A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise

Initial Configuration

Release 9.7
Document Version 1.1

August 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

This document describes the MiContact Center Enterprise and the MiContact Center Enterprise Network Operations (MiCC Enterprise NOC) setup programs, as well as various other configuration settings for the MiCC Enterprise system.

MICC ENTERPRISE SETUP

The MiCC Enterprise Setup program is the utility used to:

- Add alternate service locations for MiCC Enterprise services
- Add alternate MiCC Enterprise Systems
- Update Broker Location
- Update the Call Manager type
- Update the account used for client installations
- Update CMG Directory integration settings
- Update Telepo Directory integration settings
- Update Database Settings
- View Defined Tenants
- Copy the localization source files
- Update Script Manager Applications
- Update Script Manager nodes
- Update TCP/IP and Http/Https port settings
- Start/stop MiCC Enterprise services
- Update the SMS Gateway Server location
- View and Update the tenant ID for client applications
- Update the web server location

To access the features offered by the MiCC Enterprise Setup utility, the user must log on as a Local Administrator of the machine where the MiCC Enterprise component(s) are installed; additionally, the user must be defined as a domain user of the domain where the machine is currently logged on.

LAUNCHING THE MICC ENTERPRISE SETUP UTILITY PROGRAM

You can launch the MiCC Enterprise Setup Utility from the Windows Start menu (**Start** -> **Programs** -> **Mitel** -> **MiCC Enterprise**).

ADDING ALTERNATE SERVICE LOCATIONS FOR MICC ENTERPRISE SERVICES

1. Select **Alternate Service Location**.
2. From the **Tenant** drop-down list, select any of the defined tenants for the system. Each of the MiCC-E services that register with the Broker Service are displayed in the Services list.
3. Enter an alternative name for any of the services in the **Location** text box. To apply the same value to all of the displayed services, press the **Apply to All** button.
4. Click **OK** or **Apply** to save your changes.

When client applications connect to the MiCC-E Broker Service to request the location of other services, the entered alternate service location will be provided, if defined. Otherwise, the machine name that the service registered with will be provided.

ADDING ALTERNATE MICC ENTERPRISE SYSTEMS

5. Select **Alternate Systems**.
6. Click **New System**. Enter a user defined name for the system, and the machine name or IP address of the Web Server and Broker machine for that server. Also enter the Broker Port.
7. Click **OK** or **Apply** to save your changes.

Users defined as Host Administrators and logged on to Configuration Manager, Report Manager or Information Manager will be able to connect to any of the MiCC Enterprise systems listed. The current logged on user must exist in the alternate system with the same user name and password. If the user was logged on using single sign-on and a password has not been defined for the user, logging onto an alternate system will not be available.

UPDATING BROKER LOCATION

1. Select **Broker Location**.
2. Enter the machine name of the new Broker Server and port number.
3. Click **OK** or **Apply** to save your changes.

Note: Changing this option will apply to all local applications and services. If Setup is run on the broker machine, only the port number can be changed.

UPDATING CALL MANAGER TYPE

1. Select **Call Manager Integration**.
2. Enter the type of Call Manager. Select Open Application Server (OAS) if OAS is used to connect to the Call Manager (i.e. MX-ONE). Select Telephony Application Service (TAS) if TAS is used to connect to an alternate Call Manager.
3. Click **OK** or **Apply** to save your changes.

Note: Changing this option will require a restart of all MiCC Enterprise services. If TAS is selected, all Call Manager data must be defined in MiCC Enterprise Configuration Manager. Consult the Configuration Manager Online Help and the TAS Integration Guide for more details.

UPDATING CLIENT INSTALLATION ACCOUNT

Client Installation Account will be enabled only if the local PC is installed with the Broker Service.

