Oracle® Contact Center Anywhere SNMP Agent Configuration Guide

Version 8.1.2

June 2008

ORACLE®

Contents

Index

1 What's New in This Release

What's New in Oracle Contact Center Anywhere SNMP Agent Configuration Guide, Version 8.1.2

Table 1 lists changes described in this version of the documentation to support Release 8.1.2 of the software.

Table 1. What's New in Oracle Contact Center Anywhere SNMP Agent Configuration Guide, Version 8.1.2

Topic	Description
Installing Files and Setting Environment Variables on page 13	Changed the path of the bin directory to: `c:\Ccanywhere\bin`
Installing and Configuring the Windows 2000 SNMP Service on page 14	Changed the taw.mib reference to cca.mib.
Process of Installing and Configuring the SNMP Service for Linux on page 18	This topic describes how to install and configure SNMP for Linux.
About SNMP Agent Traps on page 8	Modified table topic. Re-arranged trap conditions as pairs. An exception goes with a clearing message.

2 Overview of SNMP Agent

This chapter provides overview information about Oracle Contact Center Anywhere's Simple Network Management Protocol (SNMP). It includes the following topics:

- About Simple Network Management Protocol
- About SNMP Agent Traps
- SNMP Support

About Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP allows network administrators to manage network performance, find and solve network problems, and plan for network growth.

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to the NMS using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, and printers.

An agent is a Network Management Software (NMS) module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

NMS executes the applications that monitor and control managed devices. The NMS also provide the bulk of the processing and memory resources that are required for network management. One or more NMS components must exist on any managed network. As seen in Figure 1, these components must be configured so that they communicate with each other.

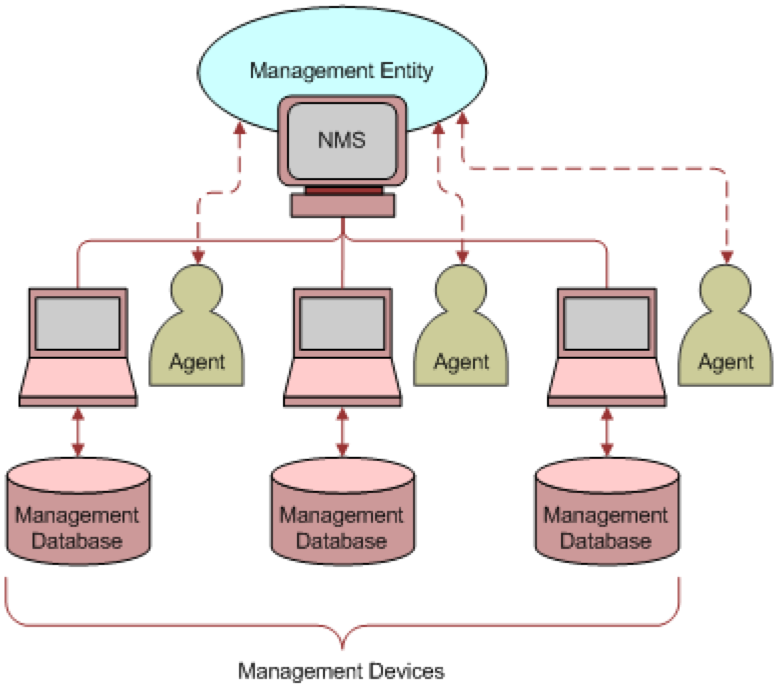

Figure 1. Simple Network Management Protocol

About SNMP Agent Traps

The Oracle Contact Center Anywhere SNMP Agent provides several SNMP traps that are used to immediately notify users if problems with the system occur.

When the SNMP Agent detects a trap condition, a notification of the trap condition is sent to the SNMP Service by the SNMP Protocol. Then, the SNMP Service delivers the notification to the MIB Browser for display to the individual responsible for SNMP Management of Oracle Contact Center Anywhere.

Table 2 describes each of the agent traps. These traps include the resource identifier in the Contact Center Anywhere trap information. For more information, see Contact Center Anywhere Trap Detail on page 25.

