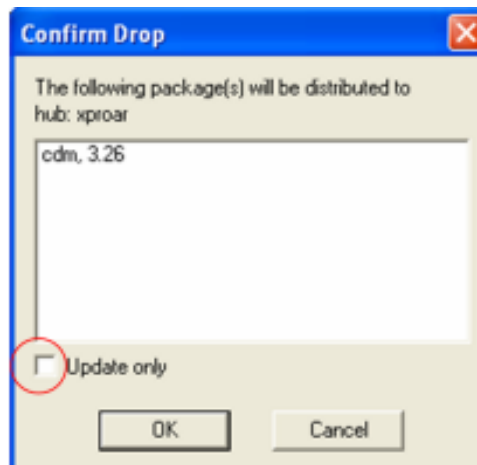
A message like the one shown below appears on the screen. Click the OK button.



3. Configure the net-connect and interface traffic probes with monitoring profiles for the devices you want to monitor. For information, see the Probes on-line documentation, made available by selecting Help > Probes from the menu bar in Infrastructure Manager.
4. Distribute the cdm probe to the servers to be monitored. Select the logon Hub icon under the Archive node in the Navigation Pane again (1). Click the “Packages in local archive only” icon (2). The Probe packages are listed in the Main Window. Drag the cdm probe package drop it on the servers to be monitored (3).
 - 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.
 - 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.



The following dialog appears. Note the Update only option. Uncheck this option (otherwise the probe packages will only be distributed to robots on which it already exists).

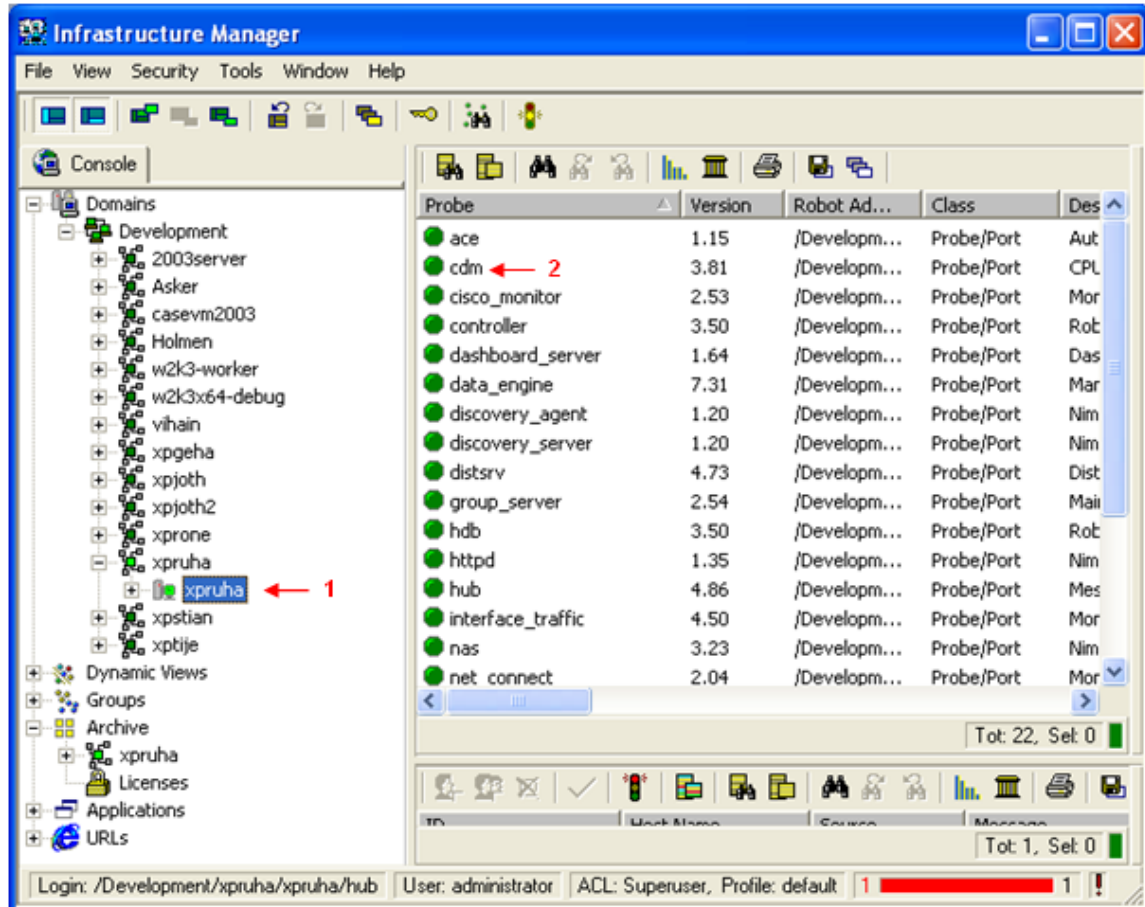


Click the OK button to continue.