1. Select **Client Installation Account**.
2. During the installation of MiCC Enterprise, which includes the Broker service, a client installation directory is setup which allows client PCs to install from a share point on the server machine using default parameters. The client installation may run under a specified account with administrator privileges allowing installation that would not normally be possible under a restricted account. The ClientSetup.ini file contains all settings to be used during client installations and upgrades. Any settings changed on the clients will be overridden by the ClientSetup.ini settings during upgrades. Ensure that the ClientSetup.ini settings are correctly configured to properly connect to the applicable servers.
3. **File name**. Select the ClientSetup.ini file to update. By default, this points to the ClientSetup.ini file located on the default share point created during the server installation.
4. In the **Domain\UserName** text box, enter a Windows user account that has administrator privileges on the local client PCs.
5. In the **Password** text box, enter the password of the Windows account. The password will be encrypted and stored for use by the client installation in the Client Installation folder located on the MiCC Enterprise server.
6. In the **Customer ID** text box, enter the customer ID used for Web installations and update operations.
7. In the **Tenant ID** text box, enter the numeric tenant ID. It may be blank for the default tenant.
8. Enable **Use Https for Web Server** if clients are to use the https protocol when connecting to any application on the Web server.
9. Enable **Use SSL for Native** Security if clients should use SSL when connecting to native back-end services.
10. Select the **WCF Client Protocol** clients should use when connecting to WCF services on the server.
11. In the **Default Features** list, select the features that are to be selected by default during the client installations.

    Note: If a `ClientSetup.ini` file is being used other that the one located in the `Client Installation` folder, it will not be updated. Refer to document *Installation Preparations* for further information on setting up client installations.

12. Click **OK** or **Apply** to save your changes.

UPDATING CMG INTEGRATION

Note: **CMG Integration** will be enabled only if the local PC is installed with the Broker Service.

1. Select **CMG Integration**.
2. Check **Enable CMG Integration** to configure a CMG server for directory integration with MiCC Enterprise.
3. Enter the name that will be displayed to agents for the directory in the **Display Name** text box.
4. If you are using HTTPS to connect to CMG, check the **Connect to CMG with HTTPS** checkbox.
5. Enter the machine name or IP address and port number of the machine running the AnA web services and the CMG services.

   Note: These fields correspond to the machines where the AnA web services and CMG services are running. They can be the same or separate machines.

6. Enter the user ID and password that will be used to authenticate and access the CMG directory data by the MiCC-E agents.

   Note: If you would like to enter unique CMG logon credentials for each tenant, these can be entered in Configuration Manager, on the General tab of Tenant System Properties.

7. Enter the **Server** and **Port** details of the BluStar Server (this allows the system to obtain Agent presence information).
8. Enter the name of the default User Defined Field (UDF) in the **Default UDF** text field. This is the field that will be selected by default as the alternate search field for agents. Agents may override this field with another selected search field.
9. To group directory search results into categories, specify a value in the **Sort UDF** field. When performing a directory search, all search results with a value set in the UDF field designated as the Sort UDF will be displayed in alphabetical order before search results that do not have the Sort UDF field set.
10. Specify a search order for CMG department search results. If you select the **Display CMG Search Order for Dept Search** option, the search results will be displayed as they are configured in the CMG directory (instead of alphabetically) when searching on the department.

    Note: To modify the search and display order for directory entries, change the User Name Format in MiCC-Enterprise Configuration Manager. The search and display order will change to First Name Last Name or Last Name First Name depending on the configured name format.

11. If you would like to define additional search options for the agents, select a MISC field number in the **MISC Search Field** drop-down lists. When the agent presses either Alt-R or Alt-S from the Agent application, a search will be invoked for other CMG directory entries with the same MISC field. For example, if 1 is selected in the **MISC Search Field** list, when the agent enters Alt-R, a search will be performed for all other directory entries with the same MISC1 field defined as the selected directory entry.

12. Click the **Select Search Fields** to launch the MiCC Enterprise CMG Field Setup utility. You can view the list of CMG user-defined fields (UDF) under the Defined UDFs column.

13. Select the UDFs from the **Defined UDFs** column and click the right arrow key to move the UDFs to the **Selected UDFs** column. The selected UDFs will be displayed for all the agents in the **Agent Directory Details**. You can use the up and down arrows next to **Selected UDFs** column to change the display order in **Agent Directory Details**. Note that if you would like all UDFs to display in the **Agent Directory Details**, leave all of the UDFs in the **Defined UDFs** column.