Table 2. SNMP Agent Traps

Trap Number	Trap Name	Trap Description
1	snmpAgentShutdown	The SNMP Agent is shutting down.
1001	snmpAgentRunning	SNMP Agent is up and running.
2	licenseFailure	The License Server cannot read the dongle.
1002	licenseSuccess	License Server is able to read the dongle.
3	systemOverflow	A system licensing overflow occurred.

Table 2. SNMP Agent Traps

Trap Number	Trap Name	Trap Description
1003	systemLicenseOK	A system overflow condition has been corrected.
4	companyOverflow	A company licensing overflow occurred.
1004	companyLicenseOK	A company licensing overflow condition has been corrected.
5	companyDeleted	The company has been deleted.
6	resourceCrashed	A resource has failed.
7	disconnectedFromTheBus	The SNMP Agent is disconnected from the local TCPIPBUS and cannot monitor the system.
1007	snmpConnectedToTheBus	SNMP Agent is connected to local TCP/IP bus and can monitor the system.
8	resourceStopped	A resource has stopped
1008	resourceStarted	A resource has started.
9	resourceIsNotResponding	A resource is not responding.
1009	resourceIsResponding	A resource is responding.
10	resourceIsSlowingDown	A resource is slowing down.
1010	resourceIsCatchingUp	A resource is catching up.
11	noLicenseConnected	The License Server is not connected to the system and has begun a 4 hour period before shutting down the ACD and Predictive Dialer Servers.
1011	licenseConnected	The license is connected.
12	disconnectedFromRemoteBus	The SNMP Agent is disconnected from remote TCPIPBUS.
1012	connectedToRemoteBus	The SNMP Agent is connected to the remote TCP/IP bus.
13	busLostConnection	The TCP/IP bus has lost its connection to another TCP/IP bus.
1013	busEstablishedConnection	The TCP/IP bus has established a connection to another TCP/IP bus.
14	statsServerLostConnection	The Stats Server has lost a database connection.
1014	statsServerRegainedConnection	The Stats Server has regained a database connection.

Table 2. SNMP Agent Traps

Trap Number	Trap Name	Trap Description
15	statsServerQueueOverflow	The Stats Server is experiencing too many queries within a short period of time. The queries are queued in a local file.
1015	statsServerNoMoreQueueOverflow	The Stats Server is now able to handle all queries, and the file of queued queries has been emptied.
16	statsServerErrorWriting	The Stats Server received an error while writing to a database connection.
1016	statsServerNoErrorWriting	Stats Server is now able to write to a database connection.
17	noServiceAvailableForDNIS	Service is not available for DNIS.
1017	serviceAvailableForDNIS	Service is available for the DNIS.
18	noOutboundChannelsAvailable	There are no available outbound channels.
1018	outboundChannelsAvailable	Outbound channels are now available.
19	channelsBlocked	Outbound channels are blocked.
1019	channelsUnblocked	Outbound channels are unblocked.
20	poorRTPquality	Real Time Transport Protocol (RTP) quality on the network is poor.
1020	acceptableRTPquality	RTP quality on the network is acceptable.
21	sipH323OutOfResources	The total number of calls sent to the CallCenter resource for SIP/H323 is larger than number of calls can be accepted.
1021	sipH323NotOutOfResources	SIP and H323 have sufficient resources to handle calls.
22	mp3ConverterFailed	The MP3 converter failed to convert files.
1022	mp3ConverterSuccess	The MP3 converter can convert files.
23	lostMailServerConnection	Email Distributor has lost its mail server connection.
1023	regainedMailServerConnection	Email Distributor has regained its mail server connection.
24	lostFtpConnection	Host Manager has lost a FTP connection
1024	regainedFtpConnection	Host Manager has regained an FTP connection.

Table 2. SNMP Agent Traps

Trap Number	Trap Name	Trap Description
25	cannotFtpFiles	Host Manager cannot send the files to the server using FTP
1025	canFtpFiles	Host Manager can send files to the server using FTP.
26	unifiedLostMailServerConnection	The Unified Server has lost a mail server connection.
1026	unifiedRegainedMailServerConnection	Unified Server has regained a mail server connection.
27	maliciousCallTrace	Administrator received a malicious call trace. The trace is included with the SNMP trap message, which contains the CID (phone number) of the caller so that the offending caller can be tracked.

