Mitel MiContact Center Enterprise

RELEASE 9.5 SP3

NOTICE

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.

TRADEMARKS

MiContact Center Enterprise – New in Release 9.5
Release 9.5 SP3 – April 2022

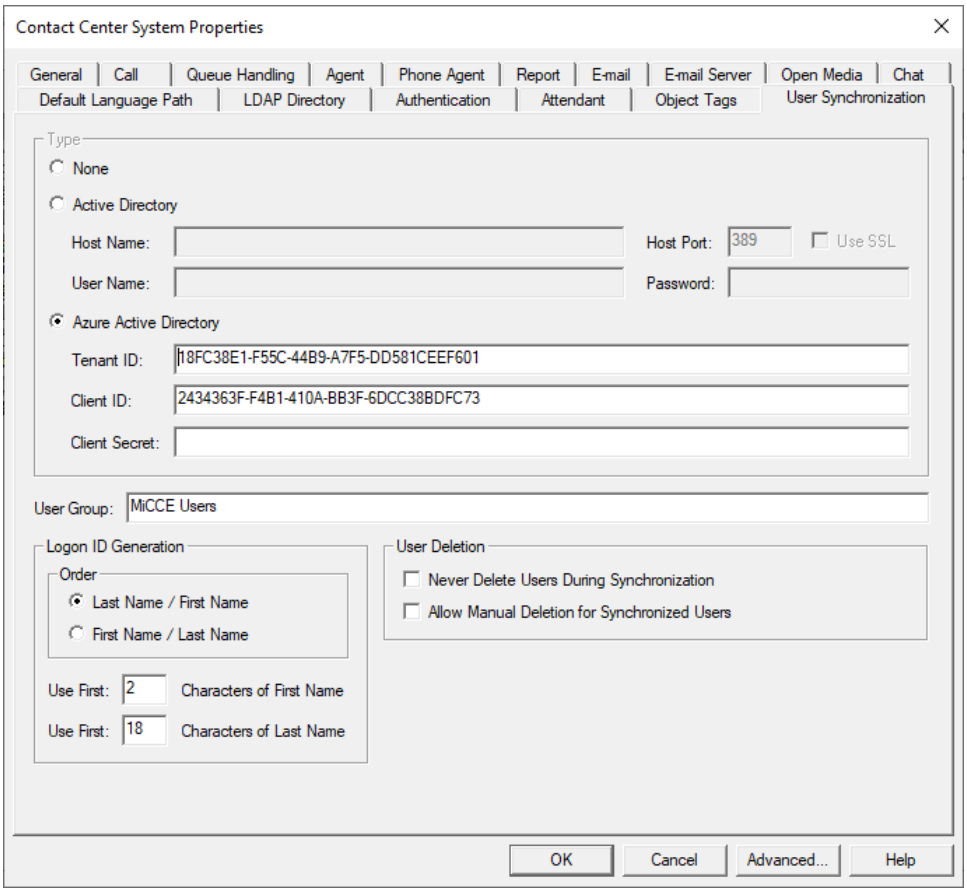
INTRODUCTION

This document describes new features introduced in Mitel MiContact Center Enterprise, TAS and OAS 9.5.

MiContact Center Enterprise is an All in One, adaptive and flexible platform for UC&C, Mobility, Contact Center, Business Process Automation, Analytics and reporting as well as service and database integration. Release 9.5 continues to build on adding value for customers by providing targeted features enhancing the agent and customer experiences.

USER SYNCHRONIZATION WITH AZURE ACTIVE DIRECTORY AND ON-PREMISE ACTIVE DIRECTORY

Automatic user synchronization has been added providing synchronization between Azure Active Directory or standard on-premise Active Directory. A connection to AD is established through the MiCC Agent Service and users are retrieved from the specified user group. Users are added, updated or deleted in MiCC Enterprise as necessary.



Scheduled synchronization is performed daily at a specified time for all tenants. Synchronization should be performed during off-peak hours when possible. The default time is midnight 00:00. This may be configured on the MiCC Agent Service tab in the MiCC Enterprise Registry Configuration application. Scheduled synchronization may also be disabled. Manual synchronization may be invoked by running the following command:

<InstallDir>\Services\Bin\AgentService.exe /adsync

New users will be assigned to the <Default> agent group and user type. Users will not have permission to run any application. An Administrator must assign the correct user type to each user.

The logon ID for new users will be generated using a specified number of characters from the first and last names. If a user already exists with that logon ID, a number will be appended to the logon ID until an available logon ID is found. For example, ksharp1, ksharp2, etc. If the generated logon ID for any user is unwanted, an Administrator may change the logon ID through Configuration or Web Manager. Subsequent synchronization for the user will not update the logon ID.

The password for new users will be blank. Users without a password may only be logged in using the Single Sign-On process. A password must be added through Configuration or Web Manager in order for the user to login using the conventional process.

All information for each user except for the logon ID, password, agent group and user type will be updated for existing synchronized users during the next synchronization.

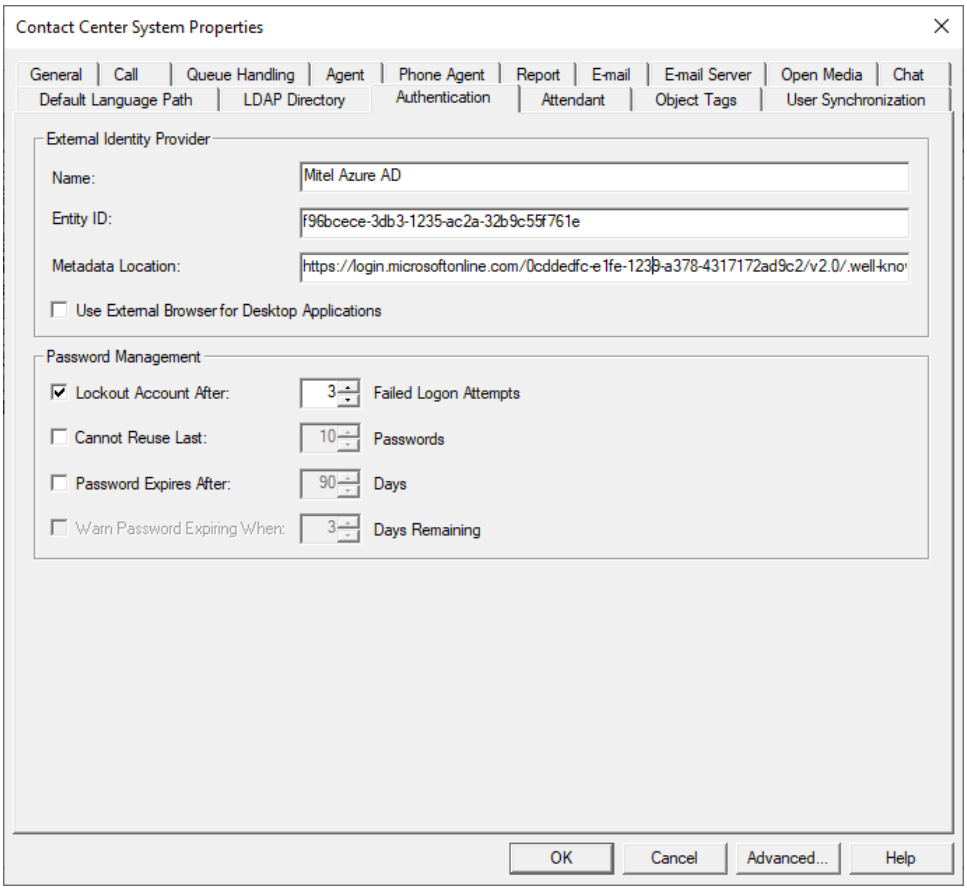
By default, synchronized users may not be manually deleted through Configuration or Web Manager. This may be enabled in the Tenant Properties.

