CA Nimsoft Monitor

Probe Guide for CA ServiceDesk Gateway

casdgtw v2.3 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 252.2277014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.22719 (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 nonDOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.22719(c)(12) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.22714 (June 1987) or DFAR 252.2277015 (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 ThirdParty Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contact CA

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Overview 7

About This Guide 7
Related Documentation 8
Preconfiguration Requirements 8
    Supported Platforms 8

Chapter 2: Configuration Details 9

casdgtw Node 9
    Field Mapping Node 13
Configure a Node 13
Add Field Mapping Details 14
Delete Field Mapping Details 15
Configuring HTTPS CA Service Desk URL 15
Advanced Configuration Settings 15

Chapter 3: Known Issues 17

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
2.4	December 2013	■ Added the **Configuring HTTPS CA Service Desk URL** section. ■ Updated the Offline Management mode details in the **Advanced Configuration** section. ■ Added the **Enhancements** section.
2.3	September 2013	Initial web-based GUI version of this probe. (Previous versions of this probe are configured using Infrastructure Manager).

Chapter 1: Overview

The casdgtw probe is a gateway between the Nimsoft Monitoring Server (NMS) and the CA Service Desk. The probe generates an incident ticket in the CA Service Desk that is based on the NMS alarm. Generating an incident helps the service desk user to take corrective actions for resolving the issue. The incident is generated when an alarm is assigned to the designated CASD user. The probe uses this alarm as a Service Desk Call Request and generates the ticket.

The probe supports the following functionalities:

- Tests the network access to the CA Service Desk (CASD) application.
- Tests the login sessions on the CASD application.
- Create an incident in the CASD application that is based on NMS alarms.
- Updates incident activity logs in the CASD application that are based on the NMS alarm updates.
- Close the incident when the corresponding alarm is acknowledged.
- Acknowledge the alarm when the corresponding incident is closed in the CASD application.

This section contains the following topics:

About This Guide (see page 7)
Related Documentation (see page 8)
Preconfiguration Requirements (see page 8)

About This Guide

This guide is for the CA Nimsoft Monitor Administrator to help understand the configuration of the CA ServiceDesk Gateway probe.

This guide contains the following information:

- An overview of the CA ServiceDesk Gateway probe.
- The related documentation for previous probe versions, release notes, and so on.
- The configuration details of the probe including information for the fields that are required to configure the probe.
- The common procedures that can be used in the probe configuration.
- Field information for the fields, required to configure the probe.

Important! The field description for intuitive terms in the GUI has not been included in the document.

Related Documentation

For related information that can be of interest, see the following material:

Related Documentation

Documentation for other versions of the casdgtw probe

The Release Notes for the casdgtw probe

User documentation for the Admin Console

Monitor Metrics Reference Information for CA Nimsoft Probes (http://docs.nimsoft.com/prodhelp/en_US/Probes/ProbeReference/index.htm)

Preconfiguration Requirements

This section contains the preconfiguration requirements for the Nimsoft CA ServiceDesk Gateway probe.

Supported Platforms

Refer to the Nimsoft Compatibility Support Matrix for the latest information about supported platforms. See also the Support Matrix for Nimsoft Probes for more specific information about the CA ServiceDesk Gateway probe.

Enhancements

The CA ServiceDesk Gateway probe is enhanced for supporting HTTPS (server-client certificate or keystore) based authentication for connecting to the CASD application.

New Features

- New feature 1
- New feature 2

Chapter 2: Configuration Details

The CA ServiceDesk Gateway probe is configured by defining the URL of the CASD application with the user account details for generating incidents by the probe. You can also specify the NMS user to whom the alarm is assigned for creating the incident. The configuration details specify the field mapping details for storing relevant alarm information in the incident.

This section contains the following topics:

casdgtw Node (see page 9)
Configure a Node (see page 13)
Add Field Mapping Details (see page 14)
Delete Field Mapping Details (see page 15)
Configuring HTTPS CA Service Desk URL (see page 15)
Advanced Configuration Settings (see page 15)

casdgtw Node

The casdgtw node contains sections for enabling the communication between the probe and the CASD application.

This section contains configuration details specific to the CA ServiceDesk Gateway probe.

Navigation: casdgtw

Set or modify the following values as required:

casdgtw > Probe Information

This section provides information about the probe name, probe version, start time of the probe, and the probe vendor who created the probe.

casdgtw > Server Configuration

This section lets you configure the URL of the CASD application and user credentials for the authorization purpose.

- Server URL: Defines the WSDL URL of the CA Service Desk application for retrieving the description of the Web Service. This Web Service exposes methods for performing necessary operations on the CA Service Desk application.
- Username: Defines the user name for logging in to the CA Service Desk application.