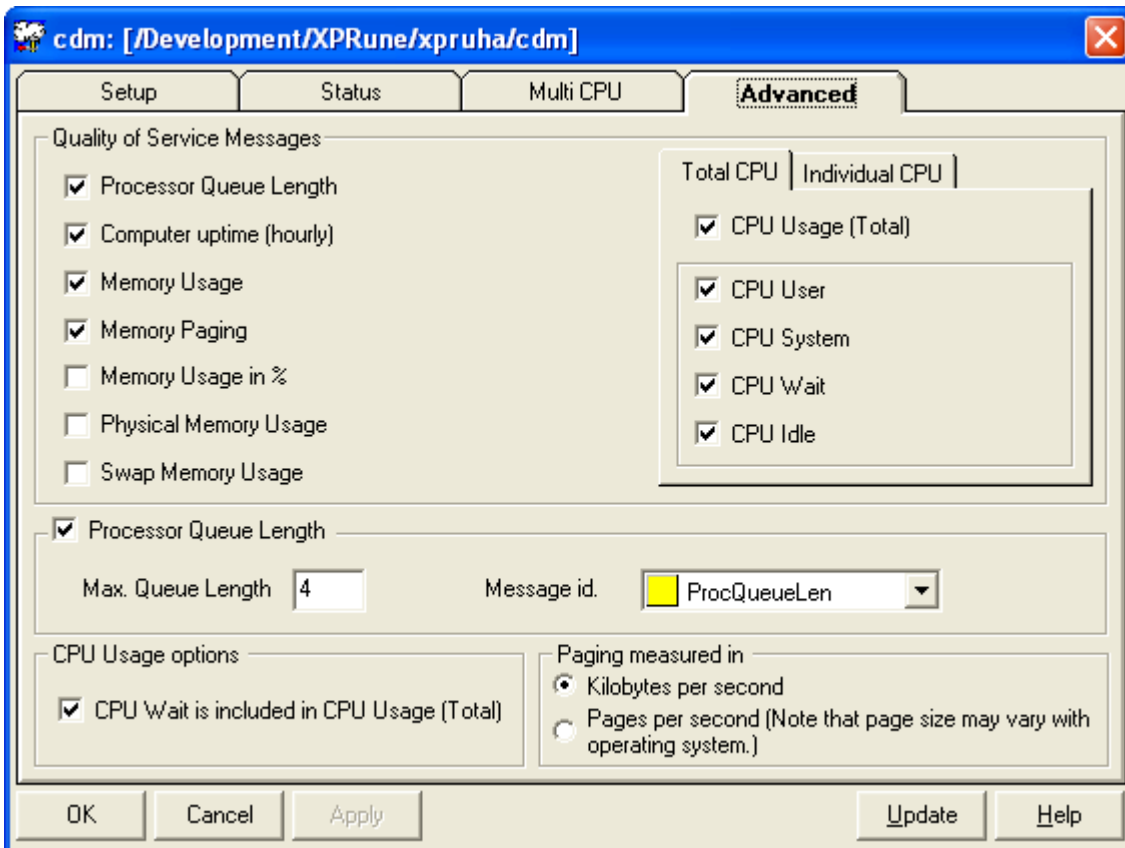
5. Configure the cdm probes to collect Quality of Service data.

Launching Dynamic Dashboards

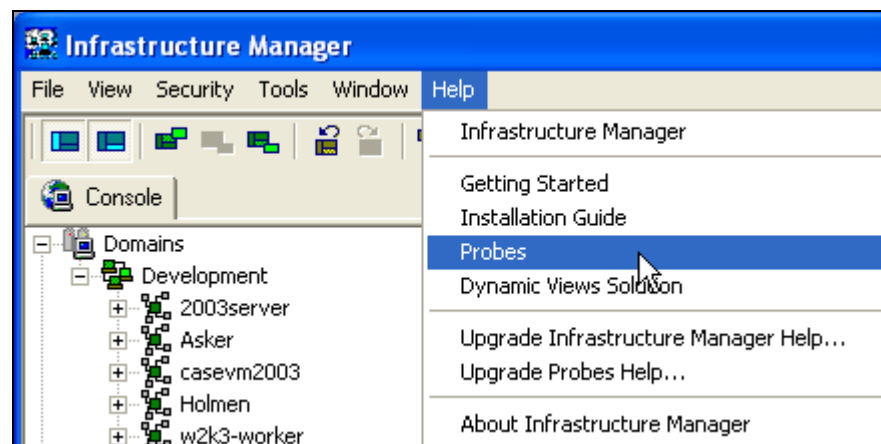
Do as described for all probes mentioned in step 1:
Select the Robot on which you want to configure the probe (1). All probes will be listed in the main window pane.
Double-click the probe to launch the probe GUI (2).



The probe GUI appears. Find the tab in the GUI where the QoS messages are selected. Select the QoS messages you want.



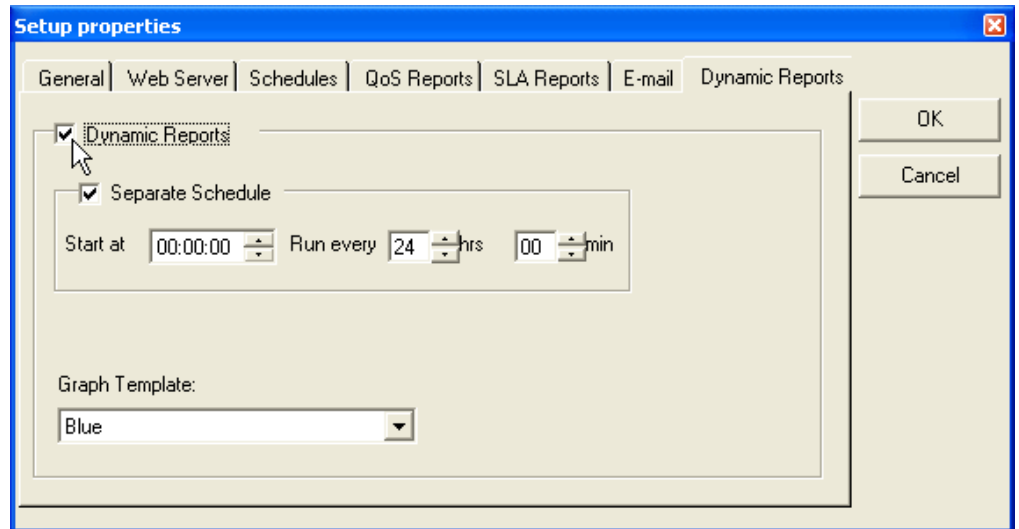
For information, see the Probes on-line documentation, made available by selecting Help > Probes from the menu bar in Infrastructure Manager.



6. Configure the report_engine and activate "Dynamic Reports" in the Setup window.

Launching Dynamic Dashboards

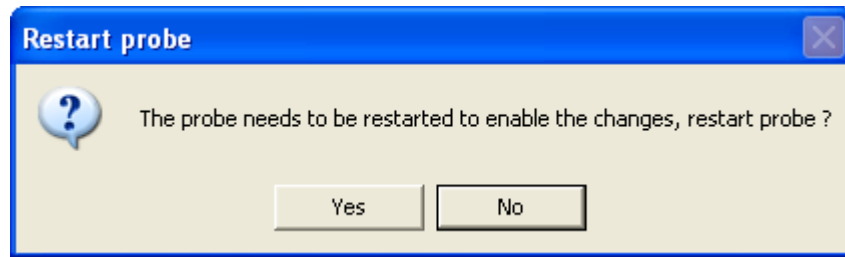
As described in step 4, double-click the report_engine probe to open the GUI. Click the Setup button in the upper left corner of the GUI, and then select the Dynamic Reports tab.