SNMP Support

The SNMP trap mechanism is implemented in all back-end servers. Some traps originate from the servers themselves (for example, the Predictive Server, the Email Distributor, and so on), and some originate from the SNMP Agent.

Each time a predefined fault occurs (see possible traps defined in the taw.mib), a trap message is sent to the SNMP Agent, and then the SNMP Agent sends an SNMP trap on the network.

Stat Server and Trap Event Logging

Active (listening) SNMP monitors catch the trap, display it, and may also send an alarm (for example, an email or a page). At the same time, the server with the fault condition sends a request to the Stats Server to enter a record in the database table TRAPSHISTORY to keep track of system problems. The Stats Server inserts a record of the trap event (timestamp, trapId, resourceId, CompanyId and description).

To allow the SNMP Agent (a shared resource) to talk to the Stats Server (a dedicated resource), the Stats Server of companyId=1 (ASP company) was designated as the resource responsible for inserting trap events in the TRAPSHISTORY table. Therefore the Stats Server of the companyId=1 must be running so that trap events can be logged in the database.

Traps and Faults at the Local Bus

If the fault condition is at the local bus, SNMP traps that originate from the server do not reach the SNMP Agent and are not logged in the database table TABLESHISTORY. But, if the trap event is generated by the SNMP Agent attached to the local bus, a SNMP trap is sent on the network for SNMP Monitors. There is no logging of that event in the TRAPSHISTORY because the SNMP Agent would need to access the local bus.

Configuration of the Resource Ping Process

Every few seconds, the SNMP Agent pings all resources and verifies whether or not each resource is responding (trap1009 or trap9), if the resource is slowing down (trap10), or if the resource is catching up (trap1010).

Some ping parameters are configurable. In the Database table, SYSTEMCONFIGURATION, you can change the following parameters:

- pinginterval

  This parameter allows you to specify the amount of time (in seconds) the SNMP Agent waits before it sends another ping request to all of its resources.

- maxpingsmissed

  This parameter allows you to specify the maximum number of pings that can be missed by a resource before the SNMPAgent sends a RESOURCE_NOT_RESPONDING SNMP trap (trapId=9).

- maxpingtimeout

  This parameter allows you to specify the time (in milliseconds) after which a ping response is considered late, and causes the SNMPAgent to send a RESOURCE_SLOWING_DOWN SNMP trap (trapId=10).

3 Configuring SNMP

This chapter provides SNMP configuration instructions for Microsoft Windows™, Sun Solaris™ and Linux. It includes the following topics:

- Process of Configuring SNMP for MS Windows 2000, 2003
- Process of Configuring SNMP for Sun Solaris
- Process of Installing and Configuring the SNMP Service for Linux
- Configuring an SNMP Agent for Dual Database Capability

Process of Configuring SNMP for MS Windows 2000, 2003

This topic details the tasks often performed by system administrators when configuring SNMP for Microsoft Windows 2000 and 2003. Your company may follow a different process according to its business requirements.

The following list shows tasks administrators typically perform to configure SNMP for Microsoft Windows 2000 and 2003. These tasks are typically performed in the following order:

1. Installing Files and Setting Environment Variables
2. Installing and Configuring the Windows 2000 SNMP Service
3. Adding IP Addresses for MIB Browser Machines
4. Editing the Registry
5. Adding the SNMP Agent Resource in Network Manager

Installing Files and Setting Environment Variables

Three files must be copied to designated CCA directories to fully install the SNMP Agent.

To install files and set environment variables

1. Add the Contact Center Anywhere bin directory to the System Path.

   The bin directory typically resides in the following location:

   ```
   C:\ccanywhere\bin
   ```

2 Copy three files from the bin directory to the target directories.

The following table describes the files and the target directory.

