Nimsoft Monitor Server

Configuration Guide

v6.00

Document Revision History

Version	Date	Changes
1.0	10/20/2011	Initial version of *Nimsoft Server Configuration Guide,* containing configuration and usage content moved from the previous *NMS Installation and User Guide.* This guide and *NMS Installation Guide* obsolete the previous *NMS Installation and User Guide.*
2.0	6/29/2012	Revised for NMS 6.00.

Contact Nimsoft

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

At http://support.nimsoft.com/, you can access the following:

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

Provide Feedback

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

Legal Notices

Warranty

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

Technology Licenses

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

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

Restricted Rights Legend

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

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

Contents

Chapter 1: NMS Overview 5

Chapter 2: Accessing NMS 6

Accessing the NMS Web Page 6
Launching Management Consoles 7
Modifying the Server Page Menu 7

Chapter 3: Deploying Probes 8

Installing Probes from the NMS Archive 8
Downloading Probes from the Internet Archive 9

Chapter 4: LDAP Configuration 10

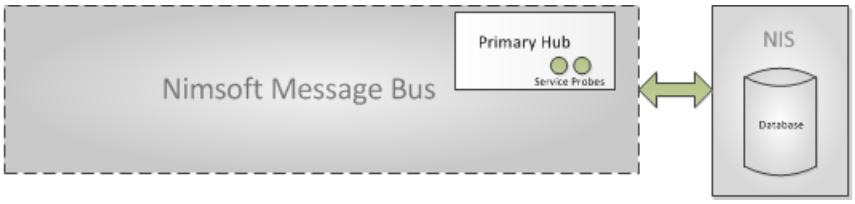
Basic LDAP Configuration 11
Advanced LDAP Configuration 12
    Codepage Values 13
Connecting Access Control Lists to LDAP Users 14

Chapter 5: SSL— Encrypting Network Traffic 15

Chapter 6: Nimsoft Online Support 16

Chapter 1: NMS Overview

Nimsoft Monitor Server (NMS) is the central data gathering and storage component of the Unified Monitoring solution. It is composed of the Message Bus, Primary Hub, Nimsoft Information Store (NIS, the database), monitoring infrastructure (hubs, robots and probes), and management applications, including Infrastructure Manager. See the *Nimsoft Monitor Installation Guide* for installation instructions.



NMS provides a web page that acts as a portal you can access through a web browser from other computers on your network.

Using this web page, you can:

- Install Nimsoft infrastructure components on your Windows and Unix® clients
- Access the NMS online documentation for all components and applications
- Install and launch Nimsoft applications (primarily Infrastructure Manager)

  Note: Functionality of Enterprise Console and SLM has been incorporated in the Unified Management Portal (UMP). See the *UMP Installation Guide* for installation instructions.

Note: For additional information on using NMS, refer to the *Infrastructure Manager* document, available from the **Documentation** tab at the Nimsoft support site.

Chapter 2: Accessing NMS

Accessing the NMS Web Page

Click the **NMS** icon on your desktop to launch the server web page. The address for this page is *nm_server*:8008, where *nm_server* is the hostname or IP address of the NMS system.

The tool bar in the upper right corner contains these buttons:

- **Home** takes you back to the initial home page as it appears at application start-up
- **Documentation** opens the NMS online help in a separate window
- **Online support** opens the Nimsoft Technical Support site in a separate window

The left frame lets you install Nimsoft Software on clients.

If you click a link in the left frame and nothing happens, try these steps:

1. Select **Tools > Internet Options**.
2. Go to the **Security** tab and select **Trusted Sites**.
3. Click **Sites** and add the server page URL (*server_name*:8008. Uncheck the https requirement and click **OK**.
4. Verify that the security level for Trusted Sites is set to **Low**.

Launching Management Consoles

Nimsoft offers the following consoles:

- Infrastructure Manager
- Service Level Manager

  Note: Functionality for Enterprise Console has been incorporated into the Unified Management Portal (UMP), the recommended and preferred console for displaying dashboards and reports.

  Note: Functionality of Enterprise Console and SLM has been incorporated in the Unified Management Portal (UMP). See the *UMP Installation Guide* for installation instructions.

To launch them:

- In Windows, select **Start > Nimsoft Monitor > Nimsoft Monitoring > *desired_console***
- On any computer in your network:

  a. Use a web browser to go the NMS web page (*server_name*:8008).

  b. Under Applications, click the desired console.

Note: If a dialog asks you to install a specific ActiveX control, follow the prompts to install it.

