CA Nimsoft Monitor Server

Configuration Guide

7.6

Document Revision History

Version	Date	Changes
7.6	June 2014	No revisions for 7.6.
7.5	March 2014	No revisions for 7.5.
7.1	December 2013	No revisions for 7.1.
7.0	September 2013	Minor revisions for 7.0.
6.5	March 2013	Minor revisions for 6.5.
6.2	November 2012	Minor revisions for 6.2.
6.1	September 2012	Minor revisions and documentation fixes for 6.1.
2.0	June 2012	Revisions for 6.0.
1.0	October 2011	Initial version of *NMS Server Configuration Guide,* containing configuration and usage content from the previous *NMS Server Installation and User Guide.* This guide and the *NMS Server Installation Guide make* obsolete the previous *NMS Server Installation and User Guide.*

Contact CA

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

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

Providing Feedback About Product Documentation

Send comments or questions about CA Technologies Nimsoft product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

CA Nimsoft Monitor Copyright Notice

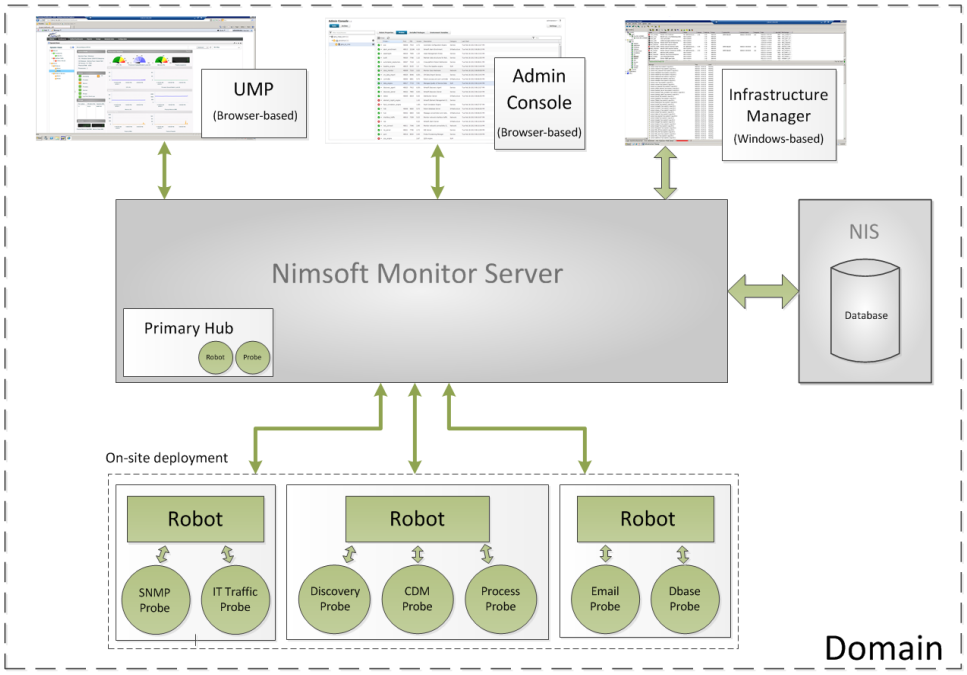
Legal information on third-party and public domain software used in the Nimsoft Monitor solution is documented in *Nimsoft Monitor Third-Party Licenses and Terms of Use (*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Contents

Chapter 1: CA Nimsoft Monitor Server Overview

CA Nimsoft Monitor Server (NMS) is the central data gathering and storage component of the Unified Monitoring solution. Server is composed of the:

- Message Bus
- Primary Hub
- Nimsoft Information Store (NIS, the database)
- Monitoring infrastructure (hubs, robots and probes)
- Management consoles, including AdminConsole and Infrastructure Manager



CA Nimsoft Monitor provides a web page (http://<*servername_or_server_IP_address*>:8080) that acts as a portal for other computers on your network.

