

Nimsoft Monitor

controller Guide

v5.7 series



Legal Notices

Copyright © 2013, CA. All rights reserved.

Warranty

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

Technology Licenses

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

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

Restricted Rights Legend

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

Trademarks

Nimsoft is a trademark of CA.

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

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

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

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

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

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

UNIX® is a registered trademark of the Open Group.

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

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

For information on licensed and public domain software, see the *Nimsoft Monitor Third-Party Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contact Nimsoft

For your convenience, CA Nimsoft provides a single site where you can access information about CA 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
- CA Nimsoft Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

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

Contents

Chapter 1: controller 5.7	7
controller General Overview	7
Supported Platforms	7
Chapter 2: controller Configuration Overview	9
How to Access the Probe Configuration GUI.....	9
Probe Configuration GUI Navigation	9
Chapter 3: Deploy Probes Using Admin Console	11
Review Probe Prerequisites	12
Log in to Admin Console	12
Deploy a Probe to the Hub/Robot	13
Verify the Probe Package Deployed.....	13
Chapter 4: How to Configure the controller Probe	15
How to View Probe Information	16
How to View Hub Activity	16
How to Set General Information	17
How to View Status	18
controller Setup Configuration.....	18
How to Configure Robot Information	19
How to Configure Advanced Information	20
Environment Variables Configuration.....	21
Virtual Robot Configuration	22
How to Configure NAT	24
How to Set controller IP Address	26

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
1.5	March 2013	Initial release of Admin Console probe GUI. (Previous versions of this probe are configured using Infrastructure Manager). <ul style="list-style-type: none">■ Added support for reading alarm tokens from configuration and support for Windows on IA64 systems.

Related Documentation

Documentation for other versions of the controller probe

The [Release Notes](#) for the controller probe

Getting Started with CA Nimsoft Probes

(http://docs.nimsoft.com/prodhelp/en_US/Probes/GettingStarted/index.htm)

Monitor Metrics Reference Information for CA Nimsoft Probes

(http://docs.nimsoft.com/prodhelp/en_US/Probes/ProbeReference/index.htm)

Chapter 1: controller 5.7

This section contains the following topics:

[controller General Overview](#) (see page 7)

[Supported Platforms](#) (see page 7)

controller General Overview

The controller is a core component of the Nimsoft robot and is responsible for scheduling the other probes and maintaining contact with the Nimsoft hub.

The controller probe focuses on keeping configured probes running according to the probe configuration and handles 'housekeeping' operations towards Nimsoft, such as telling the hub about its state, name-lookup services, license management, etc. It responds to the elements in the configuration files *robot.cfg* and the *controller.cfg* as well as to commands requested over the registered port TCP/48000.

Important! We do not support cloning of robots. We recommend you use the cloud installation option for the robot to ensure that it is not started until the vm-clone instance is created, and then using request.cfg to get the required probes and probe configurations installed.

Supported Platforms

The controller probe supports the same set of operating systems and databases as supported by the Nimsoft Server solution. Please refer to the [Nimsoft Compatibility Support Matrix](#) for the latest information on supported platforms.

Chapter 2: controller Configuration Overview

This section contains the following topics:

[How to Access the Probe Configuration GUI](#) (see page 9)

[Probe Configuration GUI Navigation](#) (see page 9)

[Deploy Probes Using Admin Console](#) (see page 11)

How to Access the Probe Configuration GUI

The probe configuration GUI is accessed using the Admin Console application.

Follow these steps:

1. Login to the Admin Console application.
2. Select the **Infrastructure** button in the upper left corner.
3. In the navigation pane, select the robot where the probe resides. You may need to expand the navigation tree in the left pane to see the robot.

The right pane displays the robot configuration options. The options include Robot Properties, Probes, Installed Packages, and Environment Variables.

4. Select the **Probes** button in the right pane.
A list of available probes on the robot appears.
5. Click on the green checkmark icon and select **Configure** from the drop down menu.

The probe configuration GUI appears in a separate window.

Probe Configuration GUI Navigation

The probe configuration GUI is a similar format to the Admin Console application. The left navigation pane displays the probe nodes and any monitored resources in a tree structure. Each node in the navigation pane will display configuration items in the right pane. These configuration items change depending on the node selected in the navigation pane.

