Document Revision History

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>10/20/2011</td>
<td>Initial version of Nimsoft Server Configuration Guide, containing configuration and usage content moved from the previous Nimsoft Server Installation and User Guide. This guide and Nimsoft Server Installation Guide obsolete the previous Nimsoft Server Installation and User Guide.</td>
</tr>
</tbody>
</table>

Contact Nimsoft

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

At [http://support.nimsoft.com/](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

Copyright © 2012, Nimsoft Corporation

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.
# Contents

## Chapter 1: Nimsoft Server

## Chapter 2: Accessing Nimsoft Server

Introduction .............................................................................................................................. 9
  Modifying the layout of the menu bar .................................................................................. 10

## Chapter 3: Deploy Probes using the Infrastructure Manager

Installing Probes from the Nimsoft Server Archive ................................................................. 15
Downloading Probes from the Internet Archive ..................................................................... 16

## Chapter 4: LDAP Configuration

Configuring your login Hub .................................................................................................... 17
  Connecting Access Control Lists to LDAP users ................................................................. 19
  Verification .......................................................................................................................... 20
Advanced LDAP Configuration ................................................................................................. 21

## Chapter 5: SSL – Encrypting Network Traffic

## Chapter 6: Launching Nimsoft Applications

Launching Infrastructure Manager, Enterprise Console or Service Level Manager .................. 27

## Chapter 7: Accessing Nimsoft Online Support

## Chapter 8: NMS Connect

nws_api ................................................................................................................................. 34
numa_importer ....................................................................................................................... 34
  Probe Configuration ........................................................................................................... 35
Configure Profile .................................................................................................................. 37
  Setup .................................................................................................................................. 37
  QOS ................................................................................................................................. 38
  SLA ................................................................................................................................... 39
  Alarm ............................................................................................................................... 40
Creating User, Account and ACL ............................................................................................. 41
Appendix A: Launching Dynamic Reports 43
Introduction .........................................................................................................................43
The Reports ..........................................................................................................................45
Preparing for Dynamic Reports ..........................................................................................47
   Enabling Dynamic Reports ..............................................................................................48
   Report_engine not installed on the same server as the main hub? ........................................54

Appendix B: Launching Dynamic Dashboards 57
Introduction ............................................................................................................................57
The Dashboards ...................................................................................................................59
Preparing for Dynamic Dashboards ....................................................................................61
Enabling Dynamic Reports ...............................................................................................62
Report_engine not installed on the same server as the main hub? .........................................68
Chapter 1: Nimsoft Server

Nimsoft Server is the central data gathering and storage component of the Unified Monitoring solution. It is composed of the Bus, primary Hub, database (NIS), monitoring infrastructure (Hubs, Robots and Probes) and management applications, including Infrastructure Manager. See the Nimsoft Monitor Installation Guide for instructions covering the download and installation of Nimsoft Server.

Nimsoft Server provides a web page that acts as a portal that you may access from other computers on your network via a web browser.

Using this web page, you may:

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

**Note:** Enterprise Console and SLM have been superseded by the Unified Management Portal (UMP). See the **UMP Installation Guide** for instructions on installing UMP.

**Note:** Additional Nimsoft Server product use information is available in the *Infrastructure Manager* document, available from the Documentation tab at the Nimsoft support site.
Chapter 2: Accessing Nimsoft Server

This section contains the following topics:

Introduction (see page 9)

Introduction

When Nimsoft Server is installed, you can access it by clicking the Nimsoft Server icon created on your desktop. This will launch a web page in your default web browser.

Make a note of the address in the browser’s address field. Use this address <'yourservername':8008> in the address field of any web browser when accessing Nimsoft Server from your other computers.

The tool bar in the upper right corner of the web page contains these selections:

■ 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 Nimsoft Online support. Clicking this button opens the Nimsoft Technical Support site in a separate window.

From the frame in the left part of the window you can choose to install Nimsoft Software on clients.