Using this web page, you can:

- Launch AdminConsole
- Install Infrastructure Manager
- Install CA Nimsoft Monitor infrastructure components on your Windows and Unix® clients
- Link to CA Nimsoft Monitor Support
- Access CA Nimsoft Monitor online documentation for all components and applications.

The CA Nimsoft Monitor documentation library (alternatively the downloads tab at http://support.nimsoft.com) provides access to the following online guides:

- overview--see the *CA Nimsoft Monitor Server Getting Started Guide*
- installation--see the *CA Nimsoft Monitor Installation Guide*
- UMP installation--see the *UMP Installation Guide*
- AdminConsole use--see the *Getting Started with AdminConsole Guide*
- configuration and use--see the *Infrastructure Manager Guide.*

Chapter 2: Accessing CA Nimsoft Monitor Server

This section contains the following topics:

Accessing the CA Nimsoft Monitor Server Web Page

Your CA Nimsoft Monitor web page lets you access installers and documentation. To access it, use one of the following:

- On the CA Nimsoft Monitor server system, click the CA Nimsoft Monitor icon on the desktop.
- From any computer in your network, browse to http://*nm_server*:8080, where *nm_server* is the hostname or IP address of the system.

The page contains the following links:

- **Documentation** opens the online documentation in a new window
- **Online support** opens the Technical Support site in a new tab
- **Management** provides links to the Admin Console management interface and to an installer package for the legacy Infrastructure Manager
- **Infrastructure Deployment** provide links to infrastructure installer packages for hubs and robots.

If you click a link 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 (http://nm_ser*ver*:8080). Uncheck the https requirement, then click **OK**.
4. Verify that the security level for Trusted Sites is set to **Low**.

Installing a Management Console on a Client

Infrastructure Manager lets you explore and configure your CA Nimsoft Monitor environment within a graphical navigation display. To use it, you can either:

- Install and run it on any Windows computer on your network. This is the most common method for most users, and it is the only method if your NMS system is a Linux or Solaris server.
- RDP to your NMS system and run Infrastructure Manager there, provided the NMS system is a Windows server and the application is installed.

Note: AdminConsole, which provides a growing number of infrastructure management features, is a platform-independent management console, accessed within a supported browser, or within UMP. It can be launched from the link available on your CA Nimsoft Monitor web page (http://*nm_server*:8080), or installed as a portlet within UMP.

By default Admin Console connects with the server by HTTP. It can be configured to connect securely with HTTPS, using either a self signed- or certificate authority-signed SSL certificate. For details, see the online help for Admin Console, available from the CA Nimsoft Monitor Documentation Library.

To install and run Infrastructure Manager on a Windows computer in your network, follow these steps:

1. Use a web browser to go your CA Nimsoft Monitor web page (http://*nm_server*:8080).
2. Click **Legacy Infrastructure Manager** and run the installer.
3. Follow the prompts to complete the installation.
4. Select **Start > Monitoring > Infrastructure Manager**.

To remotely run Infrastructure Manager on the NMS system, follow these steps:

1. In Windows, select **Start > All Programs > Accessories > Remote Desktop Connection**.

   Note: Alternatively you can select **Start** and enter **mstsc** in the Search box.
2. Connect using the following information:
   - **Computer:** IP address for your NMS system
   - **Username/password:** the CA Nimsoft Monitor user login and password you set up during installation.
3. Select **Start** > **All Programs** > **<Monitoring> Infrastructure Manager**.

   Note: If Infrastructure Manager is not present, follow the steps above to install it.

Chapter 3: Deploying Probes

Probes are small software programs. To run any probe on a system, you must first have a robot running on that system. The probe depends on a robot to manage its activities.

CA Nimsoft Monitor has two types of probes:

- **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 CA Nimsoft Monitor infrastructure.

After deployment, each probe can be configured according to the specific tasks the probe can perform.