14. To designate particular UDFs as visible only for Attendant Agents, check the **Attendant Only** checkbox for the selected UDF. Checking this option will restrict the UDF so that it is displayed only for Attendant Agents in **Agent Directory Details**, **Column Selection**, and the selection list for directory search columns. This option is only available for CMG MISC fields and the Cordless field.

15. To allow Attendant Agents to update a CMG UDF, check the **Allow Editing** checkbox for the selected UDF. This will allow Attendant Agents to update the UDF value for a CMG directory entry. This option is only available for CMG MISC fields and the Cordless field.

16. Check the **Suppress Display of Fields without Data Defined** option to ensure that UDFs that do not have any associated data are not shown in the Agent Details display**.**

17. By default, moving a UDF from the **Defined UDFs** column to the **Selected UDFs** column affects only the display of UDFs in the **Agent Directory Details**, and not the directory search columns or search results, unless the UDF is marked as Attendant Only. Check the **Hide Unselected Misc Fields from Display and Search** to restrict the MISC fields that are not in the **Selected UDFs** column from displaying in the directory search columns and search results as well.

18. Click **OK** or **Apply** to save your changes.

Note: You must restart the Agent Service for any changes made to the CMG settings to take effect.

To configure the Agent application to use specific directory views as defined in the CMG directory database, add accounts for all MiContact Center agents and Agent users to the CMG database.

Note: The CMG user ID and password must be exactly the same as the user ID and password defined in MiCC Enterprise for the agent or user.

If authentication fails at the CMG server, the globally defined User ID and Password from the MiCC Enterprise Setup application will be used.

If authentication succeeds, each view defined for the agent or user will be displayed as a separate directory option in the drop-down list of the directory dialog. The last selected view will automatically be the default view on subsequent logons for the same user. Only the selected view will be searched when performing a CMG directory search from the Agent application.

Note: To enable searches on multiple CMG databases, additional SQL scripts must be installed on the CMG systems. For further information, please consult the CMG document “CWI Developer’s Guide Basic A.pdf”.

CONFIGURING LINE STATE FOR LDAP DIRECTORY SYSTEMS WITH NO CMG DIRECTORY

The CMG server needs to be installed with BluStar Server, BluStar Web Service and Ana Server.

1. Follow steps 1 to 7 above, but leave CMG Server and Port fields blank

2. Edit the BluStarWeb web service's Web.config file and within the <configuration> section add: <InstallationType>Standalone</InstallationType>

3. On the BluStar Server , in the C:\ProgramData\Mitel\ foilder create a new folder called BluStarWeb-service and in that folder create a file named servicesetting.xml. This file will contain the location of the presence server (server name or IP plus port number). An example if where the presence server is located on a server named PSERVER and port 5062 is used:

```
<?xml version="1.0" encoding="utf-8"?>
<ServiceSettings xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <BluStarServerSettings>
        <PresenceServer>PSERVER:5062</PresenceServer>
        <PresenceUsername>blustarweb@aastra.com</PresenceUsername>
    </BluStarServerSettings>
</ServiceSettings>
```

UPDATING TELEPO INTEGRATION

Note: **Telepo Integration** will be enabled only if the local PC is installed with the Broker Service.

1. Select **Telepo Integration**.
2. Check **Enable Telepo Integration** to configure a Telepo server for directory integration with MiCC Enterprise.
3. Enter the name that will be displayed to agents for the directory in the **Display Name** text box.
4. Enter the machine name or IP address and port number of the Telepo server.
5. If you are using HTTPS to connect to the Telepo server, check the **Use HTTPS** checkbox.
6. Click **OK** or **Apply** to save your changes.

Note: You must restart the Agent Service for any changes made to the Telepo settings to take effect.

7. Additional settings must be defined per tenant before Agents may search the Telepo directory. These settings are defined on the Agent tab of Tenant Properties in Configuration Manager.

UPDATING DATABASE SETTINGS

Database Settings will be enabled only if the local PC is installed with the Broker Service.