If nothing happens when left-clicking on a link in the left frame, try these steps:

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.
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 the 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 displays the configuration tool for the probe.
Removing the Application section from the menu:

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

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

3. Select the option again if you want the section to be shown again.
Removing the Installation section from the menu:

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

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

3. Select the option again if you want the section to be shown again.
Removing the Reports and Dashboards sections from the menu:

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

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

3. Select the option again if you want the section to be shown again.
Chapter 3: Deploy Probes using the Infrastructure Manager

A Probe is a small software program that collects availability and performance data and sends the data in the form of messages to the primary Nimsoft Hub. This data is stored in the Nimsoft Information Store (NIS) and made available to display consoles such as UMP and Infrastructure Manager.

When you install Nimsoft Server, a Hub is one of the components included in the installation. The Hub includes a built-in Robot equipped with several Probes. Using Infrastructure Manager, you can view a list of these Probes by clicking on the Robot node in the Hub.

This section contains the following topics:
- Installing Probes from the Nimsoft Server Archive (see page 15)
- Downloading Probes from the Internet Archive (see page 16)

Installing Probes from the Nimsoft Server Archive

Use Infrastructure Manager to install Probes.

To deploy a Probe to a Robot running on any physical or virtual machine, you can simply select and drag the Probe name from the Archive folder in Infrastructure Manager to the Robot node. Or, you can 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. To accomplish this, log into http://support.nimsoft.com (you will have to register to have the needed credentials) and select Archive.

You can download the Probe(s) you need by clicking the Save tool at the far right of each row. The selected Probe is then downloaded to your Nimsoft Server Archive, and you can deploy it to the desired destination using the drag-and-drop procedure described in the preceding section.

To run any Probe on a machine, you must first have a Robot running on that machine. That is, the Probe depends on a Robot to manage its activities.

There are remote Probes (for example, network device monitoring probes) that run on a robot machine, which in turn can monitor remote devices. Once the Probe is deployed to the robot machine, it can be configured according to the specific tasks that the probe can perform.

For example, with the interface traffic probe, you need to type the host names or IP addresses, as well as the SNMP community strings, for the devices you wish 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, also referred to as "agentless monitoring").
Chapter 4: LDAP Configuration

The Nimsoft LDAP solution makes it possible to log on the Nimsoft consoles using LDAP rather than the Nimsoft user login method. When LDAP is the configured method to login, the Nimsoft Hub will check all login requests against the LDAP server before trying the standard Nimsoft login method.

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.

This section contains the following topics:
- Configuring your login Hub (see page 17)
- Advanced LDAP Configuration (see page 21)

### Configuring your login Hub

The Hub must be configured to forward login requests to an LDAP server and to access the container with the user groups in LDAP.

Launch the Hub GUI in Infrastructure Manager by double-clicking its icon, and click the **Settings** button on the **General** tab. A dialog lets you define the LDAP authentication settings.
1. Select the **LDAP Authentication** option to activate the LDAP authentication feature.

2. In the **Server Name** field, enter the IP address or the host name for the LDAP server to which the Hub will point. 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 using the format `CN=yyy,O=xxx`, where `CN` is the user name and `O` is the organization.

6. In the **Group Container (DN)** field, 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 **User Container (DN)** field, 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** (see page 21) 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 an LDAP user logs into a console (for example Infrastructure Manager), the request will be directed to the LDAP server for authentication. The user can be a 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 **OK**.

![Set LDAP Group dialog](image)

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

**Verification**

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

![Login dialog](image)

Verify that you can access the expected contents and have the privileges as described by the ACL with which the LDAP user is associated (see the section on Connecting Access Control Lists to LDAP Users).
Advanced LDAP Configuration

Below you will find three keys that may be added to the /LDAP/server section of 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

You are not required to add this key to use SSL. 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 components use internally. Text in the LDAP library is encoded as UTF-8. Since Nimsoft products do not have true Unicode support, all characters will be 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:


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. For further reference, see: [http://www.gnu.org/software/libiconv/](http://www.gnu.org/software/libiconv/) (not affiliated with Nimsoft)

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

The default value, if none is specified, is as follows:

<table>
<thead>
<tr>
<th>codepage value</th>
<th>OS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28591</td>
<td>WINDOWS</td>
<td>ISO 8859-1 Latin 1; Western European (ISO)</td>
</tr>
<tr>
<td>ISO-8859-1</td>
<td>UNIX</td>
<td>ISO 8859-1 Latin 1; Western European (ISO)</td>
</tr>
</tbody>
</table>
On Windows platforms, it is a numerical value, on Linux; this is a text string which can be passed into the `iconv_open` function.
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.