File	Target Directory
tawsnmp.dll	Contact Center Anywhere Home/ bin
taw_snmp_agent.cfg	%SystemRoot%/system32
taw.mib	ContactCenterAnywhere Home/ lib

3 Create or edit the taw_snmp_agent.cfg file to specify the following parameters:

```
ServerID: 14
DatabaseAlias: cc811
DatabaseUser: cc811
DatabasePassword: 6df2d81ab729858f
<empty line>
```

Installing and Configuring the Windows 2000 SNMP Service

The Windows 2000 SNMP Service must be installed and running on your system. Complete the steps in the following procedures to install and configure the Windows SNMP Service.

To install the Windows 2000 SNMP Service

- Using the Windows 2000 Server installation CD, run the installation program for the Windows 2000 SNMP Service.

Adding IP Addresses for MIB Browser Machines

From the SNMP service, add the IP address of each machine that must have the MIB Browsers installed.

To add IP addresses for browser machines

1 Edit the SNMP Service from the list of Windows services.

2 Go to the Traps tab.

3 Enter the community name (for example, Public) that is used to catch SNMP traps.

4 Select Add, and then enter the Host name or the IP Address where the MIB browser resides.

Repeat this step for each MIB browser machine.

5 Save the changes.

6 Start the SNMP Service and the SNMP Trap Service.

Editing the Registry

You must edit the registry, and then add entries to the CCA key and the SNMP key, and add a new string value. ***To edit the registry***

1 Click Start, and then Run, and in the Open field type: `Regedit`

   a Add an Entry to the Contact Center Anywhere key:

   - To add a new key to the system registry for the Contact Center Anywhere SNMP Service, the registry path is My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Telephony@Work. Add a new key, and then name the key SNMP.
   - Add String Value to the SNMP key, and then label the pathname.
   - Enter Value Data for the pathname equal to the tawsnmp.dll file location. For example: `C:\ccanywhere\bin\tawsnmp.dll`

   b Add an entry to the SNMP Service Key:

   To add a new extension Agent to handle SNMP Services the ContactCenterAnywhere SNMP service registry path is: MyComputer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents

   c Add a new string value:

   - Right-click and select New, and then String Value.
   - Use n+1 for the name (n represents the value of the last extension agent added).
   - Modify New String n+1.
   - Enter Value Data equal to the Registry path where the SNMP pathname is. This value should be set to: SOFTWARE\Telephony@Work\SNMP.

2 Save the changes and close RegEdit.

Adding the SNMP Agent Resource in Network Manager

You must add the SNMP Agent resource to the Network Manager. Use the same procedure for adding any other shared resources. See the topic on adding SNMP agent resources in *Oracle Contact Center Anywhere Network Manager Guide*.

When the SNMP Service is started, the SNMP Agent in the Network Manager is automatically started and the indicator turns green.

CAUTION: The Network Manager can only stop or start CCA SNMP Agent resource. SNMP service is a service of operating system.

Process of Configuring SNMP for Sun Solaris

This topic details the tasks often performed by system administrators when configuring SNMP for Sun Solaris. Your company may follow a different process according to its business requirements.

The following list shows tasks administrators typically perform to configure SNMP for Sun Solaris. These tasks are typically performed in the following order:

1. Installing Sun Solstice Enterprise Agent
2. Configuring the SNMP Daemon for Solaris
3. Configuring the SNMP Agent for Solaris
4. Starting the SNMP Agent from the Network Manager Application

Installing Sun Solstice Enterprise Agent

Solstice Enterprise Agent (SEA) must be installed on the machine running the SNMPAgent.

For more information on Solstice Enterprise Agent technology and software, see http://www.sun.com/software/entagents/.

Configuring the SNMP Daemon for Solaris

Complete the steps in the following procedure to configure the SNMP daemon.

To configure the SNMP daemon for Solaris

1. Stop the SEA snmpdx daemon (if it is currently running).
2. Enter the following command in the console:
3. `$> /etc/rc3.d/S76snmpdx stop`Add a single entry in enterprises.oid:

   Path: `/etc/snmp/conf/enterprises.oid`

   Value: `"telephonyatwork" "1.3.6.1.4.1.10477"`
4. Edit the /etc/snmp/conf/snmpdx.acl file:

   Add the following block under trap={...}

   ```
   trap = {

           ***leave the default value here***
              {
                  trap-community = SNMP-trap
                  hosts = hostname1, hostname2
                  {
                       enterprise = "telephonyatwork"
   ```

```
                  trap-num = 1-27,1001-1026
              }
          }
       }
```

NOTE: Hostname1, hostname2: Host name or IP Address where the MIB browser resides.

