A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise

Troubleshooting Guide

Release 9.7 SP1
Document Version 2.0

July 2024

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**

The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

®,™ Trademark of Mitel Networks Corporation

INTRODUCTION

Common problems that are related to installation, database, services and applications, might occur at different stages of the MiCC Enterprise operation. What follows is a description of the most common errors and possible solutions.

INSTALLATION PROBLEMS

A "Not Enough Disk Space" error message appears during installation even if there is enough hard disk space

This may be caused by the size of the page file created during the installation process. You will need to increase the virtual memory of the PC. Contact your Windows Administrator.

Database connection failed or disconnected

There can be three causes:

1. SQL Server is not running or paused.
   - Check to see if SQL Server is running. Click **Start** on the task bar, and select **SQL Service Manager**.
   - Click **Start** button if SQL Server is stopped or in a paused state.
2. The number of connections to the database server has exceeded the limit.
   - Run **Server Configuration Option** from Microsoft SQL Server Management Studio, to increase the number of user connections to SQL Server. For details, refer to SQL Server documentation

Note: MiCC Enterprise services require at least five connections; additionally, for each Information Manager and each Report Manager, one connection is required. Make sure that you have enough connections for the SQL Server.

3. If the MiCC Enterprise database is not installed on the MiCC Enterprise Server, make sure that SQL Client is installed on the MiCC Enterprise Server.

SQL Server not found

1. SQL Server is not running or paused.
   - Check to see if SQL Server is running. Click **Start** on the task bar, and select **SQL Service Manager**. Click **Start** if SQL Server is stopped or in a paused stated.
2. If the MiCC Enterprise database is not installed on the MiCC Enterprise Server, make sure that SQL Client is installed on the MiCC Enterprise Server.

ROUTING PROBLEMS

Calls are not immediately routed to an agent that has become Idle

Queue messages may be played repeatedly for a call that is waiting in queue for a service group. During this time, even if an agent has become Idle, the call will not be routed immediately to the agent because certain messages cannot be interrupted and must be completed before routing will take place.

Calls fail to overflow to a Group Closed destination or the system default destination

When a call fails to overflow to the Group Closed destination, it will attempt to overflow to the system default destination. If this also fails, it will continue to try to overflow again, up to the maximum attempts, according to the system parameter setting in Configuration Manager. It is, therefore, recommended that a device that has queuing capability (for example, the operator) be defined as the system default destination or the Group Closed destination.

Calls to the logon device are not answered

The logon device is out of service.

1. Verify that OAS is up and running.
2. Check the configuration in Configuration Manager, OAS and MX-ONE.

Logon for a Phone Agent has failed

1. Make sure that a correct PIN (Personal Identification Number) has been entered.
2. Verify that the logon device is correct.

Phone Agents lose their logon status after Router Service has restarted

Every time the Router Service is restarted, Phone Agents are logged off automatically. Agents must log on again using the logon script.

Personal calls to the logged off agent are not sent to the personal call default destination

The personal call default destination may be busy or it may be an invalid number. The personal call default destination must be able to queue calls, for example, the operator. Reconfigure the personal call default destination to be a number with queuing capability.

Requeued calls are not sent to some agents

If a call is manually rejected by an agent, it will not be sent to the same agent again unless the resend to the same rejected agent option is enabled. If the group is closed before the resend timer expires, the call will be sent to the Group Closed destination.

Route Manager did not resend the service call to another agent after ring time-out occurred on the original agent

The requeue device may be out of service.

1. Verify that OAS is up and running.
2. Check the configuration in Configuration Manager, OAS and MX-ONE.

Service accesses are not receiving calls

The service access device may be Out of service, misconfigured, deleted, or deactivated, or OAS may be down.

1. Verify that OAS is up and running.
2. Check the configuration in Configuration Manager, OAS and MX-ONE.

Unable to receive personal calls

The personal queue device may be out of service.

1. Verify that OAS is up and running.
2. Check the configuration in Configuration Manager, OAS and MX-ONE.

Repeat Queue Message not played

If the repeat queue message is configured with duration as a parameter, the system will attempt to play the estimated wait time (EWT) for this call. If the service group is configured with Close Group on No Logged On Agents, the EWT could become infinite when all agents are in not ready status. When the EWT is infinite, the system will not be able to play a message. The repeat queue message will be skipped in this case. It is recommended not to play the EWT in the repeat queue message when the EWT is very long, for example more than one hour.

Onhook Callback is not offered

If the service group is closed or there is no available agent, the onhook callback option will not be offered during the repeat queue message. Also make sure that the system setting has onhook callback enabled and the play messages are defined.

TIPS ON OVERFLOW

1. A call enters a service group queue when the group is closed: Group closed can be either when there is no ready agent or when no agent has logged on. The call will overflow to the Group Closed destination. If the destination for Group Closed is not defined, the call will go to the system default destination defined in Configuration Manager (System Properties).
2. A call enters a service group queue where all agents are Busy: If Overflow on Wait Time is defined to be the overflow condition and the Estimated Waiting Time (EWT) threshold has been exceeded, the call will overflow to the EWT/AWT (Actual Waiting Time) overflow destination. If this fails, it will remain in the service group queue.

3. A call is waiting in a service group queue and the AWT threshold has been exceeded: The call will try to overflow to the EWT/AWT overflow destination. If this fails, it will remain in the service group queue.
4. A call is waiting in a service group queue and the group is closed when the last ready agent becomes not ready or logs off.
    - If Overflow on Wait Time is defined to be the overflow condition and the AWT threshold has not been exceeded, the call will remain in the service group queue.
    - If Overflow on Wait Time is defined to be the overflow condition and the AWT threshold has been exceeded, the call will overflow to the “Group Closed” destination.
    - If Overflow on Wait Time is not defined as the overflow condition, the call will overflow to the “Group Closed” destination immediately.
5. Overflow conditions that are not allowed:
    - A call cannot overflow to a service group that it has queued for before.
    - A call cannot overflow to a service access that it has previously gone through.
    - A call cannot overflow to an inactive service access.
    - A call cannot overflow if the maximum attempts, according to the system parameter setting in Configuration Manager, have failed.

SERVICE PROBLEMS

In this section, solutions for service problems are described.

ALL SERVICES

Could not start the (Name of Service) service on (machine name)

Verify that all dependent DLLs are installed. Reinstall MiCC Enterprise and make sure the installation is successful.

Failed to register location to Broker Service. Lost connection to Broker Service. (Name of Service): Failed to register location to Broker Service

From the Control Panel, verify that the Broker Service and Configuration Service are running. Check the Event Viewer to see why the Broker Service or Configuration Service is not started or turn on the Configuration Service Log.