To configure SSL settings, follow these steps:

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** – Nimsoft encryption only
- **Compatibility Mode** (recommended!) – Mixed SSL/Nimsoft mode. The system checks for SSL compatibility. If there is no SSL compatibility, the system uses Nimsoft encryption.
- **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 Nimsoft secure communication for older components.

**Important:** Using SSL will significantly reduce traffic bandwidth and performance. Not all probes support SSL.

**Note:** If one Hub in a domain is changed to SSL Only mode, all hubs in the same domain in 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, this change will propagate to all Hubs over 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 for which you want to set SSL.
Chapter 6: Launching Nimsoft Applications

Launching Infrastructure Manager, Enterprise Console or Service Level Manager

From the Windows Start menu (Start > Nimsoft Monitor > Nimsoft Monitoring), you can launch any of the Nimsoft applications/consoles:

- Enterprise Console
- Infrastructure Manager
- Service Level Manager:

provided that you selected to install them when you installed Nimsoft Server.

Note: Enterprise Console is a legacy application which has been superseded by Unified Management Portal (UMP). UMP is the recommended and preferred console for displaying dashboards and reports.

Alternatively, from a web browser, you can launch the Nimsoft applications from the Nimsoft Server portal from any computer on your network.

You can 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.

You may need to install a specific ActiveX control. 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.
Chapter 7: 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 browser window.

The site offers the following services:

■ Self-Service Center: Submit, view and track technical support issues online
■ Frequently Asked Questions: 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
■ Downloads: Provides web access to Nimsoft products and documentation
■ Training: Describes Nimsoft University course offerings.
Chapter 8: NMS Connect

The NMS Connect is a package of two probes, with the purpose of loosely synchronizing selected QOS, alarm, and SLA data between two Nimsoft Servers in separate Domains.

The following figure illustrates the two types of Probes that form this solution:

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 at regular, configured intervals and can import selected QoS, SLAs and alarms.

This section contains the following topics:

- nws_api (see page 34)
- numa_importer (see page 34)
- Configure Profile (see page 37)
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, SLA and alarm 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. All the policies applicable to the Account User will be taken into consideration while assigning or closing alarms.
- 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.
- In order to be able to import the i18n data for an i18n enabled alarm, the ‘Activate Support for Internationalization’ option must be checked in the nas probe configuration where it is present under Setup -> General tab.

numa_importer

The `numa_importer` probe is responsible for importing QOS and SLA and alarm 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 and alarm 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.
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Level</td>
<td>Define the level of details to be maintained in log by moving the slider</td>
</tr>
</tbody>
</table>
Proxy Settings

User can configure proxy settings using the Proxy Settings as shown below:

- **Proxy user details**: If checked, enables the proxy settings to be used by the numa_importer probe to connect to nws_api web service.
- **Server name**: Enter name of the proxy server.
- **Proxy user name**: Enter the username to be used for accessing proxy settings.
- **Proxy password**: Enter the password for the proxy user name.
- **Proxy server port**: Enter the port being used by the proxy server.

Profiles

The list displays the profiles configured and it shows the details as:

- **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

This section describes the profile configuration for the numa_importer probe.