Synchronization may work in conjunction with Single Sign-On described in the next section. The User Principal Name (upn) or e-mail address of the synchronized user is populated into the External Logon ID field for the MiCC Enterprise user. During Single Sign-On, the MiCC Enterprise user is located by matching the External Logon ID to the upn or e-mail address of the authenticated user.

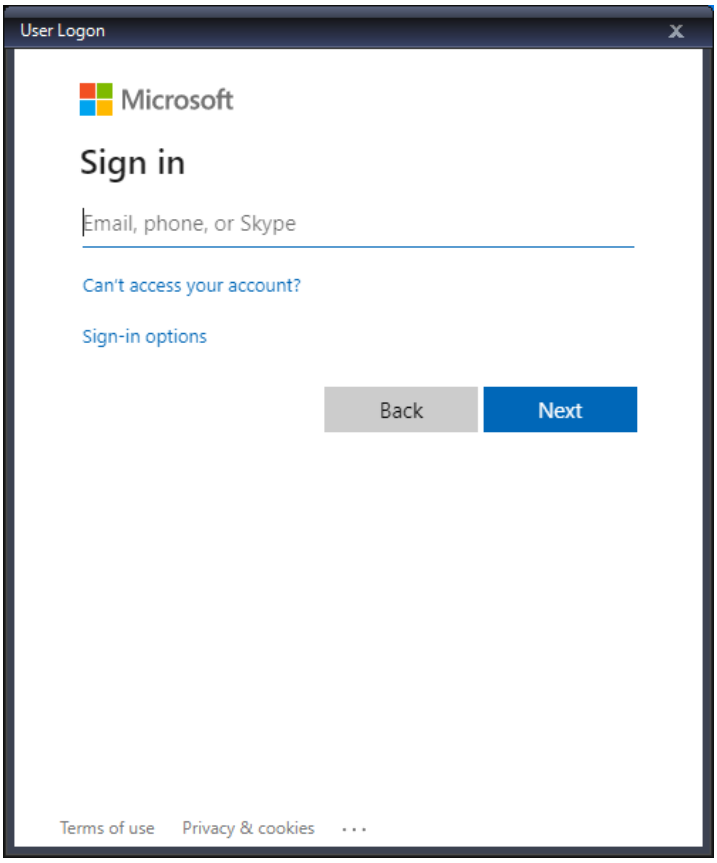
For additional command line parameters specific to each application, see the *User Synchronization* section in the *Advanced Configurations* document.

SINGLE SIGN-ON WITH OPENID CONNECT

Single Sign-On (SSO) has been added for desktop applications allowing login using any External Identity Provider (IDP) that supports the OpenID Connect 2.0 protocol. Single Sign-On allows users to be authenticated outside of MiCC Enterprise where credentials are controlled by the IDP. Users may login using their credentials from sources such as Microsoft Azure AD or standard domains.

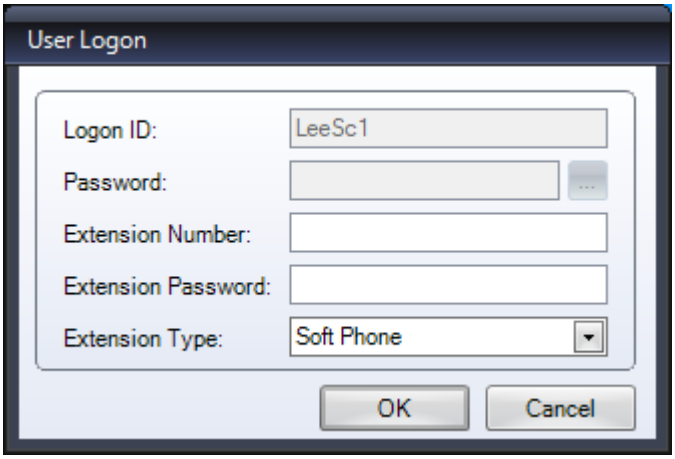


If an External Identity Provider is configured for the tenant, login for desktop applications will be performed using SSO for that provider. SSO is a Web based protocol. The SSO process may be performed through an external Browser or through an embedded browser in MiCC Enterprise. The login process and page content are controlled entirely by the IDP. The following graphic shows the login using Microsoft Azure AD.



After authenticating with the IDP, the MiCC Enterprise user is found by matching the User Principal Name (upn) or e-mail address of the authenticated user against the External Logon ID configured for each MiCC Enterprise user. The External Logon ID is populated during user syncronization if enabled. It may also be manually entered for the user in Configuration or Web Manager.

Once the MiCC Enterprise user is located, additional information may be needed such as the extension when logging into MiCC Agent.



The MiCC Enterprise user has already been determined and the Logon ID and Password will be disabled. This additional prompt may be suppressed by specfiying the necessary information on the command line. For example, MiCC Agent may be started using the following command line:

Agent.exe /extension:1234 /softphone

No further information will be needed after user authentication and the additional prompt will not be shown.

When SSO is enabled for the tenant, conventional login using standard MiCC Enterprise user credentials may be forced by speciying the /stdlogin command line parameter or by holding the SHIFT key when starting the application. Specifying /user and /password command line parameters will always use conventional login.

SSO using OpenID Connect has also been added for the Web applications, Web Manager and Web Agent. In previous versions of MiCC Enterprise, Web Manager supported SSO using the SAML 2.0 protocol along with the configured IDP information. SAML 2.0 is still supported in Web Manager; however, standard IDP configuration will use OpenID Connect. SAML 2.0 may be enabled in the web.config file for the Web Manager application overriding the OpenID Connect information. For additional information on configuring Web Manager to use external authantication with SAML 2.0 see the *External Authentication using SAML 2.0* section in the *Web Applications Configuration Guide* document.

For additional information on configuring and using SSO with OpenID Connect, see the *Single Sign-On* section in the *Advanced Configurations* document.

DESKTOP APPLICATION COMMAND LINE PARAMETERS

Command line parameters have been standardized across all desktop applications. All applications support the following base set of parameters:

/user:<LogonID>

Specifies the user logon ID.

/password:<Password>

Specifies the user password

/webserver<WebServer[:Port]>

Specfies the Web server to use. If Port is omitted, the default port will be used.

/stdlogin

Forces standard logon using MiCC Enterprise credentials when the tenant is configured to use Single Sign-On. Standard logon may also be forced by holding the SHIFT key down while starting the application.

