

# CMG Configuration Guide

Release 8.5 SP3  
December 2021



## Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MTEL®)**. 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](mailto: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  
© Copyright 2021, Mitel Networks Corporation  
All rights reserved

---

# Contents

<b>Chapter: 1</b>	<b>Introduction . . . . .</b>	<b>1</b>
<b>Chapter: 2</b>	<b>Configure CMG . . . . .</b>	<b>2</b>
	Configuration Tools . . . . .	2
	Configuration Manager . . . . .	2
	Enable active scripting for Internet Explorer . . . . .	2
	Configuration Manager – Security Restrictions . . . . .	3
	Directory Manager . . . . .	3
	Enable active scripting for Internet Explorer . . . . .	3
	User Image Deletion . . . . .	3
	Configure Logging to capture deleted users from DM application	6
	IIS Manager . . . . .	8
	Spman Tool . . . . .	8
	Configuring CMG Server Functions . . . . .	9
	Basic Configuration in Configuration Manager . . . . .	9
	Add an Application Pool . . . . .	10
	Configure BluStar Server Integration . . . . .	11
	Configure AnA to Connect to External CMG Server . . . . .	11
	Configure BluStar Presence Status . . . . .	12
	Enable Click-to-Dial . . . . .	12
	Configure which SMS Signature to use in Configuration Manager	13
	Enable Time Zone Functionality . . . . .	13
	CMG Web . . . . .	13
	InAttend client . . . . .	14
	IIS configuration to access CMG CM, CMG DM and CMG WEB applications over HTTPS . . . . .	16
	Configure NeTS WCF Server . . . . .	17
	Backing up the CMG Database . . . . .	18
	Optimizing Nicesrv . . . . .	18
	Configuring Advanced Security . . . . .	19
	User Management . . . . .	19
	Security Parameters in Configuration Manager . . . . .	20

---

Configuring EFS . . . . .	.20
Setting up Connection to the Telephony System (PBX) . . . . .	.21
Connection to Cisco Call Manager Systems . . . . .	.21
Connection to Other Systems . . . . .	.21
Setting up Connection to the E-mail System . . . . .	.21
Configuring MX-ONE Provisioning Manager Integration . . . . .	.21
Configuring Active Directory Synchronization . . . . .	.22
Information to Configure . . . . .	.22
Deletion of Users . . . . .	.24
Change of Synchronized Users in Active Directory . . . . .	.24
ADSYNCCFG tool . . . . .	.24
Mapping configuration for other fields from AD to CMG . . . . .	.25
Customize CMG Web . . . . .	.26
CUSTOMIZE CUSTOMER GROUP SEARCH . . . . .	.27
INFORMATION TO CONFIGURE . . . . .	.27
CUSTOMER GROUP SEARCH IN CMG WEB . . . . .	.28
CMG Installation-Configuration on Azure . . . . .	.29
Setting up CMG Web for Visual Voicemail in the MiCollab Client . . . . .	.33
Before you Begin . . . . .	.33
Procedure . . . . .	.33

## Chapter: 3

<b>Configure Optional Server Software . . . . .</b>	<b>35</b>
Configuring CMG Server SQL Express Backup . . . . .	.35
Configuring Mitel LDAP Server for CMG . . . . .	.37
Enable LDAP Server . . . . .	.37
Configure LDAP Server . . . . .	.38
Configuration . . . . .	.39
Database . . . . .	.39
Custom Attributes . . . . .	.39
SQL/CMG Login Information . . . . .	.40
New Country . . . . .	.40
Logging . . . . .	.41
General . . . . .	.41
Menu: File - Change Path to LDAP Server . . . . .	.42
Configuring IP Phone Services for Cisco . . . . .	.42
Cisco Call Manager Configuration . . . . .	.42
Cisco IP Phone Services Configuration . . . . .	.42
CMG System Configuration . . . . .	.43
Configuring CMG Corporate Directory for IP Phones . . . . .	.43
Configure Localized Resource Files in Microsoft IIS . . . . .	.43
Configure application settings in IIS . . . . .	.43
Configure language settings . . . . .	.44
Verify the settings . . . . .	.44
CMG Connection Settings and Dialing Plan . . . . .	.45
CMG connection settings . . . . .	.45
Configuring dialing plan . . . . .	.46

Configuring language settings .....	46
Enabling logging .....	47
Verifying settings .....	47
IP Phones Configuration .....	47
MiVoice 4425 phones .....	47
Mitel 7400 phones (End Of Life) .....	48
Mitel 67xxi SIP phones .....	48
Mitel SIP-DECT 3.0 .....	49
Mitel SIP-DECT 3.1 .....	49
Configure Prefix for Multi Node Configuration .....	50
Configuration of CMGUserInfoService (CWI) .....	50
Configuration of Corporate Directory application .....	50
Configuring CMG Personal Number Interface .....	51
Configuration in MX-ONE Provisioning Manager .....	51
Create a User .....	51
Add User to the Administrator Group .....	51
Enable CMG Personal Number in CMG Configuration Manager .....	52
Enable CMG Personal Number in CMG Directory Manager .....	54
Add Parameters to the PBXSTDNIU Process for TSW/MX-ONE .....	54
Forwarding Personal Number PROFILES– General Information .....	55

## Chapter: 4

<b>Logging .....</b>	<b>56</b>
Log Levels .....	56
Log Directory for each Component .....	56
Default software .....	57
AnA Web Service .....	57
BluStar License Manager .....	57
CMG Web and CMG Web Service .....	57
Calendar Connection .....	57
CMG Activity Information Service (CWI) .....	57
CMG Configuration manager and Directory Manager .....	57
CMG Office Web Components .....	57
CMG Server .....	57
CMG User Information Service (CWI) .....	57
Enterprise License Manager (Server and Client) .....	58
Optional software .....	58
Optional - CMG Quick (client) .....	58
Optional - BluStar Server and BluStar Presence Server .....	58
Optional - CMG AD Sync .....	58
Optional - CMG Corporate Directory for IP phone .....	58
Optional - CMG IP Phone Services for Cisco .....	58
Optional - CMG Personal Number Interface .....	58
Optional - CMG Server SQL Express backup .....	58
Optional - LSSCom Client Standalone .....	58
Optional - Mitel LDAP Server .....	59

---

<b>Chapter: 5</b>	<b>Troubleshooting . . . . .</b>	<b>60</b>
	Enterprise License Manager (ELM) . . . . .	.60
	ELM Client Installation . . . . .	.60
	ELM Server Installation . . . . .	.60
	CMG Web Trace Level . . . . .	.61
	Microsoft ODBC Drivers . . . . .	.61
	Microsoft Windows Server OS . . . . .	.62
<b>Chapter: 6</b>	<b>Appendix I – Changing to Domain Account . . . . .</b>	<b>63</b>
<b>Chapter: 7</b>	<b>Appendix II – Configuring Single Sign-On . . . . .</b>	<b>69</b>
	Single Sign-On for CMG Web . . . . .	.69
<b>Chapter: 8</b>	<b>SINGLE SIGN-ON FOR CMG WEB USING SAML . . . . .</b>	<b>71</b>
	TO CONFIGURE SINGLE SIGN-ON FOR SAML . . . . .	.71
	METADATA FILE FORMAT: . . . . .	.72
	SAML REQUEST AND RESPONSE EXPECTATIONS . . . . .	.73
	SAML AUTHENTICATION REQUEST FROM CMG WEB TO IDP: . . . . .	.73
	SAML AUTHENTICATION RESPONSE FROM IDP TO CMG: . . . . .	.73
	SAMPLE METADATA, REQUEST AND RESPONSE . . . . .	.75
<b>Chapter: 9</b>	<b>Appendix III – Using Import Export Configuration Tool . . . . .</b>	<b>79</b>
	Export Configuration . . . . .	.79
	Import Configuration . . . . .	.82
	Layout Tab . . . . .	.82
	Default Values Tab . . . . .	.83
	Import Fields Tab . . . . .	.83
	Importing the Text File . . . . .	.84
	Event Viewer . . . . .	.85
	Printing Import/Export Configuration . . . . .	.86
	Settings . . . . .	.86
	Additional Information . . . . .	.87
	Queries . . . . .	.88
	Support . . . . .	.89
<b>Chapter: 10</b>	<b>Appendix IV - Setting up User Authentication . . . . .</b>	<b>91</b>
	CMG Forms Authentication . . . . .	.91
	Windows Forms Authentication . . . . .	.91
	Windows Authentication in IIS . . . . .	.92
	Automatic Windows Forms Authentication . . . . .	.92
	Active Directory Federation Services (ADFS) Authentication . . . . .	.93
<b>Chapter: 11</b>	<b>Appendix V - CMG Web Multi-Server Deployment . . . . .</b>	<b>95</b>

---

---

	Configure Server Address for CMG Web Service . . . . .	.95
	Configure CMG Web Service . . . . .	.95
<b>Chapter: 12</b>	<b>Appendix VI - Connecting to the PBX . . . . .</b>	<b>.96</b>
	Connecting to Mitel TSW (serial) . . . . .	.96
	Before the Installation . . . . .	.96
	Installation Steps . . . . .	.96
	Verify Call Forwarding on New Activity . . . . .	.97
	Connecting to Mitel TSW (with NIU2 board) . . . . .	.97
	Before the Installation . . . . .	.97
	Installation Steps . . . . .	.98
	Verify Call Forwarding on New Activity . . . . .	.98
	Connecting to MiVoice MX-ONE . . . . .	.99
	Before the Installation . . . . .	.99
	Installation Steps . . . . .	.99
	How to add PBXSTD for multiple PBXs. . . . .	101
	Verify Call Forwarding on New Activity . . . . .	102
	Connecting to BusinessPhone . . . . .	103
	Before the Installation . . . . .	103
	Installation Steps . . . . .	103
	Verify Call Forwarding on New Activity . . . . .	104
<b>Chapter: 13</b>	<b>Appendix VII – Connecting to the E-mail System . . . . .</b>	<b>.105</b>
	Connecting to E-mail System using SMTP . . . . .	105
	Installation Steps . . . . .	105
	Configuration of the E-mail Connection in CMG CM . . . . .	106
	Verify the E-mail Function . . . . .	106
	Troubleshooting . . . . .	106
<b>Chapter: 14</b>	<b>Appendix VIII – Change Nice Password in SQL Server . . . . .</b>	<b>.107</b>
	ChangeNicePwd.exe Usage . . . . .	107
<b>Chapter: 15</b>	<b>Technical Assistance . . . . .</b>	<b>.109</b>
<b>Chapter: 16</b>	<b>References . . . . .</b>	<b>.110</b>

---

# Introduction

Mitel CMG Suite is a collaboration and presence management suite enabling business users to manage their day-to-day communications.

The **CMG package** includes the CMG Web component, enabling users to manage their activities. With the CMG Web site, users can work with “smart-search” directory services, use click-to-dial, set activity timeline and manage call-routing preferences based on the calendar/activities.

The integration with the BluStar Server enables users to see, in real-time, their colleagues’ rich presence information, including BluStar user presence status, calendar activity and line state from all available sources provided by the BluStar Server.

This document describes the configuration of **CMG**. For installation information, refer to the following documents:

- CMG Quick Installation Guide [2] - describes how to install CMG on a single server using the Mitel Installer wizard.
- CMG Installation Guide [3] - describes how to install CMG from the classic package browser, to install the components one by one.

For configuration of Calendar Connection, refer to Calendar Connection Configuration Guide [4].



# Configure CMG

When CMG has been installed, there is some configuration required for different parts of the system. This is described in the following sections, starting with an overview of the different configuration tools.

## Configuration Tools

### Configuration Manager

Configuration Manager is a web-based tool used by system administrators to configure and manage the CMG system.

You can access Configuration Manager either through Internet Explorer by entering the server address in the format: `http://<servername>/CMGCM`, or from your server where the product is installed (<http://localhost/CMGCM>).

You can also access Configuration Manager either through Edge Chromium by entering the server address in the format: `http://<servername>/CMG.CM`, or from your server where the product is installed (<http://localhost/CMG.CM>).

The starting point for working with Configuration Manager is the sidebar. The sidebar consists of headings with subheadings under which you can perform various configurations. To go to different pages, click the relevant heading.

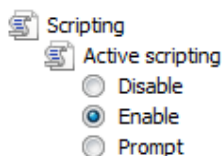
For more information about how to use Configuration Manager, see the online help. You can access the online help by clicking **Help** in the sidebar.

**NOTE:** Google Chrome and Mozilla Firefox browsers are not supported to access CMG Configuration Manager.

### Enable active scripting for Internet Explorer

Active scripting is enabled to use Internet Explorer with Configuration Manager or Directory Manager. To enable active scripting, do the following:

1. Open **Internet Explorer**.
2. Select **Tools - Internet options** from the main menu.
3. Click the **Security** tab, next click **Custom level...**
4. In the **Security Settings – Internet Zone** dialog, go to the **Scripting** section. Select **Enable** for **Active scripting**:



## Configuration Manager – Security Restrictions

As part of Polisen security issues, few characters (For example, < > ' \$ ^ -- ) are restricted, which are the malicious characters to hack the system.

Hence, it is not allowed to use these characters from CMG CM 8.4 onwards.

## Directory Manager

Directory Manager is a web-based tool including a suite of functionality for management of user information in the organization.

You can access Directory Manager either through Internet Explorer by entering the server address in the format: `http://<servername>/CMGDM`, or from your server where the product is installed (<http://localhost/CMGDM>).

You can also access Directory Manager either through Edge Chromium by entering the server address in the format: `http://<servername>/CMG.DM`, or from your server where the product is installed (<http://localhost/CMG.DM>).

The starting point for working with Directory Manager is the sidebar. The sidebar consists of headings with subheadings under which you can perform various configurations. To go to different pages, click the relevant heading.

For more information about how to use Directory Manager, see the online help. You can access the online help by clicking **Help** in the sidebar.

**NOTE:** Google Chrome and Mozilla Firefox browsers are not supported to access CMG Directory Manager.

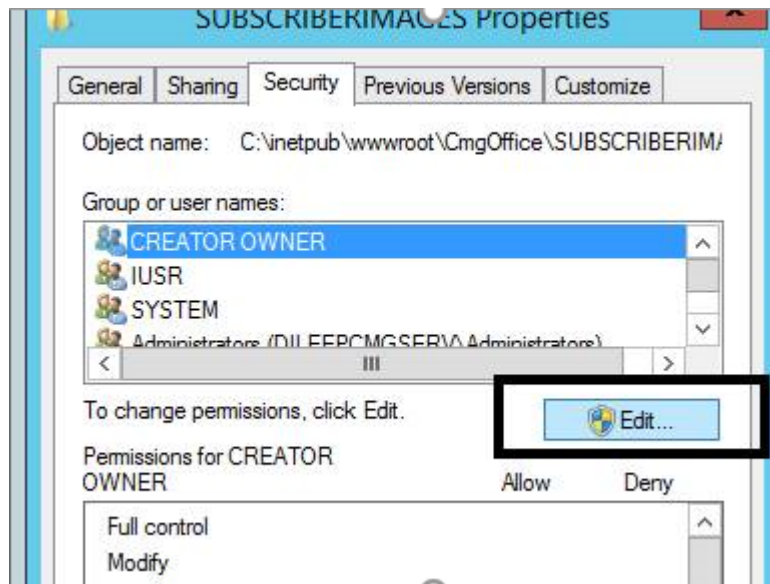
## Enable active scripting for Internet Explorer

Active scripting is enabled to use Internet Explorer with Directory Manager. This procedure is described in above section 2.1.1.1.

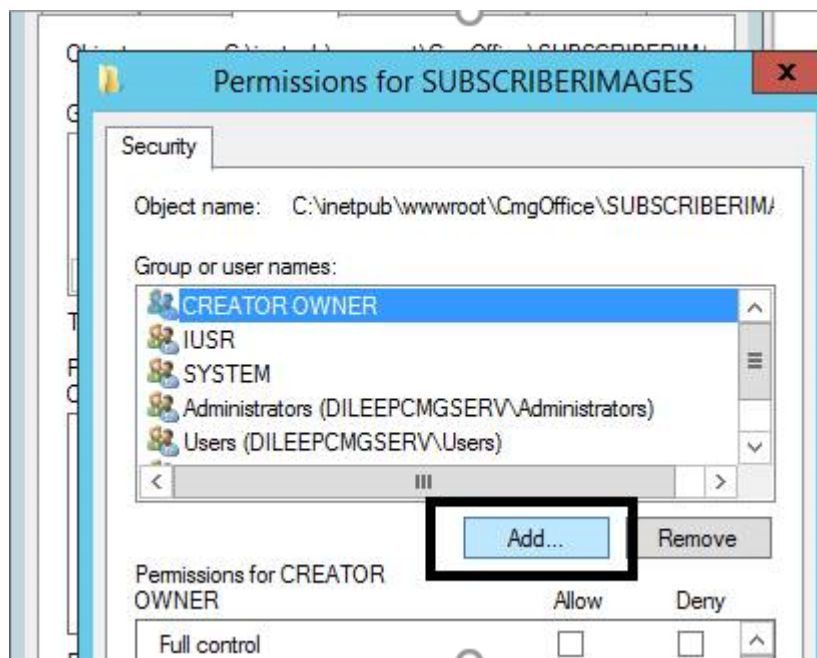
## User Image Deletion

You must configure Folder permissions to delete the User image when the User is deleted from the Directory Manager. Perform the following steps to configure the folder permissions.

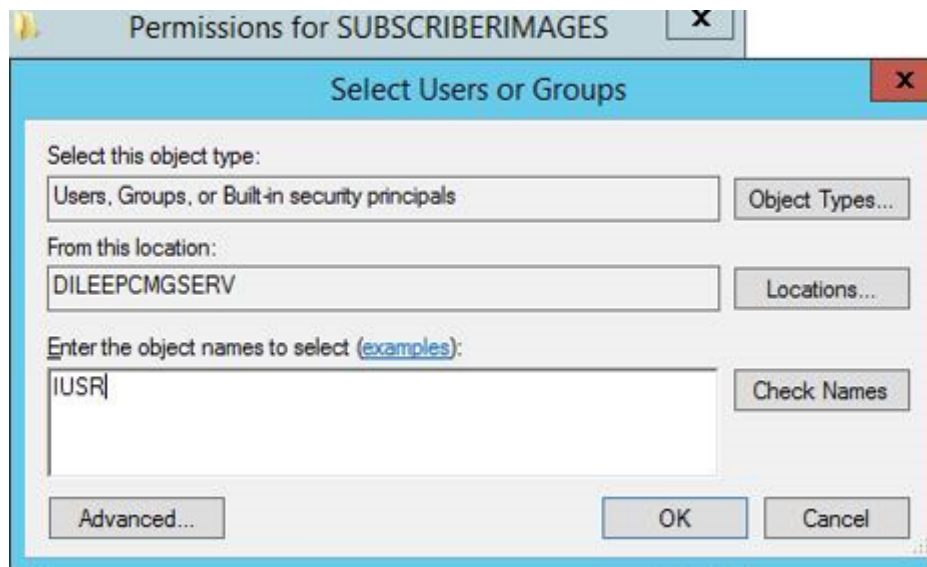
1. Browse to the physical folder that is defined in the **CMG CM > CMG Web > Parameters > LogicImageDir**.
2. Right-click, **Properties > Security tab** and click **Edit**.