- Password: Defines the password for logging in to the CA Service Desk application.

  Note: Use the **Test** option from the **Actions** drop-down list for verifying the connectivity between the probe and the CASD application.

casdgtw > General Configuration

This section lets you configure the compatibility and connection settings between the probe and the CASD application.

- Log Level: Sets the level of details to be included in the log file.

  Default: 0 - Fatal

- NAS Address: Defines the address of the local Nimsoft Alarm Server (NAS) in the **/<Domain>/<Hub>/<Robot>/nas** format where the probe is deployed. The address is case-sensitive.

- Service Desk User: Defines the username of the NMS user. Whenever you assign an alarm to the given user, the probe initiates the request to generate a new incident.

- Service Desk Version: Specifies the version of the CA Service Desk application, which the probe is connecting.

  Default: v12.1

- Check Interval (Minutes): Defines the time interval (in minutes) after which the probe checks for closed incidents in the CA Service Desk application for clearing the corresponding alarms. The recommended value is 5 minutes.

  Default: 30

- Date Format: Specifies the **Date and Time** format code for storing the time value. This field ensures that the probe and the CA Service Desk application are using the same Date and Time format.

  Default: MM/dd/yyyy HH:mm:ss

- Timezone: Specifies the time zone code for storing the time value. The time zone must be same as the time zone of the CA Service Desk application. This field ensures that the probe and the CA Service Desk application are using the same time zone.

  Default: Asia/Calcutta

- Incident Id Custom Field: Specify the custom field of the alarm (**custom_1** to **custom_5**) to save the incident id of the corresponding incident.

  Default: custom_1

- Owning System: Specifies the way of updating the incident and alarm status. Select one of the following options:
  - Nimsoft Monitor: Closes the CASD incident, when the alarm is acknowledged.
  - Service Desk: Acknowledges the alarm when the CASD incident is closed.
  - Both: Performs the bidirectional updates.

  Default: Service Desk
- Closed Ticket Status: Specifies the CASD incident status, which is set when the corresponding alarm is acknowledged in the NMS.
- Enable Incident Activity Logging: Updates the activity log (creating, updating, and closing the incident) in the CASD incident that is based on the corresponding alarm in the NMS.

  Default: Not selected

casdgtw > Configuration Item Status

The **Configuration Item Status** section lets you exclude the configuration items status from displaying in a CASD incident. This list of configuration item status represents retired or blocked configuration items. If the CASD incident is having the selected status in the **Configuration Item** list, the respective status is not displayed in the incident.

Note: The list of available Configuration Item Status is populated only after configuring the server details.

casdgtw > Ticket Assignment

This section is used to configure the assignation of the incident to the respective CASD user, when the incident is generated and updated.

- Initial Assignment Group: Defines the CASD group name to which the incident is assigned, when the incident is created. Provide the group name and not the UUID of the group. If the given group name does not exist on CASD or the field is left blank, the incident is assigned to the login user.
- Enable Reassignment: Lets you reassign the incident when the corresponding alarm updates the incident information.
- Enable Severity: Lets you to reassign the incident when the alarm severity is updated in the NMS.
- Alarm Severity: Specifies the alarm severity condition for reassigning the incident.
- Reassignment Group: Defines the CASD group name to which the incident is reassigned.

casdgtw > Edit Alarm Severity

This section is used for mapping the alarm severity with the **Severity**, **Urgency**, or **Priority** fields of the CASD incident. However, you can map only one of these fields at a time. The **Severity**, **Urgency**, or **Priority** fields are also depends on the CASD application version.

- Alarm Severity: Specifies the incident field (Priority, Severity, or Urgency) for mapping with the alarm severity.

  Note: The options available in this field depends on the **Service Desk Version** field of the **General Configuration** section.

- Clear: Specifies the **Priority**, **Severity**, or **Urgency** of the incident when the alarm severity is **Clear**.
- Information: Specifies the **Priority**, **Severity**, or **Urgency** of the incident when the alarm severity is **Information**.
- Warning: Specifies the **Priority**, **Severity**, or **Urgency** of the incident when the alarm severity is **Warning**.
- Minor: Specifies the **Priority**, **Severity**, or **Urgency** of the incident when the alarm severity is **Minor**.
- Major: Specifies the **Priority**, **Severity**, or **Urgency** of the incident when the alarm severity is **Major**.
- Critical: Specifies the **Priority**, **Severity**, or **Urgency** of the incident when the alarm severity is **Critical**.

