Mitel MiContact Center Enterprise

A WHITE PAPER ON GDPR CONSIDERATIONS

MiCC Enterprise 9.5

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 - White Paper on GDPR

March 2021

Contents

INTRODUCTION

This document describes how the MiCC Enterprise contact center system collects and safeguards private information and how this information can be erased either manually or on a time based or scheduled basis.

WHAT IS GDPR?

The European Union (EU) General Data Protection Regulation (GDPR) effective on 25 May 2018 replaces the previous EU Data Protection Directive 95/46/EC.

The intent of GDPR is to harmonize data privacy laws across Europe so that the data privacy of EU citizens can be ensured. GDPR requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. GDPR also addresses the export of personal data outside of the EU. Any business that processes personal information about EU citizens within EU must ensure that they comply with GDPR. Under GDPR, 'processing' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

GDPR applies to businesses with a presence in any EU country, and to businesses that process personal data of EU residents even if the businesses have no presence in any EU country.

To achieve GDPR compliance, businesses must understand what personal data is being processed within their organization and ensure that appropriate technical and organizations measures are used to appropriately safeguard such data. This document explains what personal data is processed by Mitel’s MiContact Center Enterprise system and highlights available security features to safeguard such data.

SCOPE

MiCC Enterprise is a very open, flexible, and highly customizable platform, and is in many instances integrated to Case Management, CRM/ERP and/or recording systems. This document will limit the scope to the MiCC Enterprise system itself and not how e.g. an integrated CRM system manages its collected personal data.

This White Paper will discuss the different ways the MiCC Enterprise system can collect personal data, where the data is stored, how it is protected and various ways to remove personal data from the system. It shall be seen as a help and guidance for partners and system administrators to develop procedures to meet the requirements of GDPR.

PERSONAL DATA

Personal data is in this context defined as “any information which can lead to identification of a data subject, directly or indirectly, by reference to an identifier such as an identification number, a name, location, online identifier such as I.P addresses”.

“Data subject” is in this context the customer who has at some point contacted (or was contacted by) the company to receive information or help. Data subject will in this document be called ‘customer’.

SOURCES OF PERSONAL DATA

There are several ways personal data can be collected by the MiCC Enterprise system. Most customer interactions will result in some personal data being made available to the MiCC Enterprise system at the time of the contact. Information such as caller id, calling name, email address, chat handle etc. are usually received at the time of contact.

Other information could be retrieved from CRM/ERP and case management systems or other databases and systems during the IVR handling of a call, email, or SMS. Information could also later on, while the agent is handling a session, be entered from an external system that is integrated with one of the desktop or server-based APIs provided by MiCC Enterprise.

Personal Data such as name and phone number plus other campaign related data can also be entered or imported to the MiCC Enterprise system as part of outbound calling campaigns.

Customer contact information received at time of contact

This type of information would typically be the phone number of the caller or sender of a SMS, possibly also Name information if that is sent together with the number. For incoming emails this would then of course be the email address of the sender as well as any name information available in the email header and for Chat sessions the request can include a Chat handle and/or email address.

This information is typically presented to the agent, used to screen-pop other applications or systems, stored in the CDR, Call Detail Record, in the database (if so configured) and could also possibly be stored in log files on the server and/or the client depending on chosen log level settings.