For additional command line parameters specific to each application, see the *Application Command Line Parameters* section in the *Advanced Configurations* document.

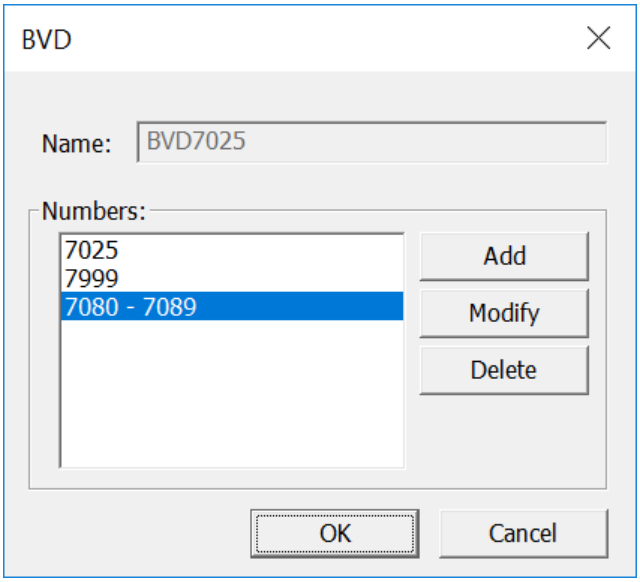
TAS ENHANCEMENTS

NUANCE 11 SUPPORT

Support for Text-to-Speech (TTS) and Automatic Speech Recognition (ASR) using Nuance 11 is now supported with TAS. This allows service group queue messages to be configured with TTS parameters, as well as the use of Script Manager service accesses with ASR and TTS enabled for more advanced scripting.

ABILITY TO ASSOCIATE A BVD WITH A BLOCK OF NUMBERS

TAS now supports the same capability as OAS to monitor a single BVD that corresponds to a block of numbers. When defining BVDs in Configuration Manager or Web Manager, individual numbers or ranges of numbers can be defined. When an incoming call arrives to TAS targeted toward any of the numbers associated with the BVD, events will be generated for the BVD.



DIVERSION BYPASS ON CISCO SYSTEMS

Previously diversion bypass was only supported for MX-ONE call managers. This has been expanded to be supported for Cisco call managers, allowing Attendant Agents to directly dial users with diversion enabled and ring through to the user's number instead of being diverted to the configured destination.

TLS 1.3 SUPPORT

TAS is able to support multiple versions of TLS, up to version 1.3. When starting, TAS will first attempt to use version 1.3. If that is not supported by Windows, it will downgrade to 1.2, 1.1, 1.0, etc. until it reaches the lowest level configured in TAS configuration.

TRANSFERRED SERVICE GROUP CALL HANDLING

When a service group call is transferred, it is now possible for it to continue to be handled as a service group call by the transferred-to agent, instead of being handled as a private call.

If the call is transferred before answer and the transferred-to agent does not answer before the ring supervision timeout, the call will be returned to the service group queue and the transferred-to agent will be forced to voice not ready state.

The Service Group Call Completed event will not be generated until the transferred-to agent completes the call. Call Detail Reporting (CDR) events will be generated for the call at each change in state until it is terminated.

Only the last agent handling the call will be counted as handling a session for the service group. If a call is transferred multiple times, the last agent completing the call is reported as the agent handling the session for the service group. Note that it will be possible for an agent to have a count of 0 Answered Calls in the Agent report, but still have time counted as Voice Busy, if the agent transferred a service group call.

Reports for the service group will calculate Alerting time as the duration of time that the service group call alerted at the first agent. Servicing time will include the time that the first agent spent in Talking state for the call, as well as time that other agents spent in Talking state after the call was transferred to the other agents. Similarly, Hold state will include the time that the first agent had the call on hold, as well as the time that other agents to which the call was transferred had the call on hold. Clerical time for the call will only be the time that the last agent handling the call spent in Clerical state.

Note that callbacks and web callbacks are not able to continue as a service group call after being transferred, since callback status must be entered by the agent performing the callback. If either of these types of calls are transferred, they will be completed when transferred and handled as a private call on the target agent.

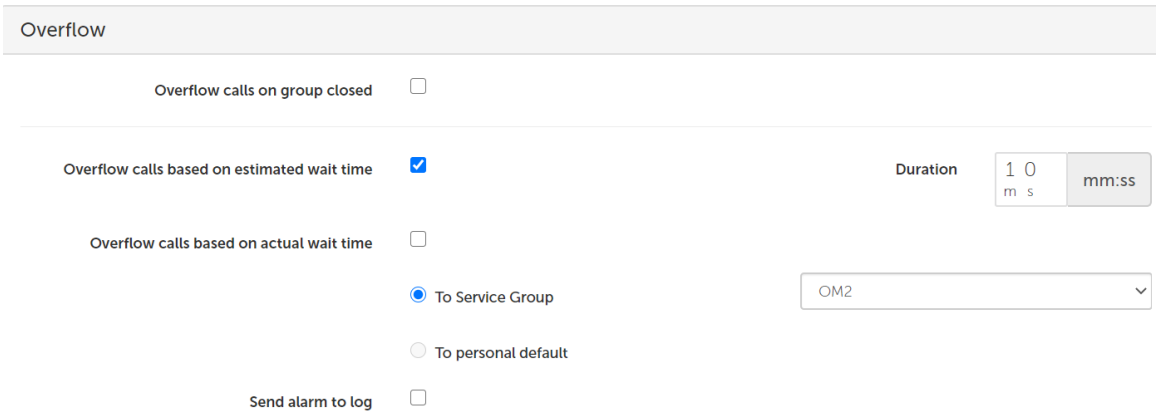
This feature only applies to agents running the Agent application, and not Web Agents or Phone Agents.

OVERFLOW FOR ALL MEDIA TYPES

It is now possible for all types of media, including e-mail, SMS, chat and open media sessions, to overflow to a configured destination. Configuration Manager and Web Manager allow configuration of an overflow destination based on Actual Waiting Time (AWT), Estimated Waiting Time (EWT) or when the service group is closed.

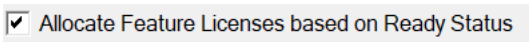
E-mail and SMS service groups can be configured to overflow to another service access or a service group. Chat and open media service groups can be configured to overflow to another service group.

The service group report will indicate that the session overflowed out, and alarms will be generated, if configured, as well as CDR events indicating that overflow occurred.



DYNAMIC FEATURE LICENSE HANDLING

It is possible to configure MiCC Enterprise to allocate licenses for Chat, E-mail, SMS and Open Media based on the agent ready status. An option is added to the MiCC Enterprise Registry Configuration application (SeCCfg.exe) on the Agent tab to set license allocation based on agent ready status:



When this option is set, feature licenses for Chat, E-mail, SMS and Open Media will not be acquired when the agent logs on. Instead, when the agent sets status to ready for the media type, MiCC-E will attempt to acquire a license for that feature. If a license is available, the agent will be allowed to change status to ready for the media type. If no license is available, the agent will remain in not ready state for the media type.