1. Select **Database Settings**. The current database settings will be displayed.
2. Update the name of the SQL Server in the **SQL Server Location** text box. If a SQL instance is used, enter the server name followed by the instance name, i.e. SECSQLSERVER\Instance1. Enter the TCP/IP port number to be used to connect to the SQL Server.
3. Specify the SQL account to use for MiCC Enterprise services and applications. If using Windows Authentication, additional steps may be required before and after applying the changes. Refer to the section *Using SQL Windows Authentication with MiCC Enterprise Services and Applications* in the *Installation Instructions* document.
4. After applying the changes, you may be prompted for additional information needed during creation or updating of the database.

DISPLAYING DEFINED TENANTS

1. Select **Defined Tenants**.
2. A list of all tenants defined in the system, and the associated tenant ID will be displayed.

COPYING LOCALIZATION SOURCE FILES

Localization will be enabled only if the local PC is installed with one or more client applications or the Report Service.

1. Select **Localization**.
2. By default, the path of the shared directory on the Broker Service machine is displayed. Click **Browse** to change the path. The **Browse For Folder** dialogue box will appear.
3. Find the files for the language that you want to load and click **OK**.
   The path you selected will now be displayed in the **Source** group box.
4. Click **OK** or **Apply** to copy the files.

Note: It is recommended to have the same Locale settings on the MiCC Enterprise Server and the MiCC Enterprise clients. Otherwise, some text in the MiCC Enterprise applications and reports will appear in mixed languages. Reports are generated by the Report service on the MiCC Enterprise Server and therefore will use the locale configured for the account that the Report service is running under. The computer must support displaying characters int the desired language. In some cases, it may be necessary to install additional language packs in the operating system.

UPDATING SCRIPT MANAGER APPLICATIONS

Define the Script Manager server that Script Designer will use to save compiled scripts.

1. Select **Script Manager Applications**. The current settings will be displayed by default.
2. Enter the new location of the Script Manager Server and click **OK** or **Apply** to save your changes.

UPDATING SCRIPT MANAGER INTEGRATION

Note: Whenever there is a change to the Script Manager Server location, be sure to perform this operation on the MiCC Enterprise server, and all machines that are installed with Configuration Manager or Script Manager client applications.

1. Select **Script Manager Integration**. The current settings will be displayed by default.
2. Enter the new location or add a new Script Manager Server and click **OK** or **Apply** to save your changes.

DYNAMIC PORT NUMBERS

The port numbers are set automatically during installation. All ports must be accessible through the firewall on the local machine or a hardware based firewall. TCP/IP ports must be opened for all traffic. HTTP ports must be open for HTTP traffic. The use of HTTP is not required. For services that support both TCP/IP and HTTP, both ports will be opened for listening. HTTP should be used for external access when possible.

Table 1: OAS Port Numbers

SERVICE	PORT NUMBER – TCP/IP
Daemon	2557
Configuration Service	2558
Start Stop Service	2559
Event Channel Service	2560
Network Resource Manager	2562
Performance Data Service	2651

Table 2: MiCC Enterprise Port Numbers

MiCC Enterprise port numbers can be changed after installation using the MiCC Enterprise Setup Utility.

SERVICE/CHANNEL	PORT NUMBER	
	TCP/IP	HTTP(S)
Broker Service	2600	

SERVICE/CHANNEL	PORT NUMBER	
	TCP/IP	HTTP(S)
Agent Service	2601	
Request Channel	2603	
Consumer Channel	2604	
Status Event Channel	2605	
Activity	2606	
Report Request	2610	
Route Manager Interface	2611	
Real Time Interface	7500	
Campaign Service	2612	12612
Agent Service	2613	12613
Call Control Service	2614	12614
Call Control Service TAS Events	2618	
SMS Gateway Service	2770	
ELM	2580	
Open Media Service		12615
Session Information Service		12620 (http support only)
E-mail Service	2617	12617
Chat Service	2616	12616

Table 3: Script Manager Port Numbers

SERVICE	PORT NUMBER – TCP/IP
Service Router	2750
Debug Router	2751
AppContactCenterServer	2752
AppMediaServer	2753
AppSMSServer	2755
AppDatabaseServer	2756
SQL	1433

UPDATING SERVICE PORT SETTINGS

1. Select **Service Port Settings**. The default values are displayed.

Note: The port number edit box will only be enabled for services installed on the local machine.