Information retrieved from the customer and external systems

Using Auto Attendant

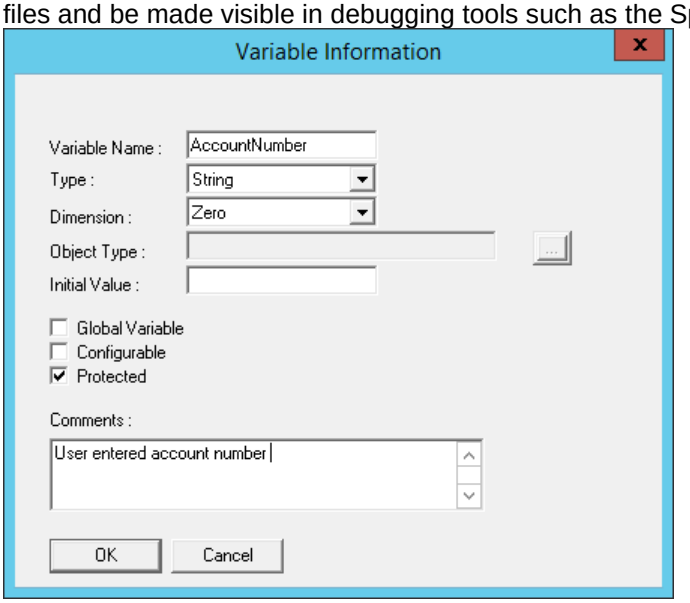
Using the built-in Auto Attendant function to greet callers, the system can also prompt the user to enter one piece of information as part of the greeting procedure. This information could be an account number or other personal information. This information is then typically presented to the agent, can be passed on to other integrated systems as part of a screen-pop and is stored in the CDR record for this call. It can also be stored in log files on the server and/or the client depending on chosen log level settings.

Using Interactive Voice Response, IVR

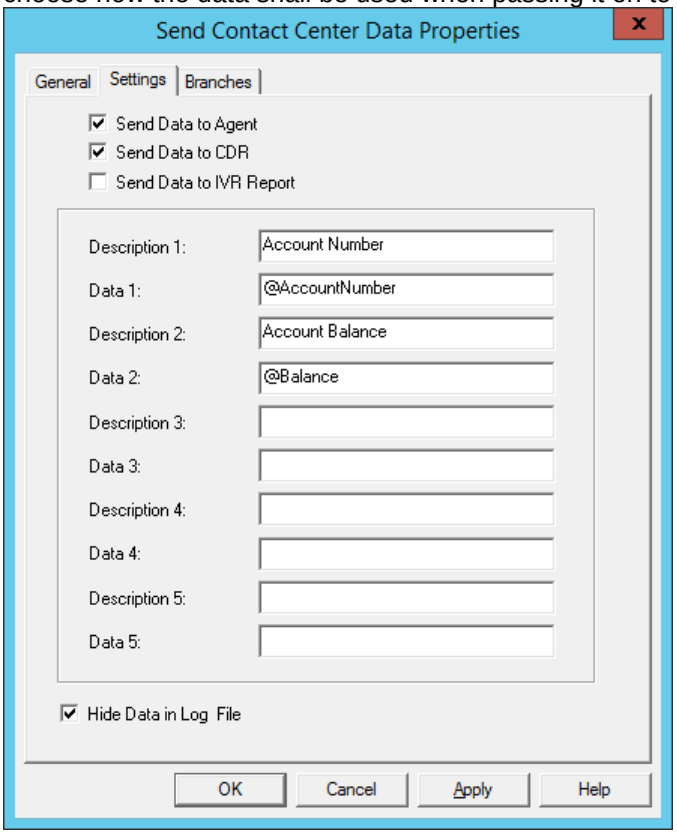
The integrated IVR function (Script Manager) can be used to ask the caller for additional information (that can be entered by DTMF tones, such as an account number, or by speech recognition). This information can the be used in the IVR application to make decisions how to proceed in the IVR script or to be collected and later on presented to the agent that is selected to handle the call.

The Script Manager IVR is also capable of retrieving information from any ODBC compliant database, from web services or from any other system via APIs. This could then of course include personal data. Script variables used to contain such data should be tagged as Protected in the IVR script. That will prevent the data in these variables to be stored in log

files and be made visible in debugging tools such as the SpyTracer tool:



The purpose of collecting this type of information is typically to present it to the agent and/or to pass it on to an integrated application as part of a screen-pop. It could also just be for having it stored in the CDR in order to be able to do reporting on. The IVR developer can choose how the data shall be used when passing it on to the system:



The data can also be hidden in log files by checking the “Hide Data in Log File” check box.

Information entered (tagged) by external system

The MiCC Enterprise system is a very open and flexible system. It does provide system integrators with APIs where external system can not only receive information from the system but also allow the external system to enter or tag data related to a call or other customer interaction. This could be data that should just be stored in the CDR for reporting or classification purpose, but it could also be data that should be made available to the IVR or to other agents if the agent transfers, diverts or rejects a specific call. This data could potentially contain personal data that can end up in CDR records and/or log files.