If this option is set, the agent will not be permitted to change status for the media type to not ready unless the agent is no longer handling media sessions for the media type. Exceptions are when the media session is in Clerical state, when the agent logs off, or when a session is rejected due to a ring supervision timeout, and the agent is forced to not ready state for the media type. When the agent sets status to not ready for the media type, the feature license will be returned so that it can be allocated to another agent.

This option applies to both Agent and Web Agent applications.

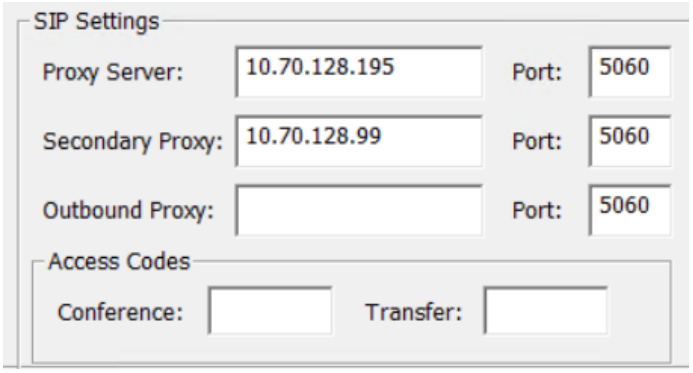
AGENT ENHANCEMENTS

The following enhancements have been added to the Agent application.

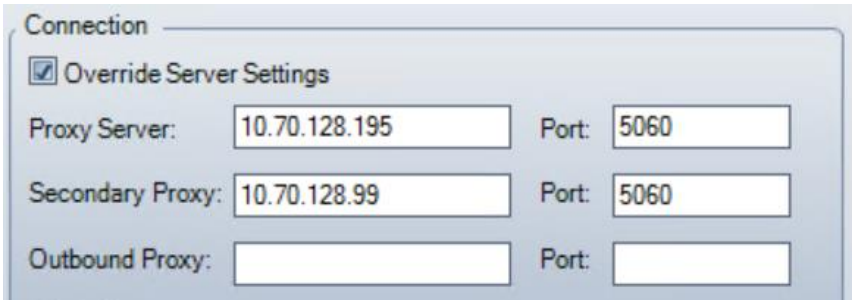
SUPPORT FOR BACKUP SIP REGISTRAR

For agents working in office as well as remote locations, it is now possible to define a primary and a backup SIP registrar. This can also be used for redundancy.

From Configuration Manager, in the Call Manager SIP settings, the Secondary Proxy information can be entered.



In addition, individual agents can override the Call Manager SIP settings in the Agent SIP Options by setting a Secondary Proxy.



If the primary proxy server is not available when Agent starts up, or if it disconnects while Agent is running, Agent will automatically connect to the secondary proxy, if configured.

Note that it is also possible to configure an Outbound Proxy, which can be used to connect to the SIP registrar via a session border controller (SBC). When the SIP softphone registers, it will send the SIP Register request to the address configured in the Outbound Proxy field, but the From and To addresses in the Register packet will be the value entered in the Proxy Server field. This allows the SIP softphone to register to the configured proxy server via the SBC.

IMPROVEMENT IN FOLDER STRUCTURE FOR RECORDED FILES

Previously all agent recorded files were stored in a folder named with the agent's record ID. This made it difficult to directly access all recorded files associated with a particular tenant, which was an issue for multi-tenanted systems.

The folder structure is modified so that the recordings for each agent are now contained in a subfolder under the tenant ID as follows:

Default Tenant – Agent ID 1
\\<AgentServiceMachineName>\SECRECORD$\-1\000001

Tenant ID 1 – Agent ID 2
\\<AgentServiceMachineName>\SECRECORD$\1\000002

If the customer has specified an alternate location for recorded files, the tenant ID and agent ID will be appended to the configured alternate location.

Existing recorded files will be moved to the new file structure when MiCC-E Agent starts up.

LAUNCH WITH SOFTPHONE

When starting Agent using Agent Integration, it is now possible to specify a softphone option as follows:

LaunchAgentWithParams()

- LogonID: The logon ID of the user
- Password: The password of the user
- Extension: The extension number to be used (optional)
- Extension Password: The password associated with the extension (optional)
- Site Name: The name of the Call Manager site to be connected to (optional)
- Web Server: The machine where the MiCC-E Logon web service is running (optional)
- Broker Server: The machine where the MiCC-E Broker Service is running (optional)
- Broker Port: The port number used to connect to the Broker Service (optional)
- Softphone: Integer value indicating whether the agent will be logged on as softphone.
  0 = use hard phone
  1 = use softphone
  -1 = unspecified, so the last used option will be selected from the Windows Registry

A command line option is also added to specify that agent should be run with hard phone by appending /hardphone to the command line startup sequence. As before /softphone indicates that the agent should be run with softphone. If both options are specified, softphone takes precedence. If neither option is specified, the last used option from the Windows Registry will be used.

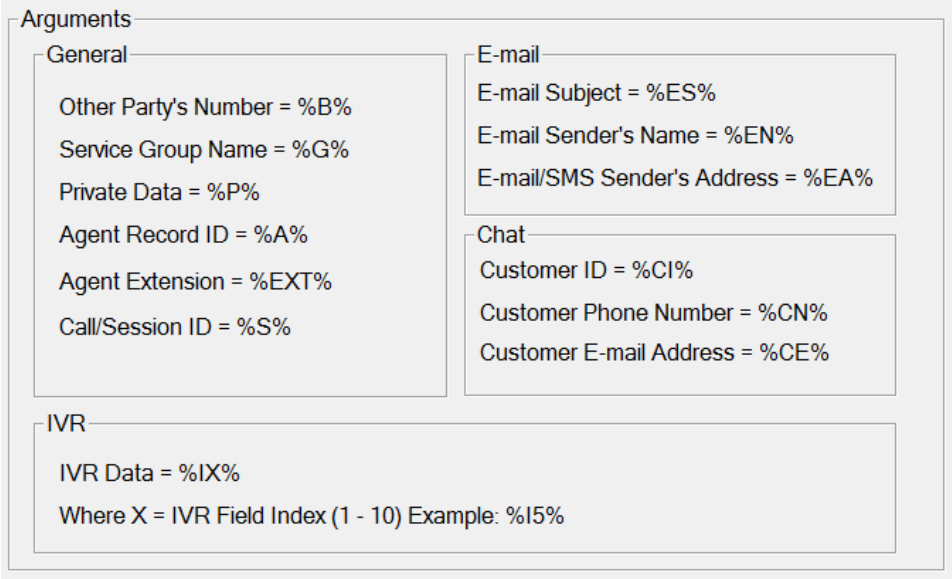
SOFTPHONE LOGGING ENABLED BY DEFAULT

The Agent option for “Detailed Logging” of SIP events is enabled by default for new agents, so that the log file for the SIP stack will automatically generated in case it is required for troubleshooting.

