CA Unified Infrastructure Management Server

CA UIM Server Configuration Guide

8.0

technologies

Document Revision History

Version	Date	Changes
8.0	September 2014	Rebranded for UIM 8.0.
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 *Nimsoft Monitor Server Configuration Guide,* containing configuration and usage content from the previous *Nimsoft Monitor Server Installation and User Guide.* This guide and the *Nimsoft Monitor Server Installation Guide make* obsolete the previous *Nimsoft Monitor 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 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 support website at http://ca.com/docs.

Copyright Notice

This online help system (the "System") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This System may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This System is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties. This System may not be disclosed by you or used for any purpose other than as may be permitted in a separate agreement between you and CA governing your use of the CA software to which the System relates (the “CA Software”). Such agreement is not modified in any way by the terms of this notice.

Notwithstanding the foregoing, if you are a licensed user of the CA Software you may make one copy of the System for internal use by you and your employees, provided that all CA copyright notices and legends are affixed to the reproduced copy.

The right to make a copy of the System is limited to the period during which the license for the CA Software remains in full force and effect. Should the license terminate for any reason, it shall be your responsibility to certify in writing to CA that all copies and partial copies of the System have been destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS SYSTEM “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS SYSTEM, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The manufacturer of this System is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

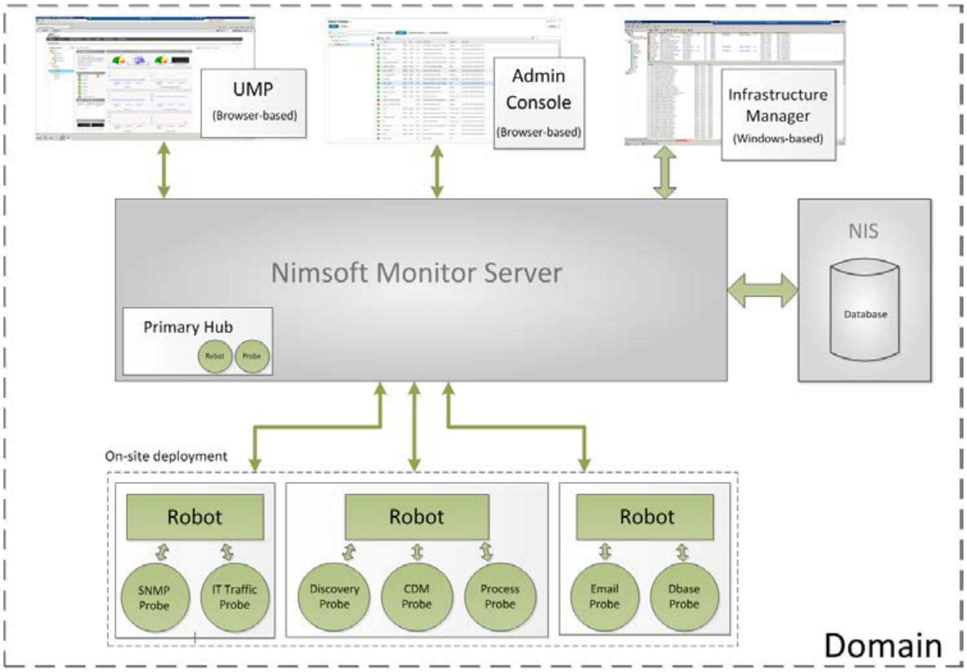
Legal information on third-party and public domain software used in this product is documented in the *Third-Party Licenses and Terms of Use* *(*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Contents

Chapter 1: CA UIM Server Overview

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

- Message Bus
- Primary Hub
- UIM database (sometimes referred to as the *NIS database*)
- Monitoring infrastructure (hubs, robots and probes)
- Management consoles, including Admin Console and Infrastructure Manager



Access the UIM Server web page at http://<*UIMServer_name_or_IP_address*>:8080. Using this web page, you can:

- Launch Admin Console
- Install Infrastructure Manager
- Install UIM infrastructure components on your Windows and Unix® clients
- Link to support
- Access online documentation for all components and applications