Campaign Information entered or imported to the system

To use the outbound Campaign feature lists of customers to call needs to be defined in the system. These lists can be defined by entering the items one by one but since that is not realistic for larger campaigns; these lists are typically imported into the system via a file or directly into the database via SQL scripts. These calling lists contain at the minimum Name and Phone number information and are thus classified as Personal Data. The calling lists can also consist of up to 10 customer defined fields. These fields can be used during the list import do hold additional information such as the nature of the call, account information etc. The calling lists are stored the SQL server.

MiCC Enterprise User information

To gain access to the system, users are created using either the Configuration Manager or Web Manager applications. These user records contain at minimum Name information as will as logon IDs and passwords. Optionally they can also contain address and phone number information. When employees leave the company, this information should be anonymized.

PROTECTION OF DATA IN TRANSIT

Web services

All MiCC Enterprise web services support encryption. HTTPS can be enabled in IIS and WCF based services can also be configured to use HTTPS. This will protect chat session between customers and agents, all data sent to and from agents using the Web Agent application as well as all communication between the MiCC Enterprise server and agents using the MiCC Agent desktop application. Also, all communication between Information and Report Manager applications and the IIS are then encrypted.

Client/Server and Server/server communication

Using the MiCC Enterprise Setup program the system administrator can enable SSL on all socket communication between server components as well as Configuration Manager clients.

STORAGE OF PERSONAL DATA

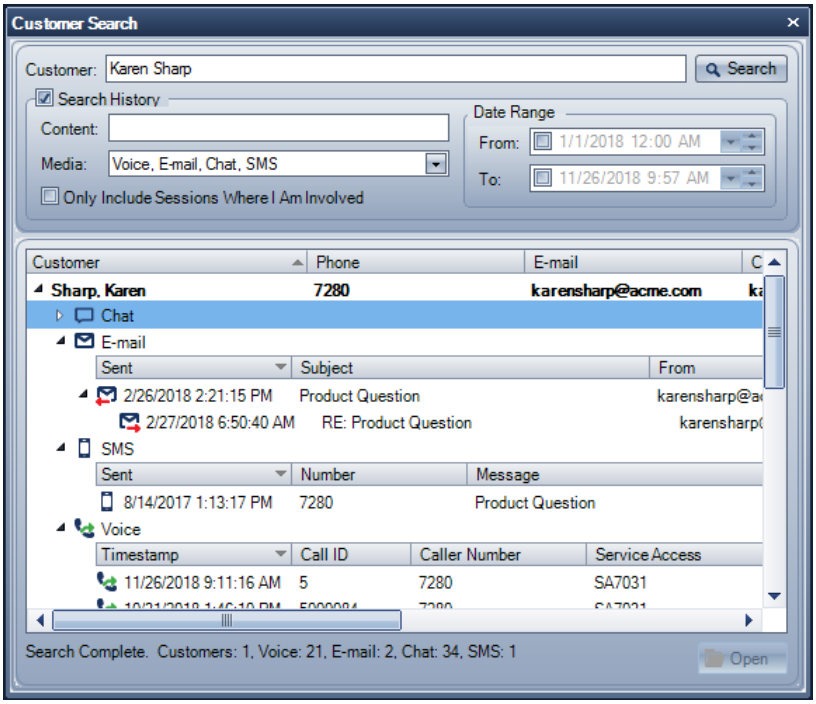
Call Detail Records (CDR)

Collection and storing of CDR records for voice, email, chat, and SMS is by default not active in the system. They are activated, individually, in the System properties. When activated, CDR records are generated and stored at completion of the customer session. A CDR record

contains an entry for each step the session went through, with time stamps. A typical CDR could look like this:

Caller Number	Time Stamp	Call Event	Name
3247	3/30/2018 9:53:50 AM	Call entered Service Access	Banking
	3/30/2018 9:54:19 AM	IVR data - Name Roger Jones	
	3/30/2018 9:54:19 AM	IVR data - Balance 54230.32	
	3/30/2018 9:54:19 AM	IVR data - Pin 1234	
	3/30/2018 9:54:19 AM	IVR data - Address 1 123 My St	
	3/30/2018 9:54:19 AM	IVR data - Address 2 My Town CA	
	3/30/2018 9:54:19 AM	Call entered Service Group queue	Banking
	3/30/2018 9:54:20 AM	Played message - 100	
	3/30/2018 9:54:27 AM	Call routed to agent - 1st choice agent...	Sally Thompson
	3/30/2018 9:54:28 AM	Call alerting	Sally Thompson
	3/30/2018 9:54:32 AM	Call answered	Sally Thompson
	3/30/2018 9:54:38 AM	Clerical time started	Sally Thompson
	3/30/2018 9:54:38 AM	Call completed - Disconnected by Agent	Sally Thompson
	3/30/2018 9:55:08 AM	Clerical time ended	Sally Thompson

CDR records can be filtered and viewed from the Report Manager application and is also the basis for the customer history search capabilities in MiCC Agent, where properly privileged supervisors and agents can search and view prior customer interaction history for voice email and chat:



It is up to the system administrator to protect this data by proper access rules for the SQL database as well as managing access to Report Manager and MiCC Agent. MiCC Enterprise implements standard paswword rules such as account lockout at a user defined number of failed attempts, password aging, password re-use rules etc.

Call recordings

When using the built-in call recording function for Agent softphone users, the recordings are stored as wav files on the server or on a network share. It is up to the system administrator to protect this storage by implementing access necessary rules using Windows security.

Campaign information in the SQL Database

As mentioned earlier, campaign calling lists containing name and number information is stored in the SQL database. When the campaign starts and calls are being made and completed, the result of the campaign call is also stored in the SQL database. The calling lists and the result information are stored independently in the database, i.e. deleting a calling list does not delete the results and vice versa.

It is up to the system administrator to protect the campaign data by proper access rules for the SQL database.

Call logs for MiCC Agent and Web Agent

The MiCC Agent and the Web Agent applications both contain a call log function. The last 1000 calls (incoming, outgoing, or missed) are remembered. This call log is stored together with the logged-on user's preferences in the SQL database. It is stored as a binary blob in a non-readable format.

Log Files

Personal information such as caller id, calling name information, email address can end up in log files on the server or on the MiCC Agent clients. The level of logging varies depending on the components involved. Some components, such as OAS, has no logging activated at all by default, but to get some useful information in case of issues, Mitel recommends or partners that NRM logging is turned on. The MiCC Services is set by default to log at level 3 on a scale from 1 to 9. This provided high level logging and error messages. For all logging, the system can be configured for how many log files that can be produced before the system starts to overwrite them. Mitel recommends our partners and customers to only activate higher levels of logging when requested by Mitel service technicians.

The location of these logs should be secured by standard Windows security mechanisms so that only authorized system administrators have access to them.

User information

Date related to users of the MiCC Enterprise system is stored in the SQL database. These records contain name, logon info and optionally address and phone information. When a user is deleted from the system, the record is not removed but marked as deleted. The reason for that is that these records are needed to be able to produce historical reporting data for time periods where the deleted user was active in the system. Mitel recommends that procedures are put in place so that this data is anonymized before the user is deleted.

REMOVAL OF PERSONAL DATA

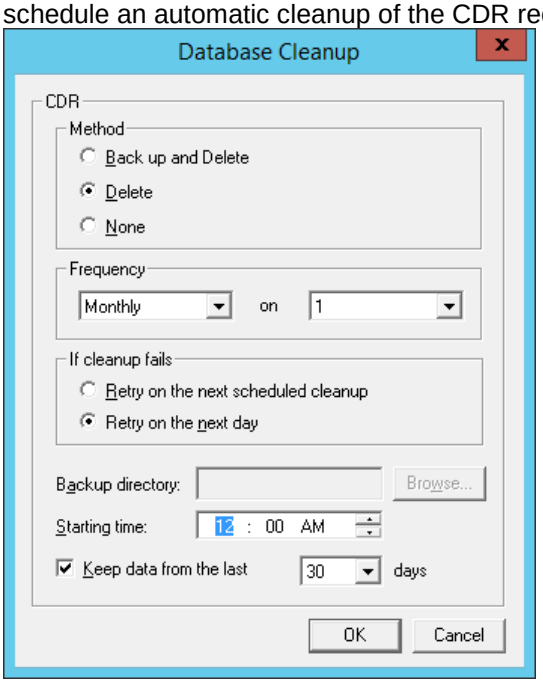
Mitel recommends its partners and customers to implement procedures for how to both secure access to personal data that could exist in the SQL database or on the MiCC Enterprise server and how to remove information upon request.