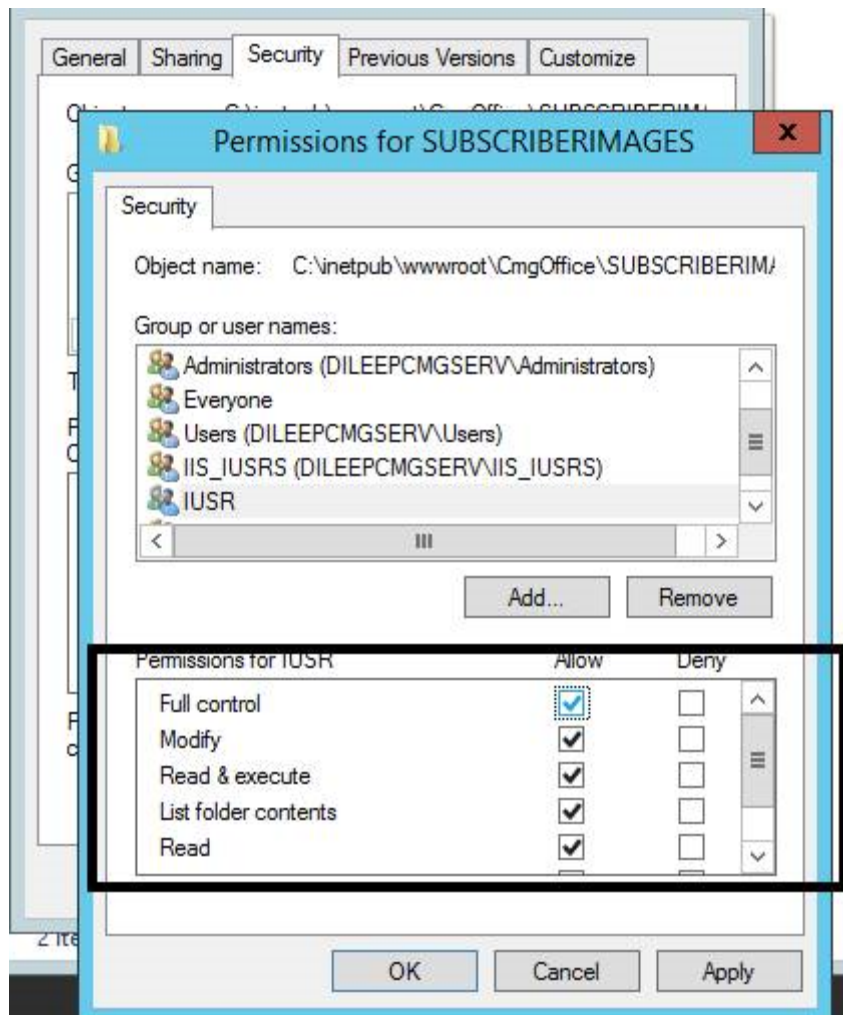
3. Click **Add**.



4. Search **IUSR** and then click **Ok**.



5. Select **Full Control** permissions for the **IUSR** user and then click **Ok**.



**NOTE:** The deletion works only when **TELNO** is mapped to **PictureField** in **CMG CM > CMG Web > Parameters > PictureField**.

PictureField	TELNO - Phone	Defines the field containing the reference to the image
--------------	---------------	---

## Configure Logging to capture deleted users from DM application

You must configure folder permissions and set the trace log level in order to generate the logs that has the details of users that are deleted from DM application:

### To Set Trace log level

Enable Trace log level by performing the following steps:

1. Log in to **CMGCM**.
2. Go to **CMG Directory manager > Advanced Parameters**.

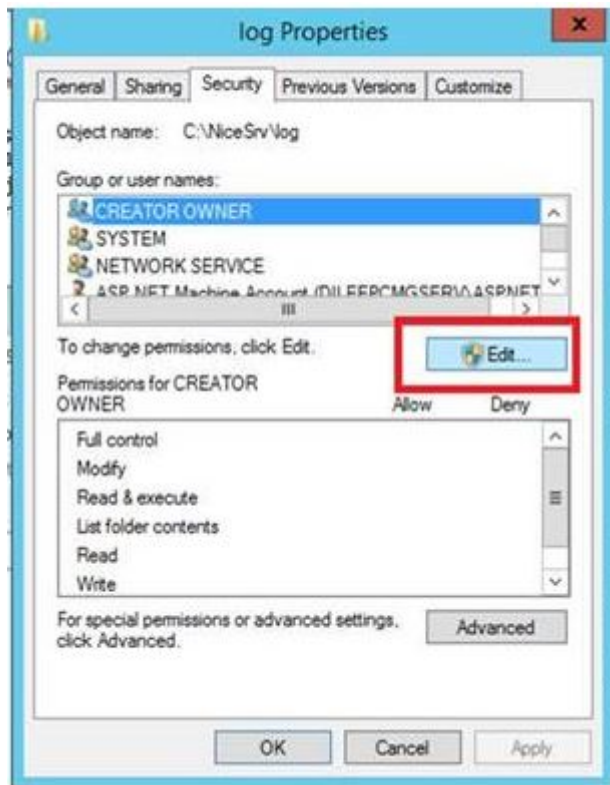
<b>CMG Directory Manager</b>
Parameters
Advanced Parameters
Standard Layouts

3. Under Log parameters, set **TraceLogLevel** to **4** and click on **Save** to save the changes.

Log Parameters		
TraceLogLevel	4	Defines trace log level. Valid values: 0,1,2,3 or 4. 0: no trace, 1:errors, 2:database update, 3: all database access, 4: MTS com components

## To Configure Folder Permissions

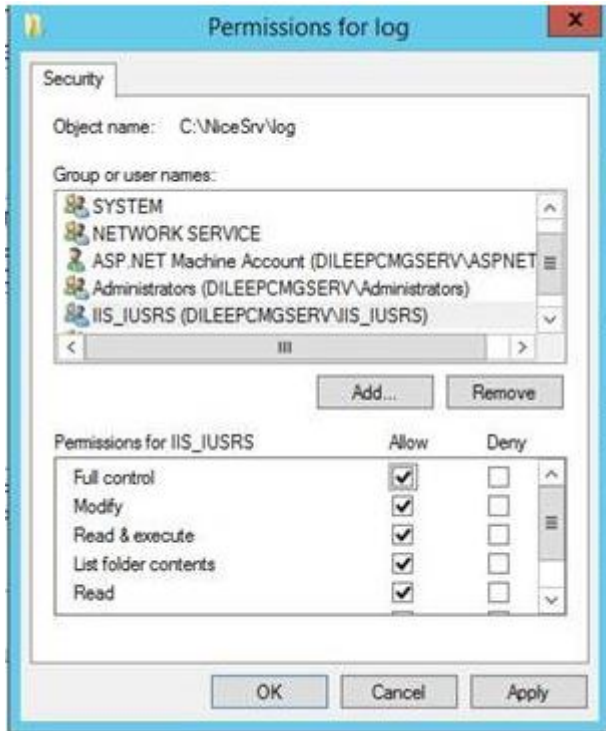
1. Browse the **C:\NiceSrv\log** folder, and then right click **log properties** dialog box opens. In that select **Properties > Security** tab. Click **Edit** button.



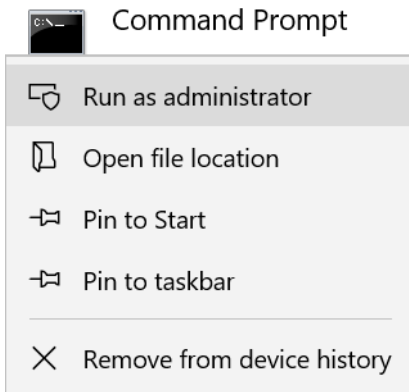
2. Click **Add**. The **Select Users or Groups** window opens.  
Enter **IIS\_IUSRS** and click **Check Names**. Click **OK**.



3. In **Permissions for IIS\_IUSRS**, select **Full control** and then click **Apply > OK**.



4. Finally reset **IIS** by following the below steps:
  - a. Open **Command prompt** with run as administrator.



- b. Type **iisreset** and click **Enter**.

## IIS Manager

IIS Manager is used to configure web applications and is opened from the Windows Control Panel.

## Spman Tool

Spman is a tool used to handle CMG processes.

To start Spman, open the **Windows Start** menu/screen and search for **Spman**.



# Configuring CMG Server Functions

This chapter includes all configuration needed for the CMG Server applications.

**NOTE:** The Windows Start Menu is not visible in Windows Server 2012/2012 R2. In Windows Server 2012/2012 R2, the different tools and applications to be used for configuration of CMG are accessed from the Windows Start Screen.

## Basic Configuration in Configuration Manager

To perform a basic configuration of CMG Server, do the following:

1. Open **CMG Configuration Manager**.
2. If needed, set up new customer groups by expanding **Site Configuration** in the sidebar and then clicking **Customer Groups**. Customer group (01) is created as default group.
3. In the database, there is a default company with default settings installed. You can edit the settings by expanding **Site Configuration** in the sidebar and then clicking **Companies/Views,Ext...** You can, for example, edit and add the following:
  - **Name**- The company name.  
**NOTE:** There can only be one company on one server.
  - **Servername** - The CMG Server.  
**NOTE:** It is recommended that you use the static numerical IP address of the server.
  - **Views** - Which customer groups that can be accessed when logged in to a certain company view. Click the **New** button, select **View** and click **OK**. In the new window, enter the name of the view in the Name field and the customer groups in the **Customer group list** field. Click **OK** when finished.
  - **Extensions**- Extensions/number series that belong to the certain company. Click the **New...** button, select **Extension** and click **OK**. In the new window, select a **PBX** from the drop-down list and enter information in the **Low number**, **High number** and **Flash ICP** fields. Click **OK** when finished.
  - Enter the activity codes of your choice by expanding **Site Configuration - Diversions** in the sidebar and then clicking **PBX Codes**. By clicking on the check boxes by the flags, you get access to editing the activity codes of different languages.  
  
**NOTE:** Consult your PBX partner to verify that the settings of the activity codes are correct.
4. Enter new users in the CMG system. Expand **Site Configuration** in the sidebar and then click **All Users**.
  - Click **New User** to set up the account. Enter values in the **Name**, **Password** and **Fullname** fields and click **OK**.
  - Click **Add Service** to set the rights for the user. Select the appropriate service rights and then click **OK**.  
  
**NOTE:** Integration with MX-ONE Provisioning Manager (user and extension management application) requires a user account with permission to access CMG Web Service Interface (CWI).
  - Select **Add User Views**by expanding **Site Configuration** in the sidebar and then clicking **Companies/Views,Ext...** Define what part of the database the user is given.



5. If desired, configure the possibility for CMG Web users to send requests to change their user information. The Change Request function is configured using Configuration Manager and Directory Manager. Do the following:
  - a. Open **CMG Configuration Manager** and expand **CMG Web**. Click **Parameters** and do the following:
    - i. Make sure **ChangeRequestMode** is set to **ENABLED**.
    - ii. Define the path to the Visitor Service webservice, **VisitorServicePath**.
  - b. Open **CMG Configuration Manager** and expand **CMG Web Components**. Click **Parameters** and do the following:
    - i. Type the e-mail address for **UpdMailTo** to the directory administrator (or an address to a group of administrators).
    - ii. Check that the path in the parameter **UpdMailSavePath** is correct.
    - iii. Create the corresponding folder for **UpdMailSavePath** at the path destination.
  - c. Open **CMG Directory Manager** and do the following:
    - i. In **Settings**, add a user with the same e-mail address as the administrator for change requests specified in CMG Configuration Manager.
6. To configure subscriber image for InAttend with CMG usage. Do the following:
  - a. Open **CMG Configuration Manager** and expand **CMG Web**.
  - b. Click **Parameters** and do the following:
    - i. Verify/change image path in: **LogicImageDir**.
    - ii. Verify/change image file extension in: **PictureFileExt**.
    - iii. If the local web server is not used, set image path (url) in: **Custom photo source URL**
7. For new parameters open **CMG Configuration Manager** and expand **CMG Web**. Click **Parameters** and do the following:
  - a. Make sure **Use live presence updates Linestate** is set to **ENABLED** for medium system with moderate requests. By default it is **DISABLED**.
  - b. Make sure **Use live presence updates Visit** is set to **ENABLED**, if Visit is used. By default it is **DISABLED**.
  - c. Make sure **Use live presence updates Voice Message** is set to **ENABLED**, if CMG Speech VM is used. By default it is **DISABLED**.

## Add an Application Pool

A classic .NET application pool is available for the **CMG web services/ applications** to enable 32-bit applications on a 64-bit Windows Server.

The application pool is automatically added during installation and named "CMG 32 Classic", but there might be situations when it has to be re-added.

To add an application pool, do the following:

1. Open IIS Manager.
2. Expand your connection.
3. Click **Application Pool...**
4. Right-click **Application Pools** and select **Add Application Pool**.

5. In the **Add Application Pool** dialog box, do the following:
  - a. Name the application pool "CMG 32 Classic".
  - b. Set the **.NET Framework** version to 2.0.
  - c. Select **Classic** from the **Managed pipeline mode** drop-down list.
6. Click **OK**.
7. Select the newly created "CMG 32 Classic" and right-click and select **Advanced Settings** from the drop down menu. Make sure the following is true:
  - a. .NET Framework Version is set to **v2.0**.
  - b. Enable 32-Bit Applications is set to **True**.
  - c. Managed Pipeline Mode is set to **Classic**.
8. Assign the CM, DM, Office, CWI, EPBXWS, and Personal Number web services/ applications to the new application pool. Do the following:
  - a. Right-click on the application name (for example CMGCM) and select **Manage application -> Advanced settings -> Application pool**.
  - b. Select the newly created application pool in the scrollbar.

## Configure BluStar Server Integration

BluStar Server integration settings are configured in **CMG Configuration Manager**. The settings can be found in the **BluStar Server** part of the **CMG Web, Parameters** section.

To integrate with BluStar Directory Server, configure the following settings:

- BluStar Directory Server
- BluStar Directory Base Path
- BluStar Directory Username
- BluStar Directory Password

To integrate with BluStar Presence Server, configure the following settings:

- BluStar Presence Server
- BluStar Presence Username

For descriptions of each setting, refer to Configuration Manager online help.

## Configure AnA to Connect to External CMG Server

The default setting is to connect to the CMG database as "localhost", using the same credentials that CMG CM/DM uses. If not default, `web.config` is configured so that the AnA web service can connect to the CMG database server.

Do the following:

1. Open `web.config` in a text editor.
2. Change the value of the below parameter by replacing `localhost` with the new CMG database server: `<add key="DefaultDatabaseServer" value="localhost"/>`
3. Change the value of the following parameter from `true` to `false`: `<add key="FetchDbUsername-Password" value="false"/>`

## Configure BluStar Presence Status

By default, the BluStar presence status function is disabled. To enable the function, do the following:

1. Open CMG Web `web.config` file in a text editor.
2. Edit the following parameter in the `<appSettings>` section, and set the value to true:  
`<add key="SetBluStarPresenceStatus" value="true"/>`
3. Restart the web service.

**NOTE:** When BSW Service connects to BluStar Presence Server for SIP presence subscriptions, the TCP protocol is used (UDP is not used).

## Enable Click-to-Dial

The Click-to-Dial function allows a user to click on a telephone number in CMG Web to call the number when using CMG Web with MiVoice MX-ONE.

**NOTE:** The call back click-to-dial option cannot be used from a “forked extension” (i.e. multiple terminals associated to the same number) in MiVoice MX-ONE. Recording of personalized voice mail greeting phrases requires that Click-to-Dial is enabled.

To enable Click-to-Dial for CMG Web, do the following:

1. Open **CMG Configuration Manager**.
2. To enable Click to Dial, expand **CMG Web** in the sidebar and then click **Parameters**.
  - a. Type in the URL to the PBX.
  - b. Set **ClickToDial** to ENABLED.
  - c. Click the **Save** button.
3. To enable Click to dial for the PBX, expand **Site configuration** in the sidebar and then click **Parameters PBX:s & Flash clients**.
  - a. Select the **Click to Dial** check-box in the **PBX:s** configuration to the right.  
**NOTE:** Click-to-Dial is only valid for MiVoice MX-ONE, not for Mitel TSW.
  - b. Specify the host name in the **Click to dial link** field.
  - c. Enter account and password in the **User Account** and **User Password** fields.  
**NOTE:** The administration user (UserAccount) and password (UserPassword) fields are not used when using MiVoice MX-ONE.
  - d. Define the prefixes for calling, in the fields:
    - i. External Prefix
    - ii. Abroad Prefix
  - e. Define the maximum number length for extensions in the **Dial Prefix** field.
  - f. Click the **Save** button.
4. Click to Dial must also be enabled for the users that should have this service. This is done in CMG Directory Manager. Do the following:
  - a. Open **CMG Directory Manager**.
  - b. For each user, click the **Settings** tab and select the **Click and dial** check-box.
  - c. Click the **Save** button.

## Configure which SMS Signature to use in Configuration Manager

Configure the SMS signature function in Configuration Manager. Do the following:

1. Open **CMG Configuration Manager** and expand **CMG Web**.
2. Click **Parameters** and do the following:
  - a. Set **SMSAutoSign** to ENABLED
  - b. Set **SMS Signature Type** to the chosen alternative:
    - i. Default (mobile)
    - ii. Extension
3. Click **Save**.

## Enable Time Zone Functionality

There are two options for time zone handling in CMG:

- **No time zone handling**  
Suitable only when all users are in the same place as the server.
- **Time zone handling**  
CMG handles different time zones and daylight saving times. All time fields are displayed and stored according to the time zone of the database server. If a CMG database contains data for subscribers from more than one time zone, the time is displayed according to the time zone of the client, but still stored according to the time zone of the server. This applies to the CMG Quick, InAttend client, and to the CMG Web application.  
**For example:** If a Danish CMG Web user surfs from a PC with a regional setting for the Danish time zone, he will get all time references in Danish time whether he looks at his own CMG data or the data of a colleague in New Orleans.