2. Modify if necessary.
3. Secure HTTPS traffic may be setup for WCF services. Set the WCF Security option, **Use Https**. HTTPS ports must have a security certificate from a verified Certificate Authority associated to them. This certificate must be installed in the Local Machine Certificate Store prior to enabling HTTPS. Select the **Apply Certificate…** option. You will be prompted for a security certificate that is already installed which will be associated to the current ports. If the ports change after applying a certificate, it must be reapplied. When the certificate expires and a new one is installed, the new certificate must also be reapplied.
4. When changing service settings, ensure that clients are properly configured to connect using these settings. Also ensure that the appropriate ClientSetup.ini files are modified to reflect these settings as during new client installations or upgrades, the current settings on the client may be overridden by the ClientSetup.ini settings.
5. Click **OK** or **Apply** to save your changes.

STARTING AND STOPPING MICC ENTERPRISE SERVICES

Note: This option only appears when Setup is run on the machine where the Broker service is installed. If one or more MiCC Enterprise services are installed on another machine, the user account must have local administrator privilege on the remote machine to start/stop services on that machine.

1. Select **Services**. All installed services, the machine they are running on, and the current status will be displayed.
2. To start or stop services, first select the individual services by checking the box next to the service name or use the **Select All** button to select all services. When the desired services are selected, click **Start Services** or **Stop Services**.

Note: Even if all services start, they might not provide full function until all dependency services are available.

UPDATING SMS GATEWAY SERVICE LOCATION

SMS Gateway Service Location will be enabled only if the local PC is installed with the Router Service or Script Manager Services.

1. Select **SMS Gateway Service Location**. The current settings will be displayed by default.
2. Enter the new location and port number of SMS Gateway Service and click **OK** or **Apply** to save your changes.

It is also possible to configure specific System ID and Password values for SMS numbers or number ranges. This information is used when SMS Gateway is connected to an SMS-C system.

If different numbers are billed to various accounts, it can be helpful to define a separate System ID and Password for each set of numbers. If this is not required, the SMS Configuration application can be used to configure a single System ID and Password for the system.

To configure multiple System ID and Password values for SMS numbers:

1. Select **New System**
2. In the **Details**, enter the System ID and Password for the system. The System ID and Password can each be a maximum of 50 characters, but the value should be based on the max characters accepted by the SMS-C that the SMS Gateway will be connected to.
3. Select **New Range**
4. Enter a single number, or a range of numbers in the **From** and **To** fields. Select the entry from the **System** drop-down list that corresponds to the System ID and Password that should be used for the number or number list. When the Router or Script Manager clients attempt to monitor the SMS number, the configured System ID and Password will be sent to the SMS Gateway.

DISPLAYING AND UPDATING THE TENANT CLIENT

Tenant Client will be enabled only if the local PC is installed with client applications.

1. Select **Tenant Client**.
   The current setting will be displayed by default.
2. To change the Tenant that will be associated with client applications, launch the MiCC Enterprise Tenant Client Utility application by clicking **Launch Tenant Client Utility**.
3. The **MiCC Enterprise Logon** dialog will be displayed. To use the utility, you must logon as a Host Administrator user. Enter the logon user ID and password.
4. If the logon ID is authenticated, the Tenant Client Utility application will appear. Select the Tenant you wish to associate with client applications. Once updated, users will only be allowed to view data for the associated tenant.
5. When the tenant is updated, click **Refresh** to display the updated data in the Tenant Client tab.

UPDATING WEB SERVER LOCATION

Web Server Location will be enabled only if the local PC is installed with a client application.