The CA Unified Infrastructure Management documentation library (alternatively the downloads tab at http://support.nimsoft.com) provides access to help on the following topics:

- Overview: see the *UIM Server Getting Started Guide*
- Installation: see the *UIM Server Installation Guide*
- UMP installation: see the *UMP Installation Guide*
- Admin Console use: see the *Getting Started with Admin Console Guide*
- Infrastructure Manager use: see the *Infrastructure Manager Guide*

Chapter 2: Accessing UIM Server

This section contains the following topics:

Accessing the UIM Server Web Page

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

- On the CA Unified Infrastructure Management server system, click the CA Unified Infrastructure Management icon on the desktop.
- From any computer in your network, browse to:

  http://<*UIMServer_name_or_IP_address*>:8080

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. Uncheck the https requirement, then click **OK**.
4. Verify that the security level for Trusted Sites is set to **Low**.

Accessing UIM Server Management Consoles

UIM Server provides two management consoles that enable you to explore and configure your UIM environment within a graphical navigation display:

- **Admin Console** is platform-independent application that is accessed from a browser or within UMP. You can launch it from the link available on your UIM Server web page (http://*<UIM_Server_name_or_IP>*:8080), or install it 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 Unified Infrastructure Management Documentation Library.

- **Infrastructure Manager** is a Windows-based application. 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: As of this release, some configuration tasks can only be performed with Infrastructure Manager.

Accessing Infrastructure Manager

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

1. Use a web browser to go your NMS 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 > All Programs > Nimsoft 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 user login and password you set up during installation.
3. Select **Start > All Programs > Nimsoft Monitoring > Infrastructure Manager**.

Chapter 3: Deploying Probes

Probes are small software programs deployed throughout your infrastructure that collect monitoring data and provide UIM services. 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 Unified Infrastructure Management has two types of probes:

- **Monitoring probes** gather availability and performance data from client systems.

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

- **Infrastructure probes** send the data to the primary hub. This data is stored in the UIM database and made available to the management consoles.
- **Service probes** (also called Utility probes), which provide product utility functions to the CA Unified Infrastructure Management infrastructure.

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

This section contains the following topics:

Installing Probes from the Archive

Follow these steps:

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 archive. You can download these probes from the central CA UIM 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 local 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 management consoles using LDAP rather than the standard UIM user login method
- Allows the primary 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.

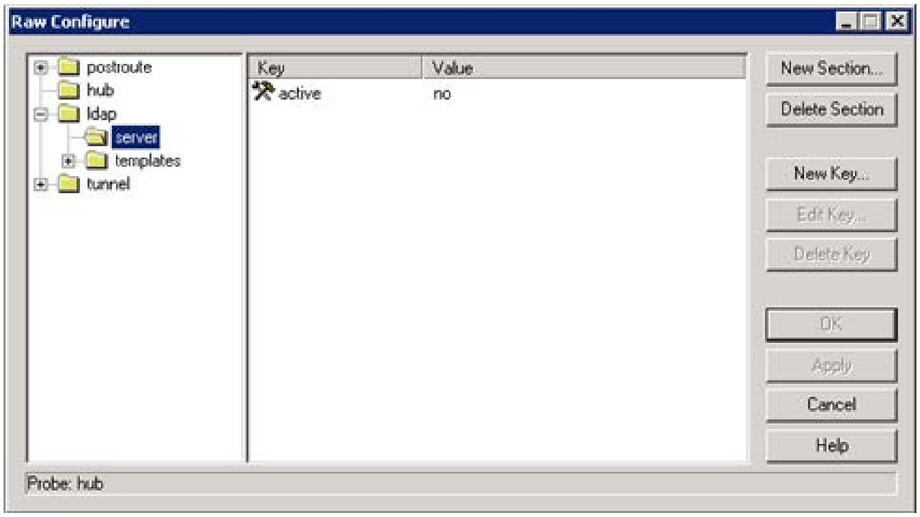
5. Click **Test** to verify that the user/password and container settings are valid.