Since in most cases, the individual contact center agent will not have the necessary access and privileges to remove customer data, procedures should be put in place how to handle this. One solution would be to appoint a properly privileged team to manage this type of requests, and hand-off requests to this team.

From CDR records and voice recordings

Scheduled removal

Using the database maintenance utility, the administrator of the MiCC Enterprise system can schedule an automatic cleanup of the CDR records from the database.

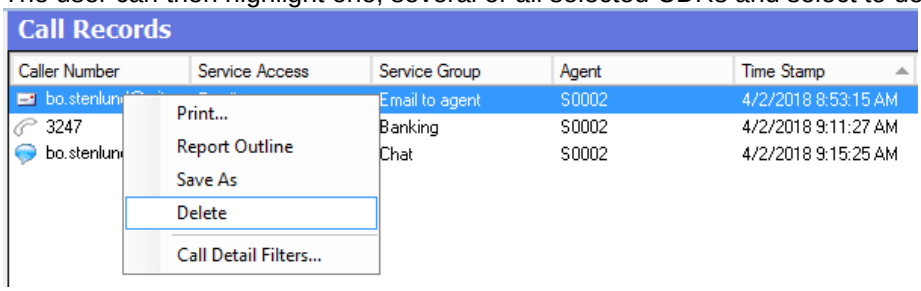


Note: the scheduled cleanup of CDRs will NOT remove any associated call recordings. If the integrated recording function is used, then he CDRs should be removed manually using Report Manager or the recordings be manually deleted from the central storage location.

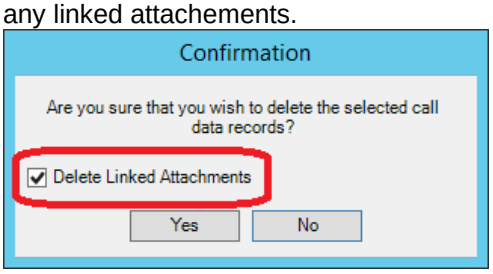
Manual removal

Using the CDR filtering capabilities in Report Manager, the user could filter on all calls or SMS messages from a specific number or all emails and chat sessions from a specific email address to see a list of CDRs.

The user can then highlight one, several or all selected CDRs and select to delete:

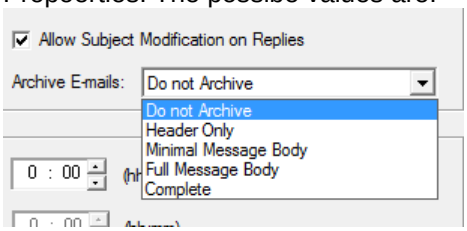


In the confirmation dialog there is a check box that should be checked in order to remove any linked attachements.



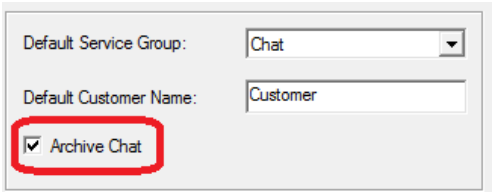
For voice calls that would be any call recordings that exist for these CDRs.

For emails this would be email content such as header info, body and any attchments. The level of information stored for emails is controlled by a system parameter set in the Sysytem Propoerties. The possibe values are:



Default value is not to archive email details.

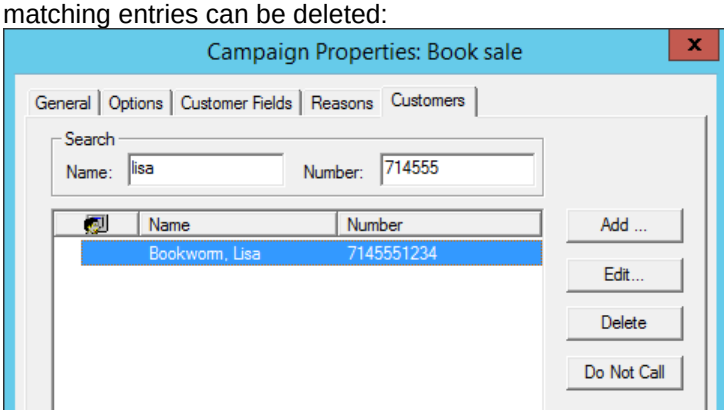
For chat, the Linked Attachments refer to the actual chat transcript. Wheather chat transcrits are stored in the database or not is controlled by a system setting in the System Properties:



From Campaign information in the SQL database

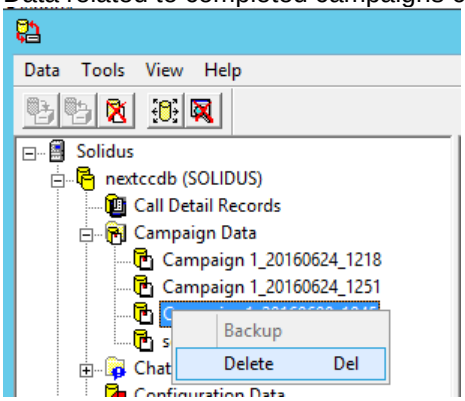
Ongoing or future Campaigns

Customer can be removed from ongoing campaigns or campaigns scheduled to start at a future date by using the Configuration Manager application. In the Customer tab of the Campaign properties dialog a search can be done on name and/or phone number and then matching entries can be deleted:



Completed Campaigns

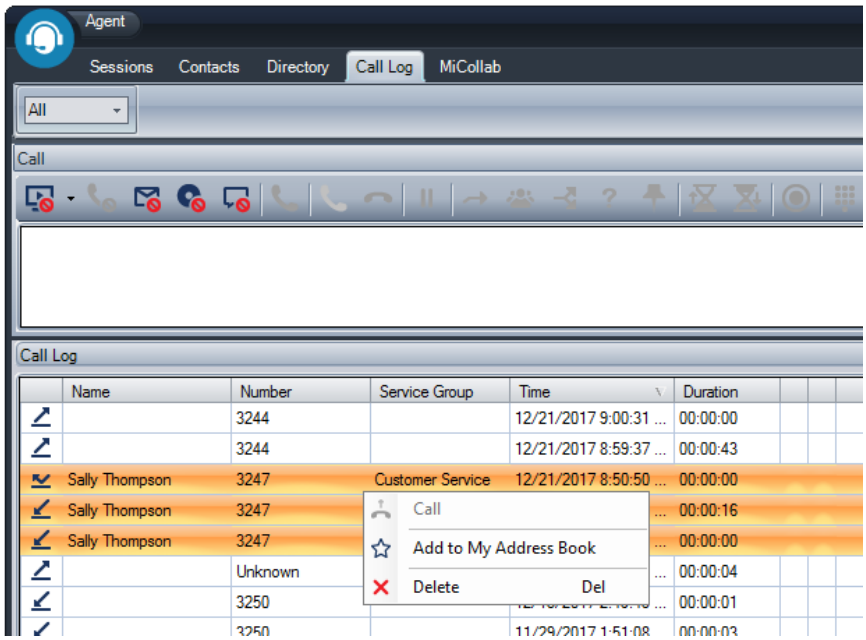
Data related to completed campaigns can be deleted using the DBMT utility.



In order to just remove individual entries for completed campaign, and not the whole campaign, then that can be done using SQL commands. For example the command *DELETE FROM campaign_customer_res WHERE number='7145551234'* would remove all entries in all campaigns for the phone number 7145551234.

From Call logs for MiCC Agent and Web Agent

The Call log items can be viewed by clicking the Call Log tab in MiCC Agent or Web Agent and sorted by clicking the column heading. One or several call log entries can be selected and then Deleted:



As mentioned above, it is recommended that procedures and training are put in place to manage Private Data. One procedure to ensure that all agents remove call log entries for a specific caller could be to use the desktop messaging or operational messages feature to send a message to all users asking them to remove specific entries.