Ensure that the Dynamic Reports option is selected and click the OK button to exit.

Click the Apply button in the probe GUI to confirm and exit the GUI.

The following dialog appears. Click Yes to finish.



Note that you must wait about 10 minutes from the option Dynamic Reports is activated before you can view the reports in Nimsoft Server.

7. Configure httpd by double-clicking the httpd probe in Infrastructure Manager. Activate Dynamic Dashboards in the Dynamic content setup, also supplying Nimsoft user and password for dashboard login. Click the Apply button to activate the modification. Click the OK button to exit the GUI. Refresh the Nimsoft Server window to reflect the changes.

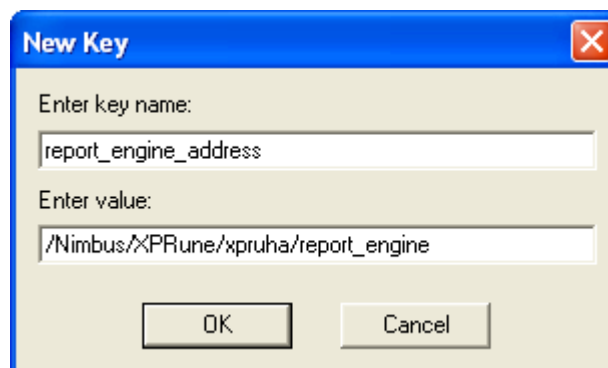
Report_engine not installed on the same server as the main hub?

If the report_engine is not installed 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.

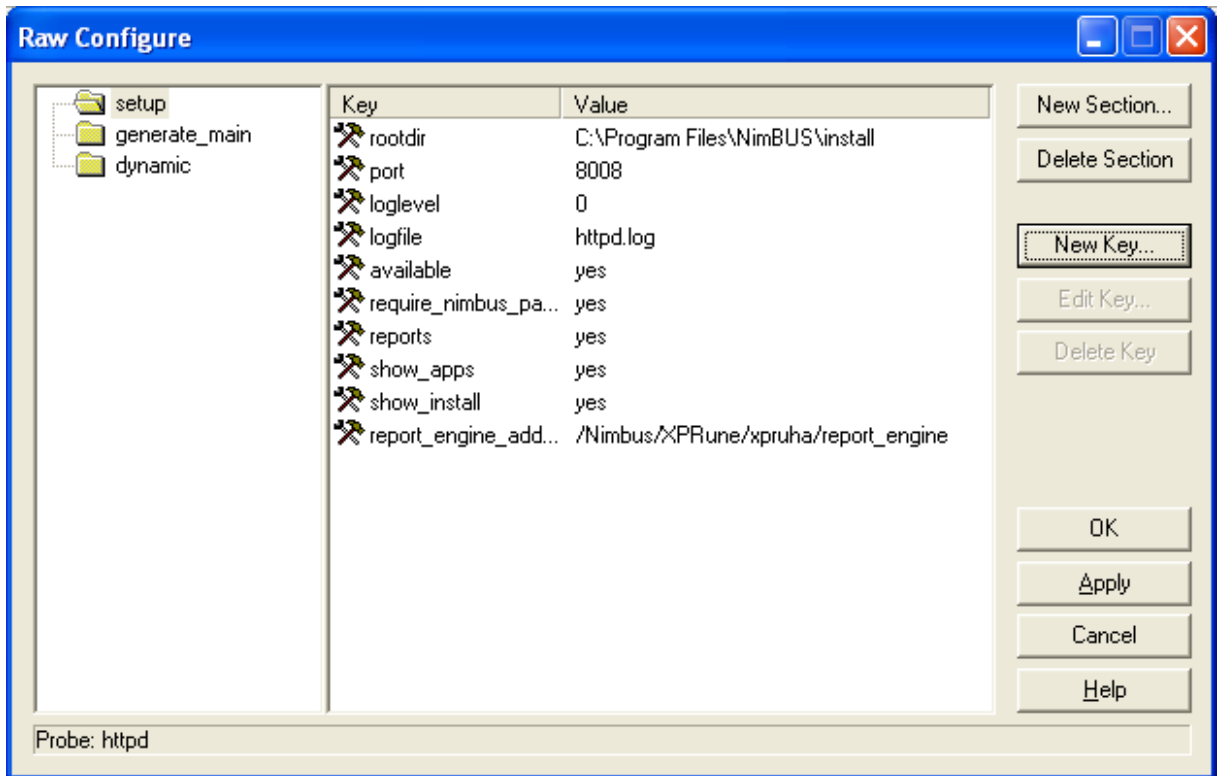
This is possible in version 1.21 of the httpd probe by configuring the address to the report_engine in the setup section.

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 inn the Key name: report_engine_address and the Value: report engine address on the format /<Domain>/<hub>/<robot>/report_engine.

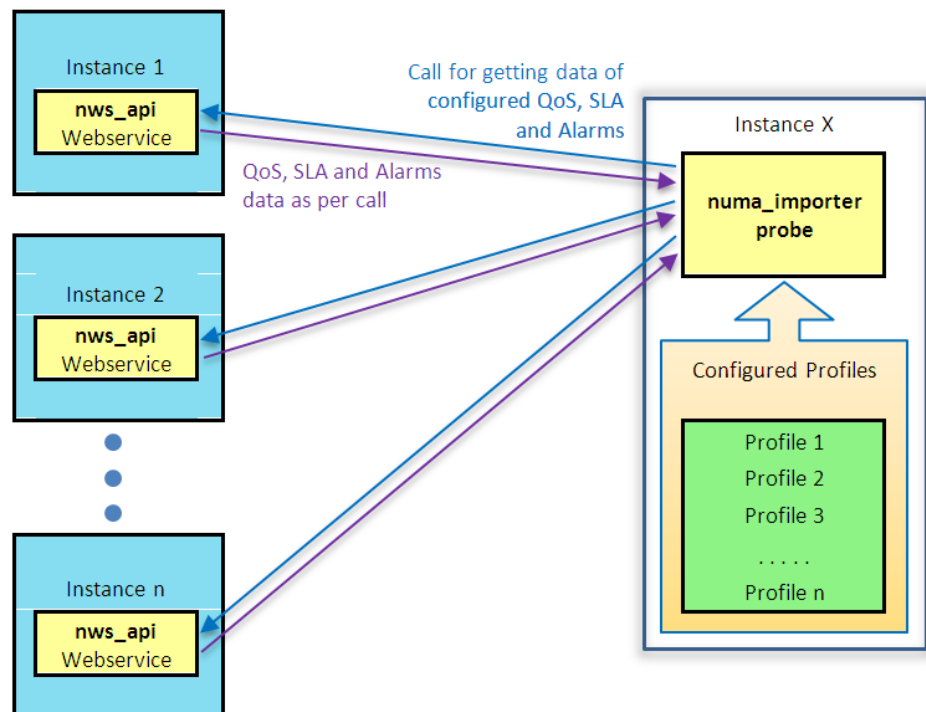


Click the Apply button to activate the new setting and exit the Raw configure dialog.