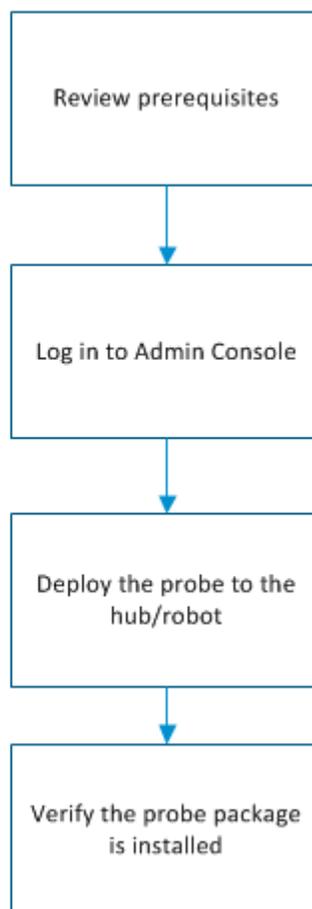
Chapter 3: Deploy Probes Using Admin Console

As a Nimsoft Monitor System (NMS) Administrator, you deploy probes using the Admin Console application. The NMS uses probes to monitor your system, send alarms and provide dashboards that display the status of your system. After deploying a probe you will need to configure the probe for your specific monitoring requirements.

How to Deploy a Probe



Administrator



This section contains the following topics:

[Review Probe Prerequisites](#) (see page 12)

[Log in to Admin Console](#) (see page 12)

[Deploy a Probe to the Hub/Robot](#) (see page 13)

[Verify the Probe Package Deployed](#) (see page 13)

Review Probe Prerequisites

The administrator reviews the prerequisites for each probe before they deploy the probe to a hub or robot. Reviewing this information enables the administrator to foresee environmental issues so probe deployment occurs smoothly. The probe prerequisite information can be found in the individual probe release notes and configuration document.

Log in to Admin Console

Admin Console can be accessed either through a standalone web page or through UMP. The procedure for accessing your Admin Console application depends on the version of the Admin Console installed on your system.

Log in to Admin Console in UMP

Follow these steps:

1. Connect to your UMP application in a web browser.
2. Enter a valid Nimsoft user name and password.

The CA Nimsoft Unified Management Portal opens to the USM portlet.

3. Click the Admin Console tab.

Note: If the Admin Console tab is not available, see the Add Portlets section to add this portlet.

The Admin Console screen appears.

Your NMS system is available for configuration.

Log in to Admin Console in a Standalone Web Page

Follow these steps:

1. Enter `https://<service_host>:8443/adminconsole` in your web browser window.
Note: `<service_host>` is the system where the `service_host` probe is installed.
2. Enter a valid NMS username and password.
The Admin Console application opens.

Deploy a Probe to the Hub/Robot

Follow these steps:

1. Click the **Archive** button at the top of the Admin Console window.
2. Click **Local Archive** or **Web Archive**.
Note: If the probe is not listed in the local archive and you deploy from the Web Archive, the probe will be download to your local archive.
3. Click the arrow button next to the hub name in the navigation pane to display the robots on the hub.
4. Select the check box(es) next to the name of the targeted robot(s) in the navigation pane.
The right pane displays the probes available on the archive you selected above.
5. Select the check box(es) next to the name of the probe(s) you want to deploy.
6. Click the **Deploy** button at the top of the probe listing.
You will receive a confirmation message.
7. Click **OK** to deploy the probe to the selected robot.

Verify the Probe Package Deployed

Follow these steps:

1. Click the **Infrastructure** button at the top of the Admin Console screen.
2. Select the name of the robot where you deployed the probe.
3. Select the **Probes** button at the top of the right pane.
The probe should be listed in the right pane.

The probe is now ready for you to configure.

Chapter 4: How to Configure the controller Probe

Open the controller Probe Configuration GUI. For more information see [How to Access the Probe Configuration GUI](#) (see page 9) section.

The left navigation pane displays the configurable items on the physical system being monitored. To view all of the configuration objects, expand the tree structure in the left navigation pane. Each configuration object in the navigation pane is configured individually.

