

# CA Nimsoft Monitor

## Probe Guide for CA ServiceDesk Gateway

casdgtw v2.4 series



## Copyright Notice

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

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

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

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

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

The manufacturer of this System is CA.

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

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Legal information on third-party and public domain software used in this product is documented in the *Third-Party Licenses and Terms of Use* ([http://docs.nimsoft.com/prodhelp/en\\_US/Library/Legal.html](http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.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 product documentation to [nimsoft.techpubs@ca.com](mailto:nimsoft.techpubs@ca.com).

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



# Contents

---

<b>Chapter 1: Overview</b>	<b>7</b>
About This Guide .....	7
Related Documentation .....	8
Preconfiguration Requirements .....	8
Supported Platforms .....	8
Software Requirements .....	8
<b>Chapter 2: Configuration Details</b>	<b>9</b>
casdgtw Node.....	9
Field Mapping Node .....	13
Configure a Node .....	13
Add Field Mapping Details .....	14
Delete Field Mapping Details .....	14
Advanced Configuration Settings .....	15
Enable Offline Management .....	15
Configure HTTPS CA Service Desk URL .....	16
Configure the subscribe_alarm_closure Key .....	16
Configure the subscribe_alarm_updates Key .....	17
<b>Chapter 3: casdgtw Metrics</b>	<b>19</b>
<b>Chapter 4: Known Issues</b>	<b>21</b>

---

## Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
2.4	October 2014	<ul style="list-style-type: none"><li>■ Updated <b>casdgtw Overview, Preconfiguration Requirements, Advanced Configuration Settings</b>, and <b>Field Mapping Node</b> topics.</li><li>■ Added <b>Software Requirements, Configure the subscribe_alarm_closure Key</b>, and <b>Configure the subscribe_alarm_updates key</b> topics.</li></ul>
2.4	December 2013	<ul style="list-style-type: none"><li>■ Added the <b>Configuring HTTPS CA Service Desk URL</b> section.</li><li>■ Updated the Offline Management mode details in the <b>Advanced Configuration</b> section.</li><li>■ Added the <b>Enhancements</b> section.</li></ul>
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 and provides the following information:

- Overview of the CA ServiceDesk Gateway probe and related documentation for previous probe versions.
- Configuration details of the probe.
- Field information and common procedures for configuring the probe.

**Important!** Description for the intuitive GUI fields is not 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 Unified Infrastructure Management Probes*

([http://docs.nimsoft.com/prodhelp/en\\_US/Probes/ProbeReference/index.htm](http://docs.nimsoft.com/prodhelp/en_US/Probes/ProbeReference/index.htm))

## Preconfiguration Requirements

The casdgtw probe has the following preconfiguration requirements:

- User account of the CA Service Desk application.
- User account of NMS.

## 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.

## Software Requirements

The casdgtw probe requires the following software environment:

- Nimsoft Monitor Server 6.5 to 7.6 and CA Unified Infrastructure Management 8.0 or later.
- Robot 6.5 or later.
- JRE 1.6 or later.
- CA Service Desk server.

# 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 14)

[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, and the probe vendor.

### 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. For example, `http://<IP/Instance Name>/axis/services/USD_R11_Webservice?WSDL`
- **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: specifies 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 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 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:**

1. Click the **Options** icon next to the **Field Mapping** node.
2. Select **Field Mapping**.
3. 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 **casdgtw** node.

4. 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
5. 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:**

1. Click the **Field Mapping** node.
2. Select the appropriate row in the **Mapping** table of the **Field Mapping** section.
3. Click the **Delete** button of the **Mapping** table.
4. Click **Save**.

The selected field mapping detail is removed.

## Advanced Configuration Settings

The advanced configuration settings let you configure the probe using the **Raw Configure** option, which is not possible through standard probe GUI.

### Enable Offline Management

The Offline Management mode lets you save alarm details that are assigned to the NMS user while the CASD server is down. The CA Service Desk Gateway probe pings the CASD server at regular intervals and receives an alert when the server is down. The probe restarts when the CASD server is up again.

The Offline Management mode checks for the alarms that are assigned to the NMS user in NAS when the server is down. The probe then initiates a request for generating incidents for those alarms.

#### Follow these steps:

1. Open the **Raw Configure** GUI of the probe and navigate to the **Setup** section.
2. Go to the **disable\_offline\_management** key.
3. Edit key value as described:
  - 1: (Default) Set the key value to 1 to turn off the Offline Management mode.
  - 0: Set the key value to 0 to turn on the Offline Management mode.
4. Click **Apply** to save the configuration.
5. Restart the probe for applying the changes.

The Offline Management mode is enabled.

**Note:** If the probe is handling more than 12500 alarms, update the value of the **java\_mem\_max** key under the **Startup > Opt** section. Set the key value as **-Xmx128m** for 12500 alarms, **-Xmx256m** for 25000 alarms, and so on.

## Configure HTTPS CA Service Desk URL

The CA Service Desk Gateway probe supports the HTTPS (server-client certificate or keystore) based authentication for connecting to the CASD application. You can use the HTTPS-based URL in the **Server Name** field of the probe GUI. The probe requires a client-side certificate or a keystore in JKS format parsable by the keytool utility of the JDK.

**Follow these steps:**

1. Copy the client-side certificate to host system.  
**Note:** 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 certificate path in the **certificatePath** key.  
**Note:** The probe supports only absolute path including the certificate file name.
4. Click **OK** to save the configuration.
5. Restart the probe for applying the configuration changes.

The HTTPS CA Service Desk URL is configured.

## Configure the subscribe\_alarm\_closure Key

The **subscribe\_alarm\_closure** key is configured to update the incident status to **Resolved** or **Closed**, when the corresponding alarm is acknowledged.

**Follow these steps:**

1. Use the **Raw Configure** option and navigate to the **Setup** section
2. Go to the **subscribe\_alarm\_closure** key.
3. Edit key value as follows:
  - 0: the probe does not update the incident status. 0 is the default value.
  - 1: the probe updates the incident status.
4. Click **Apply** to save settings.
5. Restart the probe for applying the changes.

The subscribe\_alarm\_closure key is configured.

## Configure the `subscribe_alarm_updates` Key

The `subscribe_alarm_updates` key is configured to receive alarm updates in the CASD server.

**Follow these steps:**

1. Use the **Raw Configure** option and navigate to the **Setup** section.
2. Go to the `subscribe_alarm_updates` key.
3. Edit key value as follows:
  - 0: the probe does not receive alarm updates. 0 is the default value.
  - 1: the probe updates the alarm.
4. Click **Apply** to save settings.
5. Restart the probe for applying the changes.

The `subscribe_alarm_updates` key is configured.



# Chapter 3: casdgtw Metrics

---

The casdgtw probe does not generate any QoS. Therefore, there are no probe checkpoint metrics to be configured for this probe.



# Chapter 4: 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.