### NOTE:

- By default, the time zone in the InAttend client is set to the same time zone as the server. See the InAttend user guides for information on how to change the time zone.
- By default, the time zone in CMG Web is set to the same time zone as the server.
- The time zone in CMG DM is the same as for the server, and cannot be changed.

The following sections describe how to enable time zone functionality for the different CMG applications.

### CMG Web

To enable Time Zone functionality for CMG Web, do the following:

1. Open **CMG Configuration Manager**.
2. Expand **Site Configuration** in the sidebar and click **System Parameters**.
3. Scroll to **Time zone parameters**. Do the following:
  - a. Set **TimeZone** to ENABLED.
  - b. Set **TimeZoneAdv** to ENABLED.
  - c. Set the **TimeZonedId** for the server. It is important that this time zone is the same as on the used database server.

**NOTE:** If you change the TimeZonedId, you need to restart NICESRV.

4. Click Save.
5. Restart CMG Web on all clients.
6. All users in CMG Directory Manager need to have their time zone defined. This is done from Settings for each user in CMG Directory Manager.

**NOTE:** Remember to specify time zone when adding new users.  
Also remember to remove time zone value when disabling.

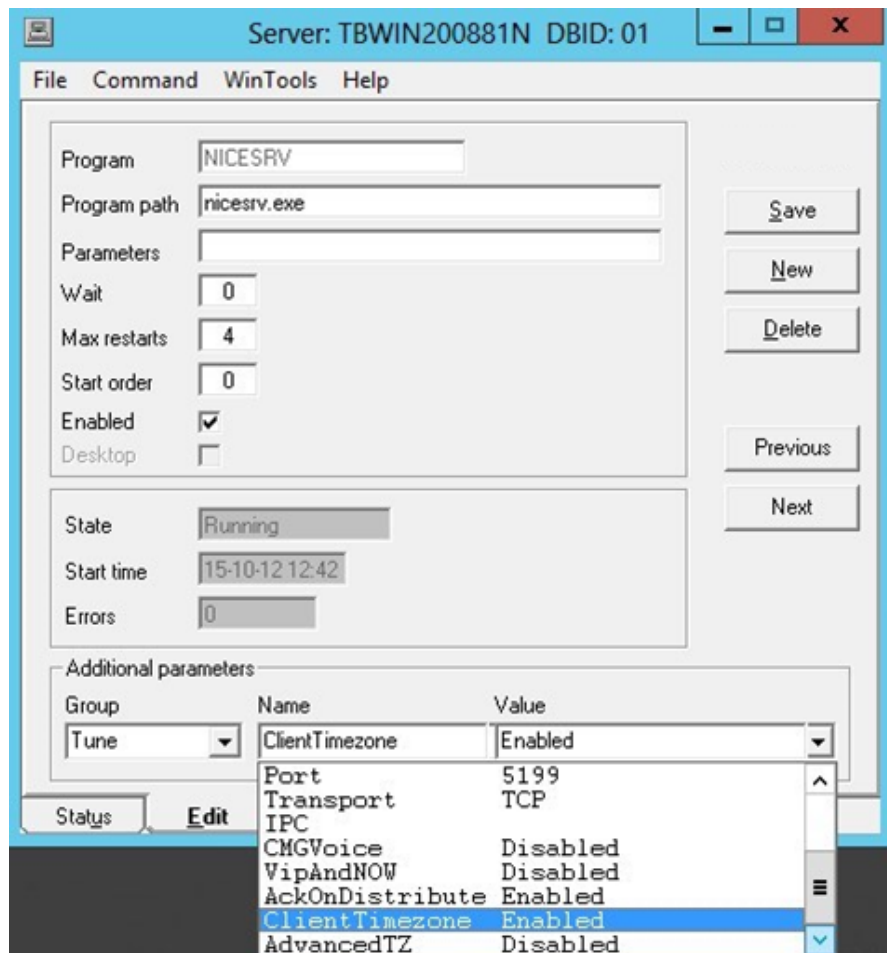
### InAttend client

To enable Time Zone functionality for the InAttend client, do the following:

1. Open Spman tool.

**NOTE:** If any of the variables listed below does not exist, create it and set it to **Enabled**.

2. For the NICESRV process, set the **ClientTimezone** variable to **Enabled**. See the example in the figure below.
3. For the NICESRV process, set **AdvancedTZ** to **Enabled**.
4. For the DBTOPBX process, set **Timezone** to **Enabled**.
5. For the PBXIR process, set **Timezone** to **Enabled**.
6. Save and restart the processes.



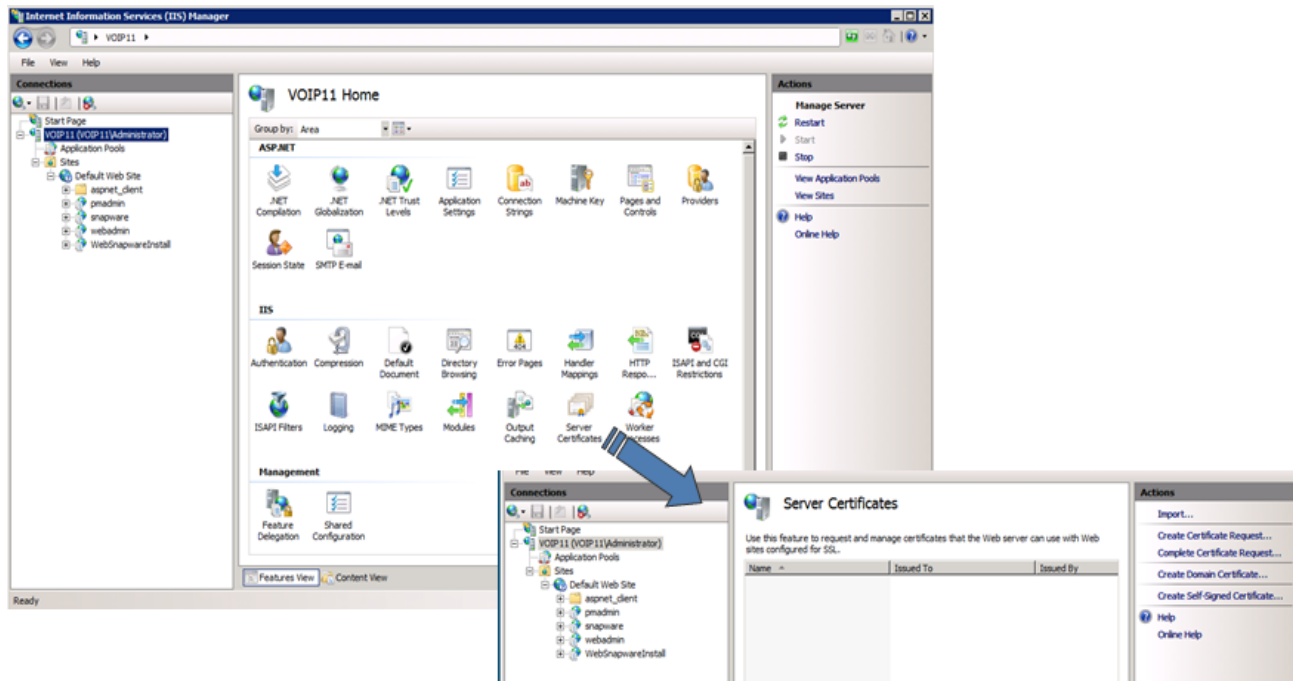
7. Restart InAttend client.
8. All users in CMG Directory Manager need to have their time zone defined. This is done from **Settings** for each user in CMG Directory Manager.

**NOTE:** Remember to specify time zone when adding new users. Also, remember to remove time zone value when disabling.

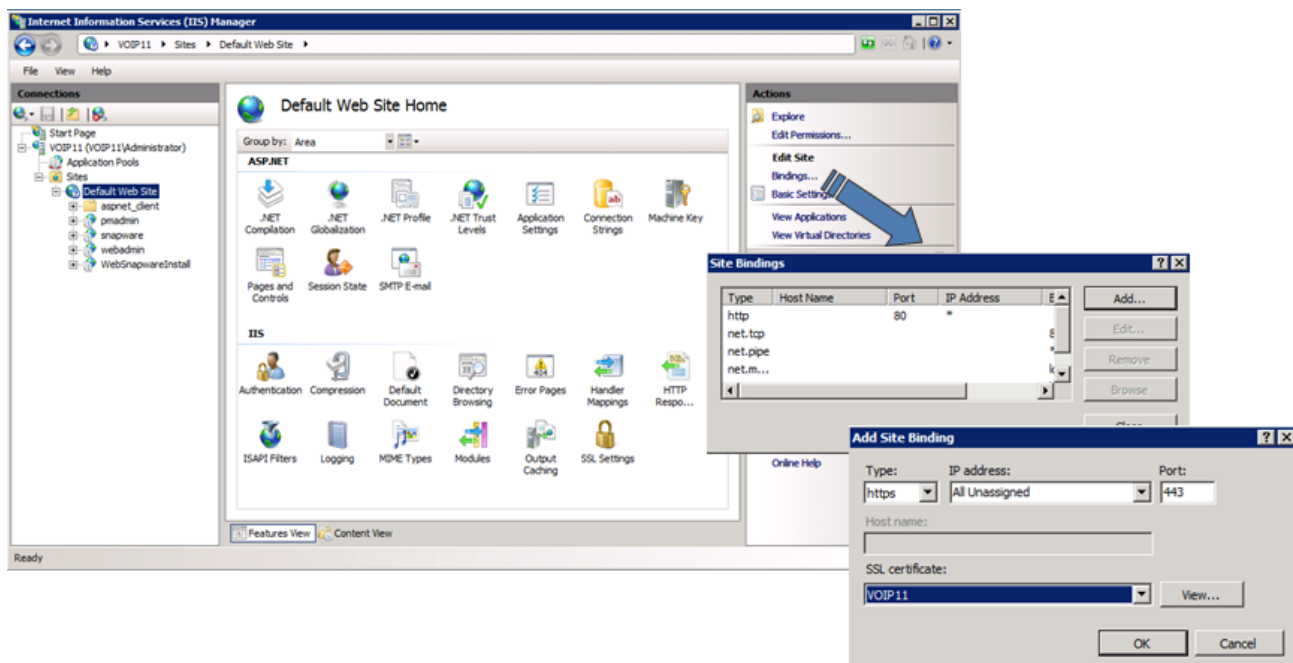
## IIS configuration to access CMG CM, CMG DM and CMG WEB applications over HTTPS

To access CMG CM and CMG DM Applications over https, do the following:

1. Create or import a server certification from the **IIS server** as shown in below screenshot.



2. Go to **Sites > Default Web Site**.
3. Click on **Bindings** in the right-side pane and add a new https binding by choosing a certificate created in the first step as shown in the below screenshot.

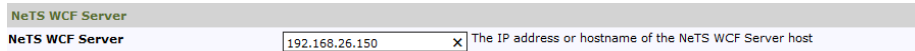


**NOTE:** All the above settings are valid for CMG Web that you can access it over https.

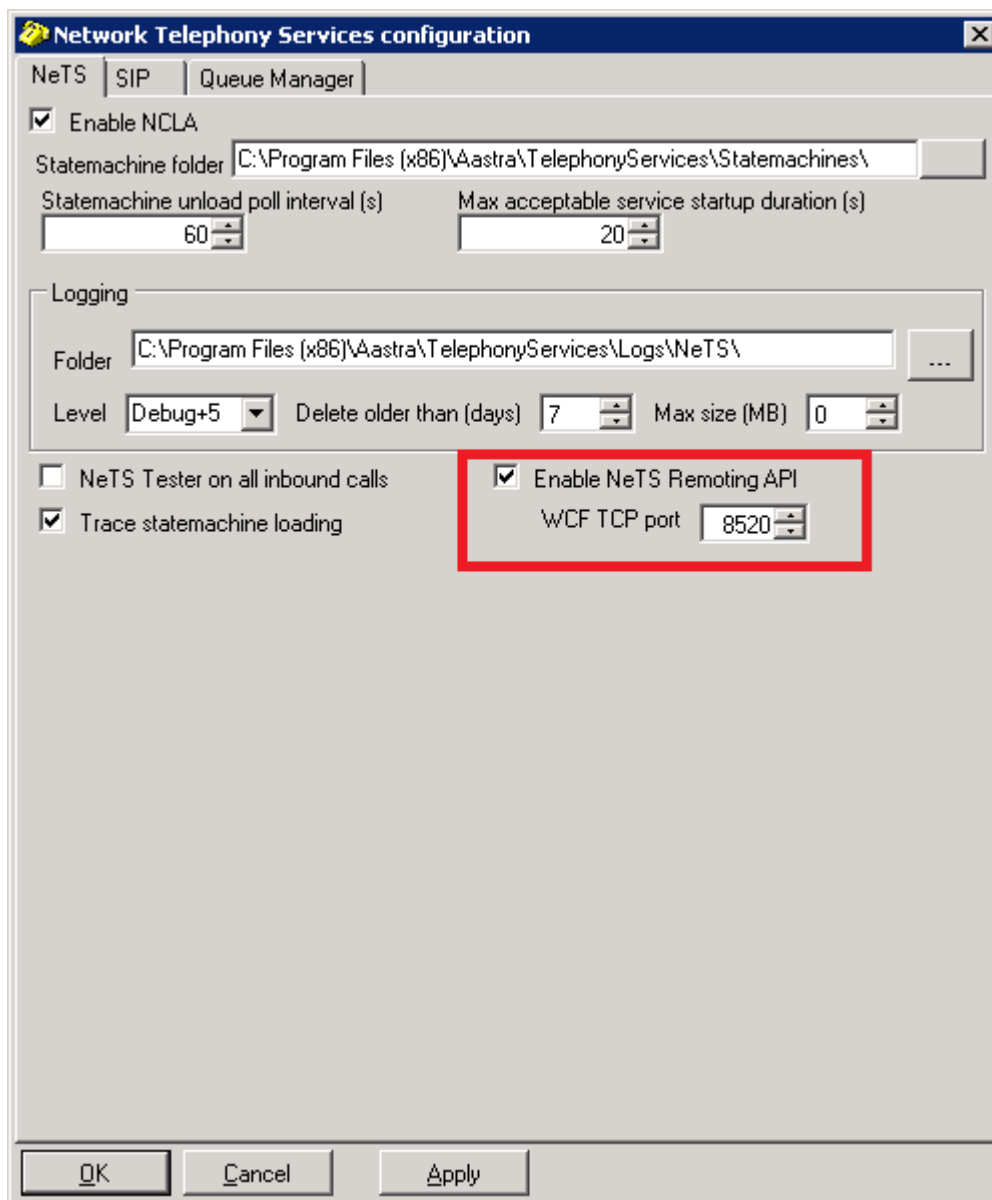
## Configure NeTS WCF Server

To record CMF Speech phrases from CMG Web, perform the following steps and make the required configuration in NeTS.

1. Go to **CMG CM > CMG Web > Parameters > Nets WCF Server**, enter the NeTs server IP address.



2. In the server where NeTS is installed, open the NeTs configuration tool.
3. In the NeTS tab, select the **Enable NeTS Remoting API** check-box.
4. Enter the port number in the **WCF TCP port** field.





5. Log on to the CMG Web application and go to **Preferences > Voice Service > Phrases**.
6. Enter a valid number to record a phrase and click **Call**.

Phrases | Menus | Notifications | Settings

Language: English (US) [v]

[Call] 1002 [x] [Hang Up]

7. Select any phrase that you want to record and click **Record**.

Greeting phrase: General | Menu: Default menu [v] | Voice: My | Length: [x]

Greeting phrase - General

[Play] [Record] [Close]

**NOTE:** The record button is enabled only if the call is made by entering the correct number in step 6.

## Backing up the CMG Database

The CMG setup program creates four backup jobs for backup and maintenance of the CMG database. A backup job is scheduled to run every night at 1.00 AM. The five most recent backups are kept and older backups are purged. The part of the registry where the CMG system stores startup information is also backed up.

The backups are created as disk files in the SQL sub directory, for example:

```
C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Backup\.
```

**NOTE:** If you run SQL Express, you need to create the backup tasks manually since scheduled tasks are not supported by SQL Express. Follow the procedure in section 3.1 to add the CMG SQL Express backup as a scheduled task.

## Optimizing Nicesrv

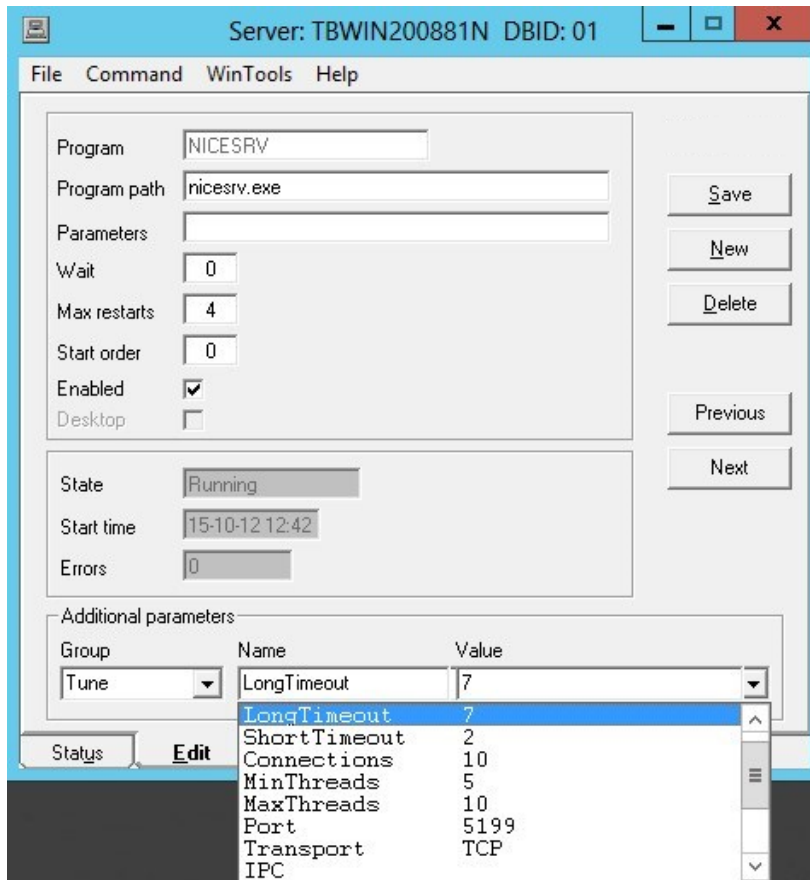
Nicesrv is the process used by InAttend client for accessing the database. Optimization of nicesrv is achieved using the following formula:

MaxThreads = NumberOfAttendants \* 4

MinThreads = 0.75 \* MaxThreads

Connections = MaxThreads

Open the **Spman tool** and set the **NICESRV** parameters:



## Configuring Advanced Security

You can set basic or advanced security for CMG users. Advanced security means that higher standards can be set for users with regard to password quality, with the possibility, for example, of locking them out after failing to log in.