The controller object configuration contains the following sections:

- Probe Information
- Hub Connectivity
- General Configuration
- Status

The setup object configuration contains the following sections:

- Nimsoft robot
- Advanced
- Environment variables
- Alarms
- Virtual
- NAT
- IP

This section contains the following topics:

[How to View Probe Information](#) (see page 16)

[How to View Hub Activity](#) (see page 16)

[How to Set General Information](#) (see page 17)

[How to View Status](#) (see page 18)

[controller Setup Configuration](#) (see page 18)

How to View Probe Information

Follow these steps:

1. Select **controller** in the left navigation.

The controller probe information appears at the top of the right pane.

This information cannot be modified.

How to View Hub Activity

Follow these steps:

1. Select **controller** in the left navigation.

The hub activity information appears in the right pane.

This information cannot be modified.

How to Set General Information

Follow these steps:

1. Select **controller** in the navigation pane.
2. Update the fields as needed.

Identification Property User Tag 1 & 2

User defined tag used as a grouping/locating mechanism.

Log Level

Sets the amount of detail to be logged to the log file. Log as little as possible during normal operation to reduce disk consumption, and increase the level of detail when debugging.

Log Size

This field allows you to change the size of the log file according to your needs. The default size of the log file is 1024 KB.

Hub Update Interval (in minutes)

Determines at what interval the hub is contacted with an "alive" message. The range is 1 to 180 minutes. Note that the hub is notified on a shorter interval when changes occur in the probe list.

On Robot uptime, reported as state changes

If this option is selected, QoS messages on robot uptime will be sent. The QoS message 'status = up' will be sent when the robot starts, and the QoS message 'status down' will be sent when the robot stops.

Set QoS source to robot name instead of computer hostname

If this option is selected, the robot name specified on the Setup > Nimsoft tab will be used instead. Otherwise the host name of the computer hosting a probe is by default used as QoS source in QoS message from the probes.

Robot mode

Normal or passive mode. Passive robots cannot initiate communication with a hub. All contact must be initiated by the hub.

3. Click **Save** to update your configuration.

How to View Status

Follow these steps:

1. Select **controller** in the left navigation.

The status information appears in the right pane. You might need to scroll down the right pane to view the status information.

This information cannot be modified.

controller Setup Configuration

The setup node in the left navigation allows you to configure your robot settings: robot information, advanced information, environment variables, alarms, virtual robots, NAT, and IP information.

How to Configure Robot Information

Follow these steps:

1. Select **setup** in the navigation pane.
2. Update the settings in the Nimsoft section in the right pane.

Robot Name

The name of the Robot.

- Automatically detect: The Host name will be used.
- Specific name: You can specify the robot name to be used.

Secondary Hub Robot Name

Defines the method used to determine the secondary hub. The secondary hub will be used if the primary hub is unavailable.

- Automatically detect (searches the subnet)

The controller searches the subnet for a responding hub within the domain when the primary and secondary hubs are unavailable.

- Specified Hub (IP/name)

Enter a specific hub when the primary hub is not available.

- Secondary Domain

Search the subnet for a temporary hub when primary and secondary hubs are unavailable

The controller will search for a temporary hub if the primary and secondary hubs are unavailable.

3. Click **Save** to update the configuration.

How to Configure Advanced Information

Follow these steps:

1. Select **setup** in the navigation pane.
2. Update the settings in the Advanced section in the right pane.

Automatically unregister from HUB at shutdown

When the robot is stopped, an unregister message is sent to the hub on which it is registered. This will make the robot disappear from Infrastructure Manager. If this is not selected, the stopped robot will appear with a red icon, enabling the operator to detect the situation.

Suspend all probes when no network connection is available

When running the robot on a computer with no network connection, you can determine whether the robot should be active or enter a sleep mode where all probes are suspended until a network connection is again available. If this option is not selected the alarm messages will be spooled and flushed when a network connection is again available.

Note: This function is available only on Windows platforms.

Configure file locking

First probe port number

Daemon type probes will normally register a command port, which is allocated run-time on probe start-up. Setting the probe port number will make the robot allocate specific port numbers for the probes as they are started. Use this option if you want the probes to have port numbers in a specific range for router / firewall purposes.

Time offset from UTC

This option lets you override the local time zone setting. The time specification must be entered as time offset from UTC (in seconds).

When no contact with hub

Set limitations for attempts to connect an unmanaged robot (a robot that has lost the contact with its hub) to a hub, using the Tools > Connect Robot option in Infrastructure Manager.