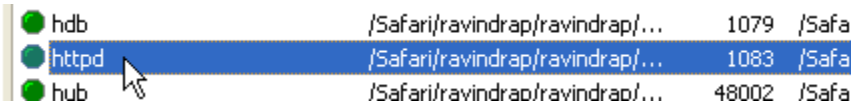
Modifying the Server Page Menu

The menu on the left of the page contains two links by default:

- **Application**
- **Installation**

You can hide either of these links by configuring the **httpd** probe on the NMS system.

1. On the NMS system, open the server web page (*nm_server*:8008).
2. Start Infrastructure Manager.
3. Double-click the **httpd** probe to display the probe configuration tool.



4. Toggle the checkboxes as appropriate for:
   - **Show application menu**
   - **Show client install page**
5. Click **OK**.
6. Click **Refresh** in your browser to verify that the desired items are shown on the server web page.

Chapter 3: Deploying Probes

Probes are small software programs. Nimsoft has two types:

- **Monitoring probes**, which gather availability and performance data from client systems and send the data to the Primary Hub. This data is stored in the Nimsoft Information Store (NIS) and made available to management consoles such as UMP and Infrastructure Manager.

  Some of these probes are *remote* probes (for example, network device monitoring probes) that run on a robot system monitoring remote devices.

- **Service probes** (also called Utility probes), which provide product utility functions to the Nimsoft infrastructure.

Robots manage the probes. Each Nimsoft client system has a robot.

The hub manages a group of robots. Each hub:

- Has its own robot equipped with several service probes
- Collects and redistributes data from the robots
- Maintains several central services and manages message subscribers

This section contains the following topics:

Installing Probes from the NMS Archive (page 8)
Downloading Probes from the Internet Archive(page 9)

Installing Probes from the NMS Archive

1. Start Infrastructure Manager.
2. To deploy a probe to a robot running on any physical or virtual machine, either:
   - Select and drag the probe name from the IM **Archive** folder to the robot node
   - Right-click the probe name to open a dialog that lets you add multiple probes in a single operation.

Downloading Probes from the Internet Archive

Some probes are not immediately found in the Nimsoft Archive; rather, you must download them from the central Nimsoft Archive. Follow these steps.

1. Log into http://support.nimsoft.com and select **Archive**.
2. Locate the desired probe and click **Save**. The selected probe is downloaded to your NMS Archive.
3. In Infrastructure Manager, either:
   - Select and drag the probe name from the IM **Archive** folder to the robot node
   - Right-click the probe name to open a dialog that lets you add multiple probes in a single operation.

To run any probe on a system, you must first have a robot running on that system. That is, the probe depends on a robot to manage its activities.

Remote probes (for example, network device monitoring probes) run on a robot system, which in turn can monitor remote devices. After deployment, each probe can be configured according to the specific tasks the probe can perform.

For example, with the interface traffic probe, you need to enter the host names or IP addresses and the SNMP community strings for the devices you want to monitor. Once the probe has been properly configured, the remote devices can be monitored via SNMP with no need for a robot or probe to be installed on the network device (referred to as *agentless monitoring*).

Chapter 4: LDAP Configuration

The **Lightweight Directory Access Protocol** (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an IP network.

The Nimsoft LDAP solution:

- Makes it possible to log into the Nimsoft management consoles using LDAP rather than the standard Nimsoft user login method
- Allows the Nimsoft hub to check all login requests against the LDAP server before trying the standard login method
- Is supported on Windows and Linux
- Requires certain configuration tasks on the hub and in Infrastructure Manager.

This section contains the following topics:

- **Basic LDAP Configuration** (page 11)
- **Advanced LDAP Configuration** (page 12)
- **Connecting Access Control Lists to LDAP Users** (page 14)

Basic LDAP Configuration

Follow these steps to configure your hub to forward login requests to an LDAP server and to access the container with the user groups.

1. On the hub system, start Infrastructure Manager.
2. Select the hub probe for the domain (domain/hub/robot/hub probe).
3. **Right click** on the hub probe and select **Configure** to open the hub configuration window.
4. On the **General** tab, click **Settings**. Go to the **LDAP** tab and specify the following.

Parameter	Value
Direct LDAP	Select if the hub connects directly to the LDAP server
Nimsoft Proxy Hub	Select if the hub does *not* connect directly to the LDAP server
Server Name	Hostname or IP for the LDAP server to which the hub will connect (click **Lookup** to test the communication)
Server Type	LDAP server type, either **Active Directory** or **eDirectory**
Authentication Sequence	Specify the order in which Nimsoft authenticates users
Use SSL	Select to use SSL during LDAP communication (most LDAP servers are configured to use SSL)
User/Password	Name and password for an account on the LDAP server to be used by the hub when accessing the LDAP server; how you specify it depends on the server type: ▪ **Active Directory**—ordinary user name ▪ **eDirectory**—path to the user in the format **CN=*username*,O=*organization***, where username and organization are replaced by appropriate values **Note**: This account does not need administrative privileges but does need the appropriate lookup privileges.
Group Container (DN)	Location in the LDAP structure where you want to search for users (click Test to check if the container is valid)
User Container (DN)	location in the Group Container where you want to search for users