CUSTOMER ID ADDED TO CHAT AGENT ACTIONS

Agent Actions for Chat service groups can now use the Customer ID, Customer Phone Number and Customer E-mail Address as arguments when defining the actions to be executed for the service group.

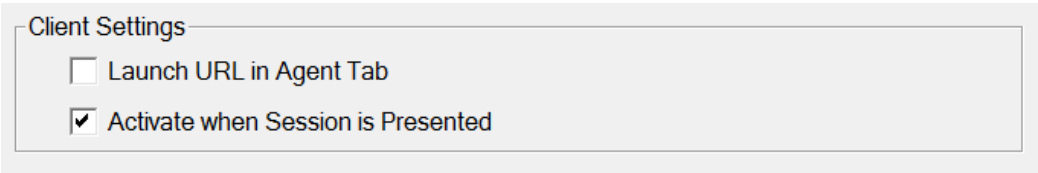
The existing argument for Other Party’s Number (%B%) will apply to Chat service groups using the first non-empty value in the following order of priority: chat customer ID, chat customer phone number, and chat customer e-mail address. The first item with a non-empty value will be populated into the Other Party’s Number argument field.



ACTIVATE AGENT ACTIONS ON PRESENTATION

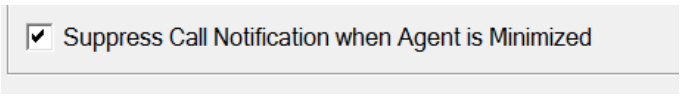
By default, Agent Actions defined for a service group are executed when the session is answered. This can be modified in Web Manager or Configuration Manager when the Agent Action is defined by specifying the option to “Activate when Session is Presented”. If this option is selected, the Agent Action will be executed when the session first is allocated to the agent instead of after it is answered.

Note that the previous configuration settings regarding agent action activation in the MiCC Enterprise Registry Configuration application (SeCCfg.exe) are removed, so if these settings were previously customized, they must now be configured using Web Manager or Configuration Manager.



OPTION TO REMOVE INCOMING CALL NOTIFICATION

If Agent is running minimized to the tray, call notifications were always displayed by default, with no option to disable them. An option is added to the MiCC Enterprise Registry Configuration application (SeCCfg.exe) on the Agent tab to suppress the notification message when Agent is running in minimized mode.



CONFIGURE CLERICAL TIME FOR FAILED CALLBACK SESSIONS

By default, if a callback or web callback fails to connect to the called customer, clerical time is not provided to the agent. To override this and allow clerical time to be entered, the option “Enter Clerical State after Failed Callbacks” is added to the MiCC Enterprise Registry Configuration

application (SeCCfg.exe) on the Agent Service tab. If this option is selected, clerical time will be entered when a callback or web callback completes, regardless of whether it successfully connected to the called customer.

CONFIRMATION BEFORE DELETING AN ACTIVITY

Attendant Agents are able to manage activities for other users. If an activity is deleted, the Attendant Agent will be asked to confirm the deletion to avoid accidentally deleting activities.

LIMITING LOAD BALANCING FOR AGENTS

By default, MiCC-E will load balance between all available TAS systems, so that agents are distributed throughout the available TAS servers. In some cases, it is desirable to limit load balancing to only selected TAS servers, such as when multiple data centers are used, or NeverFail is employed for high availability.

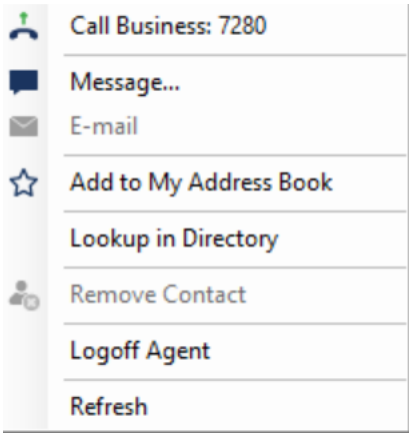
To enable this, a Windows registry value is added. If the registry value exists and contains at least one call manager server ID, only the specified call managers will be considered for agent connection.

Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mitel
Registry value name (REG_SZ): SECOASServers
Registry Value: <Comma separated list of server IDs to include>

This value is defined on the machine running the MiCC-E Agent Service (CCAS).

LOGOFF OF PHONE AGENTS FROM AGENT CONTACTS

If configured in the MiCC-E tenant parameters, phone agents are displayed in the Contacts display of Agent. Right-clicking on any entry in the Contacts, including phone agents, displays the following menu:



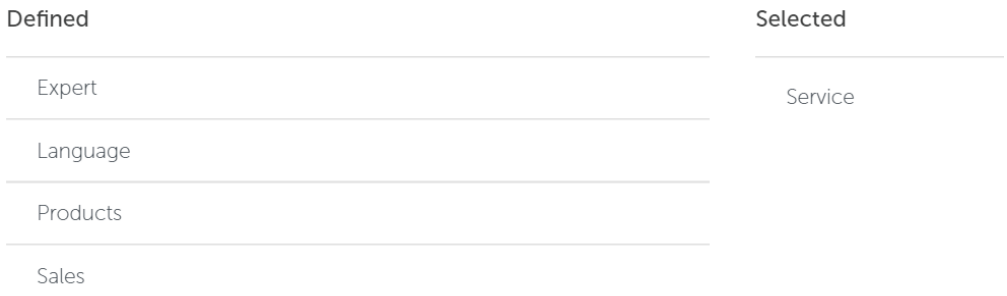
Select Logoff Agent to force logoff the selected agent. This can be applied to agents, phone agents, or web agents.

WEB AGENT ENHANCEMENTS

The following enhancements have been added to the Web Agent application.

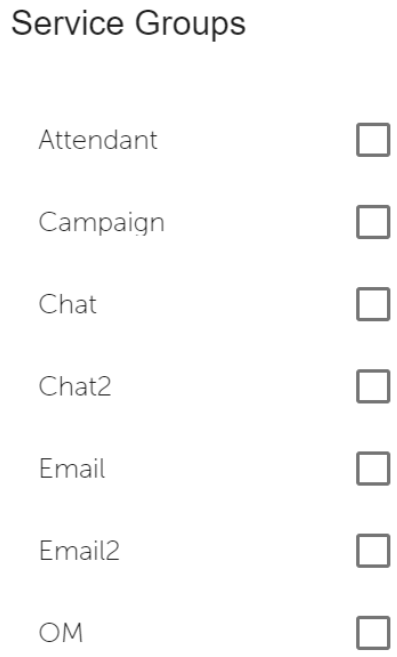
DISPLAY OF SKILLS IN SORTED ORDER

Skills in the Skill Selection display are now shown sorted in alphabetical order rather than the order in which they were defined in the database for easier searching and selection.



DISPLAY OF SERVICE GROUPS IN SORTED ORDER

Service groups displayed in Real-Time display are now shown sorted in alphabetical order rather than the order in which they were defined in the database for easier searching and selection.