1. Select **Web Server Location**.
2. Enter the new location and port number of Web Server Location.
3. If you would like to use secure HTTPS traffic when connecting to the IIS Web Server, check the box **Use Https**. HTTPS support must be enabled on the IIS Web Server for the default web site.
4. If you would like to use HTTP or secure HTTPS traffic instead of TCP/IP when communicating with the server WCF services, set the **WCF Client Protocol** option. For HTTPS traffic, the ports must be setup for HTTPS on the server through the Service Port Settings page.

5. Click **OK** or **Apply** to save your changes.

MICC ENTERPRISE NETWORK OPERATIONS CENTER SETUP

The MiCC Enterprise Network Operations Center setup utility is used for:

- Centralized Management
- Update Broker Location
- Update Client Installation Account
- Update Database Settings
- Copy the Localization Source Files
- Update Service Port Settings
- Start and Stop MiCC Enterprise Network Operations Center Services
- Update Web Server Location

To be able to launch the MiCC Enterprise NOC Setup utility, the user must be a Local Administrator of the machine where the MiCC Enterprise NOC component(s) are installed. The user must also be defined as a domain user of the domain that the machine is a member of.

LAUNCHING THE MICC ENTERPRISE NETWORK OPERATIONS CENTER SETUP

The setup utility is launched from the Start menu.

CENTRALIZED MANAGEMENT

Centralized Management is used to add managed MiCC Enterprise system(s), and to change existing ones. The parameters that can be added or changed are:

- System Name
- Web Server
- Web Server Port
- Broker Location
- Broker Port
- Activation or deactivation of the system

It is also possible to select:

- To save or not save Call Data Record
- Updating interval for the Centralized Database

UPDATING BROKER LOCATION

Enter the new location and the Broker Port and click **Apply** in the MiCC Enterprise NOC setup program to update the Broker Location.

Note: Changes to the Broker Location will apply to all local applications and services. If the Setup application is run on the broker machine, only the port number can be changed.

UPDATING CLIENT INSTALLATION ACCOUNT

Updating of the Client Installation Account is enabled only if the local computer is installed with the Broker Service.

1. Enter the Windows user account name in the **Domain\UserName** text box. The account must have administrative privileges on the local clients.
2. Enter the Windows account password in the **Password** and **Verify Password** text boxes. The password will be encrypted and stored for use by the client installation in the **Client Installation** folder located on the MiCC Enterprise server.

Note: If a `ClientSetup.ini` file other than the one located in the Client Installation folder is being used, it will not be updated. Refer to document *Installation Preparations* for further information on setting up client installations.

UPDATING DATABASE SETTINGS

Updating Database Settings will be enabled only if the local computer is installed with the Broker Service.

1. Enter the name and port number of the new SQL Server. If an SQL instance is used, enter the server name followed by the instance name, i.e. **SECSQLSERVER\Instance1**.
2. When any of the SQL Server fields have been modified, the Setup program will attempt to connect to the new SQL Server. If an existing database is found, you will be asked if you wish to recreate the database or retain the existing database.

Note: MiCC Enterprise NOC requires a MiCC Enterprise NOC database. If the existing database is a MiCC Enterprise database, the Setup program ends and a message stating that “The selected database is not a MiCC Enterprise NOC database” is displayed.

COPYING LOCALIZATION SOURCE FILES

Localization will be enabled only if the local PC is installed with one or more client applications or with the Report Service. By default, the path displayed represents the path of the shared directory on the Broker Service machine.

1. Click **Browse** to locate the files for the language to load.
2. Select the files and click **OK**. The path selected will be displayed in the **Source** field.
3. Click **OK** or **Apply** to copy the files.

UPDATING SERVICE PORT SETTINGS

Updating Service Port Settings will be enabled only for services installed on the local machine. The values that appear in the setup program are the default values.

STARTING AND STOPPING MICC ENTERPRISE SERVICES

Starting and stopping MiCC Enterprise NOC services is enabled only when the Setup program is run on a machine that is installed with the Broker Service. If one or more MiCC Enterprise NOC services also are installed on another machine, the user account must have Local Administrator privileges on the remote machine as well to start and stop services on it.

The services installed, their current status and the machine they are running on are displayed in the Setup program.