Chapter 15: NMS Connect

The NMS Connect is a package of two probes, with an objective to synchronize the selected QoS and SLA between one or more web service(s) instances with one instance.

Following figure demonstrate the utility of these probes:



NOTE: If the *numa_importer* probe has n profiles configured then it will connect to n number of instances with *nws_api* web service running after regular intervals (as configured) and can import data of configured QoS and SLAs.

nws_api

The *nws_api* web service is the package to wasp probe, which is a tomcat container. This web service is available from a port number configured to run for wasp, and ajp connector can be configured to run under DMZ scenario.

- The *nws_api* web service runs in the wasp container, so wasp must be running on the system.
- The basic responsibility of *nws_api* is to provide the asked QoS and SLA information to the calls received.

- The web service needs a table name *nws_tokens* in the database for handling the account user session. This table is generated by running a specific script.
- The Account User, Account, and ACL are required to be configured using *Infrastructure Manager* on the instance where the *nws_api* is running. The credentials of this account user are used by *numa_importer* for importing the data.
- The web service provides data as a response to the authenticated account user. The data provided to account user is limited to the account user's ACL.
- The *sla_engine* must be running so as to send the proper SLA definitions and compliances to the client.

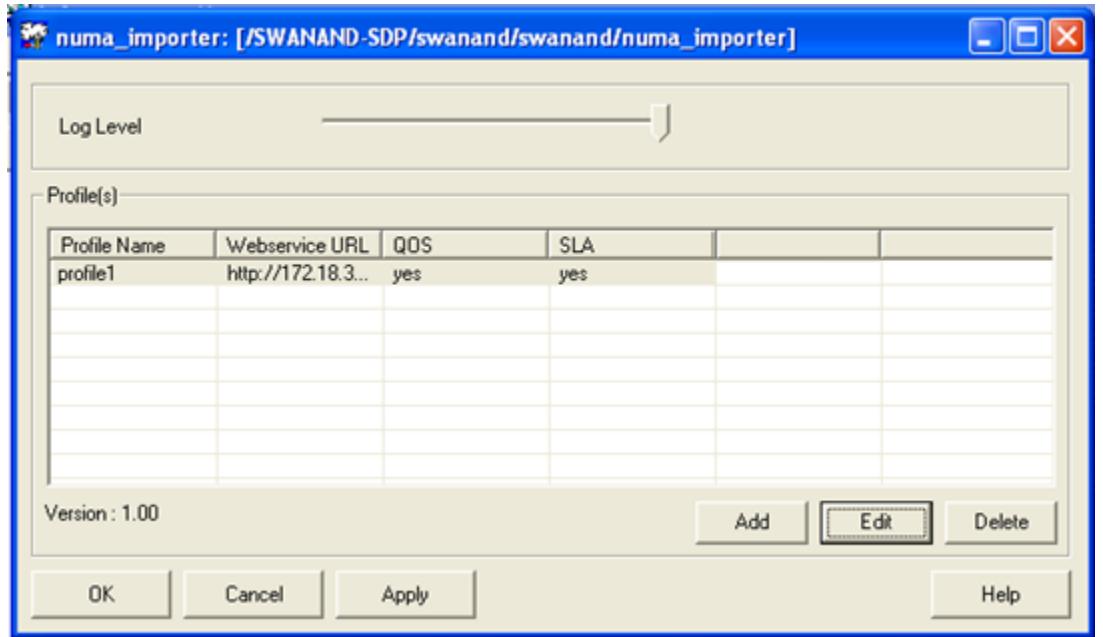
numa_importer

The *numa_importer* probe is responsible for importing QOS and SLA information from the remote site which is hosted with *nws_api* package on the wasp. The probe will not only import this information but in addition it will maintain the information up-to-date and synchronize as per the interval configured to update the QOS and SLA information.

The probe on client side is the client application which makes call to one or more *nws_api* web service for getting QOS and SLA data according to the configured profiles.

NOTE: The *numa_importer* probe uses Coordinated Universal Time (UTC) to communicate with *nws_api* web-service, which is independent of time zone. The QOS related requests are also processed using UTC. For this the web service considers the data engine time-zone as its own time-zone.

Probe Configuration



NOTE: The probe allow multiple profiles to be configured. Each profile is equivalent to one hosted on NMS server, where *nws_api* package is running under wasp.

Field	Description
Log Level	Define the level of details to be maintained in log by moving the slider
Profiles	The list displays the profiles configured and it shows the details as: <ul style="list-style-type: none"> ■ Profile Name: The name of the profile ■ Webservice URL: The url defined for webservice ■ QOS: The status - 'Yes' or 'No' is listed here ■ SLA: The status - 'Yes' or 'No' is listed here
Add	Used for adding the profile
Edit	Select the profile from the list and click this button to edit the selected profile
Delete	Select the profile from the list and click this button to delete the selected profile