From Log files

The MiCC Enterprise system consists of several major components, such as the call control and media services platforms OAS and TAS, the IVR (Script Manager), the MiCC Server components and its applications. Each of these has slightly different log file settings. Logging is typically a tool used by service technicians and developers to see how the system performs and do fault isolation in case of issues. Mitel service typically recommends partners to leave some basic level of logging active and then more comprehensive logging is only enabled when actively working on isolating an issue. These log files can then be deleted once the activity is completed.

More sensitive Personal Data such as account numbers, social security numbers, credit card numbers etc. entered by the user can be prevented from being stored in the log files at all.

The mechanism to activate this differs a bit between components. And, how to configure log file folders, number of log files and log file size varies.

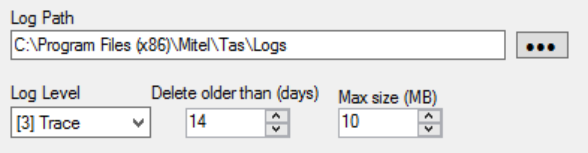
OAS

A Windows registry key can be set to prevent OAS to put entered Private Data in the log file. The key is called HidePrivateData and is set in the *HKLM\Software\Mitel\OAS\NRM* hive.

For OAS you can also specify in the Windows registry how many log files to fill up before starting to overwrite them. The log file size is not configurable and is set to 8 MB for each file.

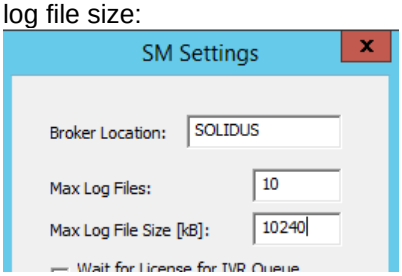
TAS

If TAS is used, it is possible to set the log file location, log level, for how many days log files will be stored and the max log file size using the TASConfig.exe utility:



Script Manager

Script Manager has a very elaborate and avanced logging system, manly used for fault isolation, but also together with the Spy Tracer utility, it is very useful when developing and debugging IVR applications. The log file settings are configured in the Script Manager Configuration utility. I the System Setting properties you can speficy number of log files and log file size:



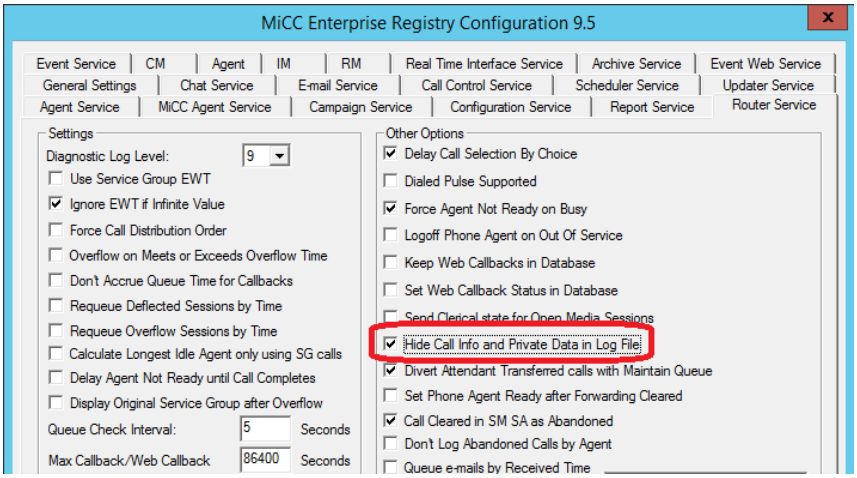
As discussed above, Personal Data handled in the IVR script can be prevented to be stored in log files by using the *Protected* attribute on the variable storing the data. And when

passing on Private Data to the system and agents it can again be prevented from being stored in log files by checking the the "*Hide Data in Log File*" check box in the *Send Contact Center Data* block.

MiCC Enterprise services

A document can be found in the User Documentation library called *Log Files Description* (6/1551-LXA119154). This document describes the many server logs, their log level settings, purpose, and much more.