SCRIPT MANAGER ENHANCEMENTS

IVR QUEUE HANDLING SYSTEM VARIABLES ADDED

The following system variables are added to the Media Component Library for scripts used for IVR Queue handling:

IVRQ_EWT – Current estimated wait time for the session (-1 if not yet calculated)

IVRQ_QueuePosition – Session's position in the service group queue

IVRQ_QueueCount – Current number of sessions in the service group queue

IVRQ_Last10QueueTime – Average wait time for the last 10 sessions in the service group queue

These variables can be accessed in the script using the nomenclature @@MediaLib.<VariableName> for scripts handling sessions in IVR Queue handling. The variables are not available for scripts not handling sessions in IVR Queue handling.

SHUTDOWN SYSTEM VARIABLE ADDED

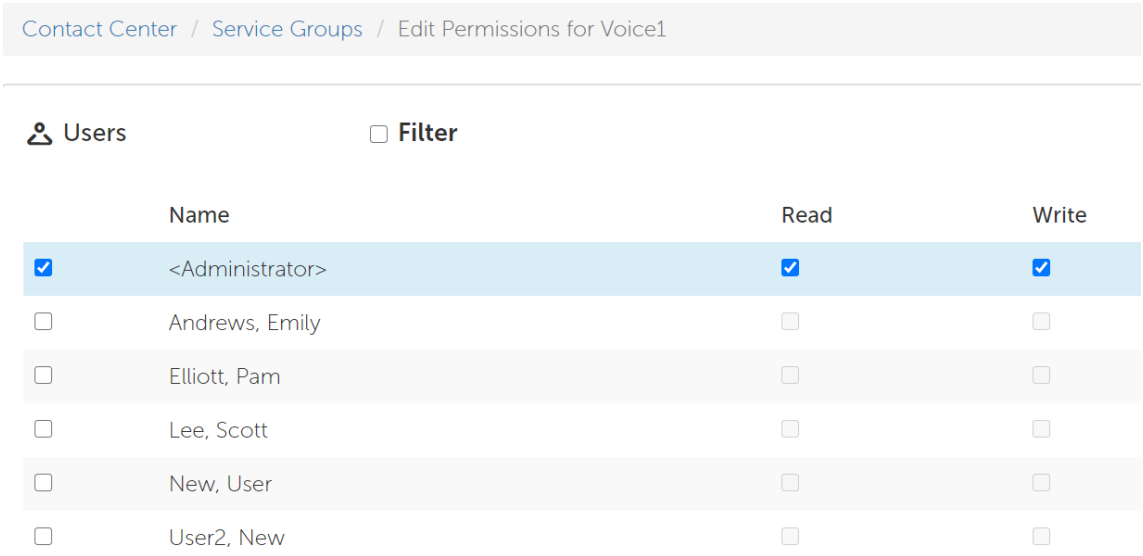
The system variable InShutdown is added to allow the script to determine if the script is currently terminating. The value will be set to 1 in this case.

This is useful for scripts that contain a loop, and are not driven by blocks such as OnCallDelivered, OnFlowEvent, OnEmail or OnSMS to terminate gracefully at shutdown.

WEB MANAGER ENHANCEMENTS

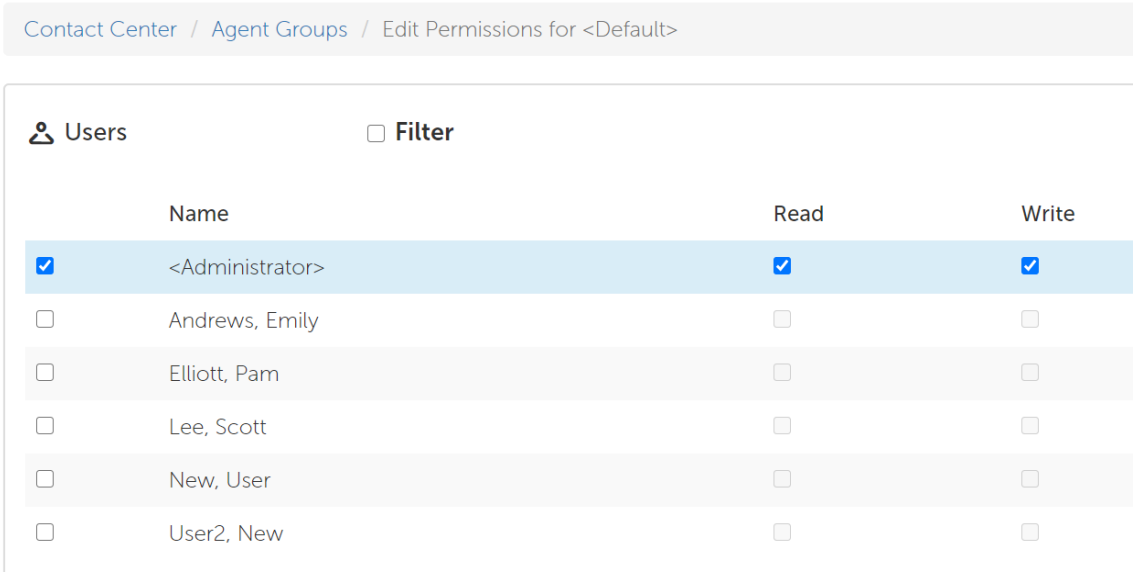
SUPPORT FOR SERVICE GROUP PERMISSIONS

It is now possible to configure permissions for service groups in Web Manager. When a service group is selected and the Edit Permissions button is pressed, the following screen will display, allowing the user to set Read and/or Write permission on the service group for any of the defined users. It is possible to use the Filter capability to limit the displayed users based on skill, service group, agent group, or object tag.