5 Edit the block under acl={...} so that public and private communities are allowed read-write access (Get, Get-Next, and Set) from any SNMP Manager.

```
acl = {
       {
       communities = public, private
       access      = read-write
       managers    = *
       }
     }
```

Configuring the SNMP Agent for Solaris

Complete the steps in the following procedure to configure the SNMP Agent for Solaris.

To configure the SNMP Agent

1 Copy the SNMPAgent.reg file into /etc/snmp/conf.

The SNMPAgent.reg file should include content similar to the following:

```
macros = {

             telephonyatwork =       enterprise.10477
          }

agents ={

          {
             name =     "SNMPAgent"
             subtrees = { telephonyatwork }
             timeout  = 4000000
             watch-dog-time = 2
          }
       }
```

2 Copy the SNMPAgent.acl file into /etc/snmp/conf.

The file is similar to the following:

```
acl = {
          {
               communities = public
               access      = read-only
               managers    = localhost
          }
       }
```

```
trap = {
         {
           trap-community = SNMP-trap
           hosts          = localhost
             {
               enterprise = "telephonyatwork"
               trap-num   = 1-27,1001-1026
             }
         }
     }
```

3. Start the SEA snmpdx daemon.

   For example, enter: `$> /etc/rc3.d/S76snmpdx start`

Starting the SNMP Agent from the Network Manager Application

Complete the steps in the following procedure to start the SNMP Agent.

To start SNMP Agent from Network Manager

1. Select SNMP resource in Network Manager.
2. Click Start.

Process of Installing and Configuring the SNMP Service for Linux

Installing and configuring the SNMP Service for Linux requires the following steps:

- Installing the Net-SNMP System
- Setting the Trap Destination
- Installing the SNMP Agent
- Running and Configuring the Net-SNMP Master Agent
- Verifying SNMP Traps on the Host Machine
- Starting the SNMP Agent from Network Manager

Installing the Net-SNMP System

Complete the steps in the following procedure to install the net-SNMP system.

To install the net-SNMP system

1 Log in as the root.

2 Copy net-snmp.tar to /usr.

3 Untar it by the command:

```
tar –xvf net-snmp.tar
```

Setting the Trap Destination

Complete the steps in the following procedure to set the trap destination. You can add as many trap receivers as are needed. The destination is the IP address of the trap receiver, or the trap receiver's host name if it was configured correctly.

To set the trap destination

1 Open the configuration file snmpd.conf.

The file is located in /etc/snmp/snmpd.conf

2 Add the following line to the configuration file:

```
“trapsink  destination public”
```

Installing the SNMP Agent

Complete the steps in the following procedure to install the SNMP agent.

To install the SNMP agent

1 Log in as the application user.

2 Copy the file SNMPAgent to the application directory.

Running and Configuring the Net-SNMP Master Agent

Complete the steps in the following procedures to run the Net-DSNMP master agent, and then configure Linux to automatically start the master agent.

To run the master agent

1 Log in as the root.

2 Type the command:

```
snmpd
```

To configure Linux to automatically start this master agent

1. Create /etc/rc3.d/S100snmpd
2. Enter the following line in the file, and then save the file.

   ```
   /usr/bin/snmpd
   ```

3. Change the /var/net-snmp mode:

   ```
   chmod 777 S100snmpd
   ```

   ```
   chmod –R 777 /var/net-snmp
   ```

Verifying SNMP Traps on the Host Machine

Complete the steps in the following procedure to verify that the SNMP traps are running on the host machine.

To verify the SNMP traps

1. Log in as root.

   Type the following command in the Linux console: `snmptrapd -f -Lod`

Starting the SNMP Agent from Network Manager

Complete the steps in the following procedure to start the SNMP agent from the Network Manager application.