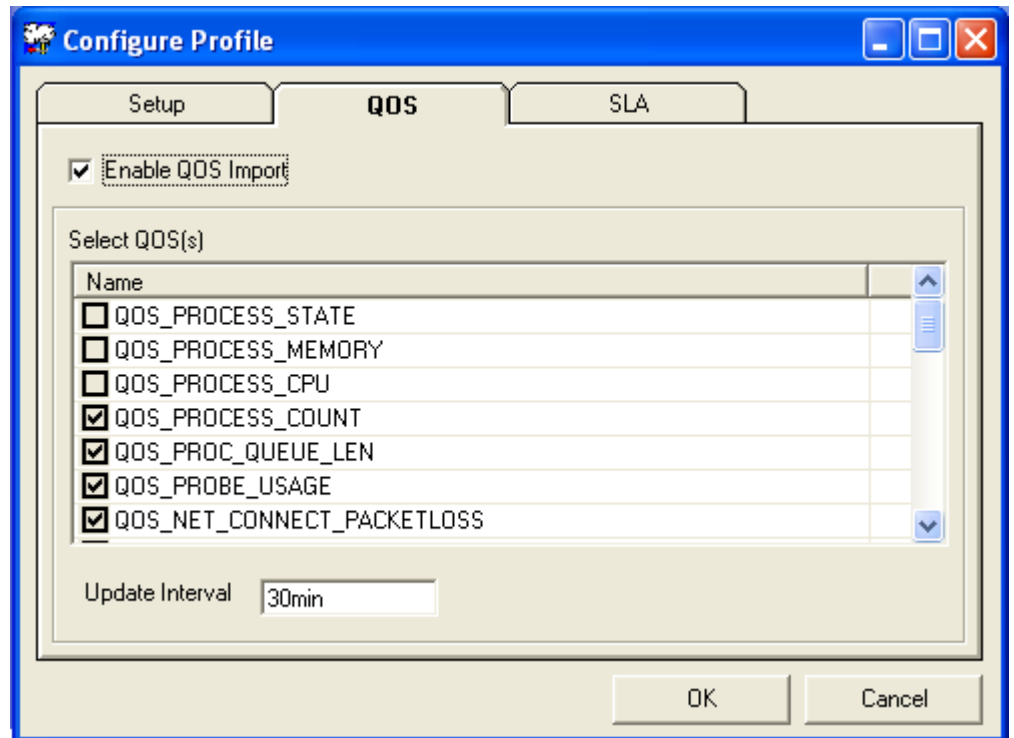
Configure Profile

Setup

The following parameters are required to configure the profile:

Field	Description
Profile Name	Name of the profile to be used for retrieval.
Webservice address	Address of <i>nms</i> with <i>nws_api</i> package installed on <i>wasp</i> and exposed over VPN or static IP address
Username	The name of the user configured to map with account and having certain ownership at remote hosting of <i>nms</i> . This information is shared with remote host user and the user using importer probe.
Password	This is a valid password of the specified user, which is required to be shared by user at remote host and the user using importer probe. The password is encrypted and stored in the <i>cfg</i> file, which is maintained by the probe.
Test Login	Click to verify the login credential entered.

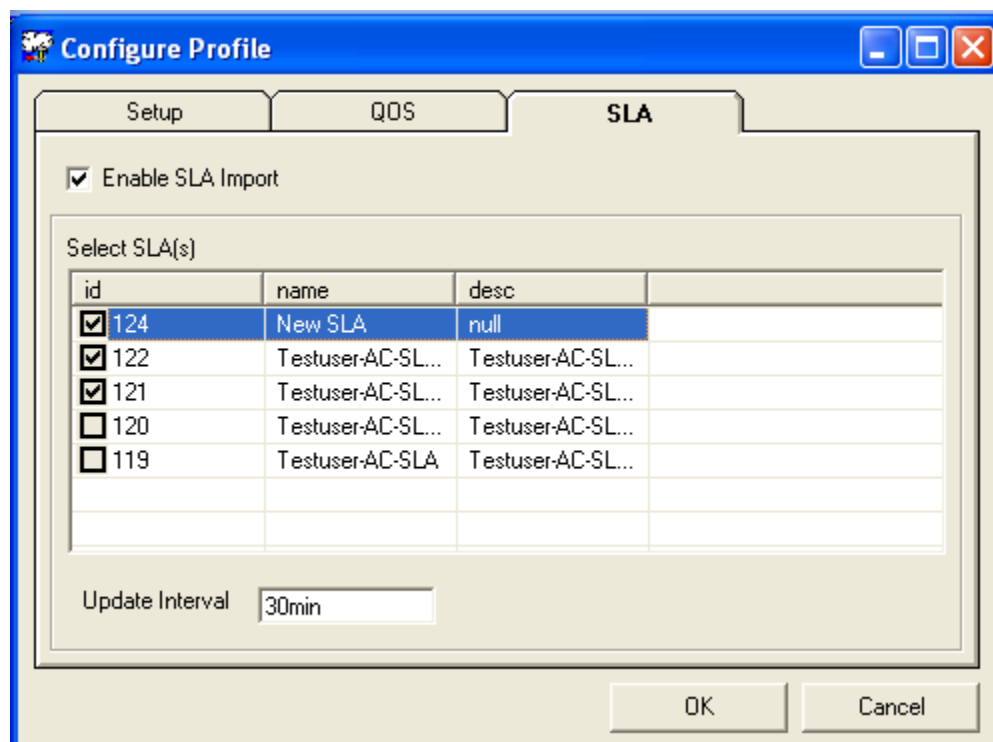
QOS



Selecting the *Enable QOS Import* option allows you to enable the QOS import and synchronization of selected QOS from the list. When this option is enabled, the QOS list is populated with a checkbox that allows you to select the specific QOS for import and synchronization.

Update Interval: The interval after which the synchronization mechanism will execute in order to fetch latest information since last retrieval.

SLA



- Selecting the *Enable SLA Import* option allows you to enable and select synchronization of selected SLAs.
- On selecting the *Enable SLA Import* check box, the SLA list is populated with a checkbox that allows you to select the specific SLA for import and synchronization.
- *Update Interval*: This is the interval after which the synchronization mechanism will execute in order to fetch the latest information since last retrieval.
- The retrieved SLA information is stored in the database. The SLA, SLO and QOS_constraints are also stored in the respective tables with ids with auto numbering, to maintain the actual ids. The additional columns representing *original id* and *host id* are added to the following tables:
 - S_SLA_DEFINITION
 - S_SLO_DEFINITION
 - S_QOS_CONSTRAINTS
- The DB Script for adding these columns is executed at the startup of *data_importer* probe.

Creating User, Account and ACL

NOTE: To create User, Account and ACL, please refer *Infrastructure Manager* documents.

Appendix

My SQL Installation Guide

Summary

This section provides a summary of information regarding the installation, configuration and tuning for MySQL in an OLTP environment. This appendix covers two aspects of the overall setup of the MySQL instance as follows:

1. An overview of the required infrastructure and details of related processes (e.g. Backups and logging)
2. Installation and configuration details for the MySQL instance to ensure that the database would be operational and tuned to a 'starting point,' after which further work would allow optimal configuration(s) to be generated based on data size, throughput and expected performance requirements.