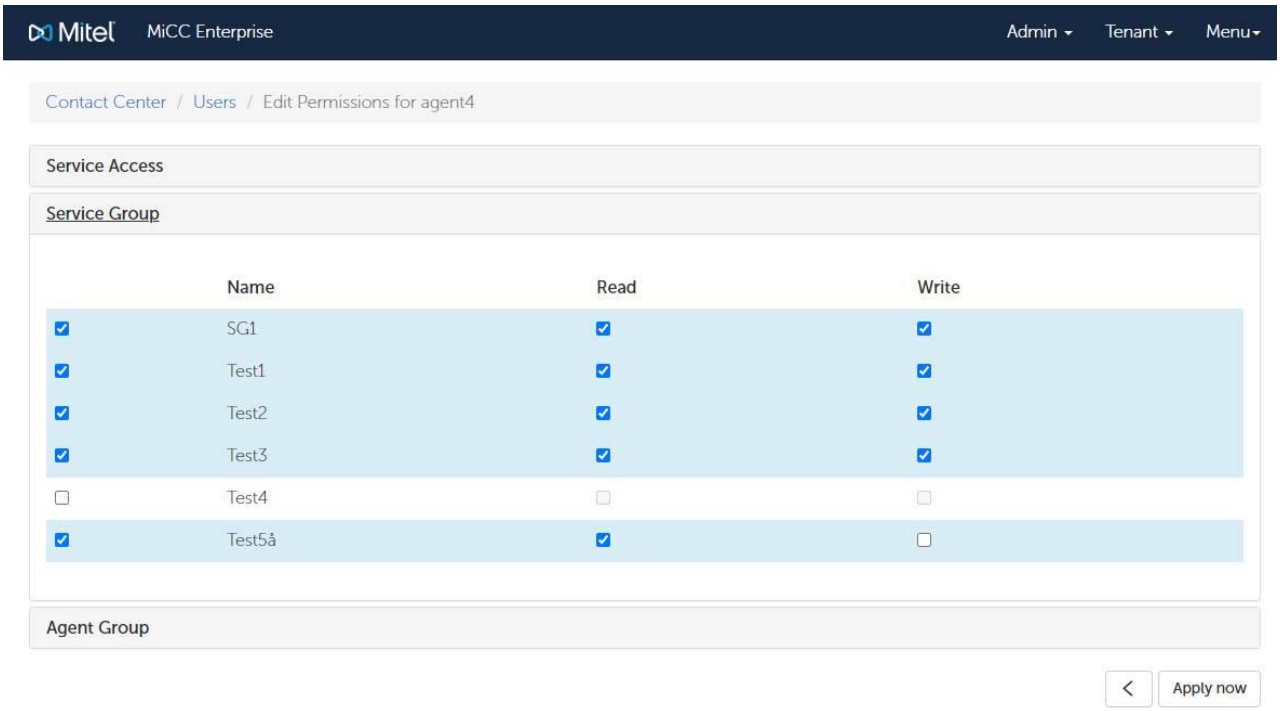
SUPPORT FOR AGENT GROUP PERMISSIONS

It is now possible to configure permissions for agent groups in Web Manager. When an agent group is selected and the Edit Permissions button is pressed, the following screen will display, allowing the user to set Read and/or Write permission on the agent group for any of the defined users. It is possible to use the Filter capability to limit the displayed users based on skill, service group, agent group, or object tag.



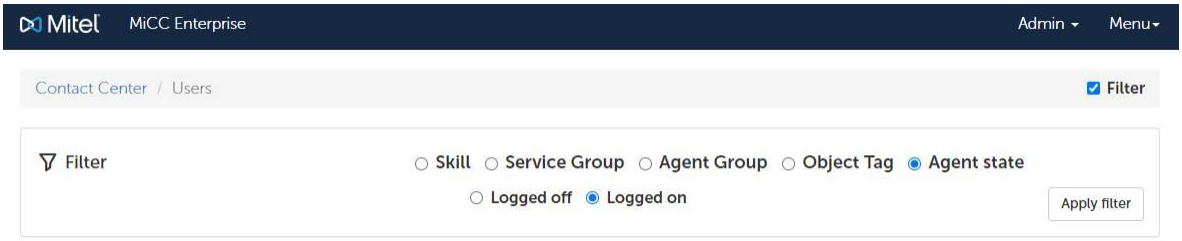
SUPPORT FOR USER PERMISSIONS

It is now possible to configure permissions for users in Web Manager. When a user is selected and the Edit Permissions button is pressed, the following screen will display, allowing Read and/or Write permission to be set on Service Accesses, Service Groups or Agent Groups for the selected user.



USER FILTERING OPTION

When the user list is displayed in Web Manager, a filtering option is added allowing the users to be displayed based on Agent Logon status, i.e. Logged on or Logged off. Only the users matching the selected logon status will be displayed.



SCHEDULES ADDED TO OBJECT TAG FILTERING

When filtering the display of service groups and users, it is now possible to filter the display based on Schedule object tags. If any Schedule object tags are associated with users or service groups, the Schedule object tags will be displayed as a filter option.

IMPROVEMENTS TO MEDIA OBJECT TTS GENERATION

The following improvements have been added to Media Object Text to Speech (TTS) generation in Web Manager when using Google Cloud Text-to-Speech services:

- Display the original text transcript when editing an existing Media Object
- Support for Speech Synthesis Markup Language (SSML) with support for pauses in speech (refer to the Google reference)
- Adjustable speaking rate per prompt, from 0.25 – 4.0 with 1.0 as the default value

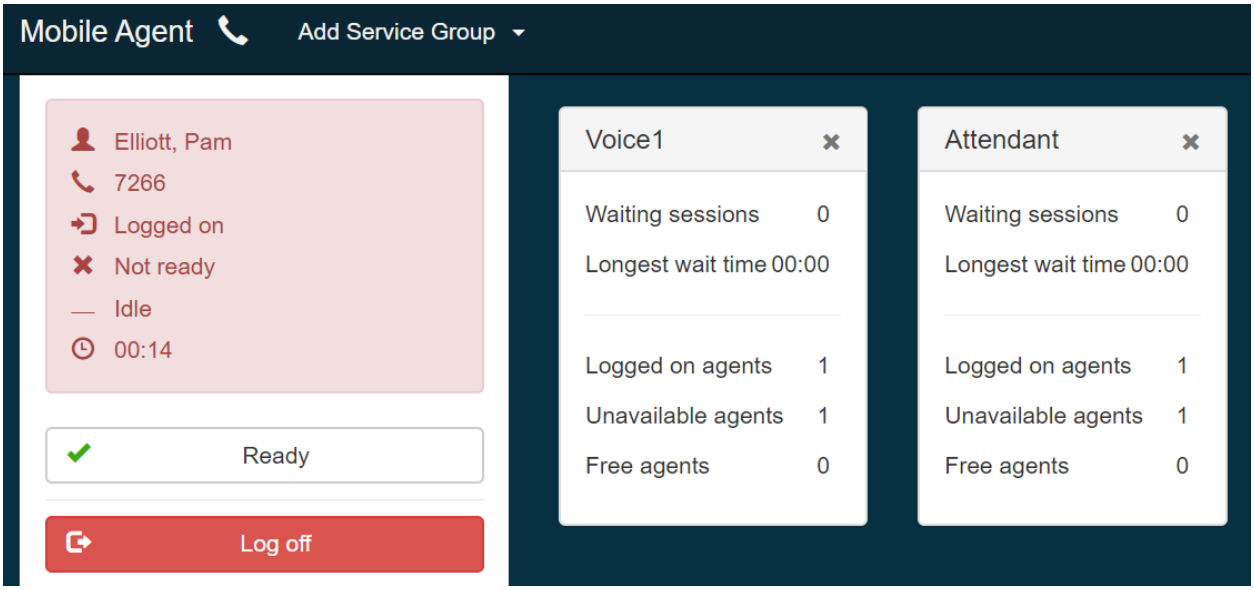
MISCELLANEOUS ENHANCEMENTS

MOBILE AGENT ENHANCEMENTS

The MiCC Enterprise Mobile Agent web application is updated with the following enhancements:

Display has three different options available:

- **Default**: Service Groups selected are displayed, and Agent Status is available via the drop-down menu.
- **Left** and **Right Sidebar**: Service Groups selected are displayed and Agent Status is shown on the left or right sidebar (as shown below).
- **Mini**: Only Agent Status is displayed.