The following options are available:

- Do not allow robot to be moved
- Allow move only within domain

3. Click **Save** to update the configuration.

Environment Variables Configuration

The environment variables for the robot are inherited by all the probes managed by the robot.

How to View Environment Variables

Follow these steps:

1. Select **setup** in the navigation pane.

The Environment Variables section appears in the right pane. You may need to scroll down to view this section.

The robot controller will read the variable/value pair in the list and insert it into the robot environment. This environment is inherited by all probes managed by the robot.

How to Add Environment Variables

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the Environment Variables section click **New**.

Empty variable and variable value fields appear to the right of the environment variables list.

3. Enter the appropriate information.
4. Click **Save** to update the configuration.

How to Modify Environment Variables

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the Environment Variables section click the variable you want to modify.

The variable and variable value fields appear to the right of the environment variables list.

3. Update the variable fields.
4. Click **Save** to update the configuration.

How to Delete Environment Variables

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the Environment Variables section click the variable you want to delete.
3. Click **Delete**.
A confirmation message appears, click **OK**.
4. Click **Save** to update the configuration.

Virtual Robot Configuration

The controller probe sets up the communication between the robot and the virtual probe running a remote probe.

Important! The netware probe is the only probe that can be set up on a virtual robot.

Virtual robots, using the proxy probe, will be created for 'remote' probes. Remote probes are installed and running on computers without a robot. The remote probe is configured with the path to the robot.

How to Add a Virtual Robot

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the Virtual section click **New**.
3. Update the attributes as appropriate.

Virtual Robot

The name of the machine where netware is installed and running.

User tag 1

User tag 2

4. Click **Save** to update the configuration.

How to Modify a Virtual Robot

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the Virtual section select a virtual robot.
3. Update the attributes as appropriate.
4. Click **Save** to update the configuration.

How to Delete a Virtual Robot

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the Virtual section select a virtual robot.
3. Click **Delete**.
The connection to the virtual robot is deleted.
4. Click **Save** to update the configuration.

How to Configure NAT

You can allocate an external IP address to a robot that resides on another IP network with incompatible addressing using Network Address Translation. The robot will be able to send alarms and QoS messages, but the hub will not be able to communicate back to the robot.

When Network Address Translation (NAT) is in effect between the robot and the hub, the robot must be configured to provide the correct address to the hub. All communication from the hub to the robot will use this address. NAT can be set for the primary and secondary hubs.

Important! When the robot issues a broadcast and a hub answers (roaming) NAT is not possible.

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the NAT section enter the IP addresses for the robot as seen from the primary and secondary hubs.
3. Click **Save** to update the configuration.

How to Configure Static NAT Mappings

You can set up static NAT mappings for each robot behind the NAT device. To configure the static NAT mappings you must use Raw Configure.

Follow these steps:

1. Login to the Admin Console application.
2. Select the **Hubs** button in the upper left corner.
3. In the right pane, double click on the robot where the probe resides.
The right pane displays the robot configuration options. The options include Robot Properties, Probes, Installed Packages, and Environment Variables.
4. Select the **Probes** button in the right pane.
A list of available probes on the robot appears.
5. Click on the green checkmark icon and select **Raw Configure** from the drop down menu.
The raw configuration GUI appears in a separate window.
6. Select **controller** in the left navigation.
7. Click **Add key**.
The Add key dialog box appears.
8. Enter **robotip_alias**, then click **Add**.
9. Select the value field next to the new key and enter the IP address.
10. Click **Apply**.

How to Set controller IP Address

Follow these steps:

1. Select **setup** in the navigation pane.
2. In the IP section update the settings as needed.

Auto detect

Select either:

- **Automatically detect** - The host IP address will be used for the automatically detect setting.
- **Specific Hub Address** - This setting is typically used when a host has more than one network interface. For more than one IP address the addresses must be separated by a comma. IP addresses can contain wildcards.

Note: The **Listen only to first valid addresses from configured IP addresses** option is only available with a specific hub address IP setting. The controller will only listen on a specific IP address on servers with multiple NICs.

IP version support

Select the appropriate IP version you are running.

Local IP validation

This setting only applies if the IP address is not set to localhost. The IP address will be verified against a list of IP addresses that are valid for that server before it is used.

3. Click **Save** to update the configuration.