Note: Even if all services start, they might not provide full function until all dependency services are available. Refer to *MiCC Enterprise System Description* for further information on dependencies.

UPDATING WEB SERVER LOCATION

Updating Web Server Location will be enabled only if the local computer is installed with client applications.

CONFIGURE REPLICATION AT PRIMARY MICC ENTERPRISE SERVER

1. Run SQL Enterprise in the primary MiCC Enterprise server.
2. Go to **Tools, Replication** and **Configure Publisher, Subscriber and Distributor**.
3. Select the **primary MiCC Enterprise** server as **Publisher and Distributor**.
4. Select the **backup MiCC Enterprise** server as the **Subscriber**.
5. Go to **Tools, Replication** and **Create and Manage Publications**.
6. Select **Nextccdb** as the database and **Create Publication**.
7. Select **Snapshot Publication**.
8. In the **Specify Articles** wizard, select **Publish All Tables**.
9. The following tables should be unselected:

   oas_language_param
   oas_server_param
   script_manager_node
   service_access
   service_access_menu
   site_access_map_code
   site_server_param
   system_param
   tenant_oas_server_param
   tenant_param
   tenant_sm
   acs_language
   acs_playmessage
   acs_playmessage_list
   acs_playmessage_param
   acs_queue

10. **Click Article Defaults,** Table **Articles** and **Snapshot**.
11. Select **Delete all data** in the existing table.
12. Select **Include declared referential integrity**. Leave the rest as default.
13. Click **Next**, and finish the wizard.
14. Click **Push New Subscription**.
15. Select **Backup MiCC Enterprise Server** as the **subscribers**.
16. Leave the rest as default and click **Next** to finish the wizard.

STARTING THE INITIAL REPLICATION

1. Go to **Replication Monitor**, **Publishers**, and **Primary MiCC Enterprise Server Name.**

2. Click **nextccdb:nextccdb**.
3. Right click **Snapshot** and select **Start Agent**.
4. Right click **Push Subscriber** and select **Start Synchronization**.

Note: Changes to the primary MiCC Enterprise server will not be automatically replicated to the backup server. Changes to the Service Access at the primary server will have to be replicated to the backup MiCC Enterprise server manually by backing up MiCC Enterprise and Script Manager configurations, and restoring the data in the MiCC Enterprise backup server.

OPTIONS FOR SETTINGS OF QUALITY OF SERVICE

It is possible to configure the Agent softphone to tag its transmitted IP packets, and in some configurations also its Ethernet packets, with Quality of Service (QoS) information.

Differentiated Services (DiffServ) is common for all cases. The softphone can be made to tag its transmitted voice packet with a Differentiated Service Control Point (DSCP).

Table 4: Overview - Settings of Quality of Service

PREREQUISITES	MEANS OF CONFIGURATION	EFFECT
SIP softphone on **Windows 10 and 11** clients	Use standard Windows tools to define a group policy for network QoS tagging. Typically, such policy is tied to the executable (i.e. NowSoftphone.exe) and protocol specifics like UDP transmissions and a range of ports.	Through mechanisms in the operating system, softphone transmissions will be tagged with QoS information according to the group policy.

HOW TO SET QUALITY OF SERVICE

The following descriptions are examples of how to set the QoS for the Agent application. QoS can be set on a computer or user group basis, depending on what suits your system configuration.

Note: Remember to configure the IP router according to the QoS settings. For more information regarding QoS, see Microsoft documentation, for example www.microsoft.com and http://technet.microsoft.com.

SIP on Windows 10 or 11 using the Local Group Policy Editor

To specify QoS from the **Local Group Policy Editor**, do the following:

1. Run **gpedit.msc**, from the **Start** menu.
2. Under Windows Settings, create a new **Policy-based QoS**. A wizard opens in which you specify the QoS.
3. Name the policy, specify the **DSCP value** according to the IP router preferences and click **Next**.
4. Set the QoS policy to apply to the files **Agent.exe and NowSoftphone.exe** and click **Next**.
5. Set the QoS policy to apply to any **source IP address** and any destination **IP address** and click **Next**.