To start SNMP Agent from Network Manager

1. Select SNMP resource in Network Manager.
2. Click Start.

Configuring an SNMP Agent for Dual Database Capability

On Win32, you can configure the SNMP Agent to use dual-database capability by adding an extra Database Alias, User name and Password to the taw_snmp_agent.cfg configuration file.

For example, if taw_snmp_agent.cfg contains the following lines:

```
ServerID:92
DatabaseAlias:ecc82
DatabaseUser:ecc82
DatabasePassword:20212d2070dac2c1
DatabaseAlias:ecc81
```

```
DatabaseUser:ecc81
DatabasePassword:20212d2070dac2c0
<empty line>
```

Then the SNMP Agent uses a dual-database context:

```
context1: alias=ecc82, user=ecc72,password=20212d2070dac2c1

context2: alias=ecc81, user=ecc71,password=20212d2070dac2c0
```

Additional Information

The following list provides additional information you will need to know when configuring the SNMP Agent for dual-database capability:

- The ServerID is the Resource ID assigned to the SNMP Agent in the Network Manager.
- The Database Alias and Database User are the same as the Database Alias and Database User used for the Network Manager.
- The DatabasePassword must be the encrypted password and can be retrieved from the TCPIPbus log after starting a resource. For example:

  ```
  Start resource [C:\ccanywhere/bin/ACDServer -acc7008 -ucc7008 -p0baf45bd6d1695d1 -
  sC:\ccanywhere -i86.
  ```

- The Management Information Base Definition (taw.mib) is a text file that defines the objects and parameters. These are the objects monitored and managed by the SNMP Agent.
- A copy of the taw.mib file must reside on any host running a MIB Browser to manage Oracle Contact Center Anywhere using SNMP. The MIB Browser reads the taw.mib file to map to the objects managed by the SNMP Agent.

4 Configuring Network Management Software

This chapter describes how to configure Network Management Software (NMS) using OpManager. It includes the following topics:

Configuring NMS Using OpManager

There are a number of software applications that can be used as SNMP network monitors. These include MIB Browser, MG-SOFT MIB Browser, and AdventNet's ManageEngine™ OpManager. The instructions that follow assume you are using AdventNet OpManager.

Adding Devices Using OpManager

Complete the steps in the following procedure to add devices to OpManager.

To add devices

1. In OpManager, click the Admin tab.
2. Click the Add Device link.
3. Enter the device information.
   - Name or IP Address of the Host
   - Net mask
   - SNMP Port: keep the default value 161
   - Community string: public as configured in SNMP Manager
4. Click the Add Device button.

Loading Traps from MIB

Some Trap Processors are defined by default in OpManager. For some MIBs, the processor is not configured; however, OpManager provides an option in the Web client to load these traps and add a processor.

To load traps

1 Copy the taw.mib file into the folder:

`C:/Program Files/…/OpManager/mibs/.`

2 From OpManager, click the Admin tab and select SNMP Trap Processors.

All of the configured processors are listed.

3 From Actions, select Load Traps from MIB.

4 From the list of MIBs, select the MIB from which you plan to load the trap variable.

The traps in the MIB are listed.

5 Select the required MIB, and click Add Trap Processor(s).

A processor for the selected trap is added, and is listed under the SNMP Trap Processors.

About MIB Browser and SNMP MIB Objects

A number of objects are defined in the taw.mib file. The SNMP Agent provides these values to the individual running the MIB browser. Table 3 describes the objects.