Advanced security is managed in Configuration Manager, and the function is enabled with the Advanced-Security parameter.

### User Management

The following is a summary of the advanced security settings for users:

- A user can be set to inactive or be deleted due to inactivity if the user has not logged for a certain number of days.
- A user can be locked out of the system after a specified number of failed log in attempts.
- An administrator can specify that a password never expires for a user.
- An administrator can force a password change for a user in the following cases:
  - After an account expiry
  - At the next log in
  - After account activation

- After an account has been unlocked
- An administrator can manage the settings for users and an administrator account can never be deleted, locked out or expire.

## Security Parameters in Configuration Manager

The following advanced security parameters can be set in CMG CM:

Security Parameter	Description
AdvancedSecurity	Set to Enabled to turn on the advanced security functions. This means that the parameters below are used.
DaysUntilLockout	Number of days an account can be inactive before it is locked. After that, the account is unlocked by the administrator.
ForcePasswordChangeOnReset	If set to Enabled, the user must change the password when the account is reset (i.e., activated after lockout or inactivation).
DaysUntilDelete	Number of days an account can be inactive before it is deleted. A system account cannot be deleted.
MaxLogonErrors	Number of failed login attempts before the account is locked. A system account is permitted an infinite number of login attempts.
PwdExpirationIntStd	Number of days a user has to change the password, before the password expires. A system account never expires.
PwdExpirationIntAdm	Number of days a Configuration Manager and Directory Manager user has to change the password, before it expires.
UserMustChangePwdFirstLogon	If set to Enabled, the user must change the password when logging in for the first time.
MinPasswordLength	Minimum number of characters in the password.
MinUserNameLength	Minimum number of characters in the user name
PasswordRules	If set to 0, all passwords with the required number of characters are allowed. If set to 1, the password can contain only alphanumeric characters (a-z, 0-9), and at least one character is numeric and one character is a letter.

## Configuring EFS

Encrypting File System (EFS) is a feature that provides filesystem-level encryption.

It is recommended to enable EFS on the folders where the application log, trace files and database backups are stored. This will ensure the prevention of unauthorized access.

You must run Nice server in service manager console using nice credentials. Nice credentials can also have administrator privileges.

Encryption for CMG should be done with nice user account only.

For Reference of log files that needs to be encrypted – see Section 4.2 Log Directory for each Component.

## Setting up Connection to the Telephony System (PBX)

There are different installation and configuration procedures for the communication between a CMG Server and a PBX system.

### Connection to Cisco Call Manager Systems

To set up the connection to a Cisco Unified Communication Manager (CUCM) system, please refer to Attendant Connectivity Server (ACS) documentation.

### Connection to Other Systems

To set up the connection to another system than CUCM, see Appendix VI - Connecting to the PBX.

## Setting up Connection to the E-mail System

After establishing the connection between the PBX and the CMG system, you must set up the connection to the e-mail system.

Supported e-mail systems are:

- IMAP (Internet Message Access Protocol)

To set up the connection to the e-mail system, see Appendix VII – Connecting to the E-mail System.

## Configuring MX-ONE Provisioning Manager Integration

When an organization unit is created or updated through the MX-ONE Provisioning Manager system, PM sends the new information on to CMG so that the changes can be reflected in the CMG system as well. For this to work, a number of parameters are configured in the `web.config` file for CWI User Information service.

The parameters in the following table are implemented to support the MP integration:

Parameter	Value
CreateOrg	Set this parameter value to “True” to create organization units that do not exist in CMG.

Parameter	Value
DeleteOrg	Set this parameter value to “True” to delete organization units that not are in use.
AddAppNameOrg	This parameter value indicates which application has created the new organization unit, or updated an existing one.

To configure the MP integration, do the following:

Open a text editor and edit the file: `C:\inetpub\wwwroot\CMGUserInformationService\web.config`

Add the parameters according to the example:

```
<appSettings>
```

```
...
```

```
...
```

```
<add key="CreateOrg" value="True"/>
```

```
<add key="DeleteOrg" value="True"/>
```

```
<add key="AddAppNameOrg" value="Created by MP"/>
```

```
...
```

```
...
```

```
</appSettings>
```

## Configuring Active Directory Synchronization

Configuration of Active Directory (AD) synchronization is performed using CMG CM. For further information regarding CMG CM, see CMG – CMG Web Configuration Guide or the built-in Help section.

### Information to Configure

When configuration of the below parameters are completed please click on the “Save” button. To activate the synchronization please mark the checkbox for “Activate” and click on “Save” again.

The parameters are located in: CMG CM >> Active Directory Sync >> Parameters

Parameter	Type	Example	Description
Address	Field	ADsrv.company.com	Address of the AD directory
Port	Field	389	Default port to access the AD directory. Verify with the customer IT department.
Username	Field	CmgAdSync	Username to connect to AD (with read rights)
Password	Field	*****	Password to the above user
Use TLS/SSL	FALSE/TRUE (Will be checkbox)	False	Specifies whether SSL has to be used or not to connect to AD
Activate	FALSE/TRUE (Will be checkbox)	False	To enable or disable the AD synchronization
Directory	Field	DC=Mitel, DC=com	Path to retrieve users from AD
Prefix	Field	+468123	Prefix for internal number (i.e. presence of the prefix in the number identifies it as an internal number)
Extension length 1	Field	5	Length of extension for internal number (i.e. if number in E.164 format is +46812345678, internal number is 45678)
PBX ID 2	Scrollbar	1	ID of PBX for every user who has an internal number. This parameter can be undefined. In this case, no PBX ID is set for the user.
Msg sys ID	Scrollbar	1	Message system number in CMG to access e-mail address of the user (i.e. to know where to store and retrieve e-mail address of the user)
Poll Interval	Field	5	Minimum interval between each synchronization (in minutes)

1. If extension length is changed after the first synchronization (not typical), the phone number of users already imported will not be changed, unless some data are changed in AD for this user (which means that a new synchronization is performed). In this case, the phone number is re-imported with the new extension length.
2. PBX ID is only set during the first synchronization (i.e., creation of the user in CMG database). If PBX is changed in CMG database after this first synchronization, it is not changed if a new synchronization is performed on this user (synchronization is performed if some data is changed in AD for this user).

## Deletion of Users

When a user is deleted in AD, it is not deleted in CMG, but it is rendered inactive. Specifically:

- Phone number is removed from the Phone field in CMG
- PBX is set to None
- The checkbox for “Main record” is set to be un-marked
- All privileges (such as CMG Web user, Visit user, etc) are removed
- Calendar synchronization is disabled

**NOTE:** If a user existing in AD is removed in CMG, it will not be created in CMG again until:

- any data for the user is changed in AD
- the AD Synchronization service is restarted

## Change of Synchronized Users in Active Directory

If an already synchronized user gets the TelePhoneNumber removed in AD, it is kept in CMG. The same applies for mail addresses as well.

## ADSYNCCFG tool

More fields can now be synchronized from AD to CMG with the ADSyncCfg tool

```
(\nicesrv\pgm\ADSyncCfg.exe) .
```

This tool creates a XML-file that ADSync Service uses.

The required parameters are:

1. Filter: LDAP filter filters the records that have to be synchronized. Example: Company=Mitel, co=Sweden, co=se, co=dk (can also be empty).
2. Field in AD: The name of the field in AD.  
Example: title, description, homePhone, pager, physicalDeliveryOfficeName.
3. Field in CMG: The name of the field in CMG.  
Example: misc1, misc2...misc30, cordless, division, dep1, dep2.
4. InitOnly:
  - If checked, synchronization will only be executed the first time ADSync runs and the record is created in CMG.
  - If unchecked, synchronization is executed every x minute.
  - The interval is set in CMG CM ADSync Parameters.  
Further configuration is done in CMG CM ADSync Parameters.

## Mapping configuration for other fields from AD to CMG

**NOTE:** The easiest way to add or remove fields is to use the ADSyncCfg tool.

Editing the config file in Notepad (or similar) will not be reflected in the ADSyncCfg tool. Only use Notepad, if more than 12 fields are going to be synchronized.

To synchronize other fields from AD to CMG predefined fields, update the config file: %Program Files%\Mitel\ADSyncService\ADSyncConfiguration.xml as below:

```
<ADSyncConfiguration filter="(|(co=sweden)(co=se)(co=dk))">
```

```
<Mapping AD="title" CMG="misc7" InitOnly="false"/>
```

```
<Mapping AD="description" CMG="misc19" InitOnly="false"/>
```

...

...

```
</ADSyncConfiguration>
```

PARAMETER	EXAMPLE	DESCRIPTION
Filter	<code>( (co=sweden)(co=se)(co=dk))</code>	Filter specifies the conditions that have to be met for a user to be sync from AD to CMG.() is used to separate each filter.  is used for OR condition between every specified filter.



AD	Title	Name of the field in the AD.
CMG	misc7	Name of the field in CMG.
InitOnly	"true" or "false"	true: the value of the AD mapping field is only imported when you make the first synchronization. false: if the mapping field value is changed in AD, then always synchronization is performed and the value is changed in CMG.

To change the Log Level in AD Sync, edit:

```
%Program Files%\Mitel\ADSyncService\ADSyncService.exe.config
```