6. Set the QoS policy to apply to **UDP.**
7. Set the source port number **From any source port.**
8. Set the destination port number **To any source port** and click **Finish**.

Note: The computers involved must be members of an Active Directory domain.

SIP on Windows 10 or 11 using Active Directory

To specify QoS from the **Active Directory**, do the following:

1. Open **Group Policy management** from the **Start > Administrative Tools** menu.
2. Create a **Group Policy Object**. Set the appropriate Group.
3. Right click and choose **Edit** to open the **Group Policy Management Editor**.
4. Create a QoS policy either in **User Configuration > Windows setting >Policy-based QoS** or in **Computer Configuration > Windows setting >Policy-based QoS**
5. Create a new **Policy-based QoS**. A wizard opens in which you specify the QoS.
6. Name the policy, specify the **DSCP value** according to the IP router preferences, and click **Next.**
7. Set the QoS policy to apply to the files **Agent.exe and NowSoftphone.exe** and click **Next.**
8. Set the QoS policy to apply to any **source IP address** and any destination **IP address** and click **Next**.
9. Set the QoS to apply to **UDP**.
10. Set the source port number **From any source port.**
11. Set the destination port number **To any source port** and click **Finish.**

Note: The computers involved must be members of an Active Directory domain.

AUTOMATIC LOGON TO MICC ENTERPRISE APPLICATIONS THROUGH WINDOWS USER ID

It is possible to configure the MiCC Enterprise applications to logon automatically, with the user's Windows logon ID and password.

To configure this feature, the following steps must be executed:

1. Run MiCC Enterprise Configuration Manager and ensure that the defined MiCC Enterprise Logon ID for the user matches the Windows Logon ID that will be used on the client workstation. It is not necessary for the Password to match.
2. Run the MiCC Enterprise Registry Configuration Application (SeCCfg.exe) on the client machine. From the General Settings tab, check the option "Logon with Windows User ID".

Note: This step must be executed on every MiCC Enterprise client machine that will use the Windows Logon ID to logon to MiCC Enterprise applications.

3. Restart the MiCC Enterprise application. No logon prompt will be displayed. The MiCC Enterprise application (Report Manager, Information Manager, Configuration Manager or Agent) will immediately start up without any prompt.

Note: If Command Line parameters are used to start the MiCC Enterprise application, this will override the Windows Logon ID and the user ID and password entered through the command line will be used to logon the user to the MiCC Enterprise application.

REPORT SERVICE LOGON ACCOUNT

By default, all MiCC Enterprise services run under the LocalSystem account. To enable printing of scheduled reports, the MiCC Enterprise Report Service must run under a designated user account that has access to local and network printers.

To enable printing of scheduled reports:

1. Create a user account in the same domain as the MiCC Enterprise server. The account must have Local Administrator privileges.
2. Logon to the desktop under this account and install any printers that may be used for scheduled reports.
3. Open the Service Control Manager and change the logon settings for the CCReport service to use this account.
4. Restart the CCReport service.

Note: The MiCC Enterprise Report Service uses the locale of the specified user account for formatting characteristics such as date/time formats. To changes the formats that the Report Services uses, logon to the desktop under the user account and modify the regional settings. The Report service will not apply the new settings until it has been restarted.

Note: During upgrades and maintenance operations, the existing logon account for the Report Service is maintained.

USING ENHANCED CHARACTERS IN SERVICE GROUP AND SERVICE ACCESS NAMES

It is now possible to include non-alphanumeric characters, including @&|#%?!$*£+<>/\()[]{} in the names of MiCC-E configuration items, including service groups.

If the integrated call recording feature for the MiCC Agent softphone is used, the following characters should not be included in the names of service groups used for voice calls: : \ / : * ? < > | “

These characters are not valid as part of a file name, and the service group name is used to create the file name for the recorded file. If these characters are used in the service group name, the recorded file will not be created.

If you use the Service Access Properties dialog to modify the Service Access Name then the above mentioned characters must also be avoided since it will prevent the creation of the .dat file for the Service Access.