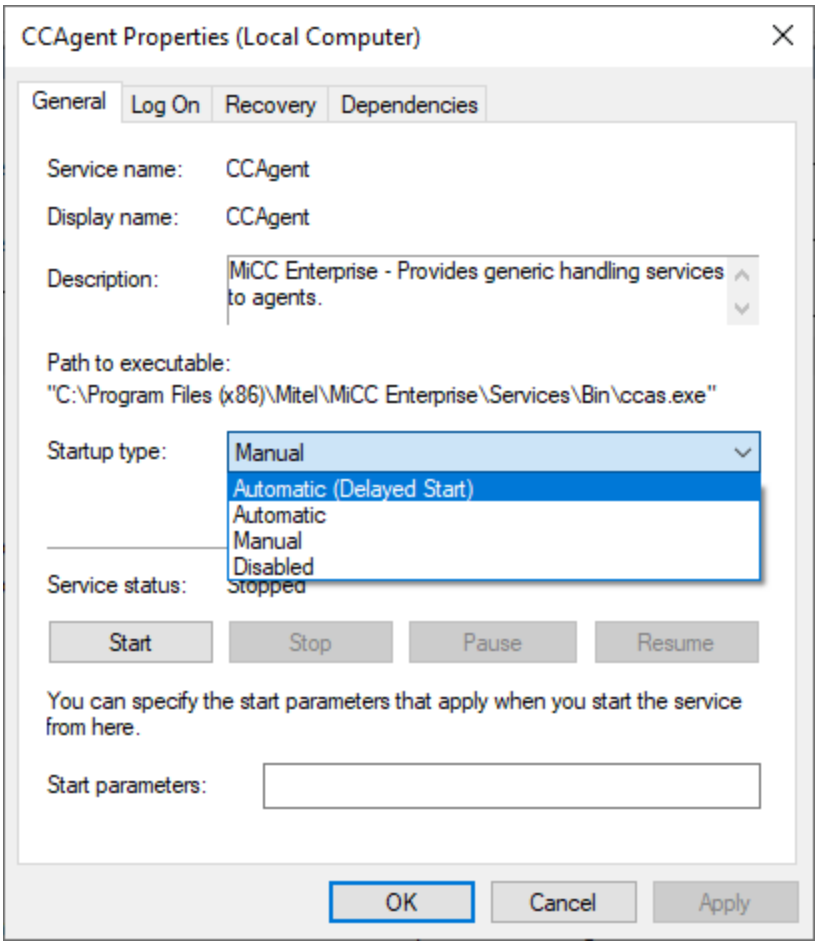
Service is running, but does not accept any client connections

Verify that all dependent services are running and have been successfully connected to by the service. Make sure the license server is available and licenses have been allocated to the tenant.

Service fails to start automatically after reboot of machine

Most services depend on the MiCC-E Configuration Service, so if that service is delayed in connecting to the database, it can affect the ability of other services to start. If services consistently fail to start automatically after rebooting the MiCC-E server, it is suggested to set the service to **Automatic (Delayed Start)** in Windows Service Control Manager. This will cause the service to start 120 seconds after all other services set as **Automatic** have started.

To set this option, select the MiCC-E service that is failing to start automatically, and set **Startup Type** to **Automatic (Delayed Start)** as shown below.



CONFIGURATION SERVICE

Could not start Configuration Service

1. Verify that the OAS Server is present on the current domain or a domain that has a trust relationship set with the domain in which the MiCC Enterprise services are running.
2. Verify that SQL Server is running.

REPORT SERVICE

Report Service cannot be started

1. Make sure that the Windows user account that is to be used to start Report Service has been assigned with the “Log on as a service” right.
2. Also, verify that the user account has not been disabled and that the password has not been modified.

APPLICATION PROBLEMS

Make sure that both the Broker Service and Configuration Service are running.

ALL APPLICATIONS

Application text appears in mixed languages

Verify that the locale setting on the MiCC Enterprise Server matches the setting on the MiCC Enterprise client. Otherwise, mixed language text will be displayed.