A hub manages a group of robots. Each hub:

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

This section contains the following topics:

Installing Probes from the Archive

1. Start Infrastructure Manager.
2. Locate the desired probe in the **Archive** folder.
3. Deploy the probe to a robot running on any physical or virtual machine, by dragging the probe from the **Archive** folder and dropping it onto the robot node.

Downloading Probes from the Internet Archive

Some probes are not immediately found in the NMS Archive. You can download these probes from the central NMS Archive.

Follow these steps:

1. Log in to http://support.nimsoft.com and select **Archive**.
2. Locate the desired probe and click **Save**. The selected probe is downloaded to your NMS Archive.

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 LDAP solution:

- Makes it possible to log in to the CA Nimsoft Monitor management consoles using LDAP rather than the standard CA Nimsoft Monitor user login method
- Allows the CA Nimsoft Monitor 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

Configure your hub to forward login requests to an LDAP server and to access the container with the user groups.

Follow these steps:

1. On the hub system, start Infrastructure Manager.
2. Select the hub probe for the domain (domain/hub/robot/hub probe).
3. Right-click 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 settings.

   Direct LDAP

   Select this if the hub connects directly to the LDAP server.

   Nimsoft Proxy Hub

   Select this 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 that the hub will use to 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.

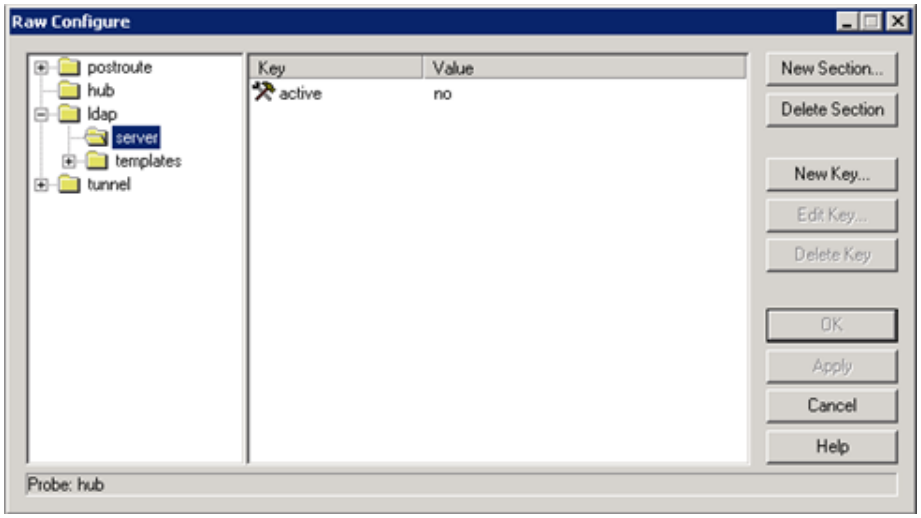
5. Click **Test** to verify that the user/password and container settings are valid.

See Advanced LDAP Configuration **(see page 15)** 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 the hub probe to open the **Raw Configure** window.
4. In the left pane, navigate to **ldap > server**.



5. Click **New Key** and enter the tree key and value:

   Timeout

   Number of seconds to spend on each searching or binding (authentication) LDAP operation.

   Accepted values are:

   - 10 (default)
   - Desired number

   codepage

   Specifies which codepage to use when translating characters from UTF-8 encoding to ANSI (which all CA Nimsoft Monitor components use internally). Text in the LDAP library is encoded as UTF-8. Because CA Nimsoft Monitor products do not have true Unicode support, all characters are translated into ANSI using this codepage.

   Accepted values are:

   - 28591* (Windows default)
   - Valid codepage number (Windows)
   - ISO-8859-1* (Linux default)
   - Text string that is passed to the iconv_open function (Linux)

   ** ISO 8859-1 Latin 1; Western European (ISO)*

6. Click **OK**.

The tree key is added.

Codepage Values

The hub LDAP library uses these functions.