Table 3. SNMP MIB Objects Defined in taw.mib

Object	Description
releaseVersion	Release version of Oracle Contact Center Anywhere
aboutString	General information about Oracle Contact Center Anywhere
numberofInteractions	Total number of interactions in the system
companyTable	Includes all instances of companyEntry defined in this instance of Oracle Contact Center Anywhere
companyEntry	The company entry, one for each Company Definition in Oracle Contact Center Anywhere
companyIndex	Sequential number starting with 1 used to order multiple companies
companyId	Oracle Contact Center Anywhere Company ID
companyAlias	Company alias
CompanyInteractions	Number of interactions currently in the company
companyAgentLoggedIn	Number of agents currently logged in for the company

Table 3. SNMP MIB Objects Defined in taw.mib

Object	Description
companyACDCall	Number of ACD Calls currently being handled by the company
companyACDChat	Number of ACD Chats currently being handled by the company
companyACDCallback	Number of ACD Callbacks currently being handled by the company
companyACDWebCallBack	Number of ACD Web Callbacks currently being handled by the company
companyACDPredictive	Number of Predictive Calls currently being handled by the company
companyACDEmail	Number of ACD Emails currently being handled by the company
companyACDFax	Number of ACD Faxes currently being handled by the company
companyACDVoiceMail	Number of ACD Voicemails currently being handled by the company

Viewing Object Properties

Complete the steps in the following procedure to review object properties.

To view the objects

1. From the OpManager Admin tab, choose MIB Browser.
2. Click Load MIB.
3. Choose taw.mib in the list, and then click Load.
4. Select the TELEPHONYATWORK-MIB that appears in the Loaded MIB List.
5. A tree view appears.Select an object, and then click GET to see more information about the object.

Contact Center Anywhere Trap Detail

After uploading taw.mib to OpManager, you can view all traps sent from the Oracle Contact Center Anywhere servers' Alarm tab. These traps are defined in the TRAPDEINITION table. When a trap is sent, each server may add specific detail for a trap, which is appended to the trap description (static). The resourceId is appended to both the trap definition and the detail. If there is no detail, then the resourceId is appended to the trap definition.

Detail for SNMP traps on SNMP Monitors is provided in the following format:

```
<description TRAPSDEFINITION for trapX> : <detail> [resourceId=YY]
```

For example, if a trap 9 was sent from resource 55, the SNMP Monitor would receive the following trap description:

```
Resource is not responding: [resourceId=55]
```

Configuring Gateway Alarms

Alarms can now be configured for SIP Gateways for errors received via the Proxy Server in a network configuration. SNMP Alarms will be created for the general SIP event failure message when attempting to send to a specific host and for the clearing message when the condition is cleared. A database table has been created for vendor specific errors for which the customer wishes to create alarms. All other error messages received will be ignored.

To configure gateway alarms

1. Configure agent SJ (soft) phone with SIP protocol and G.711 U-law codec.
2. Open Network Manager|Call Center and note resource ID of SIP Call Center.
3. In the trapsdefinition Database table, check whether following traps are defined:
   - 28. Sip Send Message Failure
   - 1028. Sip Send Message Success
   - 29. Sip Dial Out Failure
   - 1029. Sip Dial Out Success
4. In the SipAlarmCodes database table, enter the following:
   - errorcode-reported-alarminfo
   - 11-1-Call Rejected By Peer
   - 15-1-Unknown Gateway Address
5. In the SipAlarmCodes database table, enable the key for 'errorcode'.
6. Login to OpManager.
7. Open the Admin|MIB Browser.
8. In Network Manager, configure CallCenter|SIP Gateway with the IP address of agent SJ phone.

Table 4 provides a list of the gateway alarms and the expected results.

Table 4. Gateway Alarms

Alarm Name	Sub Area	Configuration	Result
Agent Does Not Accept Call			
VoiceGatewayAlarming_Trap Info001	Disconnect cause	"In DB, check 'disconnectedcause' in table 'billing' For example: SELECT disconnectedcause FROM billing ORDER BY startdate DESC"	Disconnectedcause '15' is returned.