Slow startup of .NET based applications

If the computer does not have Internet access, this may cause slow startup of some .NET based applications such as Agent, Report Manager and Information Manager. Microsoft .NET performs an Authenticode validity check and if it cannot access the Certificate Revocation List due to no Internet access, a delay of up to 30 seconds may occur until the check times out. The check must be disabled on these systems. This can be done system system wide or for each .NET based application. The **generatePublisherEvidence** XML element must be added to the configuration file.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
        <runtime>
                <generatePublisherEvidence enabled=”false” />
        </runtime>
</configuration>
```

Note that the <configuration> and <runtime> sections may already exist. The generatePublisherEvidence element should be added to the existing sections.

For system wide, add the element to the following file:

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

For individual applications rather than system wide, add the element to the application configuration file. The configuration file may or may not already exist.

Agent	<InstallDir>\Applications\Bin\Agent.exe.config
Report Manager	<InstallDir>\Applications\Bin\RM.exe.config
Information Manager	<InstallDir>\Applications\Bin\IM.exe.config

CONFIGURATION MANAGER

Connection to other components were disrupted

Configuration Service has been restarted. Configuration Manager will attempt to connect to Configuration Service again.

SQL Server has been restarted, the application will be terminated.

Cannot perform any addition or modification to any objects

Verify that neither the MiCC Enterprise database nor the tempdb database is full.

Cannot update system properties or Service Access due to no Basic Virtual Device (BVD) list or play message.

The connection between Configuration Service and OAS is disrupted. Make sure that the Event Channel Service (ECS) and OCS are running.

Cannot update Campaign information and Campaign customer

Connection to Campaign Service might be disrupted.

Cannot create/update Script Manager service access

One or more Script Manager components are not running. Check the Script Manager Online Help for a list of components and confirm that all Script Manager services are running.

Cannot see all the configured OAS Servers

The Virtual Contact Center license must be installed before all the configured OAS Servers are available in Configuration Manager. If the Virtual Contact Center license is not available, only one OAS server will be allowed to use even multiple OAS Servers can be configured in the MiCC Enterprise Setup.

MICONTACT CENTER AGENT

Agent Service has been restarted. Please restart the application to connect to the server.

Connection to Agent Service has been restored. The following messages will be written to the Event Viewer:

1. Connected to Broker Service
2. CCAS Connected to Configuration Service
3. Connected to Router Service
4. Agent Service Started

Agent status of Phone Agents cannot be updated

The extension where the agent logged on might not have been configured properly. Check the Router Service log file (that is, RouteSvc.log) or the configuration in OAS.

Call Control is disabled

Connection to OAS or the Call Control Service has been disrupted and MiCC Agent will not be able to perform any call processing functions. MiCC Agent will try to reconnect. Also, check that the connection to the OAS Server is intact.

Error Connecting to the Server

MiCC Agent Service has failed to start and MiCC Agent cannot be launched. Start the Agent Service from the Control Panel.

Connection to the Server has been lost

Connection to MiCC Agent Service has been disrupted. MiCC Agent remains operative; however, only non-service calls can be handled. Start the service from the Control Panel.

Restored Connection to the Router Service

Connection to the Router Service has been restored and statuses of agents will be restored. However, all the calls that were in the queue prior to the disruption will be lost and new calls will be received. The following messages will be written to the Event Viewer:

1. CCRouter Service started
2. CCAS Reconnected to Router Service

Disconnected from the Router Service. No sessions will be allocated.

Connection to the Router Service has been disrupted. When the Router Service is shut down, service calls, media sessions, E-mail sessions and personal number calls will not be sent to MiCC Agents. Start the service from the Control Panel.

Unable to monitor extension. MiCC Agent is exiting.

Connection to the OAS Server or Call Control Service has been disrupted.

1. Check that the connection to the OAS Server and Call Control Service is maintained and that all services are up and running.
2. Verify that the extension entered is a valid extension.
3. Restart the MiCC Agent application.

Values reported in MiCC Agent real time windows are set to extremely large or negative values

The time zone environment variable **TZ** should not be set on the MiCC Enterprise servers. If this variable is set, it will affect the reporting of time values from the Servers to the MiCC Enterprise Clients. Please ensure that this variable is not set via any logon startup scripts. If it is set, make sure that it corresponds to the configured Date/Time setting for the PC. (To remove a setting in this variable, run autoexec.bat and remove the line **Set TZ = (variable)**.

MiCC Agent is not running properly under Terminal Server

For MiCC Agent to run properly under Terminal Server, do the following on the Terminal Server PC:

1. Open **Administrative Tools** and click Local Security Policy.
2. Expand Local Policies, and then click **User Rights Assignment**.
3. Double-click **Create global objects** in the right pane.
4. Click **Add** in the Local Security Policy Setting dialog box.
5. Click the user account that you want to add (in the Select Users or Group dialog box), click **Add** and then click **OK**.

Rejected E-mail not rerouted to Agent

If a MiCC Agent logs off while handling an E-mail or rejects an E-mail, the E-mail will not be rerouted to that agent until the **Resend Rejected Calls to Same Agent** duration has expired.

INFORMATION MANAGER

Real time information is not displayed

This problem is usually preceded with one or more problems caused by the errors listed under **Broker Service** or **Configuration Service** problems. The Internet Information Service is not running or the web services are not properly configured.

Device is out of service appears in the alarm log.

OAS is down or the device might have been misconfigured or deleted. Verify that OAS is up and running. Check the configuration in Configuration Manager, OAS and MX-ONE.

Values reported in Information Manager real time windows are set to extremely large or negative values