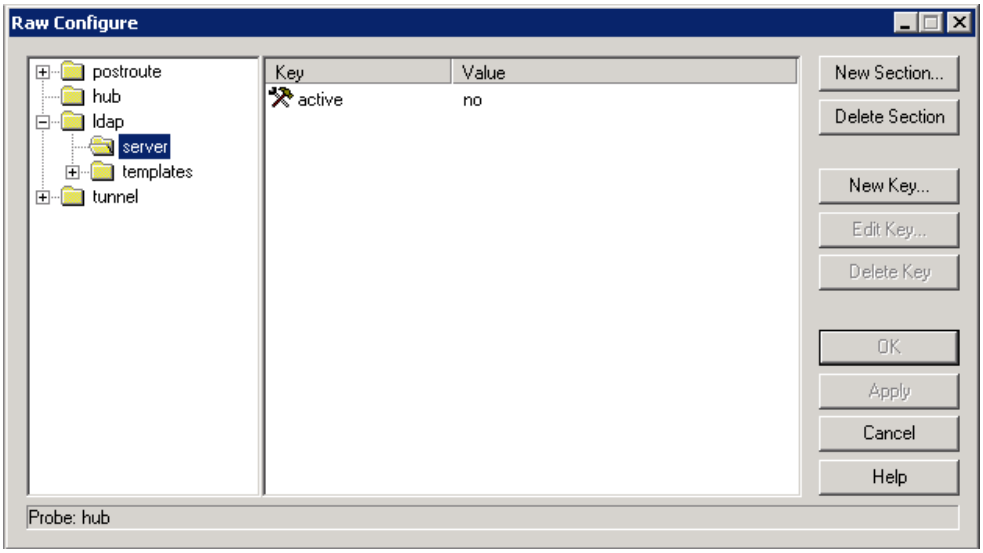
5. Click **Test** to verify that the user/password and container settings are valid.

See **Advanced LDAP Configuration** (page 12) for more configuration information.

Advanced LDAP Configuration

If you do not want to use the default configuration values, you can add tree keys to the hub configuration. These keys are read by the hub LDAP engine and affect how the hub communicates with the LDAP protocol.

1. On the hub system, start Infrastructure Manager.
2. Select the hub probe for the domain (domain/hub/robot/hub probe).
3. **Shift+right click** on the hub probe to open the **Raw Configure** window.
4. Navigate to **ldap > server**.



5. Click **New key**, enter the tree key and value, and click **OK**.

Tree Key	Purpose	Accepted Values
Timeout	Number of seconds to spend on each searching or binding (authentication) LDAP operation.	▪ 10 (default) ▪ Desired number
codepage	Specifies which codepage to use when translating characters from UTF-8 encoding to ANSI (which all Nimsoft components use internally). Text in the LDAP library is encoded as UTF-8. Because Nimsoft products do not have true Unicode support, all characters are translated into ANSI using this codepage.	Windows ▪ 28591* (default) ▪ Desired codepage number Linux ▪ ISO-8859-1* (default) ▪ Text string passed to the iconv_open function (Linux) * ISO 8859-1 Latin 1; Western European (ISO)

The tree key is now added.

Codepage Values

The hub LDAP library uses these functions.

- Windows

  MultibyteToWideChar and **WideCharToMultiByte** to translate to and from ANSI/UTF-8. These functions take a codepage as a parameter.

  For a list of Windows codepage numbers, go to:

  http://msdn.microsoft.com/en-us/library/ms776446(VS.85).aspx
  (not affiliated with Nimsoft)

- Linux

  iconv functions. For further reference, go to:

  http://www.gnu.org/software/libiconv/
  (not affiliated with Nimsoft)