Physical/Virtual machine considerations

Operating systems

MySQL can be installed on various operating systems and hardware. However, this guide only deals with installations on **Linux** and **Windows**.

Licensing options

MySQL is not only available as a free, community installation but also as an enterprise product with approved binaries, extra management tools and additional support provided by Oracle/MySQL.

Logging

MySQL allows for various levels of logging, all of which can be stored in a different location from the data-files to help with disk IO.

- Binary log: Used for replication, but as they contain records of all queries which modify data, they can also be used to complete point-in-time recovery
- Slow log: Will record any queries that take too long to execute. The threshold is configured in the my.cnf
- General log: As this log records every query sent to the server, it is not normally enabled except for troubleshooting issues at known times to identify what's being sent.

- Error log: This is a dedicated MySQL error log. With more recent versions of MySQL (e.g. 5.5) this can be sent to syslog.

Hardware considerations

MySQL has been designed to work on commodity hardware, and performs well on many hardware configurations. However, the throughput and size of data being queried will dictate how much memory should be installed on the system. A starting point of 4 GB RAM would allow data gathering based on query rates along with the information in [Schema and data management](#) section of this guide to identify more optimal RAM settings and requirements

Network

It is a good practice to have at least two network interfaces on the database servers which can be connected for redundancy. It is further good practice to connect each network interface to different switches to ensure redundancy.

Backup and Restore

There is no single backup tool which provides a complete solution in providing MySQL backups.

- **ySQLDump** can be used to provide a dump of the SQL code required to rebuild the database and its data, however it has its limitations and can be both slow and output large SQL files.
- InnoDB provides **ibbackup**, a hot InnoDB backup tool. It can provide consistent backups of InnoDB tables. However while providing backup of any **MyISAM** tables, consistency cannot be guaranteed due to differences in the transactional nature of **InnoDB** and **MyISAM**. **InnoDB Hot Backup** is also a commercial product with an annual license fee.
- **Xtrabackup** is an open-source backup tool designed to replace InnoDB Hot Backup.
- A final option is a simple binary copy of the data files to a safe location. To ensure a totally consistent snapshot of the data, however, it is suggested that the database should be taken offline for the duration of the copy to ensure data integrity.

Monitoring

MySQL can be monitored using a number of tools; however there are no single 'out-of-the-box' monitoring tools that can provide remote monitoring using our own toolset. If, however, MySQL's enterprise licensing option is taken, the **Enterprise Monitor** product would be available, which provides a consolidated view of MySQL operations, such as:

- Operating system and MySQL variables

- MySQL sessions, connections and latency
- Real-time query analysis to identify troublesome SQL
- Replication monitoring (if required)
- Security monitoring
- Schema changes

Regardless of the monitoring solution chosen, the key metrics which should be monitored are:

- CPU utilization
- Memory utilization
- Swap file utilization
- Mount points free space
- Load average
- InnoDB tablespace
- Database sessions
- Slow query log

Configuration and Tuning

Scope and Objectives

The main purpose of this initiative is to provide a concise and easily understandable guide to allow the installation and configuration of MySQL for those who have little or no prior technical knowledge of the MySQL installation process and requirements.

Assumptions and Prerequisites

1. The relevant version and distribution of MySQL has been provided to those carrying out the installation and instructions on identifying and obtaining the correct version of MySQL is not required. The version recommended to take advantage of the partitioning by timestamp is minimum 5.5.
2. Installation will be carried out on a system using a Unix/Linux/Solaris, or some other similar and compatible “*nix” operating system or a MS Windows operating system.
3. The installation will be using the “binary distribution” in .tar archive format for *nix and .msi installer package for Windows.

4. The system had no prior installation of MySQL or it has been completely removed. For *nix systems which may have had MySQL installed via a native package management system (e.g. yum or apt-get) it's imperative that any previous installation is removed completely including old versions of data files, configuration files and any mysql directories.
5. The installation is carried out by the administrator, system root user, or a user with equivalent permissions.

*nix installation

Basic setup information

The 'tar' archive, once unpacked at the installation location, will create and populate the following directories.

Directory	Contents of Directory
bin	Client programs and the server binaries
data	Datafiles and logs
docs	Manuals and documentation
man	Unix Man pages
include	Include (header) files
lib	Libraries
scripts	mysql_install_db
share/mysql	Error message files
sql-bench	benchmarks

A number of locations will need to be identified.

1. Install location (normally /usr/local/mysql)
2. datafile location ()
3. location of logs ()

A "mysql" system user and group will also be required.

Required system tools

To install a "tar" binary distribution of MySQL, the following tools are required:

1. GNU 'gunzip' to uncompress the distribution
2. A compatible 'tar' program to unpack the distribution such as GNU tar. Some operating systems bundle a preinstalled version of tar which is known to have problems. e.g. the version of tar provided with early versions of Mac OS X, SunOS 4.x, Solaris 8, Solaris 9, Solaris 10 and OpenSolaris, and HP-UX are known to have problems with long file names.

Basic 'bare bones' MySQL installation

The following are the steps required to install MySQL with a minimal, default configuration.

1. Create required the user and group using the following commands.

```
groupadd mysql
useradd -g mysql mysql
```

2. Uncompress the distribution into the relevant location, and symlink a «simple» name

```
cd /usr/local
gunzip < /path/to/mysql-VERSION-OS.tar.gz | tar xvf -
ln -s full-path-to-mysql-VERSION-OS mysql
```

3. Go into the MySQL directory and change ownership of all files to the MySQL user.

```
cd mysql
chown -R mysql .
chgrp -R mysql .
```

4. Execute the installation scripts.

```
scripts/mysql_install_db --user=mysql
```

5. Change the ownership to that required for a running system, including the now-present datafile directory (which must be owned by MySQL).

```
chown -R root .
chown -R mysql data
```

6. Start mysql using the safe-startup method to test it's working

```
bin/mysqld_safe --user=mysql &
```

There is now a basic and operational MySQL instance available.

At this stage, however, there are neither database users nor passwords created, nor is there an easy way to start and stop the MySQL process.