The time zone environment variable **TZ** should not be set on the MiCC Enterprise Servers. If this variable is set, it will affect the reporting of time values from the Servers to the MiCC Enterprise Clients. Please ensure that this variable is not set via any logon startup scripts, or if it is set, that it corresponds to the configured Date/Time setting for the PC. (To unset this variable, run autoexec.bat and remove the line "Set TZ = (variable).")

WALL DISPLAY

Certain extended character set is not displayed

The Spectrum wall display can only display a limited number of characters. For details, refer to the document *Wall Display and Real Time Messaging*.

Wall Display messages are not displayed

Verify that a test message can be displayed. If no message is displayed, check the physical connection.

REPORT MANAGER

A date in the 1970s appears in the Time Setup column of a report

If there are Callback calls in the queue yet to be answered while the Callback Failure category report is generated, the **Agent** column will appear blank and a date in the 1970s will appear in the **Time Setup** column. This is not a fault.

A row of zeros appears in a report

In some reports, a row of zeros is printed. This is not a fault.

Zeros are displayed because there are no activities in the selected columns from the Report Categories provided. However, there are activities in the columns that were not selected. For example, in the Agent Activity report category, a row of zeros is shown for agents that did not have any call activities during selected time range and if the user did not select the **Agent Group**, **Logged In** and **Ready** columns.

Configuration Service connection failed. Report Manager will continue but will not receive updated configuration data.

Connection to Configuration Service has been disrupted. When the connection to Configuration Service is disrupted, configuration data (that is, data for agents, service groups, service accesses, and so on) will not be received even though Report Manager will continue running. Additionally, the entry **Report Service Failed to Connect to Configuration Service** will be added to the Event Viewer.

Could not connect to the database

The SQL Server is down and reports cannot be generated. Contact your SQL Administrator.

Disconnected From Report Service. Report Manager will now shut down.

Connection to Report Service has been disrupted and Report Manager will be forced to shut down; other services will continue running. Start the service either by:

- Using the MiCC Enterprise Setup Utility.

  OR

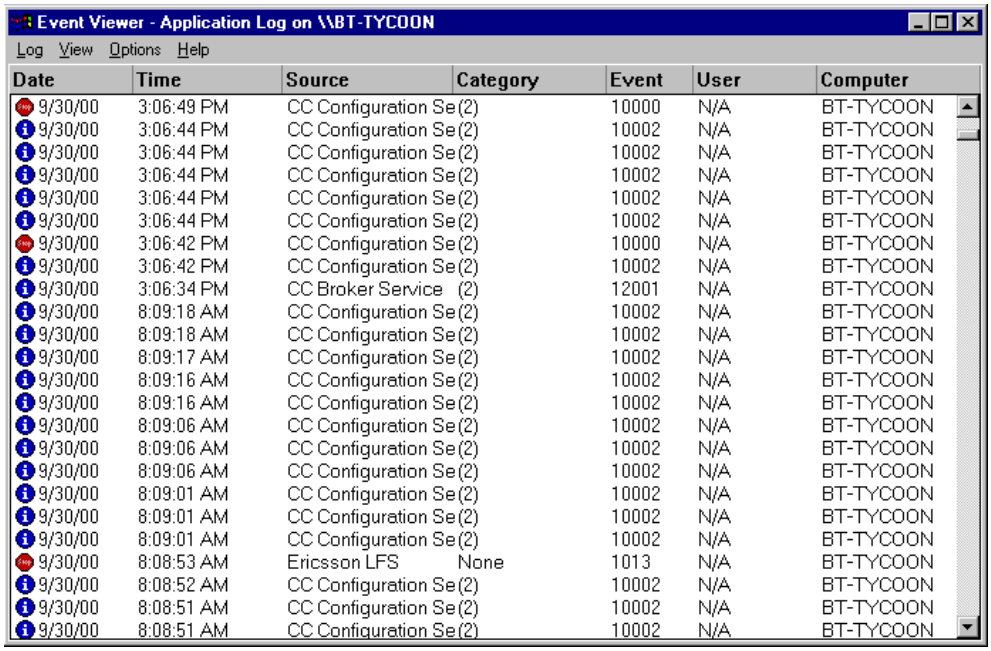
- Start it via the Control Panel.

Incorrect report data between a 6 - day report and a 30 - day report

The MiCC Enterprise database stores all data in GMT time format. In this particular case, the period covered by these two reports extended two different time frames (that is, daylight-saving time and standard time). For the first report, when Report Manager queried data from the database, the time used was based on daylight-saving time; for the second report, when Report Manager queried data from the database, the time used was not based on daylight-saving time. This caused the data for the second report to be short of that of the first report by one-hour's worth of data.

No data in reports

1. Verify that Archive Service, Event Service and Report Service are all running via the Control Panel.
2. Verify that when the three services are started, the following messages are displayed in the Windows Event Viewer (Application Log) without any error. If not, take action upon any error messages. When all the services are started correctly, similar messages will appear in the Windows Event Viewer (Application Log).



Date	Time	Source	Category	Event	User	Computer
9/30/00	3:06:49 PM	CC Configuration Se	(2)	10000	N/A	BT-TYCOON
9/30/00	3:06:44 PM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	3:06:44 PM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	3:06:44 PM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	3:06:44 PM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	3:06:44 PM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	3:06:42 PM	CC Configuration Se	(2)	10000	N/A	BT-TYCOON
9/30/00	3:06:42 PM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	3:06:34 PM	CC Broker Service	(2)	12001	N/A	BT-TYCOON
9/30/00	8:09:18 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:18 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:17 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:16 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:16 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:06 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:06 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:06 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:01 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:01 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:09:01 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:08:53 AM	Ericsson LFS	None	1013	N/A	BT-TYCOON
9/30/00	8:08:52 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:08:51 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON
9/30/00	8:08:51 AM	CC Configuration Se	(2)	10002	N/A	BT-TYCOON

Figure 1: Event Viewer - Application Log

3. For report objects that have had no activity during the specified time interval, the associated columns in the report will be displayed as blank, or with a **–** or **0**.
4. Verify that events are received from the MiCC Enterprise Event Service to the MiCC Enterprise Archive Service by activating the Report Data Log from the CM application.
5. Generate some traffic and wait at least ten minutes or the duration specified on the **Report** tab of the **Contact Center System Properties** dialog box (in Configuration Manager).
6. View the log file via any text editor such as Windows Notepad.
7. If no events are received, check for error messages in the Error Log via any text editor such as Notepad. Take action upon any error messages.

Scheduled reports cannot be printed

1. Verify that a network printer has been assigned to the user account that was used to log on to the MiCC Enterprise Report Service and that the printer is shared.

2. If the size of the scheduled report exceeds the size that can be handled by the system log in the tempdb, expand the size of the `tempdb` in the SQL Server. Refer to SQL Server documentation for details.

3. Check the information in the Report Manager User Log.

4. Check the Report Service Log in the MiCC Enterprise Server Log Directory (`C:\Program Files\Mitel\MiCC Enterprise\Services\Bin\Log\`, assuming C: drive is the installation drive), or open the System Report Log window from the Report Manager application.

5. Check the starting day of the month.
   - If the starting day of the month is 29, scheduled reports will not be printed in the month of February except in leap years.