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

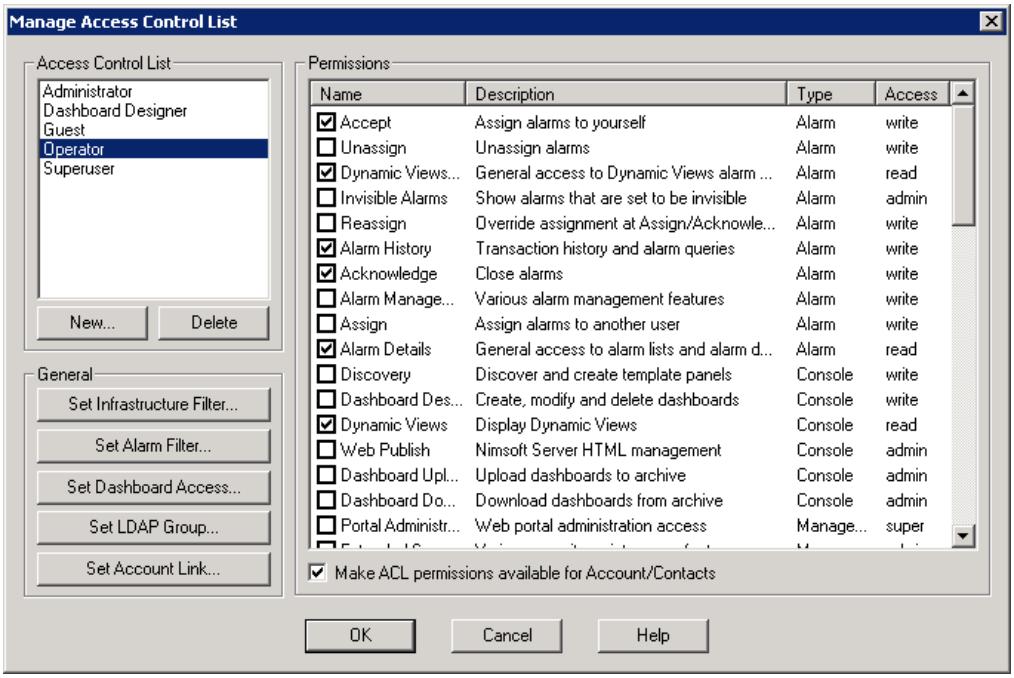
Connecting Access Control Lists to LDAP Users

You can create Access Control Lists (ACLs) and associate them with specific LDAP groups. The users in the LDAP group are then assigned the privileges for the associated ACL.

When an LDAP user logs into a console (such as Infrastructure Manager), the request is directed to the LDAP server for authentication. If the user name is found in a group attached to an ACL, the user is assigned privileges in Nimsoft as defined in the ACL. If the user belongs to multiple groups, privileges are assigned from the ACL with the most extended privileges.

Follow these steps.

1. In Infrastructure Manager, select **Security > Manage Access Control List** to open the **Manage ACL** dialog.



2. If you are creating a new ACL:
   a. Click **New** in the **Access Control List** area.
   b. Name the new ACL, select an ACL (if any exist) to copy its settings, and click **OK**.
   c. Select the desired options in the **Permissions** area.
3. Select an ACL, then click **Set LDAP Group**.
4. The **Set LDAP Group** dialog lists all groups in the container specified during configuration. Select a group and click **OK.**
5. Click **OK** in the **Manage Access Control List** dialog to exit and activate the new setting.
6. To verify the configuration, start Infrastructure Manager and log in as an LDAP user who is not a Nimsoft user. Verify that you have the appropriate privileges and can access the expected contents.

Chapter 5: SSL— Encrypting Network Traffic

Nimsoft Secure Communication gives you the option of using SSL encrypted communication between all Nimsoft components. This feature:

- Encrypts only network traffic; it is not used for authentication.
- Has a compatibility mode that lets you use old and new components in the same environment (with and without SSL). The SSL feature only

Important: Using SSL significantly reduces traffic bandwidth and performance. Not all probes support SSL.

SSL settings are specific to each hub. Repeat this procedure for every hub requiring SSL.

1. On the hub system, start Infrastructure Manager.
2. Locate the hub probe for the domain (domain/hub/robot/hub probe).
3. **Right click** on the hub probe and select **Configure** to open the hub configuration window.
4. On the **General** tab, click **Settings**, then go to the **SSL** tab.
5. Select a **Mode**:
   - **Normal**— Nimsoft encryption only
   - **Compatibility Mode** (recommended!)— Mixed SSL/Nimsoft mode; all components try SSL communication first, but switch to Nimsoft secure communication (Normal mode) for older components
   - **SSL Only**—SSL encryption only

   Note: If one hub in a domain is changed to **SSL Only**, all hubs in that domain that are set to **Off** will also change to **SSL Only**. (Hubs with Compatibility Mode are not affected.) Because all hubs exchange security and address information often, this change will propagate to all hubs over time.
6. Specify the **Cipher Type**.
7. Click **OK**. The hub propagates the SSL settings to the robots, which in turn propagate the settings to the probes.

Chapter 6: Nimsoft Online Support

The **Online support** link in the upper right corner of the NMS web page 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**—Questions from our users
- **Forum**— World Wide User Forum where customers discuss Nimsoft product
- **Announcements**—Information about Nimsoft product and service releases
- **Archive**—Product and service downloads, datasheets and release notes for all Nimsoft products
- **Downloads**—Nimsoft products and documentation
- **Training**—Nimsoft University course offerings