Setup

The following parameters are required to configure the profile:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Name of the profile to be used for retrieval.</td>
</tr>
<tr>
<td>Webservice Address</td>
<td>Address of nms with nws_api package installed on wasp and exposed over VPN or static IP address. Note:</td>
</tr>
<tr>
<td>Username</td>
<td>保定文。</td>
</tr>
<tr>
<td>Password</td>
<td>出口。</td>
</tr>
</tbody>
</table>

- Webservice address is either of the form http://domain/nws_api/services/nws_api or http://host:port/nws_api/services/nws_api.
- Example: http://172.18.7.76:8084/nws_api/services/nws_api
- wasp version should be 2.80. numa_importer and nws_api version is 2.0. nws_api fetches alarms from UDM.
Configure Profile

<table>
<thead>
<tr>
<th>Username</th>
<th>The name of the user configured to map with account and having certain ownership at remote hosting of nms nws_api probe. This information is shared with remote host user and the user using importer probe.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>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 cfg file, which is maintained by the probe.</td>
</tr>
<tr>
<td>Test Login</td>
<td>Click to verify the login credential entered.</td>
</tr>
</tbody>
</table>

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.
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.
# Alarm

## Configure Profile

### Alarm

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Alarm Import</td>
<td>When selected this enables alarm import.</td>
</tr>
<tr>
<td>Update Interval</td>
<td>The interval after which the synchronization mechanism will execute in order to fetch latest information since last retrieval.</td>
</tr>
<tr>
<td>Send update to remote server for imported alarm acknowledge</td>
<td>When selected, sends a notification when a remote alarm is closed/acknowledged locally.</td>
</tr>
<tr>
<td>Send update to remote server for imported alarm assignment</td>
<td>When selected, sends a notification when a remote alarm is assigned locally.</td>
</tr>
<tr>
<td>Apply remote assignment</td>
<td>When selected, determines whether remote assignment affects local.</td>
</tr>
<tr>
<td>Override existing Assignment</td>
<td>When selected, lets the user override the local alarm assignment. This field is enabled only when Apply remote assignment option is selected.</td>
</tr>
<tr>
<td>Remote close should close local alarms</td>
<td>When selected, closes imported alarm when it is closed remotely.</td>
</tr>
</tbody>
</table>
Creating User, Account and ACL

**NOTE:** To create User, Account and ACL, please refer *Infrastructure Manager* documents.
Appendix A: Launching Dynamic Reports

Note: Nimsoft Server-based Dynamic Reports and Dynamic Dashboards have been superseded by the reporting and dashboarding features included in the Unified Management Portal (UMP). See the UMP Installation Guide, which you can download from the Documentation tab at Nimsoft support, to install UMP. Then access the UMP Online help for information on setting up reports and dashboards.

This section contains the following topics:

Introduction (see page 43)
The Reports (see page 45)
Preparing for Dynamic Reports (see page 47)

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 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* (see page 47).

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? (see page 54) and Enabling Dynamic Reports (see page 48).
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).
Preparing for Dynamic Reports

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.

![Setup properties]

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.

![Restart probe]

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 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 in the Key name: report_engine_address and the Value: report engine address on the format /<Domain>/<hub>/<robot>/report_engine.
Click **Apply** to activate the new setting and exit the Raw configure dialog.
Appendix B: Launching Dynamic Dashboards

Note: Nimsoft Server-based Dynamic Reports and Dynamic Dashboards have been superseded by the reporting and dashboarding features included in the Unified Management Portal (UMP). See the *UMP Installation Guide*, which you can download from the Documentation tab at [Nimsoft support](http://nimsoft-support.com), to install UMP. Then access the UMP Online help for information on setting up reports and dashboards.

This section contains the following topics:
- **Introduction** (see page 57)
- **The Dashboards** (see page 59)
- **Preparing for Dynamic Dashboards** (see page 61)
- **Enabling Dynamic Reports** (see page 62)
- **Report engine not installed on the same server as the main hub?** (see page 68)

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 **Apply**.
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* (see page 47).

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.
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? (see page 54) and Enabling Dynamic Reports (see page 48).
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.

![Dynamic Reports GUI](image)

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

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

The following dialog appears. Click Yes to finish.

![Restart probe dialog](image)

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 **Apply** to activate the modification. Click **OK** 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.

**New Key**

Enter: key name:

```
report_engine_address
```

Enter value:

```
/Nimbus/XFRune/xaruha/report_engine
```

Fill in the Key name: report_engine_address and the Value: report engine address on the format 
Click **Apply** to activate the new setting and exit the Raw configure dialog.