   - If the starting day of the month is 30, scheduled reports will not be printed in the month of February.
   - If the starting day of the month is 31, scheduled reports will not be printed in the months of February, April, June, September and November.

The name of the agent appears as asterisks in the report

When the Agent Privacy feature is enabled, the names of the selected agents will appear as asterisks (that is, ***) in the report.

The number of "Offered Calls" on the Agent report is greater than the number of "Offered Calls" on the Service Access or the Service Group reports

When a call is requeued as a result of being rejected by the agents or ring time out, Route Manager will redistribute the same call to the next available agent. Thus, the same call which is counted once in the Service Access and in the Service Group tables is actually counted twice from the Agent standpoint. This is not to be considered as a fault.

Unable to find the network printer while creating a scheduled report

Make sure that printers have been created under the Windows user account that is to be used to start the Report Service.

Unable to retrieve Report Service location from Broker

Report Service has failed to start and Report Manager will not be able to launch until Report Service has started. Reenter the Windows user name and password in the Service dialog box (of CCReport) accessed via the Control Panel.

Cannot Generate Reports

If the database is more than 80% full, reports cannot be generated. Use the Database Maintenance Utility to expand the database.

SCRIPT DESIGNER

Problem Compiling Script

While logged on as a Domain User, scripts cannot be compiled.

Problem Opening Script with Extended ASCII characters

Scripts with filenames containing extended ASCII characters like æ, ø, å fail to open if the Windows Regional format is set to English (XX) where XX represents another country other than the United States or the United Kingdom. To correct this problem, set the Windows Regional format to English (United States) or English (United Kingdom), or use only ANSI characters in the script file name.

DATABASE MAINTENANCE PROBLEMS

Alert notification does not work

The SQL Server and SQL Server Agent must be run as administrator accounts, with administrator privileges. Both SQL Server and SQL Server Agent must be members of the Administrators domain to be able to run as a service and send/receive E-mail.

Backup and Restore

In order to ensure accuracy and consistency among activity data as well as configuration data, all Call Detail Records (CDRs) must be backed up and restored within the same time zone and with the same Regional Setting.

CDR data are not cleaned up as scheduled. The scheduled cleanup of CDR data is not thorough.

1. To prevent data corruption that may be caused by "overnight calls" (that is, calls that extend beyond midnight), by default, call detail records for the day immediately prior to the day selected in the Frequency group box of the CDR Cleanup dialog box will be excluded from the cleanup process even if this check box is not selected.
2. Check the DBMT Utility Service Log in the MiCC Enterprise Server Log Directory (`C:\Program Files\Mitel\MiCC Enterprise \Services\Bin\Log\`, assuming `C:` drive is the installation drive).

"Error retrieving report service location from broker service" appears at the end of the report data restore process

DBMT fails to connect to the Report Service, thus making it impossible to update the report data start date to the Report Service. Start or restart the Report Service to retrieve the updated report data starting date.

"Error updating database start date on report service" appears at the end of the report data restore process

DBMT fails to update the report data starting date to the Report Service. Start or restart the Report Service to retrieve the updated report data starting date.

Location of the call detail data backed up by Database Maintenance

The default location for the CDR Backup Directory is the System Temporary Directory.

Schedule CDR Cleanup and Log Call Detail Data

If the Log Call Detail Data feature has been enabled from Configuration Manager, make sure that the Schedule CDR Cleanup feature is set up as desired.

MiCC Enterprise database or log device is 80% (95%) full

Run Database Maintenance Utility to check the current database usage and to expand the database.

Note: When the database is more than 80% full, reports cannot be run. Historical data is still archived to the database.

The MiCC Enterprise DBMT service is not currently running

Start DBMT to allow CDR cleanup.

Database Maintenance Service has not been started

Regardless of the status of Database Maintenance Service, the Database Maintenance utility program will start; however, the scheduled cleanup of call detail records will not occur. Start the service from the Control Panel.

If the Log Detail Record feature is deactivated by Configuration Manager, then ignore this message.

COMMUNICATION PROBLEMS

ANSI extended character handling in the MiCC Enterprise Database

When saving data into the database, it is essential that you follow the rules, as described below, regarding character sets. Otherwise, incorrect data will be saved to the database or data will be incorrect when performing the Backup or Restore operation through MiCC Enterprise Database Maintenance.

A Code Page, also known as Character Set, is a set of 256 letters (uppercase and lowercase), numbers and symbols. The Code Page of the SQL Server is different from the Code Page of the operating system. Windows has an ANSI Code Page as well as an OEM Code Page, both depending on country settings.

For example, if Code Page 850 (Multilingual) Character Set is selected when installing the SQL Server, all Windows-based clients (such as ISQL/W, SQL Server Management Studio, Notepad and MiCC Enterprise applications) will be considered as ANSI clients and MS-DOS or console-based applications such as ISQL and BCP will be considered as OEM clients. A SQL Server with Code Page 1252 is considered to be an ANSI Server, while a SQL Server with any other Code Page (for example, 850 or 437) is considered to be an OEM Server.

The (Windows) registry entry **AutoAnsiToOem** controls the default conversion behavior when data is inserted to or retrieved from the SQL server database. If **AutoAnsiToOem** is enabled (that is, the default setting in SQL Server), conversion is enabled in the following cases:

1. ANSI clients to OEM servers
2. OEM clients to ANSI servers

In order for the input characters to be converted and saved (through **AutoAnsiToOem**) to the SQL Server (OEM Server for MiCC Enterprise) database correctly, you must input regular and extended characters (foreign language other than English) by using the enhanced keyboard (corresponding to the particular country). If you enter an ANSI extended character by holding the **ALT** key and then typing the ASCII code of the character preceded by a zero (0), the character may or may not exist in the corresponding OEM Code Page, and hence may not convert to the correct character.