Personal user input information can also in this case be prevented from being logged at all. Using the SecCfg.exe configuration utility, in the Router tab, you can specify to hide *Call Info and Private Data* in the log:



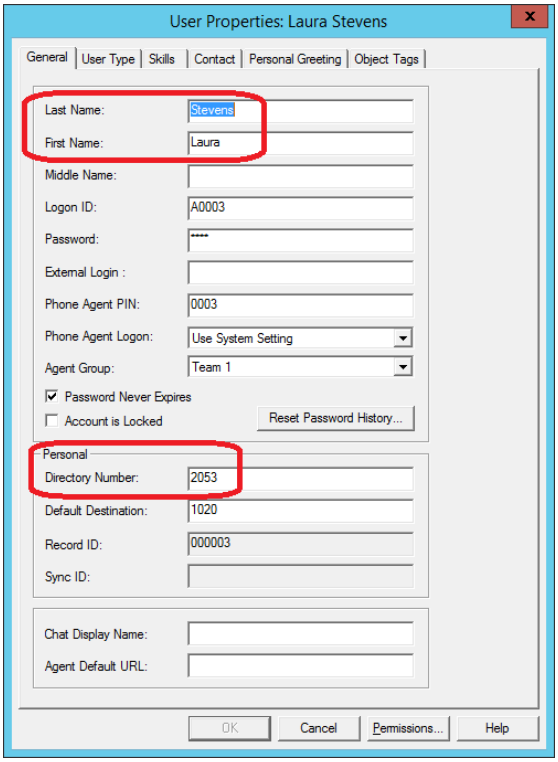
Client PCs

Log location for Windows clients is in the hidden *C:/Users/<Windows user>/AppData/Local/Mitel/MiCC Enterprise* folder.

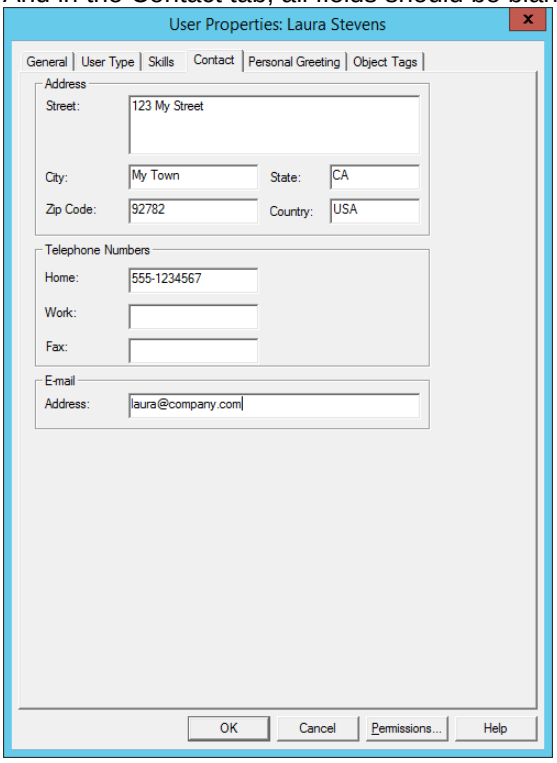
By default, the log level for the Agent application, which potentially is the only application handling potential Private Information, is set to 3. At this level no Personal Information is stored in the client logs for MiCC Agent. If detailed SIP logging or more detailed Agent logging is activated during fault isolation, then Mitel recommends that these log files should be permanently discarded at completion of these activities.

User Information

When a user of the MiCC Enterprise system leaves the company and the user record is to be deleted Mitel recommends that any personal data for this user is anonymized before the user is deleted using Configuration or Web Manager. The First and Last name fields should be changed to e.g. Deleted User 1 and Personal Directory Number should be removed:



And in the Contact tab, all fields should be blanked out:



Then the User can be deleted.

To clean up old information for users that has been deleted before this procedure has been put in place then the SQL database will have to be updated manually. Using the SQL Management console a database administrator could open the nextccdb database and

manaully anonymize the data for deleted records in the cc_user table. Any record in the table that has a delete date that is not set to 2035-01-01 is a deleted record that should be modified to remove any personal information.

PRODUCT SECURITY INFORMATION

MITEL PRODUCT SECURITY VULNERABILITIES

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:
www.mitel.com/mitel-product-security-policy

MITEL PRODUCT SECURITY PUBLICATIONS

Mitel Product Security Publications are available at:
www.mitel.com/security-advisories

DISCLAIMER

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of MiCC Enterprise and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.