Field Mapping Node

The **Field Mapping** node lets you map the CA Service Desk fields with one of the following values:

- NMS Alarm Field: Maps value of the corresponding field of the NMS alarm.
- Custom Value: Maps a custom Value, which is a combination of one or more variables representing the NMS Alarm fields. For example, the **Description** field of the CASD is mapped with **${Message} because the current value ${value} is exceeding the threshold value ${threshold}**.
- Default Value: Maps a fixed value.

Navigation: casdgtw > Field Mapping

Set or modify the following values that are based on your requirement:

Field Mapping > Field Mapping

This section contains a **Mapping** table for displaying the list of the mapped fields and its associated value. The CA ServiceDesk Gateway lets you to map fields for three different scenarios:

- On Alarm Create
- On Alarm Update
- On Alarm Close

Use the **Delete** button of the mapping table for removing the mapping details.

Note: Use the **Options** icon next to the **Field Mapping** node for adding the mapping details.

Configure a Node

This procedure provides the information to configure a particular section within a node.

Each section within the node lets you configure the properties of the probe. These properties are used for generating incident in the CASD application that is based on the NMS alarm.

Follow these steps:

1. Navigate to the section within a node that you want to configure.
2. Update the field information and click **Save**.

   The specified section of the probe is configured.

The probe is now ready for generating incidents in the CASD application.

Add Field Mapping Details

The field mapping details are added for saving necessary information from the NMS alarm in the incident. This information helps the CA service desk user for resolving the incident.

Follow these steps:

Click the Options icon next to the Field Mapping node.

Select Field Mapping.

Specify the Service Desk Field in the Field Mapping dialog.

Note: The service desk field list appears only if valid credentials are provided in the Server Configuration section of the nsdgtw node.

Specify Alarm Field or define a Default Value of the selected Service Desk Field. for the following three scenarios:

- Alarm Create
- Alarm Update
- Alarm Close

Click Submit.

The mapping details are saved and displayed in the Mapping table of the Field Mapping node.

Note: You can map a field (an Alarm field or a Service Desk field) again for updating the field mapping details.

Delete Field Mapping Details

The field mapping details are removed or deleted when there is no need of displaying certain information in the incident.

Follow these steps:

Click the Field Mapping node.

Select the appropriate row in the Mapping table of the Field Mapping section.

Click the Delete button of the Mapping table.

Click Save.

The selected field mapping detail is removed.

Configuring HTTPS CA Service Desk URL

The CA ServiceDesk Gateway probe is enhanced for supporting HTTPS (server-client certificate or keystore) based authentication for connecting to the CASD application. The probe requires a client-side certificate or a keystore in JKS format, which is parsable by the keytool utility of the JDK.

Follow these steps:

1. Copy the client-side certificate to host system, where the probe is installed.

   Note: Recommendation is to copy the client-side certificate in the probe installation directory.
2. Use the **Raw Configure** option and navigate to the **Setup** section.
3. Define the path of certificate in the **certificatePath** key.

   Note: The probe supports only absolute path including the certificate file name too.
4. Click **OK** to save the configuration.
5. Restart the probe for applying the configuration changes.

You can now configure the HTTPS-based URL in the **Server Name** field of the probe GUI.

Advanced Configuration Settings

The advanced configuration setting enables the **Offline Management** mode of the CA ServiceDesk Gateway probe. The Offline Management mode lets you save alarm details that are assigned to the NMS user while the CA Service Desk server is down. Therefore, no incident is generated for the corresponding alarm.

The CA ServiceDesk Gateway probe pings the CA Service Desk server at regular intervals and receives an alert when the server is down. When the CA Service Desk server is up again, the probe restarts. The **Offline Management** mode checks for the alarms that are assigned to the NMS user in NAS when the server is down. Then the probe initiates a request for generating incidents for those alarms.

Follow these steps:

1. Open the raw configuration GUI of the probe.
2. Go to the **disable_offline_management** key under the setup section.
3. Edit key value as follows:
   - 1: Set the key value to 1 to turn off the Offline Management mode. 1 is the default value.
   - 0: Set the key value to 0 to turn on the Offline Management mode.
4. Click **Apply**.
5. Close the raw configuration GUI.
6. Restart the probe for applying the changes.

   The **Offline Management** mode is configured.

You are also required to configure the **java_mem_max** key under the **startup > opt** section when the probe is handling more than 12500 alarms. Set the key value as **-Xmx128m** for 12500 alarms, **-Xmx256m** for 25000 alarms, and so on.

Chapter 3: Known Issues

The **Edit Alarm Severity** section of the casdgtw node saves the mapping details to the configuration file of the probe. The probe reads the mapping details but does not display details on the probe GUI.