MISCELLANEOUS PROBLEMS

Cannot allocate media resources for any media

When a call is originated from an MX-ONE Operator to a BVD, allocation of media resources will not be available. This is an MX-ONE Operator limitation. When a customer calls an MX-ONE Operator and the Operator transfers the call by calling the Service Access, the allocate resource operation will fail if the Service Access is configured with voice messages or is getting input from the caller. In this situation, the Service Access (both IVR or non-IVR) will take the configured error or default path instead of the requested destination.

As a work around, it is recommended that a delay be set on the Service Access before allocating any media resources. This allows enough time for the MX-ONE Operator to transfer the call to the customer before the commencement of the resource allocation process.

Agent logged on to mobile extension forced not ready

It is not possible to know if an outbound call was made by the agent using the mobile extension. If a call is routed to the agent while they are on an outbound call, the agent will be forced not ready. The system can be configured to automatically make the agent ready again. To do this, configure the **Temporary Not Ready Timer** in the Configuration Manager system properties.

Voice prompts do not play when Irish English is selected as the language

MiCC Enterprise does not ship default voice prompts for Irish English. To have MiCC Enterprise play prompts for Irish English, a directory named IrishEnglish must be created on the OAS Server and the voice prompts must be recorded.

Cannot connect to OAS

The OAS Server must be present on the current domain or a domain that has a trust relationship set with the domain in which the MiCC Enterprise services are running.

Daylight Saving Time and Campaign Start and Stop Time

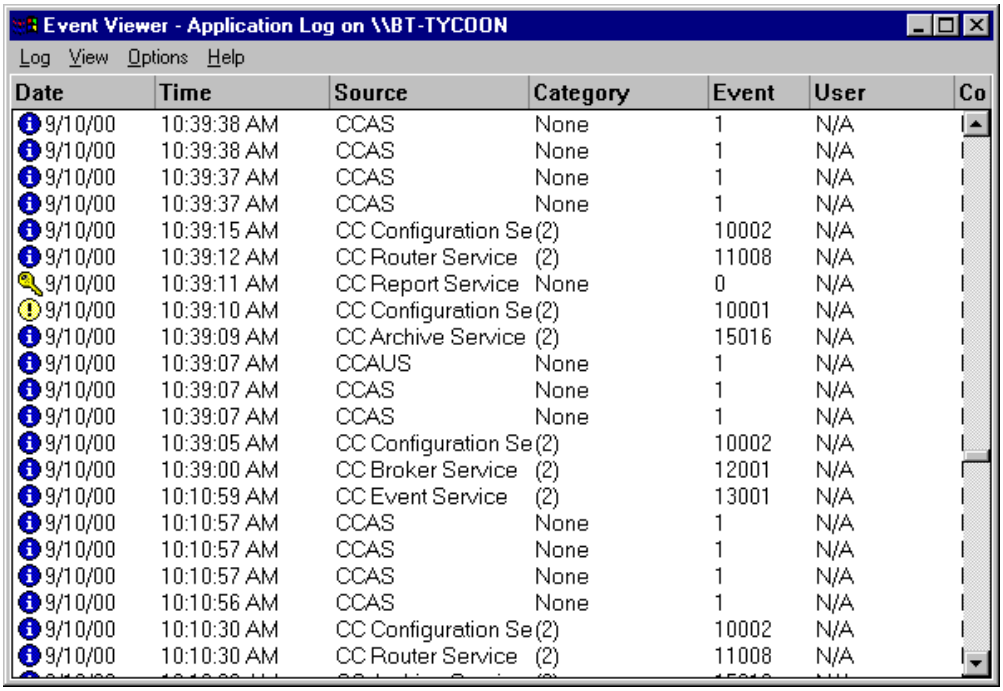
For any campaign that starts or stops at or after the time when Daylight Saving Time begins, that is, at 2:00 a.m. on the first Sunday of April, the Start/Stop Time will automatically be rolled back by one hour. For any campaign that starts or stops at or after the time when Daylight Saving Time ends, that is, at 2:00 a.m. on the last Sunday of October, the Start/Stop Time will automatically be increased with one hour. For example, if a campaign is to start at 1:15 a.m. on the first Sunday of April and it is to stop at 2:15 a.m. on the same day, the system will automatically roll back the Stop Time to 1:15 a.m. In this scenario, it is therefore impossible to create a campaign that is to start at 1:15 a.m. and to end at 2:15 a.m.

Configuration Manager will display the error message End time cannot be less than Start time.

Ensuring that all MiCC Enterprise services are successfully started

After completing the setup procedure for MiCC Enterprise:

1. Start the Windows Event Viewer by clicking **Start**, point to **Programs**, point to **Administrative** Tools, and then select **Event Viewer**
2. Click **Application** from the **Log** menu. The startup messages for different MiCC Enterprise services will be displayed in the Application log, see figure below.



Date	Time	Source	Category	Event	User	Co
9/10/00	10:39:38 AM	CCAS	None	1	N/A	
9/10/00	10:39:38 AM	CCAS	None	1	N/A	
9/10/00	10:39:37 AM	CCAS	None	1	N/A	
9/10/00	10:39:37 AM	CCAS	None	1	N/A	
9/10/00	10:39:15 AM	CC Configuration Se	(2)	10002	N/A	
9/10/00	10:39:12 AM	CC Router Service	(2)	11008	N/A	
9/10/00	10:39:11 AM	CC Report Service	None	0	N/A	
9/10/00	10:39:10 AM	CC Configuration Se	(2)	10001	N/A	
9/10/00	10:39:09 AM	CC Archive Service	(2)	15016	N/A	
9/10/00	10:39:07 AM	CCAUS	None	1	N/A	
9/10/00	10:39:07 AM	CCAS	None	1	N/A	
9/10/00	10:39:07 AM	CCAS	None	1	N/A	
9/10/00	10:39:05 AM	CC Configuration Se	(2)	10002	N/A	
9/10/00	10:39:00 AM	CC Broker Service	(2)	12001	N/A	
9/10/00	10:10:59 AM	CC Event Service	(2)	13001	N/A	
9/10/00	10:10:57 AM	CCAS	None	1	N/A	
9/10/00	10:10:57 AM	CCAS	None	1	N/A	
9/10/00	10:10:57 AM	CCAS	None	1	N/A	
9/10/00	10:10:56 AM	CCAS	None	1	N/A	
9/10/00	10:10:30 AM	CC Configuration Se	(2)	10002	N/A	
9/10/00	10:10:30 AM	CC Router Service	(2)	11008	N/A	

Figure 2: Application Log

3. Double-click the message to read it. The **Event Detail** dialog box for the selected message will appear, as shown in figure on page 25.

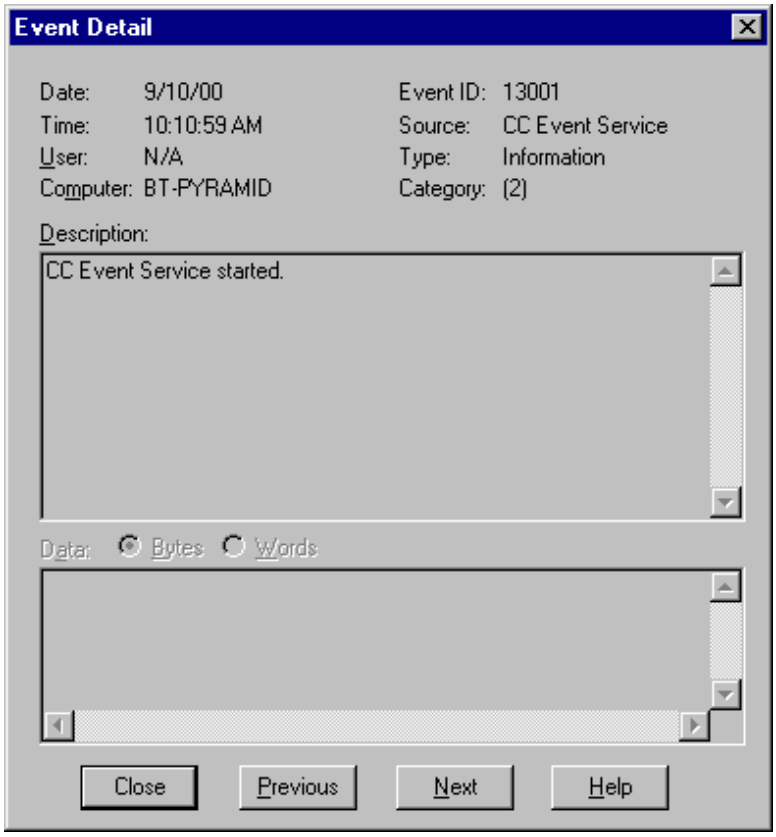


Figure 3: Event Detail

4. Verify that the services are actually running by starting the Services program from the Control Panel.

Resetting the PC clock

If the clock of the PC that is installed with any of the MiCC Enterprise services (except Broker Service) has been reset manually, restart the PC as well as the services.

It is highly recommended that the **Automatically adjust clock for daylight saving changes** check box (which is on the **Time Zone** tab of the **Date/Time Properties** dialog box accessed via the Control Panel) is selected; otherwise, the following error message will appear in the Archive error log when you attempt to reflect the daylight saving changes by manually adjusting the PC clock backward:

(Date) (Time) Archive Service Group Activity data failed. ODBC code = -1; message = Violation of PRIMARY KEY constraint (Name of Key): Attempt to insert duplicate key in object (Name of Object). Command has been aborted.

If the clock is to be set backward manually, be sure that the data in the database is removed (by using DBMT) prior to the actual clock change.

Using Microsoft Systems Management Server (SMS) for Client Installation

If SMS is used to install the MiCC Enterprise Client applications, there may be an issue with registry key accessibility. When the MiCC Enterprise installation executes, it grants full permission to the group **Everyone** for the required registry keys used by MiCC Enterprise client applications. If only read permission is granted to this group, the MiCC Enterprise client applications cannot startup properly. To avoid this problem, the Microsoft utility **Regini** can be used to first setup the registry key permissions on all client machines. Regini is available with the **Windows Resource Kit**. Prior to installing MiCC Enterprise client applications, Regini can be run from a network machine with a Windows account that has Administrator access to all of the network machines. To update the registry, and add the appropriate MiCC Enterprise registry keys with full permission, execute the following from the command line:

regini -m \\machinename solidusreg.txt where **machinename** is the name of the client machine which is being updated, and **solidusreg.txt** is the text file containing the registry keys to be added or modified. Repeat this command for every client machine that will be installed automatically.

The contents of solidusreg.txt should be as follows:

```
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters [1 5
7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters\Applic
ations [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters\Applic
ations\BSA [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters\Applic
ations\CM [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters\Applic
ations\RM [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters\Applic
ations\IM [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters\Applic
ations\SM [1 5 7]
\Registry\Machine\SOFTWARE\Wow6432Node\Mitel\SEC\Common\Parameters\Applic
ations\ATB [1 5 7]
```

BACKUP AND RESTORATION OF THE MICC ENTERPRISE SYSTEM

Manually backing up and restoring MiCC Enterprise data may be necessary in case of reinstallation to a new server, where you wish to retain the previous configuration completely.

BACKUP OF MICC ENTERPRISE DATA

Following is the procedure to follow in order to completely backup data from your MiCC Enterprise system.

1. Prior to backing up data, it is recommended to stop all MiCC Enterprise services and applications, except for the Broker service, which is required for running Database Maintenance (DBMT).
2. Backup the Database Server
3. Backup the MiCC Enterprise Server
   a. Agent Signature Files
      - On the MiCC Enterprise Server machine, backup the following directory: `\Program Files\Mitel\MiCC Enterprise\Services\ccadata`

        This directory contains all of the agent signature files for E-mail, if configured.

   b. Report Files
      - On the MiCC Enterprise Server machine, backup the following directory, including all subdirectories: `\Program Files\Mitel\MiCC Enterprise \Services\Report`

        A subdirectory is created for each MiCC Enterprise Report Manager user that has stored report logs and files.

   c. Greeting Files
      - On the MiCC Enterprise Server machine, backup the following directory, including all subdirectories: `\Program Files\Mitel\MiCC Enterprise \Services\SeCGreeting`

        This directory contains all agent and service group greeting files, if configured.

   d. Logo Files
      - On the MiCC Enterprise Server machine, backup the following directory, including all subdirectories: `\Program Files\Mitel\MiCC Enterprise \Services\SeCLogo`

        This directory contains all of the custom logo files, if configured.

   e. Recording Files
      - On the MiCC Enterprise Server machine, backup the following directory, including all subdirectories: `\Program Files\Mitel\MiCC Enterprise \Services\SeCRecord`

        This directory contains all of the agent and supervisor recorded calls.

   f. Registry Information
      - If you have configured special registry values for the MiCC Enterprise services, run the MiCC Enterprise Registry Configuration application (SeCCfg.exe), and check the values for each option.

4. Backup the MiCC Enterprise Clients
   a. Registry Information

- If you have configured special registry values for the MiCC Enterprise applications, run the MiCC Enterprise Registry Configuration application (SeCCfg.exe), and check the values for each option.

b. Backup Script Manager Data

- Use Script Manager Configuration to backup Script Manager Configuration data. For a complete description of backup and restoration of Script Manager Configuration data, please refer to the MiCC Enterprise Script Manager On-line Help.

5. To backup Configuration data stored in the SQL Server database, use SQL Server Management Studio. Select the “nextccdb” database, then select the **Backup Database** menu option to backup the database to a text file.

Transaction Log Backup for Nextccdb Fails

If MiCC Enterprise and SQL Server are installed on different servers, and the CCDBMT service is installed on the same server as the SQL Server, then the backup of the database (nextccdb) transaction log will fail. This failure is caused by the changes in Recovery model that the CCDBMT service makes every 24 hour.

To solve this, a registry key has to be manually created and enabled. Use the following procedure:

1. Open the **Registry Editor**
2. Set up the following key path using **Edit -> New -> Ke**y
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CCConfiguration\Parameters\`
3. In the menu, select **Edit -> New -> DWORD Value**
4. Name the new registry key DisableTransactionDump
5. In the menu, select **Edit -> Modify**
6. In the **Edit DWORD Value** window, enable the key by setting **Value data**: to 1
7. Click **OK**

RESTORATION OF MICC ENTERPRISE DATA

To restore data from a previously backed up MiCC Enterprise system, use the following procedure:

1. Stop all MiCC Enterprise services and applications, except for the Broker service, which is required for running Database Maintenance (DBMT).
2. Restore the Database Server
3. On the machine where the MiCC Enterprise Database is installed, run the Database Maintenance application. Select Configuration data, CDR data, Campaign data, Monthly Report data (if previously backed up) and Registry data for restoration from the previous backup. Refer to the MiCC Enterprise Database Maintenance Online Help for details.
4. Restore the MiCC Enterprise Server

a. Agent Signature Files

- On the MiCC Enterprise machine, copy the previously backed up agent E-mail signature files to the following directory:
  `\<installation dir>\MiCC Enterprise\Services\ccadata`

  This directory contains all of the agent signature files for e-mail.

b. Report Files

- On the MiCC Enterprise Server machine, copy the previously backed up subdirectories with report files to the following directory:
  `\<installation dir>\MiCC Enterprise\Services\Report`

  A subdirectory is created for each MiCC Enterprise Report Manager user that has stored report logs and files.

c. Registry Information

- If you had previously configured special registry values for the MiCC Enterprise services, run the MiCC Enterprise Registry Configuration application (SeCCfg.exe). Modify the default values as necessary to match your previous configuration.

d. Greeting Files

- On the MiCC Enterprise Server machine, copy the previously backed up greeting files to the following directory: `\<installation dir>\MiCC Enterprise\Services\SeCGreeting`

e. Logo Files

- On the MiCC Enterprise Server machine, copy the previously backed up logo files to the following directory: `\<installation dir>\MiCC Enterprise\Services\SeCLogo`

f. Recording Files

- On the MiCC Enterprise Server machine, copy the previously backed up recorded files subdirectories to the following directory: `\<installation dir>\MiCC Enterprise\Services\SeCRecord`

5. Restore the MiCC Enterprise Clients

a. Registry Information

- If you had previously configured special registry values for the MiCC Enterprise services, run the MiCC Enterprise Registry Configuration application (SeCCfg.exe). Modify the default values as necessary to match your previous configuration.

6. Restore Script Manager Data

7. Use Script Manager Configuration to restore Script Manager Configuration data. For a complete description of backup and restoration of Script Manager configuration data, please refer to the MiCC Enterprise Script Manager On-line Help. When restoring Script Manager Configuration data, make sure the same MiCC Enterprise configuration data is restored as well. Otherwise, there will be a mismatch between Script Manager Configuration data and MiCC Enterprise configuration data.

8. To restore Configuration data stored in the SQL Server database, use SQL Server Management Studio. Select the **nextccdb** database, then select the **Restore Database** menu option to restore the database from the previously selected text file.

Note: After database restoration, make sure that the dbo user is configured to use the Login Name “nextccuser” for the nextccdb database.

OPEN APPLICATION SERVER TROUBLESHOOTING

The OAS document Handling Faults has a comprehensive troubleshooting section. In this section some issues that may be encountered specific to MiCC Enterprise are presented.

When calls are transferred between 2 sites, the call is treated as a private call instead of a service group call

Ensure that all patches listed in the MiCC Enterprise release notes are installed.

Note: Each OAS server must have a unique node id defined when multiple OAS servers are used with MiCC Enterprise. Each OAS Server node id in the entire virtual contact center, not just the site, must be unique. If a node id was not entered during OAS installation or you wish to change the node id in OAS, configure/change the Node ID in the NRM Configuration section of the OAS Management Console and restart NRM on the OAS Server.

IT AND SECURITY ISSUES

This section details all network share points created and any registry key or NTFS permissions changes made by the MiCC Enterprise installation program.

SERVER INSTALLATION

User Rights

To install, the logged on user must be a local administrator.

Registry Permission Changes

During installation, `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mitel\SEC` and subkeys are created. The installer modifies the registry permissions on the created keys to be full control.

Share Points and Permissions

Assuming a complete installation is done, the share points listed in Table 1 Share Points and Permissions are created.

Note: Share names ending with a "$" are hidden share points. The subdirectory column refers to the subdirectory under `\<installation dir>\MiCC Enterprise`.

Table 1: Share Points and Permissions

SHARE NAME	PURPOSE	SUBDIRECTORY	PERMISSIONS		
			SET BY INSTALLATION		REQUIREMENTS
			SHARE	NTFS	
NextCCClient	MiCC Enterprise Client Installation file.	`\Client Installation`	Read	Default	Read for all users needing to install the MiCC Enterprise Client.
NextCCLocalizationFiles	Localized GUI files and voice prompts.	`\Localization`	Read	Default	Read for all users needing to install the MiCC Enterprise Client with localized files.
ScriptManager	Script Manager Client installation directory. Used by MiCC Enterprise Client installation.	`\SMClientInstall`	Read	Default	Read for all users needing to install the MiCC Enterprise Client.
UpdateInstall	Storage of auto-update hotfix files.	`\Update Install`	Read	Default	Read for all users with the MiCC Enterprise Client installed.
CCAData$	Storage of MiCC Enterprise Agent client signature	`\Services\CCA Data`	Read/Change	Everyone Full Control	Read/Change for all users running MiCC Enterprise Agent

SHARE NAME	PURPOSE	SUBDIRECTORY	PERMISSIONS		
			SET BY INSTALLATION		REQUIREMENTS
			SHARE	NTFS	
	files.				
NCEmail$	Temporary storage location for e-mail attachments. An alternate location can be specified in Configuration Manager	\Services\NCEmail	Read/Change	Everyone Full Control	Read/Change for Agent Service account.
NextccReport$	Storage of reports generated in Report Manager.	\Services\Report	Read/Change	Everyone Full Control	Read for all users running Report Manager. Read for Report Web Service account (Default: Network Service set in IIS App Pool). Read/Change for Report Service account.
SeCRecord$	Storage of recording files generated by MiCC Agent.	\Services\SeCRecord	Read/Change	Everyone Full Control	Read/Change for Agent Service account and MiCC Agent Service account.