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 robot's hub probe (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**.



Key	Value
active	no

Probe: hub

5. Click **New Key** and enter the following tree keys and values:

   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 Unified Infrastructure Management components use internally). Text in the LDAP library is encoded as UTF-8. Because CA Unified Infrastructure Management 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)* and search for *Code Page Identifiers*.

- **Linux:** iconv functions

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

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

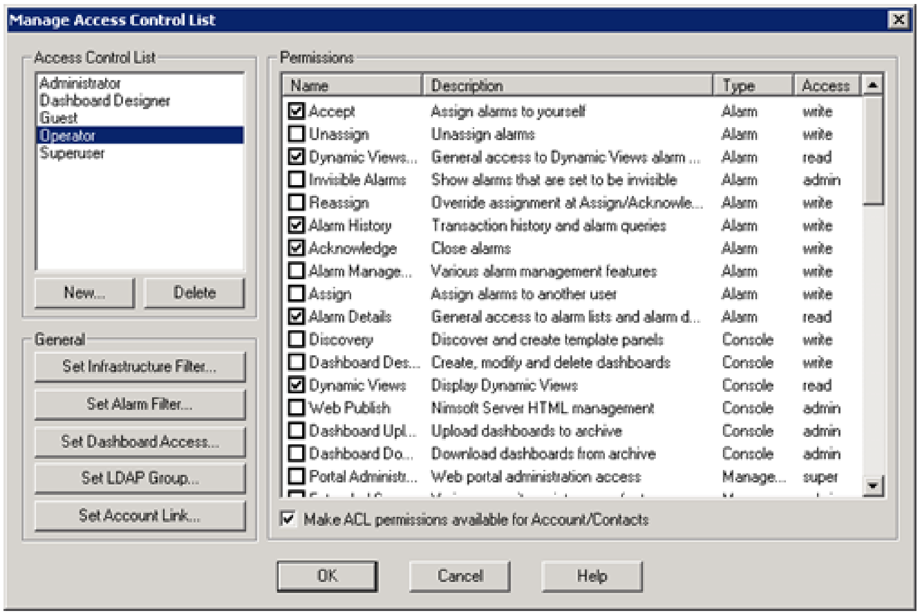
Connecting Access Control Lists to LDAP Users

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 a UIM component, 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**.



Name	Description	Type	Access
☑ Accept	Assign alarms to yourself	Alarm	write
□ Unassign	Unassign alarms	Alarm	write
☑ Dynamic Views...	General access to Dynamic Views alarm ...	Alarm	read
□ Invisible Alarms	Show alarms that are set to be invisible	Alarm	admin
□ Reassign	Override assignment at Assign/Acknowle...	Alarm	write
☑ Alarm History	Transaction history and alarm queries	Alarm	write
☑ Acknowledge	Close alarms	Alarm	write
□ Alarm Manage...	Various alarm management features	Alarm	write
□ Assign	Assign alarms to another user	Alarm	write
☑ Alarm Details	General access to alarm lists and alarm d...	Alarm	read
□ Discovery	Discover and create template panels	Console	write
□ Dashboard Des...	Create, modify and delete dashboards	Console	write
☑ Dynamic Views	Display Dynamic Views	Console	read
□ Web Publish	Nimsoft Server HTML management	Console	admin
□ Dashboard Upl...	Upload dashboards to archive	Console	admin
□ Dashboard Do...	Download dashboards from archive	Console	admin
□ Portal Administr...	Web portal administration access	Manage...	super

☑ Make ACL permissions available for Account/Contacts

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 Unified Infrastructure Management user. Verify that you have the appropriate privileges and can access the expected contents.

Chapter 5: SSL— Encrypting Network Traffic

CA Unified Infrastructure Management secure communication gives you the option of using SSL encrypted communication between all UIM 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 robot's hub probe (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**:
   - **Norma**l — 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 Unified Infrastructure Management web page opens the 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 Unified Infrastructure Management University course offerings