Table 4. Gateway Alarms

Alarm Name	Sub Area	Configuration	Result
VoiceGatewayAlarming_Trap Info002	Trap ID	In DB, check 'trapid' in table 'trapshistory' For example: SELECT * FROM trapshistory WHERE resourceid=x ORDER BY trapdate DESC	trapid '29' and '28' are returned.
VoiceGatewayAlarming_Trap Info003	Alarm	Check Alarm on OpManager Client.	Receive the sipDialOutFailure trap with Trap # = 29. Receive the sipSendMsgFailure trap with Trap # = 28.
Agent Accepts Call			
VoiceGatewayAlarming_Trap Info004	Disconnect cause	In DB, check 'disconnectedcause' in table 'billing' For example: SELECT disconnectedcause FROM billing ORDER BY startdate DESC	Disconnectedcause '15' is returned.
VoiceGatewayAlarming_Trap Info005	Trap ID	"In DB, check 'trapid' in table 'trapshistory' For example: SELECT * FROM trapshistory WHERE resourceid=x ORDER BY trapdate DESC"	trapid '29' and '28' are returned.
VoiceGatewayAlarming_Trap Info006	Alarm	Check Alarm on OpManager Client.	Receive the sipDialOutFailure trap with Trap # = 29. Receive the sipSendMsgFailure trap with Trap # = 28.
SIP Gateway Down			

Table 4. Gateway Alarms

Alarm Name	Sub Area	Configuration	Result
VoiceGatewayAlarming_Trap Info007	Disconnect cause	"In DB, check 'disconnectedcause' in table 'billing' For example: SELECT disconnectedcause FROM billing ORDER BY startdate DESC"	Disconnectedcause '16' is returned and indicates normal channel clearing.
VoiceGatewayAlarming_Trap Info008	Trap ID	In DB, check 'trapid' in table 'trapshistory' For example: SELECT * FROM trapshistory WHERE resourceid=x ORDER BY trapdate DESC	trapid '1029' and '1028' are returned.
VoiceGatewayAlarming_Trap Info009	Alarm	Check Alarm on OpManager Client.	Receive the sipDialOutSuccess trap with Trap # = 1029. Receive the sipSendMsgSuccess trap with Trap # = 1028.
SIP Gateway Up			
VoiceGatewayAlarming_Trap Info010	Disconnect cause	In DB, check 'disconnectedcause' in table 'billing' For example: SELECT disconnectedcause FROM billing ORDER BY startdate DESC	
VoiceGatewayAlarming_Trap Info011	Trap ID	In DB, check 'trapid' in table 'trapshistory' For example: SELECT * FROM trapshistory WHERE resourceid=x ORDER BY trapdate DESC	
VoiceGatewayAlarming_Trap Info012	Alarm	Check Alarm on OpManager Client.	
Failover			

Table 4. Gateway Alarms

Alarm Name	Sub Area	Configuration	Result
VoiceGatewayAlarming_Failover001	One gateway up, other gateway down --- Alarm	■ In agent IM|Dialer, make an outbound call. ■ Agent SJ phone rings. Accept the call. ■ The SIP CallCenter then makes the outbound call to Master (SJ phone). As it is shut down, it tries to complete the outbound call through backup SIP gateway. ■ Check Alarm on OpManager Client.	Receive the sipDialOutSuccess trap with Trap # = 1029. Receive the sipSendMsgSuccess trap with Trap # = 1028.
VoiceGatewayAlarming_Failover002	Log	Check CallCenter log.	Call completes through Backup SIP Gateway.
VoiceGatewayAlarming_Failover003	Both Gateways Down	■ In agent IM|Dialer, make an outbound call. ■ Agent SJ phone rings. Accept the call. ■ The SIP CallCenter then makes the outbound call to Master (SJ phone). As it is shut down, it tries to complete the outbound call through backup SIP gateway but fails again. ■ Check Alarm on OpManager Client.	Receive the sipDialOutFailure trap with Trap # = 29. Receive the sipSendMsgFailure trap with Trap # = 28.

Table 4. Gateway Alarms

Alarm Name	Sub Area	Configuration	Result
VoiceGatewayAlarming_Failover004	Both Gateways Up	■ In agent IM|Dialer, make an outbound call. ■ Agent SJ phone rings. Accept the call. ■ The SIP CallCenter then makes the outbound call to Master (SJ phone). Accept the call. ■ Check Alarm on OpManager Client.	Receive the sipDialOutSuccess trap with Trap # = 1029. Receive the sipSendMsgSuccess trap with Trap # = 1028.
VoiceGatewayAlarming_Failover005	Log	Check CallCenter log.	Call completes through Master SJ phone.

Index