SeCLogo$	Storage of customer logo files.	\Services\SeCLogo	Read/Change	Everyone Full Control	Read/Change for all users running MiCC Agent. Read/Change for Configuration Service account.
SeCGreeting$	Storage of agent personal greeting files.	\Services\SeCGreeting	Read/Change	Everyone Full Control	Read/Change for Agent Service and Configuration Service accounts.
N/A	Storage of all server based log files. Folder is not shared.	\Services\Bin\Log	N/A	Everyone Full Control	Read/Change for all service accounts and web service accounts including Network Service and Local Service.

Default TCP and HTTP Ports

Please see the document MiCC Enterprise Port Numbers for a complete list of ports used in MiCC Enterprise. These values can be modified through the Setup utility.

CLIENT INSTALLATION

User Rights

To install, the logged on user must be a local administrator.

Registry Permission Changes

During installation, `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mitel\SEC` and subkeys are created. The installer modifies the registry permissions on the created keys to be full control.

NTFS Permission Changes

If Script Designer is installed, the NTFS permissions on the `\Program Files\Mitel\MiCC Enterprise\ScriptManager\Config` directory are set to full control. This is necessary to allow the scripts to be compiled while logged on as a normal Domain User.

Share Points

None

SMS GATEWAY

The following section provides a description of the most common errors related to SMS, and the possible solutions. It also explains how the SMS messages will be handled when some components are not available.

GSM modem does not work after configuration

Check the Enterprise License Manager that GSM modem port licenses are installed, and not both SMS-C and GSM modem port licenses.

If after adding a GSM modem to the configuration, you are not able to activate a Service Access with the modem address, it is possible that the COM port is not configured correctly. Check the smsgsvc.log file in `<InstallDir>\log` directory for the following message:

GSM-Modem:COM1 for Address=17141112222,SCA=+9703769301 open failed, cause=reset modem failed 'COM1:':{}

Use the SMS Gateway Configuration application to set the correct COM port. Make sure the GSM modem is connected to the configured COM port.

If the modem is still not working, unplug the power supply from the modem. Wait for one minute and plug the power supply back to the modem.

If the modem is still not working, restart the SMS Gateway Service from the Control Panel Services applet. Reboot the machine if it still fails.

Unable to send or receive SMS messages

There are conditions that could cause the SMS Gateway unable to send or receive SMS messages. Following is a check list to ensure the SMS function is working properly.

1. Make sure the Enterprise License Manager is installed and can be accessed from the SMS Gateway server. At least one of the SMS licenses must be installed. Check the smsgsvc.log file for one of the following messages

   For GSM modems, you should see the following message (“New=” indicates the number of modem port licenses installed). If you see the “SMS Site license is enabled”, make sure the SMS-C license is removed before continue.

   SMS GSM-Modem license is enabled, LicenseNum{Old=0,New=4} For SMS-Center (SMPP Server), you should see the following message:

   SMS Site license is enabled

   The following message indicates that licenses are not installed, or the SMS Gateway Service is having problems reading the licenses:

   SMS license is not available

2. Make sure the Database Connectivity is configured properly

The SMS Gateway Server reads and archives unanswered SMS messages for fault recovery. Check the smsgsvc.log for the following message:

Error At connect:SQLConnect Cause{[Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'smsuser'., NativeError=18456, SQLState=28000}"

If this error appears, use the SMS Gateway Configuration application to reconfigure the database settings (Login Name and Pass word).

3. Make sure the Listening port is configured properly

The SMS Gateway Server opens the listening port for client appli- cations to receive and send SMS messages. Check the smsgsvc.log for the following message to ensure there is no conflict with the default port (the default port is 2770):

Created a client listener on port=2770

The following messages indicate a successful connection to the SMS Gateway Configuration service:

Connected to config server <MachineName>:2771
Received response: { GetSystemParamResponse: CmdLen=28,SeqNo=1,CmdStatus=0,CmdVer=0} Received response: { GetNodeByHostResponse: CmdLen=78,SeqNo=2,CmdStatus=0,CmdVer=0} Received response: { GetSMSGInfoResponse: CmdLen=68,SeqNo=3,CmdStatus=0,CmdVer=0} Received response: { GetModemInfoResponse: CmdLen=148,SeqNo=4,CmdStatus=0,CmdVer=0}

4. Make sure the GSM Modem is configured properly

If you are using GSM modems, check the smsgsvc.log for the following message to confirm that the GSM modems are properly configured:

[0]Loaded
GSM-Modem:{Addr=17141112222,ComPort=,SCA=+1907831930
1, BaudRate=38400}
[1]Loaded
GSM-Modem:Addr=17146866109,ComPort=COM1,SCA=+19703
769301, BaudRate=38400}

You should see one message for each GSM modem configured. If this message is not displayed, use the SMS Gateway Configuration application to modify the GSM modem configuration.

5. Make sure the Client can connect to the SMS Gateway Server

Check the smsgsvc.log for the following message indicating a successful connection from the client:

New Client connected:1

6. Make sure the SMS Address is configured correctly

   Check that the SMS address configured in Script Manager or Configuration Manager matches the one configured in the SMS Gateway Configuration application.

7. Make sure the Network signaling is working properly

   If the modem is unable to send messages, it is possible that the GSM modem is not able to receive/transmit signals from the network. Unplug the modem and relocate the modem to a different location with a stronger network signal. Check the LED indication on the modem for the signal strength. Check the smsgsvc.log for the following message:Error: Submitsm GSM-Modem:COM1 for Address=17141112222,{SubmitSMS: SeqNo=2,Ext=0,Cross-refId=5,RefSMSId=0,ESMClass=0,ProtocolId=0,Data- Coding=0,Msg(Def=0,Len=9,***), Src(Addr=17141112222,TON=0,NPI=0),Dest(Addr=17142229999 ,TON=0,NPI=0)} cause=bind error:unexpected character in PDU handshake{}

Receive incoming SMS messages but cannot send outgoing messages

If the system can receive SMS messages but cannot send outgoing messages, it is possible that the Service Center Address is not configured correctly. Use the SMS Gateway Configuration application to check if the Service Center Address is correct. Check with your service provider for the Service Center Address.

MiCC Enterprise Router Service is not running

The SMS Gateway Server will retrieve the unanswered SMS messages as soon as the Router Service is running and the Service Access is activated. The SMS Gateway Server will retain the SMS message in the SMS Gateway database until the maximum time has been exceeded. The maximum time is defined in the SMS Gateway Configuration. The SMS message will be discarded after the maximum time even if a reply has not been sent.

MiCC Agent sends new SMS message when the SMS Gateway is not running

MiCC Agent disables the ability to send new SMS messages if the SMS Gateway is down or the GSM modem defined for the SMS Service Group is not available. If MiCC Agent sends a SMS message before detecting such an error, the SMS message will be queued by the Router Service until the GSM modem or the SMS Center is available. The system will periodically try to send the message, based on the interval defined in the Router registry value “ServiceReconnectIntv”. The number of attempts is defined in Configuration Manager, in the System Properties/Queue Handling/Callback Options/Maximum number of attempts parameter.

If the message fails to be sent out after the configured number of attempts are made, the message will be discarded. An alarm will be generated in the Information Manager Alarm Log. A Call Detail Record will be generated if this message is a reply to an incoming SMS message.

If the modem is unavailable after a send request is received by the SMS Gateway Server, the SMS Gateway Server will continuously attempt to reconnect to the modem. If the SMS Gateway Server is still unable to send the message within the time interval (as defined in the SMS Gateway Configuration application), the SMS message will be discarded. This will be logged as an error in the CDR log and an alarm will be generated in the Information Manager Alarm Log.

Customer sends SMS messages but SMS Gateway Server is not running

The SMS Gateway Server will receive the message as soon as the SMS Gateway Service starts up and a Service Access is activated with the corresponding SMS Address.

Router Service stops while SMS messages are in the Service Group queue

If the Router Service is stopped while there are SMS messages waiting in the service group queue, all the SMS messages in the queue will be retained in the SMS Gateway database. As soon as the Router Service starts and the service access is activated for that SMS address, the SMS messages will be immediately sent to the queue. If the maximum wait time, as configured in the SMS Gateway Configuration application, is exceeded, the message will be discarded.

If an agent receives a SMS message and has not yet replied, the SMS message will be removed from MiCC Agent. It will later be reallocated when the Router Service starts and the service access is activated.

SMS Gateway keeps disconnecting from SMS Center

Make sure the Status Check Interval in the SMS Gateway Configuration (SMS Center) is set correctly. This value should be less than the time out value from the SMS Center. Check with your service provider for the time out value. For example, if the time out value from the SMS Center is 30 seconds, the Status Check Interval should be set to 20000 ms (20 seconds). A heartbeat every 20 seconds to the SMS Center will prevent the disconnection in case of inactivity.

WINDOWS ERROR REPORTING

When using Windows Server 2012 or Windows 7 it is possible to configure the system to store local dumps instead of sending the application crash dumps automatically to Microsoft.

ENABLE WINDOWS ERROR REPORTING

Prerequisites

You must be logged in as a local administrator.

Configuration

- Go to Windows registry and locate the following key:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps
  ```

- Change the value of the following items:

NAME	DESCRIPTION	EXAMPLE
DumpFolder	Path to store the dump file	c:\drw
DumpCount	Maximum number of dump files to store in the folder	0x0000000a(10)
DumpType	Type of dump to create * 0: Custom Dump * 1: Mini Dump * 2: Full Dump	0x00000002 (2)
CustomDumpFlags	Custom dump options to be used. This value is used when DumpType=0	0x00000000

Note: Change the DumpFolder path to a local folder where everyone has write access.

Refer to Microsoft Windows Error Reporting for a complete desription of the different dump types