Standard Post installation configuration

To enable mysql startup at boot time, and simplify the server control, copy the server startup scripts to the relevant location:

From the mysql directory

```
cp support-files/mysql.server /etc/init.d/mysqld
```


This allows the server to be started using:

```
/etc/init.d/mysqld [start|stop|restart|status]
```

Create an empty file: `/etc/my.cnf` (or modify one of the standard configurations as specified in [Basic tuning configuration changes](#))

Insert the following into the `my.cnf` file under the «mysqld» section.

```
[mysqld]
innodb_file_per_table
slow_query_log_file=[path/to/chosen/location/for/slow
log.log]
datadir=[path/to/datafile/location]
```

Windows Installation

Supported Windows versions are Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, or Windows Server 2008. Both 32-bit and 64-bit versions are also available where relevant.

MySQL should be installed using the 'administrator' user to mitigate against problems with paths, environment variables or accessing the 'service control manager'. Once the installation is complete, however, MySQL does not require to be run as the administrator user.

Windows specific prerequisites and considerations

There are a number of potential issues to be aware of when installing MySQL on Windows. In no particular order:

1. If table sizes are expected to exceed 4GB, then MySQL must be installed on an NTFS or newer file-system.
2. Virus scanning software can sometimes, generate erroneous alerts incorrectly identifying the datafile contents as malicious. This is due to the combination of the frequency of update of the MySQL datafiles and the fingerprinting used by some anti-virus packages. It is recommended that after installation, any anti-virus software be prevented from scanning the main data directory (`datadir`) and any other directory used by MySQL for temporary datafile creation.
3. Windows XP and later include a firewall which specifically blocks ports. If you intend to use MySQL through a network port then you should ensure the relevant ports are open before installation.

Installation procedure

The steps to perform the initial install of MySQL on windows, using the GUI interface of the MSI installer, is relatively straightforward.

1. Run the installer package
2. Acknowledge any security warnings.

3. Select install type: For this installation, the Complete option is recommended. (If you wish to specify datafile locations, such as on a separate, high-performance disk, then select «custom» and specify the paths where required. This can be done post-install by rerunning the installer and selecting «modify» on the basis that there's no data installed as yet, as existing datafiles will not be copied)
4. In the Ready to install dialogue window select the Continue option. The installation proceeds.
5. Information regarding MySQL Enterprise appears on your screen, which can be ignored.
6. The basic install Wizard is now complete.

You now have the option to configure the MySQL instance, where you have the options to create the root password, additional users and other configurations such as the location of the datafiles.

On completion of the basic configuration, the installer allows you to «Register MySQL as a Service». This is the recommended option, as it allows control of MySQL from Window's Service Manager and ensures the database is started automatically, if required.

There are no specific post-installation steps to carry out from a Windows install, as the paths, directories, system tables and service manager registration are all carried out by the installer.

Basic tuning configuration changes

These basic tuning parameters are dependent on the hardware, memory, number of expected connections and throughput/queries per second. As more of this information is available and known, the configuration and tuning parameters can be modified to ensure optimal performance for the NIS database environment. However, without this information we are still able to establish a good initial setup with the parameters and configuration settings as follows.

There are, , a number of pre-populated my.cnf or my.ini configuration files bundled with MySQL, which are 'my-small', 'my-medium', 'my-large', and 'my-huge'.

Within those configuration files are indicators of the size of system for which they might be appropriate.

Once a configuration file has been chosen, additional adjustment of the parameters can be made depending on the performance of the hardware.

The **max_connections** parameters can be estimated based on the total RAM available with the following calculation:

$$([Total\ available\ RAM] - [Global\ Buffers]) / [total\ size\ of\ thread\ buffers]$$

(The values of the following variables can be obtained by executing a «show variables» from the MySQL command line)

The [Global Buffers] can be calculated by summing the values of:

```
key_buffer_size
innodb_buffer_pool_size
innodb_log_buffer_size
innodb_additional_mem_pool
net_buffer_length
```

The thread buffers size can be calculated by summing the values of:

```
sort_buffer_size
mysam_sort_buffer_size
read_buffer_size
join_buffer_size
read_rnd_buffer_size
```

An estimate of the `open_files_limit` can also be calculated as double the number of `max_connections` summed with the `table_cache`

Considering that this installation is InnoDB specific, we can suggest the following parameters as a starting point:

- `innodb_buffer_pool_size`: Typically 70%-80% of the RAM available.
- `innodb_log_file_size`: Depending on recovery speed requirements, 256Mb is seen as a good balance.
- `innodb_log_buffer_size`: 4 MB is a standard setting and is effective for most installations unless large amounts of binary data are in use.
- `innodb_flush_log_at_trx_commit`: This can make a significant difference to performance at the risk of losing the last second or two of data in the event of a crash, then this can be set to «2».
- `innodb_thread_concurrency`: The default value is 8 and is a good starting point.
- `innodb_flush_method`: To avoid double buffering and reduce swap usage, this setting of «O_DIRECT» can improve performance. (n.b. Without a battery-backed-up RAID cache write, IO may suffer)
- `innodb_file_per_table`: This must be set to take full advantage of disk data allocation in partitioning. It does not affect performance directly, but makes data management and disk/OS housekeeping more manageable.

All of the above parameters will appear in the `my.cnf` and can be changed there to be made available when the server is restarted.

Some parameters are dynamic and can be changed via the MySQL client for immediate benefit.

A complete list of the server option parameters, and their status as dynamic or configuration only can be seen in:

<http://dev.mysql.com/doc/refman/5.5/en/server-system-variables.html>

More accurate tuning can be performed once throughput, load and data-size are known.

Deployment statistics and estimations

The average row-length for the schema as seen in appendix [Schema and data management](#) is 170bytes.

Deployments can be considered small, medium or large if they operate with insert rates of 1000 rows/second, 5000 rows/second or 20000 rows/second respectively.

- Small Deployment:
1000 rows/second
Average row length 170bytes
Data growth rate would be approximately 9.7Mb/min or 12GB per day.

- Medium Deployment:
5000 rows/second
Average row length 170bytes
Data growth rate would be approximately 48Mb/min or 68GB per day.

- Large deployment:
20000 rows/second
Average row length 170bytes
Data growth rate would be approximately 194Mb/min or 273GB per day.

There are no specific disk configurations required to accommodate this data, as MySQL does not use the same logging configurations as other RDBMSs.