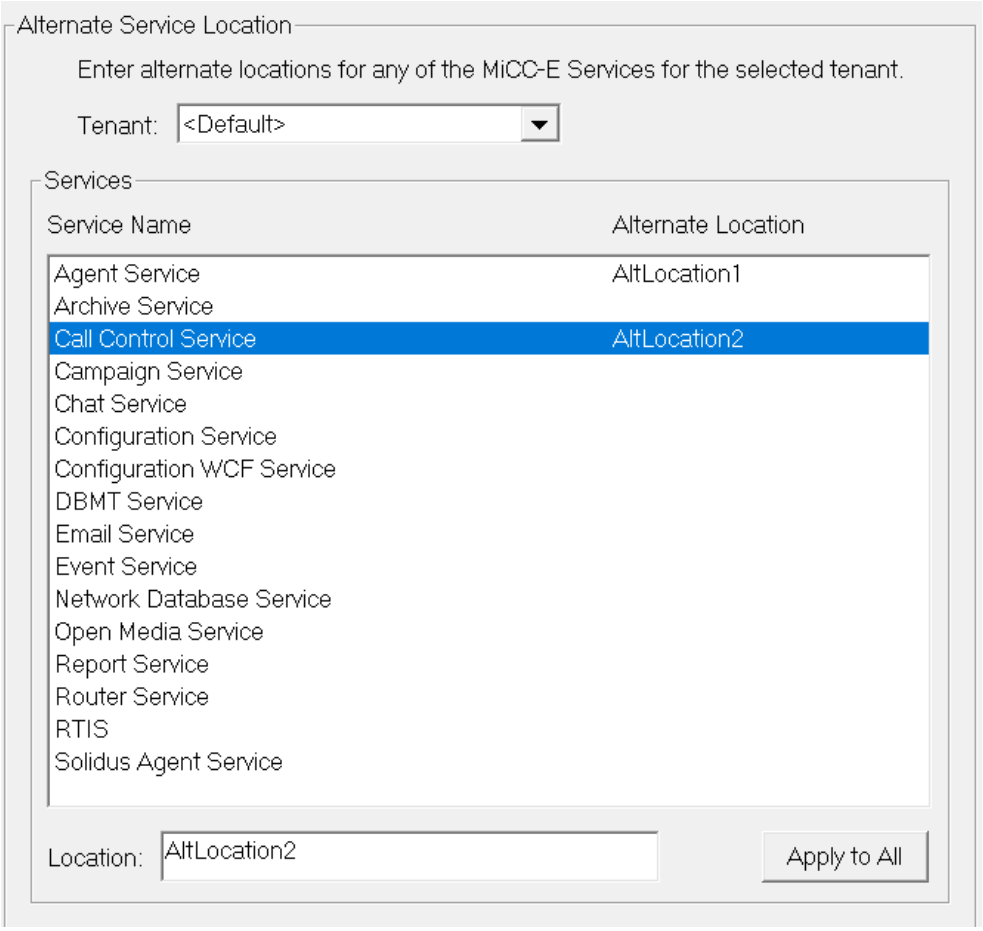


White labelling settings are also configurable, including the displayed product name, application name, and label displayed at login. Custom styling including foreground and background colors are also customizable. For more details, consult the Web Applications Configuration Guide (41/1553-LXA119154).

ABILITY TO DEFINE ALTERNATE SERVICE LOCATION FOR MICC-E SERVICES

Alternate locations for any of the MiCC-E services can be defined for a tenant through the MiCC-E Setup utility on the Alternate Service Location tab.

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. This is useful when client applications are located outside the MiCC-E domain and require a proxy to connect to the services.

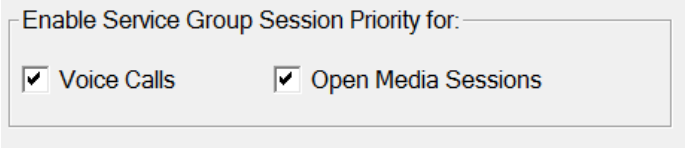


QUEUE PRIORITY OPTION FOR OPEN MEDIA SESSIONS

When an Open Media session is added to the system, a priority value can be assigned to the session, allowing it to bypass other sessions currently in queue with lower priority.

The AddOpenMediaRequest interface is expanded to allow an optional SessionPriority parameter, ranging from 1-100, with 1 representing the highest priority value.

Just as session priority can be enabled for voice service groups, there is a setting in Configuration Manager Tenant Parameters on the Call tab allowing it to be enabled for Open Media sessions:



If this option is set, Open Media service groups will allow adding sessions with an assigned priority value. If no priority value is assigned to the Open Media session, the priority value assigned to the service group will be set for the session. The session will be inserted in the queue ahead of other lower priority sessions.

If a session is added with both a queue time set and a session priority value, the queue time value will take precedence, so the session will be added to the service group queue based on the calculated wait time instead of the priority.

OPEN MEDIA MODIFY REQUEST

ModifyRequest is added to the Open Media interface, allowing an existing open media session to be modified. The values that can be updated include the following:

- IVR Data and/or Labels
- Private Data

If the IVR label provided in the ModifyRequest is already associated with the open media session, the corresponding IVR data will be updated. If the IVR label does not exist, a new IVR label and data will be appended to the existing data.

Private data in the open media session will be replaced with the private data provided in the ModifyRequest, if specified.

In order to be modified, the open media session must be currently in the service group queue and not allocated to an agent or terminated.

OPEN MEDIA TEST TOOL ENHANCEMENTS

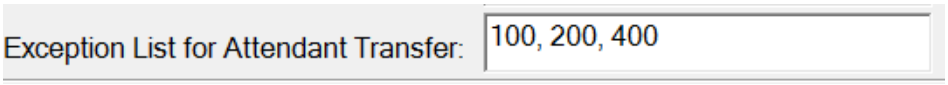
For easier use, the Open Media test tool is modified to support selecting all of the text from the Information field using Ctrl-A and copying the items to the Windows clipboard using Ctrl-C.

EXCEPTION LIST FOR ATTENDANT AGENT TRANSFERS

In some cases, it is desirable to override the automatic recall feature for Attendant Agent call transfers, such as when the call is transferred to a Group Hunt position. In this case, the call will be routed through the Group Hunt, so there is no need to recall to an Attendant Agent.

To configure destination numbers that should not provide recall, an option is added to the MiCC Enterprise Registry Configuration application (SeCCfg.exe) on the Router Service tab. The

exception numbers can be entered as a comma separated list. If an Attendant Transfer is made to any of the entered numbers, no recall attempt will be made, and the call will be transferred without the “maintain queue” option. It will be considered as successfully transferred once it is sent to the destination number entered.



ADDITIONAL REPLACEABLE IDENTIFIERS FOR CHAT AND E-MAIL

Templates used with e-mail and SMS sessions, as well as e-mail signature files, allow the use of replaceable identifiers. Chat response files and KnowledgeBase responses can also use replaceable identifiers to replace text with information regarding the agent and the session.

The following replaceable identifiers are added for use with templates, signature files, response files, and transcripts:

$Agent.FirstName$ - represents the agent’s defined first name

$Agent.LastName$ - represents the agent’s defined last name

$Agent.ChatName$ - represents the agent’s defined Chat Display Name. If this is not configured, it will default to the agent’s name.