- **Windows**—MultibyteToWideChar and WideCharToMultiByte

  These functions translate to and from ANSI/UTF-8. Both take a code page as a parameter. For a list of Windows code page numbers, go to http://www.microsoft.com *(not affiliated with CA Nimsoft Monitor)* and search for *Code Page Identifiers*.

- **Linux**—iconv functions

  For further reference, go to http://www.gnu.org/software/libiconv *(not affiliated with CA Nimsoft Monitor).*

The code page key is not shipped with the hub configuration file.

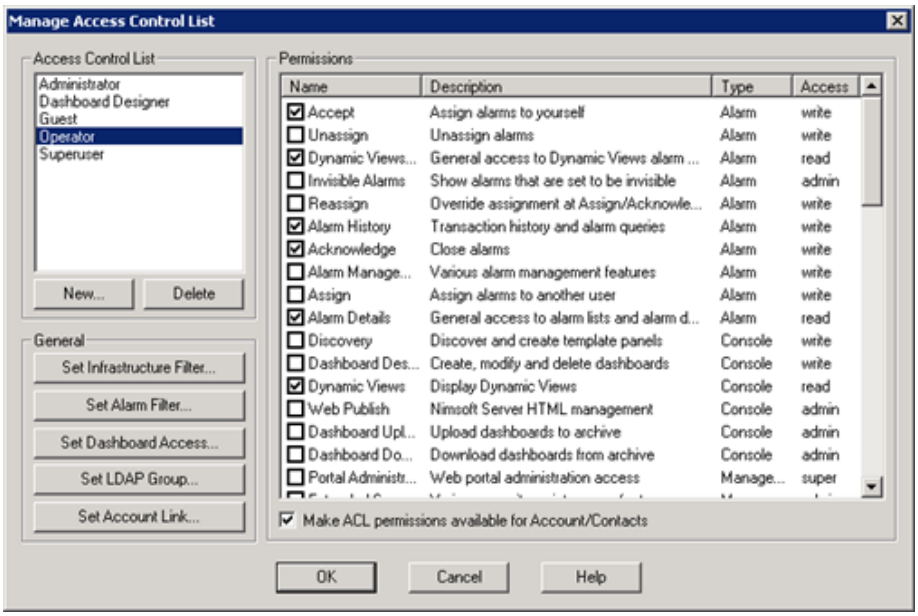
Connecting Access Control Lists to LDAP Users

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.

For example, if an LDAP user logs into Infrastructure Manager, the request is directed to the LDAP server for authentication. If the user name is found in a group that is attached to an ACL, the user is assigned privileges 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**.



2. To create an ACL:
   a. Click **New** under **Access Control List**.
   b. Name the new ACL, then select an ACL (if any exist) to copy its settings. Click **OK**.
   c. Select the desired options in the **Permissions** area.

3. To associate a group with an ACL:
    a. Select the new or existing ACL.
    b. Click **Set LDAP Group**. All groups in the container are listed.
    c. Select a group and click **OK.**
4. Click **OK** in the **Manage Access Control List** dialog.

The new setting is active. To verify the configuration, start Infrastructure Manager and log in as an LDAP user who is not a CA Nimsoft Monitor user. Verify that you have the appropriate privileges and can access the expected contents.

Chapter 5: SSL— Encrypting Network Traffic

CA Nimsoft Monitor secure communication gives you the option of using SSL encrypted communication between all CA Nimsoft Monitor 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).

  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 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**—NMS encryption only
   - **Compatibility Mode** (recommended)—Mixed SSL/NMS mode

     All components try SSL communication first, but switch to NMS 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 using 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: Online Support

The **Online Support** link in the CA Nimsoft Monitor web page opens the *Technical Support Site* (http://support.nimsoft.com) 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 products
- **Announcements**—Information about product and service releases
- **Archive**—Product and service downloads, datasheets and release notes for all products
- **Downloads**—products and documentation
- **Training**—CA Nimsoft Monitor University course offerings