Schema and data management

The table schema is as follows:

```
CREATE TABLE `test`.`RN_QOS_DATA_xxxx` (  
  `table_id` int(11) NOT NULL,
```

```

`samptime` timestamp NOT NULL,
`samplvalue` bigint(20) DEFAULT NULL,
`samplstdev` bigint(20) NOT NULL,
`samplerate` bigint(20) NOT NULL,
`samplmax` bigint(20) NOT NULL,
`compressed` tinyint(4) DEFAULT '0',
`tz_offset` bigint(20) NOT NULL,
`inserttime` timestamp NOT NULL,
PRIMARY KEY (`samptime`,`table_id`)
) ENGINE=InnoDB PARTITION BY RANGE (samptime) (
    PARTITION p0 VALUES LESS THAN (XXXX-XX-XX
XX:XX:XX),
    PARTITION pn VALUES LESS THAN (nnnn-nn-nn
nn:nn:nn)
);

```

The table is partitioned by samptime, hence it's included in the primary key identifier, and will have multiple partitions depending on the data retention and partition size requirements. The partitioning time range can be controlled in the stored procedure which follows.

The stored procedure to manage the partitioning will automatically create new partitions and remove old ones, based on time parameters which are passed to the procedure on execution. The stored procedure is as follows:

```

CREATE PROCEDURE partition_logs(in tblname
varchar(100),in partsize int,in lwater int,in hwater
int)
BEGIN
    DECLARE p_start_time bigint;
    DECLARE p_end_time bigint;
    DECLARE p_start_name bigint;
    DECLARE p_end_name bigint;
    DECLARE p_low_water bigint;
    DECLARE p_high_water bigint;
    DECLARE p_new_name bigint;
    DECLARE p_new_time bigint;
    DECLARE cnt int;

```

```
DECLARE deld int;
DECLARE partition_column varchar(100);
set partsize = partsize * 60;

SELECT cast((substr(partition_name from 2)) as
SIGNED ) into p_start_name FROM
information_schema.PARTITIONS where table_name =
tblname order by partition_ordinal_position limit 1;

SELECT cast((substr(partition_name from 2)) as
SIGNED ) into p_end_name FROM
information_schema.PARTITIONS where table_name =
tblname order by partition_ordinal_position desc
limit 1;

SELECT partition_description into p_start_time
FROM information_schema.PARTITIONS where table_name =
tblname order by partition_ordinal_position limit 1;

SELECT partition_description into p_end_time
FROM information_schema.PARTITIONS where table_name =
tblname order by partition_ordinal_position desc
limit 1;

SELECT partition_expression into partition_column
from information_schema.PARTITIONS where table_name =
tblname limit 1;

select unix_timestamp(date_sub(now(), interval
lwater minute)) into p_low_water;

select unix_timestamp(date_add(now(), interval
hwater minute)) into p_high_water;

set @plw := p_low_water;
set @tbl := tblname;
set @col := partition_column;
select p_start_time,p_low_water;
set deld = 0;
while (p_start_time < p_low_water)
do
select p_start_time,p_low_water;
set @pstart := p_start_name;
set @droppart := concat('ALTER TABLE ',@tbl,'
drop partition p',@pstart);
prepare dropstate from @droppart;
execute dropstate;

SELECT partition_description into p_start_time
FROM information_schema.PARTITIONS where table_name =
tblname order by partition_ordinal_position limit 1;

SELECT cast((substr(partition_name from 2)) as
SIGNED ) into p_start_name FROM
```

```
information_schema.PARTITIONS where table_name =
tblname order by partition_ordinal_position limit 1;

    set deld = deld+1;
    END WHILE;
    set cnt=0;
    while (p_end_time < p_high_water)
    do
        set p_end_name = p_end_name + 1;

        IF (p_end_time < p_low_water)
        THEN set p_end_time = p_low_water;
        ELSE set p_end_time = p_end_time + partsize;
        END IF;

        set @pendname := p_end_name;
        set @phighwater := p_end_time;
        set @alter_log := concat('ALTER TABLE ',@tbl,'
ADD PARTITION (PARTITION p',@pendname,' VALUES LESS
THAN(',@phighwater,')')');

        prepare stmt from @alter_log;

        execute stmt;

        set cnt = cnt+1;

    END WHILE;

    select partsize as 'seconds',p_low_water as
'start at',p_high_water as 'stop at',cnt as
'partitions created',deld as 'partitions dropped';

END
```

Index

A

Access the Nimsoft Server	51
Alarm Server	97
Alarm SubConsole	81
Automatic Install	100

B

Browser setup.....	57
--------------------	----

C

<i>case</i>	13
<i>case INSENSITIVE</i>	13
<i>Client Install</i> icon 63, 75, 79, 83, 87, 97, 108, 125, 133	
Client Installation window 75, 79, 83, 87, 97, 108, 125, 133	
Client Installations	63
Cluster	135
Custom Install.....	100

D

<i>database</i>	13
Default destination folder	127
direct QoS Access	67
distributed SLM system	35
Distribution server.....	97
DMZ	68
DMZ Install.....	100
DMZ wizard.....	97

E

EnterpriseConsole.exe file.....	76, 127
---------------------------------	---------

F

firewalled environment.....	67, 97
-----------------------------	--------

I

Infrastructure Manager.exe file	79, 134
Infrastructure.exe	99
Infrastructure.exe file	89
Install Nimsoft Server in an active/passive Microsoft Cluster	135

Install Nimsoft Software on a client computer	63
Installing a Unix Robot.....	108
Installing a Windows Robot	87, 97
Installing Enterprise Console	75
Installing Infrastructure Manager.....	79
Installing Nimsoft components in a DMZ	68
Installing Service Level Manager	83

L

Launch Nimsoft applications	52
License Agreement dialog ..	21, 76, 79, 84, 89, 99

M

Microsoft .NET Framework.....	65, 66
Microsoft Cluster	135
Mobile Panel Client.....	66

N

nimldr.tar.z	108
Nimsoft Server Installation	12
Nimsoft Server Installation Wizard	21
nix installation	199

O

open ports	71
------------------	----

P

port 48000	72
port 48002	72
port 48004	72
Port 80	71
ports open	71

S

SLM.exe file	84
--------------------	----

T

tunnel	69
--------------	----

W

WebService	66
Windows Installation	201