for AD Sync and update LogLevel:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
...
<setting name="LogLevel" serializeAs="String">
<value>7</value>
</setting>
...
</configuration>
```

Valid values are 1, 2, 3, 4, 5, 6 and 7. If not set, the log level is set to 3.

## Customize CMG Web

How to customize CMG Web with customer logo/pictures and text:

- The CMG Web images are stored on the web server and can be replaced by more customized images.
- The welcome title and text for CMG Web are changed in CMG CM.
- The directories names to search in, are also changed in CMG CM

[Corporate Phone Book](#) [BluStar Server](#) [Quick Info](#) ▼

**NOTE:** Any change of the images must be approved by Mitel.

# CUSTOMIZE CUSTOMER GROUP SEARCH

## INFORMATION TO CONFIGURE

1. User can add more than one customer groups by selecting Customer groups tab under Site Configuration in CMG CM.

The screenshot shows the Mitel CMG Configuration Manager interface. On the left is a sidebar with the 'Customer Groups' tab selected under 'Site Configuration'. The main area is titled 'Customer Groups' and contains a table with columns 'Custgrp ID', 'Name', and 'Delete'. A single entry is visible with 'ID : 1' and 'Name: CUSTGRP1'.

Custgrp ID	Name	Delete
ID : 1	CUSTGRP1	[Delete Icon]

2. Enable **Search all customer groups (Cust-grp)** parameter under **CMG Web - Parameters** in CMG CM.

The screenshot shows the 'CMG Web - Parameters' configuration page. A table lists various parameters. The 'Search all customer groups' parameter is highlighted in green and is set to 'ENABLED'.

Parameter	Value	Description
Welcome Text		Override the welcome text displayed in the web browser for CMG Web
BlueStar/LDAP Directory Server		The IP or hostname of BlueStar/LDAP Directory Server
BlueStar/LDAP Directory Base Path		The LDAP Base Path for BlueStar Directory searches
BlueStar/LDAP Directory Username		Username for BlueStar/LDAP Directory Server
BlueStar/LDAP Directory Password		Password for BlueStar/LDAP Directory Server
BlueStar Presence Server	localhost:5062	Hostname or IP to BlueStar Presence Server. Port name can optionally be specified using :port
BlueStar Presence Username	blustarweb@aantra.com	Specify the From SIP address when connecting to BlueStar Presence Server.
BlueStar Presence Local Address		Local IP address of the interface to use for communication with BlueStar Presence Server. Parameter needed if multiple network interfaces are used.
OfficeWeb	cmgoffice	Virtual directory of Office Web, e.g. CMGOffice.
Default Quick Activities	1, 0, 8, 1	A comma separated list of activity reason identifiers to use as default for Quick activity buttons
Search all customer groups	ENABLED	If enabled, possible to search in all selected customer groups, else its only limited to user logged in customer group.
View Customer Group Name	DISABLED	If enabled, the customer group name will be display on the web
LogicImageDir	/CMGOffice/subscribeimages	Defines the logical image directory (Format: E.g. /CMGOffice/subscribeimages)

3. Assign users to the Customer groups (**Cust-grp**) in CMG DM when the above configuration is done as shown in the following figure.

4. Click **Save**.

## CUSTOMER GROUP SEARCH IN CMG WEB

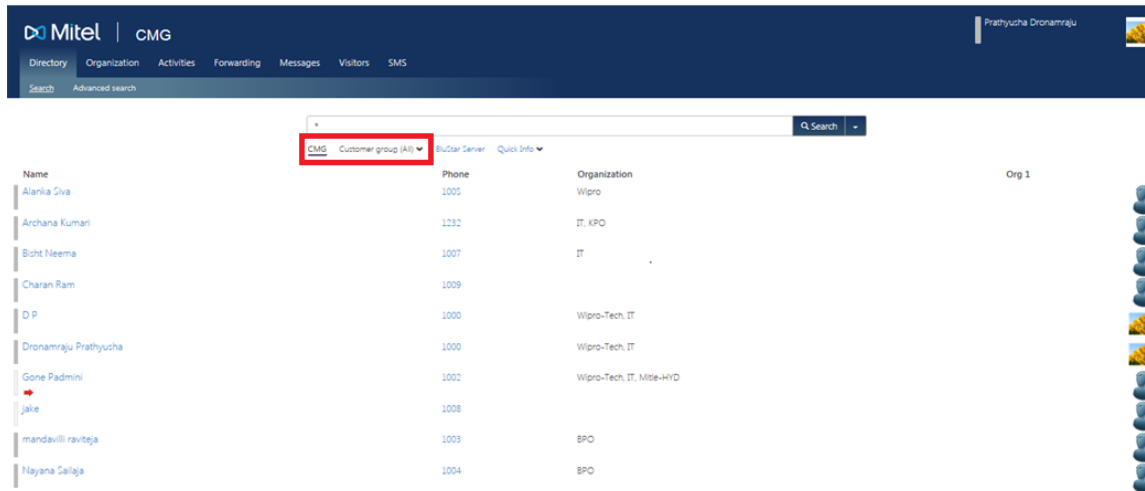
1. If **Search all customer groups** parameter in CMG CM is enabled, then the customer groups list is shown in CMG Web as shown in the following figure.

**NOTE:** The **All** option only gets displayed when the **Search all customer group** parameter is enabled.

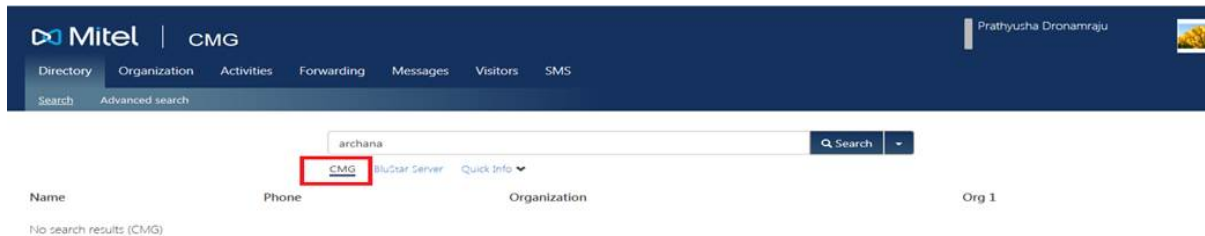
2. Select a **Customer group** from the drop-down list and search for the desired users.

Name	Phone	Organization	Org 1
Archana Kumari	1232	IT, KPO	
mandavilli raviteja	1003	BPO	
Nayana Sailaja	1004	BPO	
Racharla Akhila	2222		
Sai Kumar	1010		
thadakamalla jagadish	1001	Wipro	

3. If you select **All** as an option, then you can able to see all the added/existing users irrespective of **Customer groups** assigned.

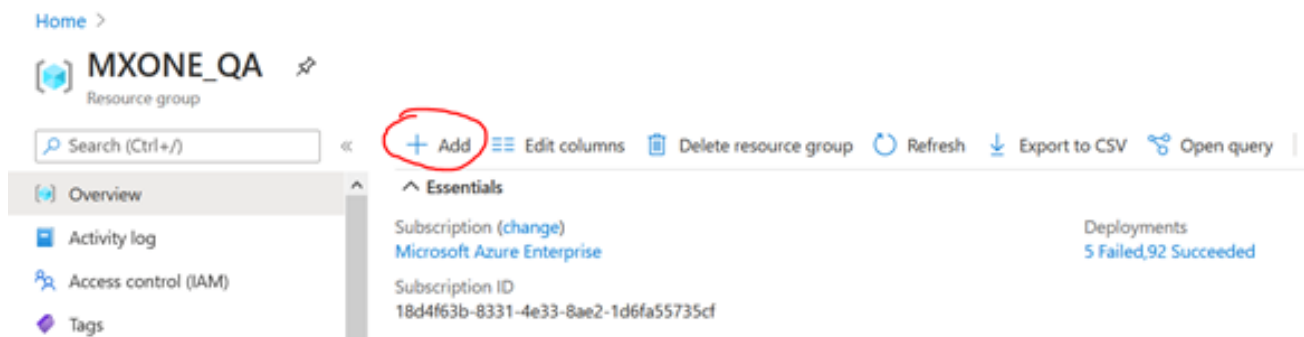


**NOTE:** If **Search all customer groups** parameter is disabled in CMG CM, then **Customer group search option** is not visible in CMG Web. The searches are done against currently logged in user's customer group.

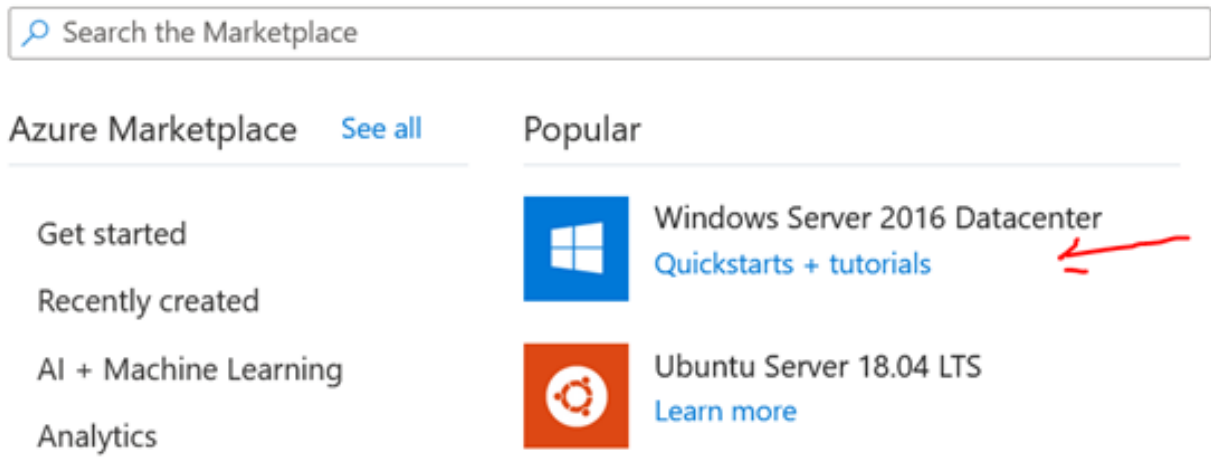


## CMG Installation-Configuration on Azure

1. Log in to the Azure portal.
2. Go to the Resource group and click Add to create a virtual machine.



3. Choose any Windows server version; for example, Windows Server 2016.



4. Provide all the necessary details as shown in the following screen capture.

[Home](#) > [MXONE\\_QA](#) > [New](#) >

## Create a virtual machine

Subscription \* ⓘ

Microsoft Azure Enterprise (18d4f63b-8331-4e33-8ae2-1d6fa55735cf) ▼

Resource group \* ⓘ

MXONE\_QA ▼

[Create new](#)

### Instance details

Virtual machine name \* ⓘ

Region \* ⓘ

(US) South Central US ▼

Availability options ⓘ

No infrastructure redundancy required ▼

Image \* ⓘ

Windows Server 2016 Datacenter - Gen1 ▼

[Browse all public and private images](#)

Azure Spot instance ⓘ

☐ Yes ☒ No

Size \* ⓘ

Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (CA\$197.10/month) ▼

[Select size](#)

### Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \* ⓘ

☐ None ☒ Allow selected ports

Select inbound ports \*

HTTP (80), HTTPS (443), RDP (3389) ^

☒ HTTP (80)☒ HTTPS (443)☐ SSH (22)☒ RDP (3389)

### Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing Windows ☐ Yes ☒ No

Server license? \* ⓘ

[Review Azure hybrid benefit compliance](#)

5. Select the review+create tab. The virtual machine is created.
6. Go to Networking and check the Network Interface details.

Search (Ctrl+/) << Connect Start Restart Stop Capture Delete Refresh Share to mobile

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Security

Advisor recommendations

Essentials

Resource group (change) MXONE\_QA

Status Stopped (deallocated)

Location South India

Subscription (change) Microsoft Azure Enterprise

Subscription ID 18d4f63b-8331-4e33-8ae2-1d6fa55735cf

Tags (change) Click here to add tags

Operating system Windows

Size Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address -

Virtual network/subnet MXONE\_QA\_Subnets/Subnet\_172\_20\_112.0-24

DNS name -

Attach network interface Detach network interface

certificate-server-s182

IP configuration ipconfig1 (Primary)

Network Interface: certificate-server-s182 Effective security rules Topology

Virtual network/subnet: MXONE\_QA\_Subnets/Subnet\_172\_20\_112.0-24 NIC Public IP: - NIC Private IP: 172.20.112.46 Accelerated networking: Disal

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group CertificateServerSubhankarnsg125 (attached to network interface: certificate-server-s182) Add inbound port rule

Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination
300	RDP	3389	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork

- Go to IP configurations and provide the static IP address.

Search (Ctrl+/) << Add Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

IP forwarding settings

IP forwarding Disabled Enabled

Virtual network MXONE\_QA\_Subnets

IP configurations

Subnet Subnet\_172\_20\_112.0-24 (172.20.112.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	172.20.112.46 (Static)	-

- After the IP address is assigned, use remote desktop and start CMG installation and configuration. Refer to CMG documentation for CMG installation and configuration for details.

# Setting up CMG Web for Visual Voicemail in the MiCollab Client

## Before you Begin

Before you can set up CMG Web for Visual Voicemail in the MiCollab Client, CMG Web must be enabled for HTTPS and the value of the HTMLAudioControlPlay setting in the Web.MiCollab.config file must be set to true. If it is not possible to do these in the existing CMG Web, create a new website for MiCollab's usage.

**NOTE:** If the MiCollab application is accessible from the internet (Teleworker), the CMG Web must be accessible from internet as well, otherwise this will only be accessible in LAN mode.

## Procedure

To set up CMG Web for Visual Voicemail in the MiCollab Client:

1. Edit the Web.MiCollab.config file in the (C:\inetpub\wwwroot\CMGWeb) location.
2. Update **MiCollabFQDN** and **CMGWebFQDN** (in two places) to the MiCollab server FQDN and the CMGWeb server FQDN.
3. Copy or rename the Web.MiCollab.config to Web.config on C:\inetpub\wwwroot\CMGWeb.
4. Log in to the **Server Manager Configuration** panel for the MiCollab application.
5. Go to **Applications > MiCollab Client Service > MiCollab Client Service Configuration**.

**Mitel | MiCollab**

**Applications**

- Users and Services
- Audio, Web and Video Conferencing
- MiVoice Border Gateway
- NuPoint Web Console
- MiCollab Client Service**
- MiCollab Client Deployment
- Licensing Information

**ServiceLink**

- Install Applications
- Status

**Administration**

- Web services
- Backup
- Restore
- View log files
- Event viewer
- System information
- System monitoring
- System users
- Shutdown or reboot
- Virtualization

**Configuration**

- Integrated Directory Service
- MiCollab Client Integration Wizard
- MiCollab Settings

**MiCollab Client Service Configuration**

Enterprise Synchronization PBX Nodes Accounts Corporate Directory ACD Settings Collaboration Features Peering Federation User Profiles

This page contains enterprise-wide configuration settings, including the ability to create and delete enterprises.

**Settings**

Enterprise ID: micollab

Description: MiCollab Client Service on micollab.enterprisedemo.net

Enterprise domain: micollab.enterprisedemo.net

Voice mail server type: ☐ NuPoint ☒ MiCollab Advanced Messaging ☐ EMEM

MiCollab AM URL: CMGWEBFQDN/CMGWeb/messages/

Administrator e-mail: brousk@enterprisedemo.net

Switch type: MiVoice MX-ONE

Collaboration server type: MiCollab Audio, Web and Video Conferencing

Avatar URL: http://micollab.enterprisedemo.net/uos/avatar/dn/micollab/

Language: Swedish

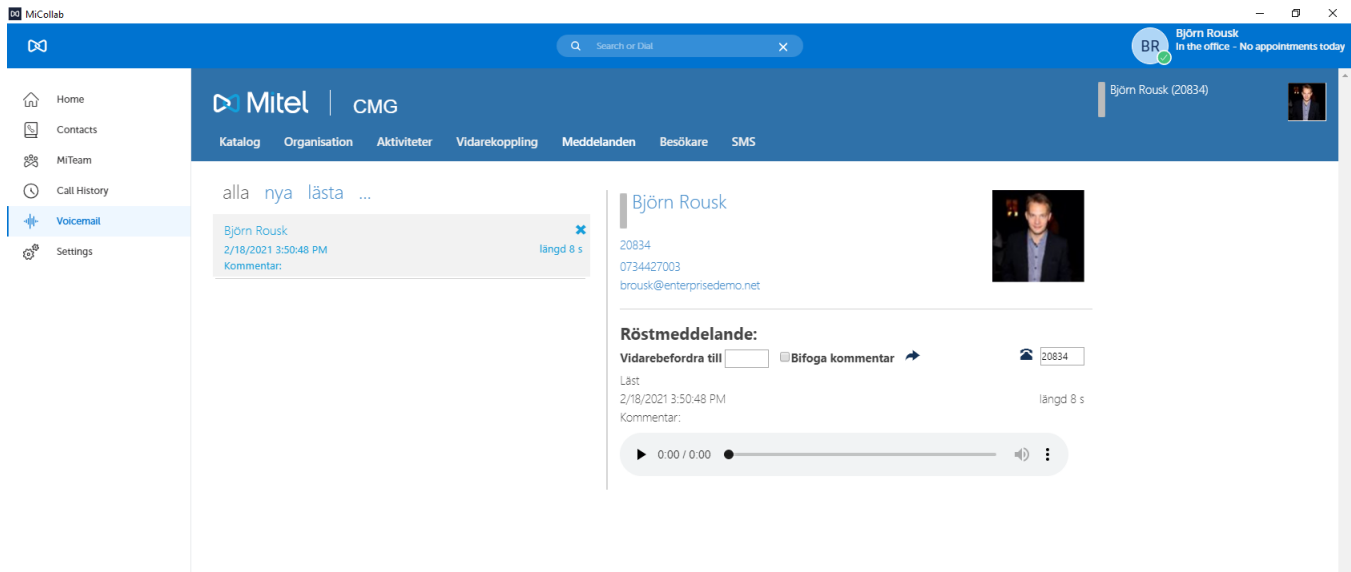
Time zone: EUROPE/STOCKHOLM

6. Select **MiCollab Advanced Messaging** as Voice mail server type.



7. Enter the URL for the CMG website in the **MiCollab AM URL** field.

Example: (CMGWEBSERVERFQDN/CMGWeb/messages/). The MiCollab Client by default prepends HTTPS:// to the URL.



**NOTE:** Using **Click to Call** from the embedded CMGWeb in the client is not supported but you can copy the number to the client.

This completes the setup of CMG Web for Visual Voicemail in the MiCollab Client.

# Configure Optional Server Software

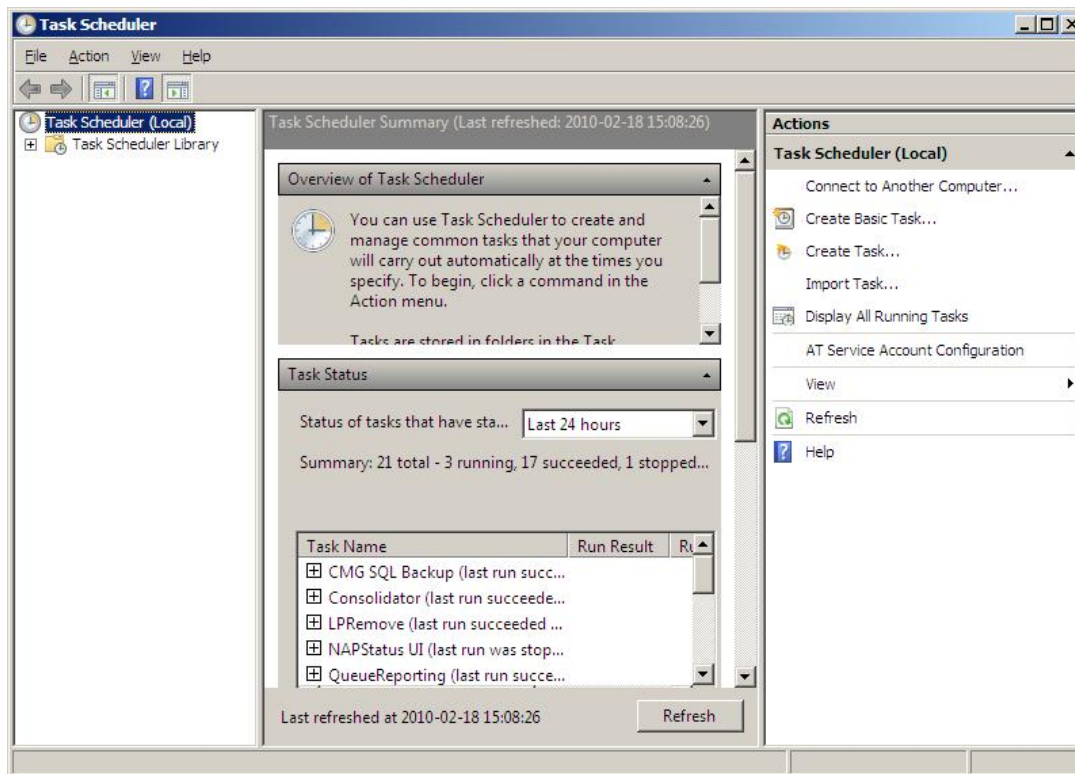
## Configuring CMG Server SQL Express Backup

If you run SQL Express, you must create the backup tasks manually since scheduled tasks are not supported.

To add the CMG SQL Express backup as a scheduled task, do the following: **NOTE:** *The screenshot examples below are from Windows 2008.*

1. Open **Task Scheduler**.

The **Task Scheduler** window is displayed:

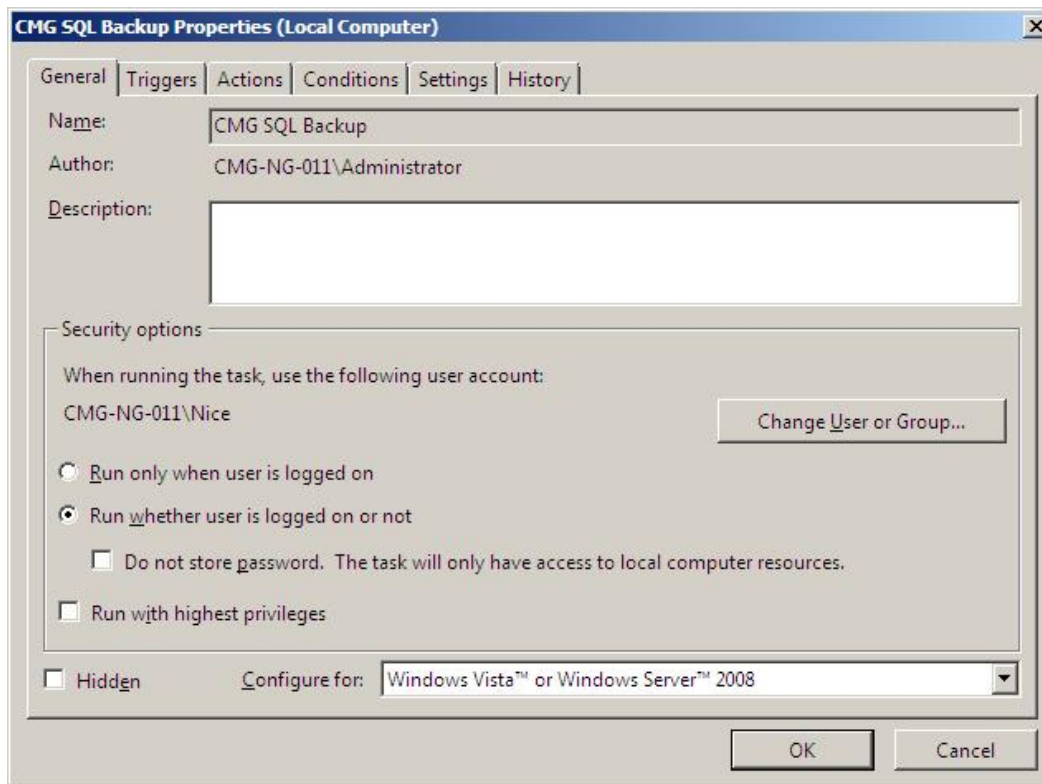


In the Task Scheduler (Local) column to the right, click **Create Basic Task...**

2. In the **Create a Basic Task** dialog, do the following:

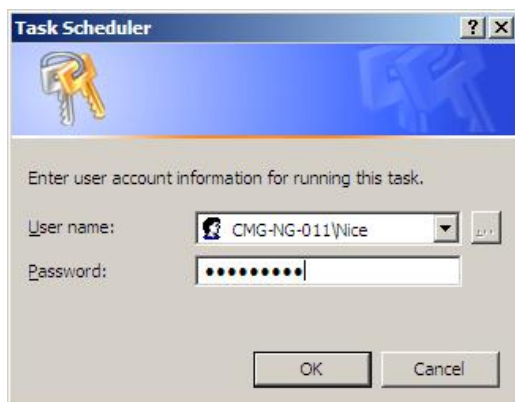
- a. Type a name for the task. Then click **Next**.
- b. In the **Task Trigger** dialog, select how often you want the task to be performed (for example **Daily**). Then click **Next**.
- c. In the **Daily** dialog, select the time and day the task should run, and click **Next**.
- d. In the **Action** dialog, select **Start a program**, and click **Next**.
- e. In the **Start a program** dialog, click **Browse....**
- f. In the **Open** dialog, select the file **CMGExpressBackup.cmd** and click **Open** to return to the **Start a program** dialog. Then click **Next**.
- g. In the **Finish** dialog, select **Open the Properties dialog for this task when I click Finish**. Then click **Finish**.

3. The **Backup Properties** dialog is now displayed:



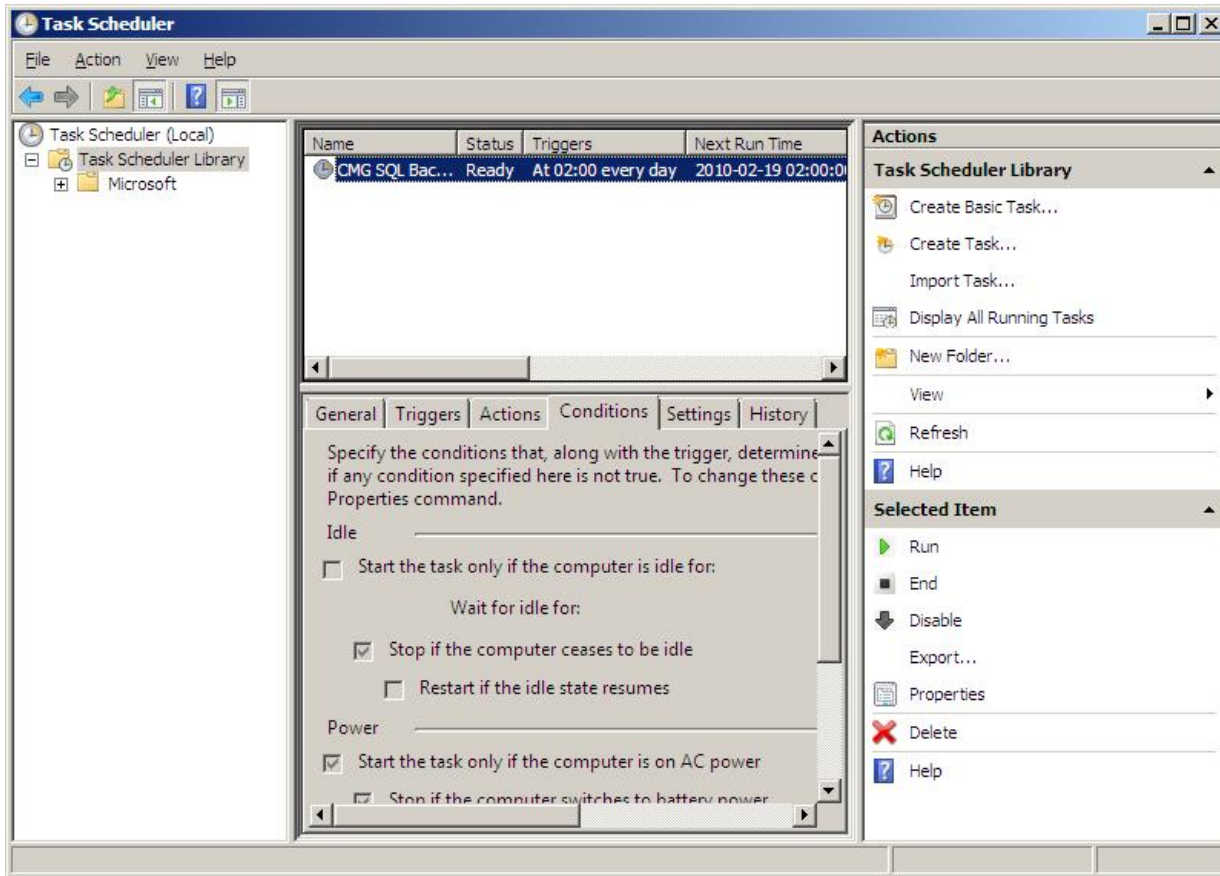
- a. Click the button **Change User or Group...** to select the user to run this job. This user has to be Local Administrator.
- b. Select **Run whether user is logged on or not**.
- c. Select the correct Windows Server version in the **Configure for:** list.
- d. Click **OK**.

4. The **Task Scheduler** dialog is displayed:



Enter the user's password. Click **OK**.

The job has now been created in Task Scheduler Library:



## Configuring Mitel LDAP Server for CMG

### Enable LDAP Server

The LDAP server is enabled and disabled for CMG in CMG Configuration Manager.

To activate the import of the data to the LDAP server, expand **Site Configuration** in the sidebar and click **System Parameters**. The **System parameters** page is displayed:

**Mitel CMG Configuration Manager**

COMPANY01

Site Configuration

- Field Names
- All Licenses
- System Parameters**
- Customer Groups
- Divisions
- All Users
- Companies/Views, Ext.
- Message Systems
- PBXs & Flash clients
- Contact Profiles

CMG Directory Manager

CMG Operator Workstation

CMG Web Components

CMG Configuration Manager

CMG Speech

**System parameters**

Reset Save

Parameter	Value	Description
Weekend	DISABLED	Defines whether or not weekends will be taken into consideration when calculating ending times for activities
FlexPlanField	DISABLED - Not in Use	Misc field [1-30] that indicates if the employee is a FlexPlan user
SecondaryPbxField	Not Used	Specifies the field (TELNO, ICPT, CORDLESS, MISC1 - MISC30) that holds the user's secondary PBX extension number
SecondaryPbxId		Specifies the id of the user's secondary PBX
ThirdPbxField	Not Used	Specifies the field (TELNO, ICPT, CORDLESS, MISC1 - MISC30) that holds the user's third PBX extension number
ThirdPbxId		Specifies the id for a third PBX. (Example: a second Voice or a ASR system.)
AutogeneratePhonetics	ENABLED	If enabled - phonetic normalized alternatives will be automatically generated
AutogenerateNickNames	ENABLED	If enabled - Nickname alternatives will be automatically generated. Only relevant if "AutogeneratePhonetics" is enabled
SipField	DISABLED - Not in Use	Defines where to put the URI (uniformed resource identified) SIP address.
<b>LDAP</b>	<b>ENABLED</b>	Defines whether or not the LDAP directory integration is activated
WarningMessagePath		Path and file name containing warning message to display after login (Format: E.g. C:\ICESRV\PGM\LoginWarning.txt)

Set **LDAP** to **ENABLED**.

## Configure LDAP Server

The LDAP Server is administered using the **TsLdap Administrator** tool. The configuration settings for this tool are stored in the **TsLdapAdmin.ini** file in the **Windows** directory.

1. Open **TsLdapAdministrator**. The main window is displayed:

**TsLdap Administrator**

File Help

**Configuration**

Path and name of the configuration file:

C:\Program Files (x86)\Aastra\TSLDAP\slapd.conf

Load Configuration Save Configuration

**Database (backend: SQL/CMG)**

Attributes

Backend settings

Change country code

**Logging**

☐ Active ☒ Status mode ☐ Debug mode

Logfile size (KByte): 4000 Number of logfiles: 100

**Start**

**Stop**

Current state: STARTED

Current country code:

com

Port number (default 389): 389 ☐ SSL/TLS: 636

Size limit of search: 5000 entries

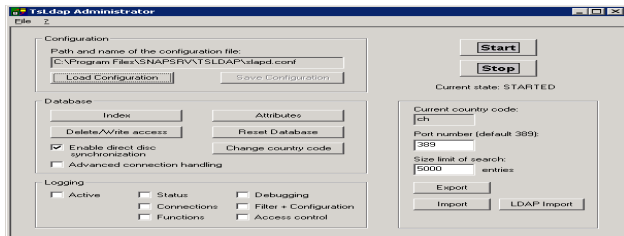
2. Follow the instructions in the coming sections in order to configure the different parts of **TsLdap Administrator**.

## Configuration

The `slapd.conf` file contains the configuration of the Mitel LDAP Server.

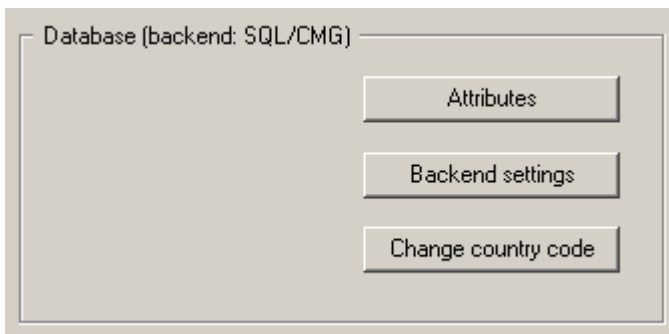
In the **Configuration** section of the **TsLdap Administrator** GUI, click **Load Configuration** to load the current settings of the LDAP Server.

Save the current configuration by clicking **Save Configuration**.



## Database

In the **Database** section, it is possible to configure the following:



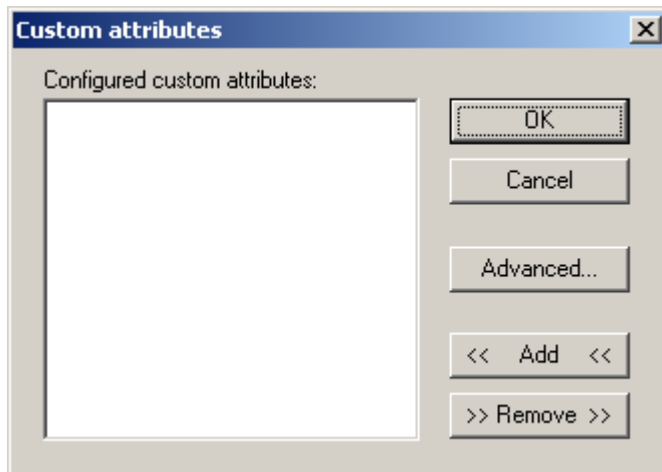
- **Attributes** - the attributes of the LDAP Server
- **Backend settings** - the connection to the CMG database (NICE)
- **Change country code** - the country code of the LDAP Server

See the coming sections for further descriptions.

## Custom Attributes

Custom attributes can be added when needed.

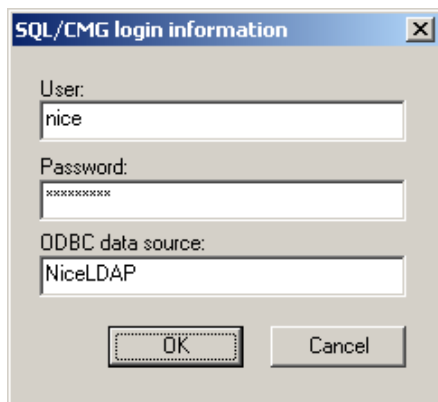
**NOTE:** Attributes configured in the CMG table **ldap\_attr\_mappings** (for mapping CMG fields to LDAP attributes) must also be configured in the LDAP Server.



Click the **Advanced...** button to show the already existing built-in attributes of the LDAP Server.

## SQL/CMG Login Information

The LDAP Server connects to the CMG database using ODBC to retrieve the data through the SQL Backend. The initial configuration for the access to the database is configured during the setup of the LDAP Server.



**User:** Authorized user to access the CMG database NICE.

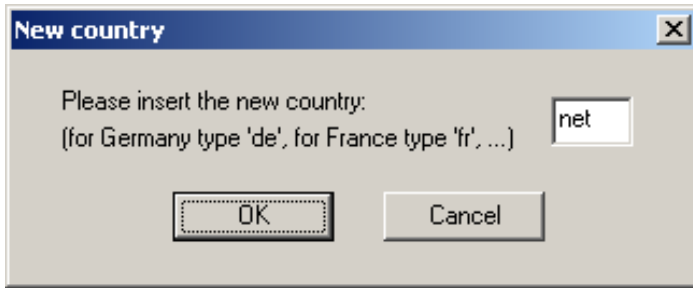
**Password:** Password of the authorized user.

**ODBC data source:** Name of the ODBC data source used for the connection.

**NOTE:** The data source has to be configured using the Control Panel.

## New Country

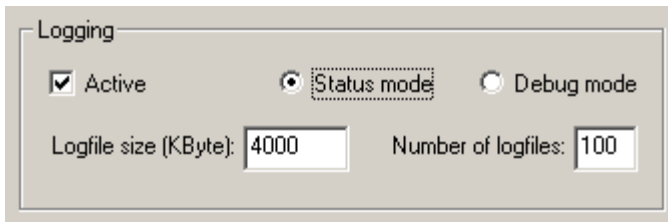
Click the **Change country code** button to change the current country. After the installation, the country code is configured to com in the LDAP Server and in the CMG database.



**NOTE:** After changing the country code in the LDAP Server, the configured value has to be changed in the CMG table LDAP\_config.

## Logging

In the **Logging** section, you can activate and configure the LDAP Server logging function. The log files can be found in the log subfolder under the program directory of the LDAP Server.

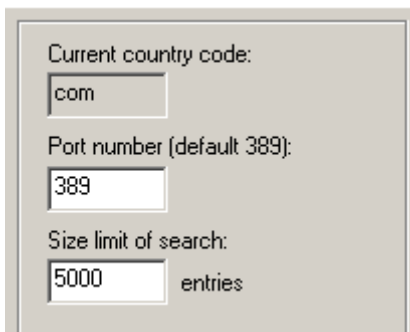


More logging can be found in the SQL LDAP\_messages table, which contains messages pointing to inconsistencies in the NICE database.

This table is populated by sp\_LDAP\_checkDatabase. Messages older than 30 days are deleted/updated when sp\_LDAP\_fillLDAPEntries is executed.

## General

In the **General** section, the following can be configured:



- **Current country code** - The country code com results in a default search base c=com to access the data of the LDAP Server.
- **Port number** - It is possible to reconfigure the port number used to access the Server. By default the LDAP Server access TCP port is 389.

**NOTE:** If using a firewall, the LDAP TCP port has to be opened.



- **Size limit of search**— This is the maximum number of entries that is returned on a single search request (maximum is 10 000).

## Menu: File - Change Path to LDAP Server

The **File - Change path to LDAP Server** menu allows you to change the path to the LDAP Server.



## Configuring IP Phone Services for Cisco

Cisco Call Manager and Cisco IP Phone services are configured in **Cisco Unified CM Administration** (<https://<Cisco server name>/ccmadmin>).

### Cisco Call Manager Configuration

1. Open **Cisco Unified CM Administration**.
2. Navigate to the **Cisco IP Phone Services Configuration** section in **Call Manager Administration**.
3. Add the **CMG Activity Service**:
  - a. In the **Service Name** field, add the name CMG ACTIVITY.
  - b. In the **Service URL** field, add the URL you created during installation. For example:  
`http://<CMG_Server_name>/cmgoffice/ipphoneservice/start.asp`
4. Add the **CMG Directory Service**:
  - a. In the **Service Name** field, add the name CMG DIRECTORY.
  - b. In the **Service URL** field, add the URL you created during installation. For example:  
`http://<CMG_Server_name>/cmgoffice/ipphoneservice/searchmenu.asp`

### Cisco IP Phone Services Configuration

Open **Cisco Unified CM Administration** and define and maintain the list of Cisco IP Phone Services to which users can subscribe at their site.

Users can then log on to the Cisco Call Manager User Preferences panel and subscribe to these services for their Cisco IP phones.

For more information, see to the help section in **Cisco Unified CM Administration**.

## CMG System Configuration

Configure IP Phone Services from CMG Configuration Manager.

1. Open **CMG Configuration Manager**.
2. Expand **CMG Web Components** and select **Parameters**.
3. Set the **DefLanguage** parameter to the chosen language.
4. For the **CMGIpPhonePath** parameter, point at the destination folder where IP Phone Service is installed.
5. Set the **CiscoIpPhone** parameter to ENABLED.
6. Click **Save**.

## Configuring CMG Corporate Directory for IP Phones

This section describes how to configure the different IP phones to function with the Corporate Directory application. This section also describes how to configure localization files.

### Configure Localized Resource Files in Microsoft IIS

For Mitel 7400 and MiVoice 4400 phones.

#### Configure application settings in IIS

To configure the ASP.NET application settings with IIS 7.0, do the following:

1. Open **IIS Manager**.
2. Select **CorpDir web site**.
  - a. Right-click **ASP.NET/Application setting** and select Open Feature.
  - b. Use **Add** or **Edit** to match the configuration at your site.

Key	Value
cmg_server	The name or IP address of the CMG directory server.
cmg_port	The port number configured for the web server where the CMG CWI web service is running.
cmg_user	The name of the CMG user account that is used to search the directory. Note! The user must have the CMG Web User Interface enabled.
cmg_password	The password for the CMG user account that is used to search the directory.
cmg_results	The maximum number of results shown on the telephone. Note! If set too high, a buffer overrun error occurs in the phone browser.

## Configure language settings

Localized resource files are installed in the `CorpDir/App_GlobalResources` folder on the web server. Additional translated resource files can be copied to this folder. Localized resource files have to be named according to the following naming convention: `Translation.<locale>.resx`.

Example: The Swedish localized resource file is named `Translation.sv-se.resx`

To change the language being used, do the following:

1. Open **IIS Manager**.
2. Select the **ASP.NET** tab in **CorpDir Properties**.
3. Click **Edit Configuration...**
4. Select the **Application** tab.

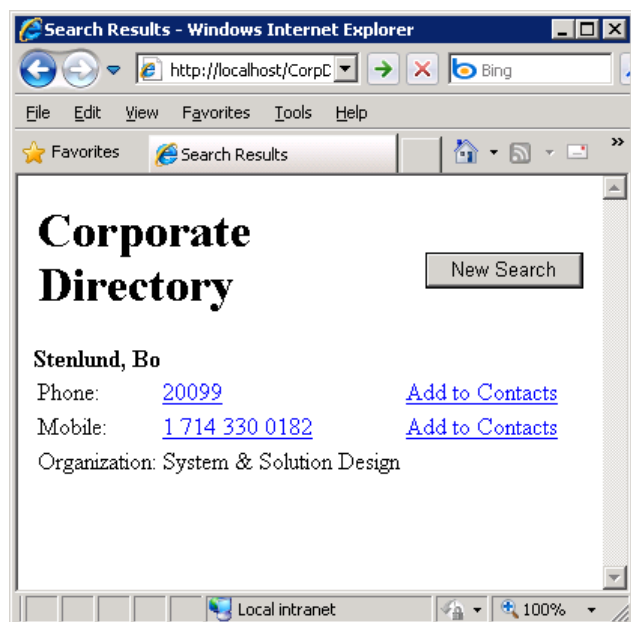
Select the desired language in the **Culture and UI culture** drop-down list. For example: For Swedish, select **sv-SE**.

## Verify the settings

Start Internet Explorer and type <http://localhost/CorpDir/default.aspx> in the Address bar:



Type a name you know exists in the directory and click **Search**:



If correctly configured, the **Search Result** page is shown.

## CMG Connection Settings and Dialing Plan

For Mitel 67xxi, 68xx, 69xx, and SIP-DECT phones.

### CMG connection settings

To configure CMG connection settings, do the following:

1. Open the file `CorpDir\xml\config\cmg_directory.conf` in Notepad.
2. Edit the parameters in section **[CMG\_Server]** to match the configuration at your site:

Parameter	Value
hostname	The server name or IP address of the CMG directory server.
port	The port number configured for the web server where the CMG CWI web service is running.
username	The name of the CMG user account that is used to search the directory. Note! The user must have the CMG Web User Interface enabled.
password	The password for the CMG user account that is used to search the directory.
cmg_results	The maximum number of results shown on the phone. Note! If set too high, a buffer overrun error occurs in the phone browser.

## Configuring dialing plan

To configure a dialing plan, do the following:

1. Open the file `CorpDir\xml\config\cmg_directory.conf` in Notepad.
2. Edit the parameters in section **[Dialplan]** to match the configuration at your site:

Parameter	Value
countrycode	Country code. If phone number starts with "+<countrycode>", this is removed.
international	International Dialing Code. This prefix replaces the + sign in the dialing strings.
longdistance	Long distance prefix. This prefix is added to the number in case own country code (+<countrycode>) has been removed.
outgoing	Outgoing prefix (trunk access code). Prefix that has to be appended for outgoing calls (all call but local calls), for example 0 or 9.
local	List of local PBX number prefixes separated by a comma (in national format). Prefix is removed no outgoing prefix is added. Examples: local=905760,978262 --> 9057602222 are replaced by 2222 --> 9782623333 is replaced by 3333.
localextlen	Internal number length. Numbers with this number of digits or less are treated as local PBX extensions. No prefix added.

## Configuring language settings

Directory Search uses the configured input language as the phone's Screen language. You can force another specific language for the whole system by doing the following:

1. Open the file `CorpDir\xml\config\server.conf` in Notepad.
2. Edit the Language parameter.

This parameter can, for example, be set to en for English, fr for French, and es for Spanish.

The actual translated strings are kept in the `language.ini` file, stored on the web server in the folder named `CorpDir\xml`. In this file, translations for each text string used in the application are stored.

Example:

```
[Name or Phone:]
en=Name or Phone:
fr=Nom ou Téléphone:
de=Name oder Nummer:
es=Nombre o Teléfono:
pt=Nome ou Telefon:
sv=Namn eller telefon:
fi=Nimi tai numero:
no=Navn eller telefon:
da=Navn eller Telefon:
it=Nome o Telefono:nl=Naam of Telefoonnr:
```

Additional translations can be added to this file when needed.

## Enabling logging

If required, logging can be enabled by setting the parameter `trace` to 1 in the file:

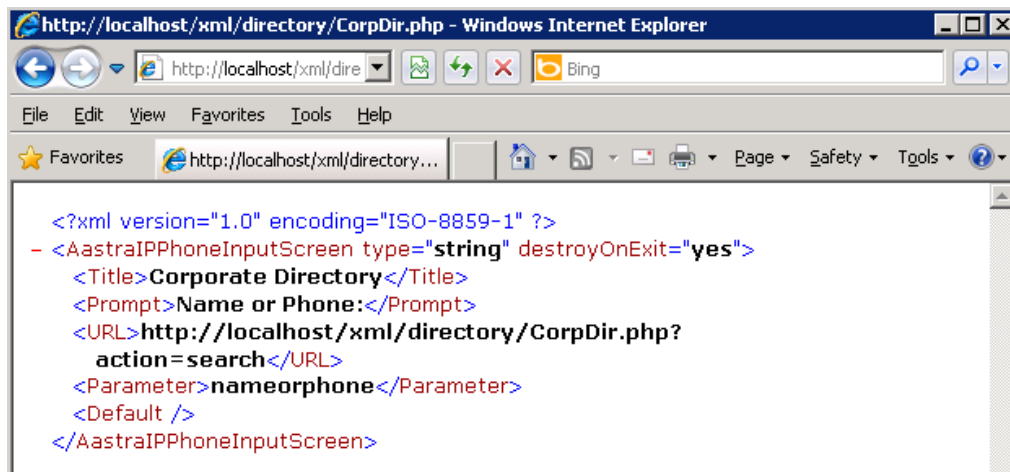
`CorpDir\xml\config\server.conf`

The default location of the log files is: `CorpDir\xml\log`

A new log file is created every day and the file name is `<date>.log`, where date is in the format: `mmddyy`.

## Verifying settings

Start Internet Explorer and go to `http://localhost/xml/directory/CorpDir.php`



If correctly configured, the web server returns an XML structure as shown above.

## IP Phones Configuration

This section describes how to configure the IP phones to function with the Corporate Directory application.

### MiVoice 4425 phones

#### Enabling menu on the phone

To enable the **CorpDirectory** menu item on the IP phone to load the Corporate Directory application, the configuration file for DBC42x IP phone has to be changed. The configuration file is `d42x02-config.txt` and it is stored in the `dbc42x02` directory on the IP Phone Software Server.

You must set the **DirectoryAddress** parameter (under the `[WAP]` section) to the IP address of the web server where the Corporate Directory is installed and the path to the `.aspx` file.

Example: If the web server is running on a server with IP address 192.168.1.10 then the parameter has to be set as:

```
DirectoryAddress=http://192.168.1.10/CorpDir/d4/d4.aspx
```

There are additional parameters that has to be set in the configuration file. For more detailed information, see the description for Configuration File for DBC 42x and Installation Instructions for DBC 425 in the CPI for MiVoice MX-ONE.

## Configure number translation

Number translation settings can also be configured under the [WAP] section of the `d42x02-config.txt` file, see description for Configuration File for DBC 42x in the CPI for MiVoice MX-ONE.

## Mitel 7400 phones (End Of Life)

### Enabling menu on the phone

- Mitel 7433 and 7434 terminals:

To enable the Corporate Directory application in the Contacts menu, the configuration file for DBC43x IP phone has to be edited. The configuration file is `d43x01-config.txt` and it is stored in the `dbc43x01` directory on the IP Phone Software Server.

You must set the **DirectoryAddress** parameter (under the [WEBBrowser] section) to the IP address of the web server where the Corporate Directory is installed and the path to the `.aspx` file.

Example: If the web server is running on a server with IP address 192.168.1.10 then the parameter has to be set as:

```
DirectoryAddress=http://192.168.1.10/CorpDir/d4/d4.aspx
```

There are additional parameters that has to be set in the configuration file. For more detailed information, see the description for Configuration File for DBC 43x and DBC44x and Installation Instructions for DBC 43x and DBC 44x in the CPI for MiVoice MX-ONE.

- Mitel 7444 and 7446 terminals:

To enable the Corporate Directory application in the Contacts menu, the configuration file for DBC44x IP phone has to be edited. The configuration file is `d44x01-config.txt` and is stored in the `dbc44x01` directory on the IP Phone Software Server.

The parameter to be changed is located under the [WEBBrowser] section and is dependent on the phone model. This parameter can be set to the IP address of the web server where the Corporate Directory is installed and the path to the `.aspx` file.

Example: If the web server is running on a server with IP address 192.168.1.10 then the parameter can be set as:

```
http://192.168.1.10/CorpDir/d4/d4.aspx
```

There are additional parameters that has to be set in the configuration file. For more detailed information, see the description for Configuration File for DBC 43x and DBC 44x and Installation Instructions for DBC 43x and DBC 44x in the CPI for MiVoice MX-ONE.

## Configure number translation

Number translation settings can also be configured under the [WAP] section of the `d43x02-config.txt` and `d44x02-config.txt` files, see description for Configuration File for DBC 42x in the CPI for MiVoice MX-ONE.

## Mitel 67xxi SIP phones

To set the Corporate Directory application to one of the function keys, one of the configuration files has to be updated. Normally, it is the model-specific configuration file that has to be edited.

Example: If the web server is running on a server with IP address 192.168.1.10 and the wish is to put a Corporate Directory button on the soft key 6, the parameters can be set as:

```
softkey6 label: Corp Dir
```

softkey6 value: `http://192.168.1.10/xml/directory/CorpDir.php`


### Mitel SIP-DECT 3.0

Within SIP-DECT 3.0, the Corporate Directory for IP Phone can be used as XML Application when the handset is in idle state. This requires adding the Corporate Directory for IP Phone as XML application in the OMM using OMP.

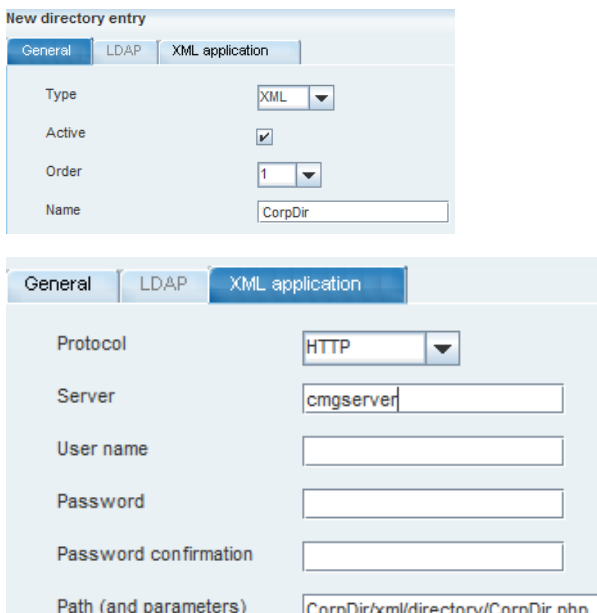
Connect to the OMM using OMP and go to **Configuration > System features > XML Applications**.

<p>Configure a new XML application</p> <p>Create:</p> <p>Name: CorpDir</p> <p>Protocol: HTTP</p> <p>Server: &lt;IP address of CMG Server&gt;</p> <p>Path: /xml/directory/CorpDir.php</p> <p>To access CMG with a 600c/d handset use <b>»»» &gt;</b></p> <p>Applications &gt; CorpDir or create a softkey to link to this application </p>	
--	--

### Mitel SIP-DECT 3.1

SIP-DECT 3.1 supports XML directories. The handset can access the directory in idle or call state using the Directory  function. (e.g. Key Up: **▲**, **»»»** within call /dial state).

This requires adding Corporate Directory for IP Phone as XML directory in the OMM using OMP. Connect to the OMM using OMP or Web service and System features > Directory.

<p>Configure a new directory entry</p> <p>Create:</p> <p>Type: XML</p> <p>Name: CorpDir</p> <p>Protocol: HTTP</p> <p>Server: &lt;IP address of CMG Server&gt;</p> <p>Path: /xml/directory/CorpDir.php</p> <p>To access the CMG directory with a 600c/d handset, use the built in central directory functions and softkeys.</p>	
--	--



## Configure Prefix for Multi Node Configuration

If the PBX system includes multiple nodes, prefixes have to be specified in order to setup calls between the different PBXs through the Corporate Directory application.

### Configuration of CMGUserInfoService (CWI)

The CWI specific information is configured in the `web.config` file.

Parameter	Value
PrefixAdd	If prefix is used, set this parameter to value "True"
PrefixMaxExtLen	The maximum length of the internal number. A value of 5 means that the prefix is added for internal numbers containing a maximum of 5 digits.
PrefixExternal	The outgoing prefix (trunk access code) that has to be appended for external calls (all calls but local calls), for example 0 or 9.
PrefixInternational	The international Dialing Code, for example, 00. This prefix replaces the + sign in the dialing strings.

To configure multi node configurations, do the following:

1. Open a text editor and edit the file: `C:\inetpub\wwwroot\CMGUserInfoService\web.config`
2. Add the parameters according to the example:

```
<appSettings>
  <add key="CMGUserInfoService.theAnAComputer.AnA"
    value="http://localhost/NwAnA/AnaService.asmx"/>
  <add key="CMGversion" value="75"/>
  <add key="LoginModeWindows" value="True"/>
  <add key="LocalDBNoAnA" value="False"/>
  <add key="ValidateAnAToken" value="False"/>
  <add key="PrefixAdd" value="True"/>
  <add key="PrefixMaxExtLen" value="5"/>
  <add key="PrefixExternal" value="0"/>
  <add key="PrefixInternational" value="00"/>
  <add key="TraceLevel" value="0"/>
</appSettings>
```

**NOTE:** If the PBXs are configured with different extension length, the **PrefixMaxExtLen** parameter has to be configured with the maximum extension length in the PBX network.

### Configuration of Corporate Directory application

The value for **localextlen** has to set to a high value, for example "99", to disable the built-in logic for local numbers.

See section 3.4.2.2 for more information about the **localextlen** parameter.

# Configuring CMG Personal Number Interface

## Configuration in MX-ONE Provisioning Manager

For more information, refer to the Provisioning Manager documentation.

### Create a User

1. Start **Provisioning Manager**.
2. Click **Users** and then **User**. On the **User** page, click **Add**.  
On the **Add User - step 1/3** page, fill in the fields: **Last Name** and **User ID**, of the user.  
A password is optional (minimum 6 characters).
3. Select one or more options in the list **Existing Department(s); Location(s)** and click on the right-arrow. The selected option appears under **Selected Department(s) Location(s)**. When finished click **Next**.
4. On the **User - Add - step 2/3** page,  
click the tab **Service Summary** to add an IP extension.
5. Click **Add** to the right of the field **Add New Extension**.
6. On the **Extension - Add - step 1 / 2** page,  
select **IP** from the **Extension Type** list and click **Next**.
7. On the **Extension - Add - step 2 / 2** page, select whether the user allows dialing internal, regional, national or international phone calls, from the **Common Service Profile** list.  
**NOTE:** This depends on how the system was configured in the startup.
8. Click **Continue**.
9. On the **User - Change** page, click **Apply** and on the next page click **Done**.

### Add User to the Administrator Group

1. Start **Provisioning Manager**.
2. Click **Administrators** and then **Administrator** tab.
3. On the **Administrator** page, click **Add** and choose a User.
  - a. **AssignUser to:** - a pre-defined **Security Profile** (with Manage/View User Data).
    - Department(s): All
    - Locations(s): All
  - b. Click **Apply** and on the next page click **Done**.

### Administrator - Add

Apply Cancel

---

? User Name(s), Extension Number, Department: \*  Search

? Security Profile: \* ☐ sven , Sven Svensson , Mitel Networks Corp

? Access to Department(s): \*  View... Edit...

Existing Department(s), Location(s):  Selected Department(s), Location(s):

--> <--

Move Up Move Down

? Access to Subsystems in Location(s): \*  Globen

## Enable CMG Personal Number in CMG Configuration Manager

To turn on this function in CMG, do the following:

1. Open **CMG Configuration Manager**.
2. Expand **Site Configuration** and select **PBX:s & Flash clients**.
3. Set the following PBX variables:

**PBX:s**

**PBX:s**

Type  PBX ID **1**

Name

IPC

Forward ICP

IVR

Voice mail

---

Extension length  ICP length

Log level  Delay

Fill char

---

Message wait ☒ Call setup ☒

Display support ☒ Individual ICP ☒

---

Personal number ☐

PBX version

IP address

IP port

Node user

Node password

---

Click to dial ☐

Click to dial link

MX-ONE e.g <https://XXX.XXX.XXX.XXX:9443/mts/callback?calling=%mynum&called=%tonum&dir=%mynum>

- Individual ICP: Enabled
- Personal number: Enabled
- PBX version (MiVoice MX-ONE or Mitel TSW)
- IP address (to the PBX)
- IP port (PBX port)

**NOTE:** For MiVoice MX-ONE use port 80.

For Mitel TSW use port 23.

- Node user
- Node password

#### 4. Expand **CMG Web Components** and select **Parameters**.

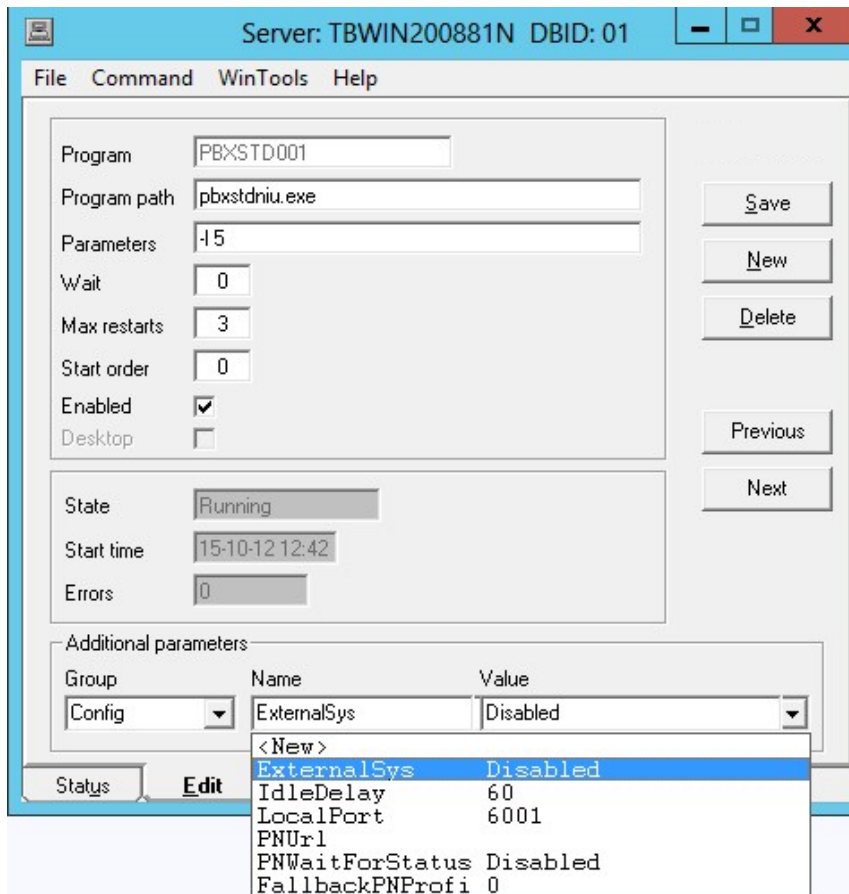
- a. In the **Enable/Disable functions** section, set **PersonalNumberMode** to ENABLED.
- b. In the **Personal number parameters** section, set the following:
  - i. **CMGServerAddress**: The IP address to the CMG Server.
  - ii. **PNConfigUrl**: The URL to the personal number configuration directory.
- c. Click **Save**.

## Enable CMG Personal Number in CMG Directory Manager

1. Open **CMG Directory Manager**.
2. Click the **Settings** tab and enable **Personal number** for the users that shall use the Personal Number function.
3. Click **Save**.

## Add Parameters to the PBXSTDNIU Process for TSW/MX-ONE

1. Open the **Spman tool** and set the PBXSTDNIU parameters:



2. Set the following parameters:

**PNUrl:** The CMG Server IP address and the web service URL, example; `http://<CMG_Server_IP_address>/epbxws/epbxws.asmx`

**PNWaitForStatus:** Enabled

**FallbackPNProfile:** 1

If a variable does not exist, create it and set it to the relevant value.

3. Click **Save** and restart the process.

## Forwarding Personal Number PРоFILES– General Information

1. To display the Personal Number profiles in CMG Web to users, go to **CMG CM > CMG Web > Parameters** and set the parameter **PersonalNumberMode** to ENABLED.
2. To set the Personal Number profiles, go to **CMG Web > Preferences > Call Routing Profiles > Personal Number – Forwarding Profiles**.
3. You cannot remove the first profile (profile1) from CMG Web. You can remove it only in the MX-ONE PBX or through the phone. (However, you can remove the other profiles in CMG Web.)
4. If you have only one profile (profile1) then it will be the active one. You cannot de-activate it in CMG Web. It can be de-activated only in the MX-ONE PBX or through the phone.
5. Use the **Active** radio button to alter the active state of profiles. Using this button, you can choose the profile that you would want to be the active profile.

**NOTE:** The **Personal Number - Forwarding Profiles** field now list upto 10 profiles.

### Preferences

General Calendar Call Routing Profiles Voice Services

Activity Routing											
Personal Number – Forwarding Profiles											
Active	Profiles	Choice 1	Choice 2	Choice 3	Choice 4	Choice 5	Choice 6	Choice 7	Choice 8	Choice 9	Choice 10
<input checked="" type="radio"/>	PN1	4744640000	4744640001	4744640002							
<input type="radio"/>	PN2	3005	3008	3007	3001	3004					
<input type="radio"/>	PN3	4744640171	4744640175								
<input type="radio"/>	PN4	4744640130	4744640138	4744640134							
<input type="radio"/>	PN5	4744640088	4744640093	4744640076	4744640062	4744640098	4744640063	4744640042			
<input type="radio"/>	PN6	4744640215	4744640217	4744640225	4744640210						
<input type="radio"/>	PN7	4744640260	4744640261	4744640262	4744640263	4744640264	4744640265	4744640266	4744640267	4744640268	4744640269
<input type="radio"/>	PN8	4744640413									
<input type="radio"/>	PN9	4744640450	4744640453	4744640454	4744640451	4744640464	4744640444	4744640487	4744640456	4744640432	
<input type="radio"/>	PN10	4744640578	4744640555								

# Logging

All components in CMG have log files for troubleshooting.

Make sure that enough hard drive space is available, as there is no size limiter (except for number of days) for the logging. This could, in extreme cases on servers with a small C:drive, fill up the hard drive. For example, the individual log files for CMG Web Service can reach 900 MB in size each.

## Log Levels

The log levels are set in the Registry. The levels are from lowest level (Error) to highest (Debug). The higher log level the more information is written to the log file.

Log Level	REGISTRY Value	Description
Error	0	Error logs are written when errors occur.
Warnings	1	Warning logs are written when the system diverges from normal behaviour.
Info	2	Info logs are written for normal events in the system. This is the default log level for customer site installations.
Trace	3	Detailed logs but without extra data output needed for debugging.
Debug	4,5,6 or 7	The most detailed log level. Logs debug data.

## Log Directory for each Component

This section describes where find the log files for each component.

On new installations, the default log directory starts with:

```
C:\ProgramData\Mitel\...
```

```
C:\Program Files (x86)\Mitel\...
```

On upgraded system, the default log directory starts with:

```
C:\ProgramData\Aastra\...
```

```
C:\ProgramData\Netwise\...
```

```
C:\Program Files (x86)\Aastra\...
```

## Default software

### AnA Web Service

The default log directory for Ana Web Service:

```
C:\nicesrv\log
```

### BluStar License Manager

The default log directory for BluStar License Manager is:

```
C:\Program Files (x86)\Mitel\BluStarLicensemanager\
```

### CMG Web and CMG Web Service

The default log directories for BSW Web respective BSW Service are:

```
C:\ProgramData\Mitel\CMGWeb.Web\
```

```
C:\ProgramData\Mitel\CMGWeb.Service
```

Change of log level (1-7, default 3) for CMG Web Service:

```
C:\Program Files (x86)\Mitel\CMGWebService\CMGWebServiceConfig.xml
```

### Calendar Connection

The default log directory for Calendar Connection is:

```
C:\Program Files (x86)\Aastra\Calendar Connection\Default\logs
```

### CMG Activity Information Service (CWI)

The default log directory for CMG Activity Information Server is:

```
C:\nicesrv\log
```

### CMG Configuration manager and Directory Manager

The default log directory for CMG CM and CMG DM is:

```
C:\nicesrv\log
```

### CMG Office Web Components

The default log directory for CMG Office Web Components is:

```
C:\nicesrv\log
```

### CMG Server

The default log directory for CMG Server is:

```
C:\nicesrv\log
```

### CMG User Information Service (CWI)

The default log directory for CMG User Information Service is:

```
C:\nicesrv\log
```



## Enterprise License Manager (Server and Client)

The default log directory for ELM server and client is:

```
C:\Program Files (x86)\Mitel\License Manager\log
```

## Optional software

### Optional - CMG Quick (client)

The default log directory for CMG Quick (client) is:

```
%LOCALAPPDATA%\Mitel\BluStarQuick
```

### Optional - BluStar Server and BluStar Presence Server

The default log directory for BluStar Server is:

```
C:\Program Files (x86)\Mitel\BluStar Server\Trace
```

The default log directories for BluStar Presence Server are:

```
C:\Program Files (x86)\Mitel\BluStar Server\Trace\PresenceServer
```

```
C:\Program Files (x86)\Mitel\BluStar Server\PresenceServer\logs
```

### Optional - CMG AD Sync

The default log directory for CMG AD Sync is:

```
C:\ProgramData\Mitel\ADSync\
```

### Optional - CMG Corporate Directory for IP phone

The default log directory for CMG Corporate Directory for IP Phone is:

```
C:\Program Files (x86)\Aastra\CorpDir
```

### Optional - CMG IP Phone Services for Cisco

The default log directory for CMG IP Phone Services for Cisco is:

```
C:\nicesrv\log
```

### Optional - CMG Personal Number Interface

The default log directory for CMG Personal Number Interface is:

```
C:\Program Files (x86)\Aastra\PersonalNumber\EPBXWS\Log
```

### Optional - CMG Server SQL Express backup

The default log directory for CMG Server SQL Express Backup is:

```
C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup
```

### Optional - LSSCom Client Standalone

The default log directory for LSSCom Client Standalone is:

```
C:\Program Files (x86)\Aastra\CfgAgent\Logs\CfgAgent_YYMMDD.log
```

## Optional - Mitel LDAP Server

The default log directory for Mitel LDAP Server:

```
C:\Program Files (x86)\Mitel\TSLDAP\log
```

# Troubleshooting

This section describes what kind of information that is useful and has to be kept ready when troubleshooting the CMG Server applications.

## Enterprise License Manager (ELM)

The ELM setup contains software for both Server and Client (if required).

### ELM Client Installation

**NOTE:** If BluStar License Manager and ELM Server are installed on separate servers, the ELM Client has to be installed on the same server as BluStar License Manager.

### ELM Server Installation

When installing ELM on a Windows 2012 R2 server, the following error may occur:

General	View	Manage	About
---------	------	--------	-------

We are sorry...

but Your request cannot be fulfilled at this time.

2014-05-28

Unspecified failure

Error number : 429

Error source : Microsoft VBScript runtime error

Error description : ActiveX component can't create object

Enterprise License Manager

To correct this error, make sure that the following boxes are checked in **Windows 2012 Server Manager**  
**-> Manage -> Add Roles and Features -> Web Server -> Management Tools**



If the error remains, please contact the Mitel Support.

## CMG Web Trace Level

A new appSetting must manually be added to change the log level in CMG Web. Edit `\inetpub\wwwroot\CMGWeb\web.config` for CMG Web and add the appSetting LogLevel.

```
<appSettings>
...
...
<add key="LogLevel" value="3" />...
...
</appSettings>
```

Valid values are 1, 2, 3 and 4. If not set, the log level is set to 3.

## Microsoft ODBC Drivers

For problems connecting a database through ODBC drivers, verify the connection parameters using MS Query (`MSQUERY32.EXE`) from MS Office.

MS Query makes it possible to access the database through ODBC and see the structure of tables, available views and field names. For advanced troubleshooting, tracing can be activated within Windows ODBC configuration.

Default update intervals:

- **Server** - The Server checks for updates in the update folder at startup and every 60 minutes thereafter.
- **Client** - The client checks for updates at startup and every 15 hours thereafter.

Please refer to the Microsoft documentation for details.

## Microsoft Windows Server OS

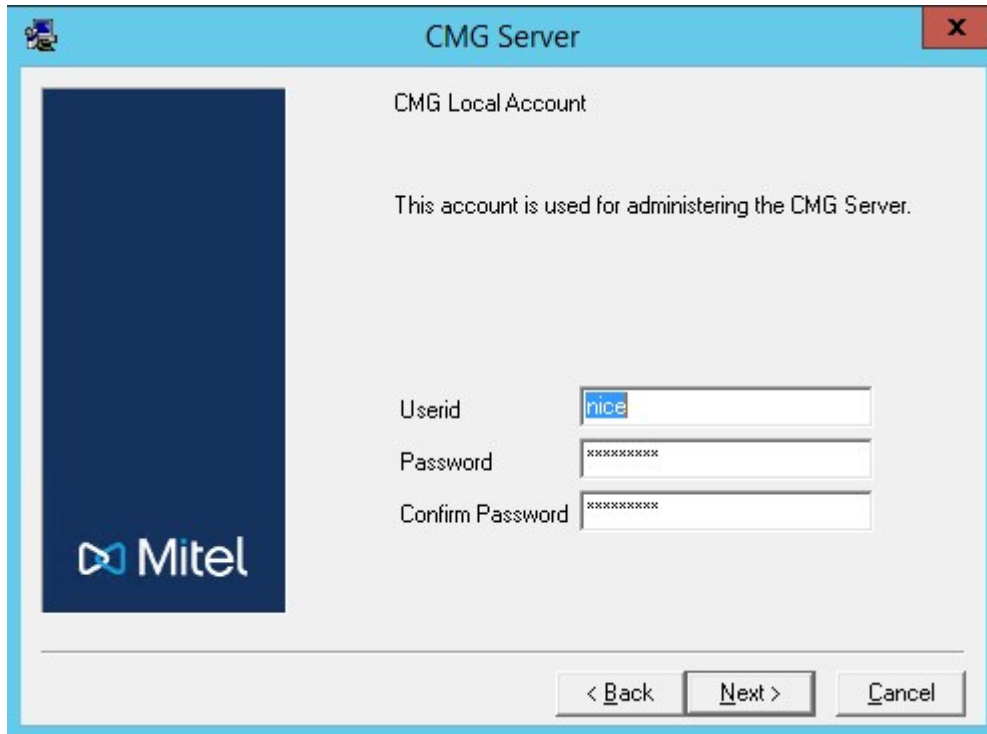
There is no particular method for tracing the communication between Mitel products and the Windows Server operating system (OS) using only one specific trace tool. However, it is possible to activate product specific tracing, as described in this document.

# Appendix I – Changing to Domain Account

This appendix describes how to change from the local nice account to a domain account.

It is now possible to install CMG with both a local account and a domain account.

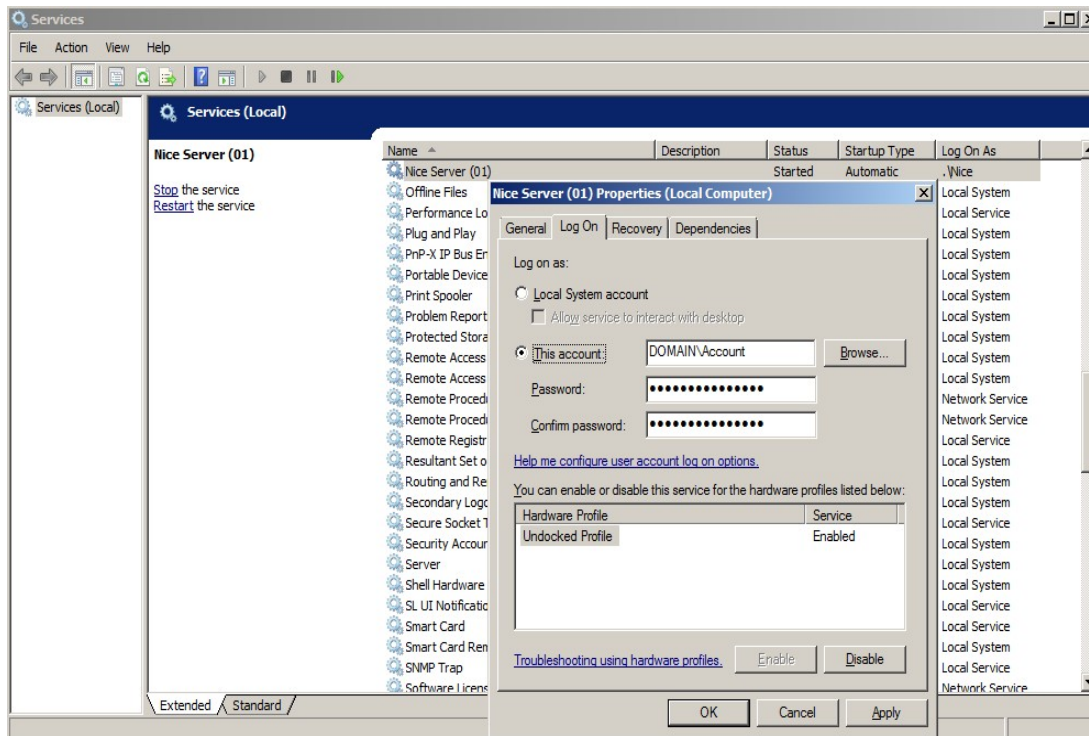
**Important!** Future updates of CMG will fetch the account and the encrypted password from the registry. If you plan to use a domain account, be sure to create the domain account with the exact same password as the local nice account, or install nice with the password that the existing domain account already has.



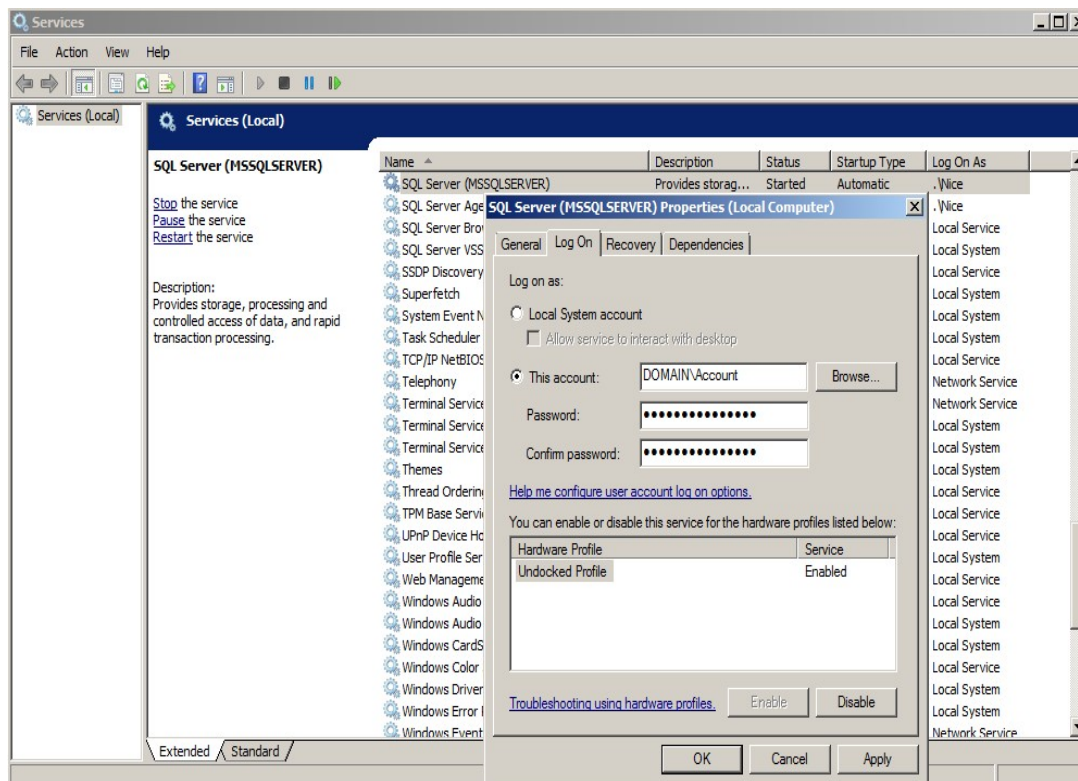
The image shows a Windows-style dialog box titled "CMG Server". On the left is a dark blue vertical bar with the Mitel logo at the bottom. The main area is light gray and contains the text "CMG Local Account" and "This account is used for administering the CMG Server." Below this are three input fields: "Userid" with the text "nice", "Password" with masked characters "xxxxxxxx", and "Confirm Password" with masked characters "xxxxxxxx". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

To change CMG to run on a domain account after the installation, do the following:

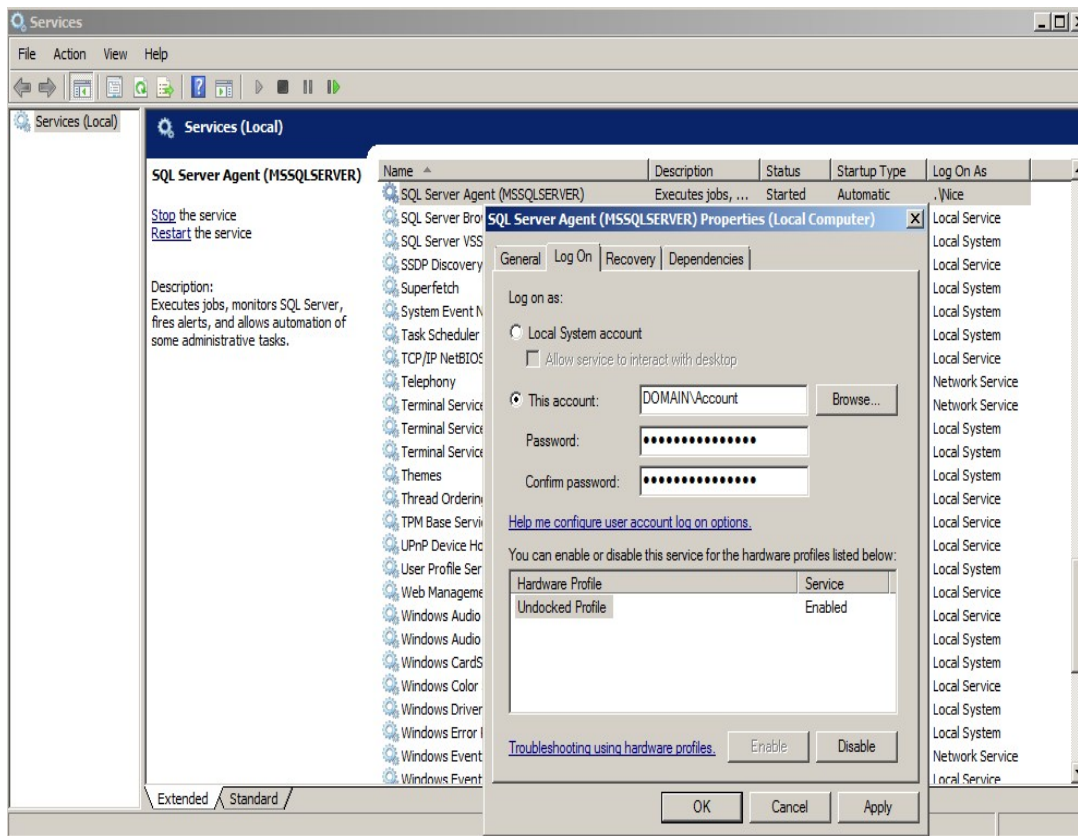
1. Start Windows Services.
2. Double-click on the Nice Server (01) service and change to the domain account. See the following example:



3. If there is a need to run SQL Server on the same account, double-click on the **SQL Server (MSSQLSERVER)** service and change to the domain account. See the following example:

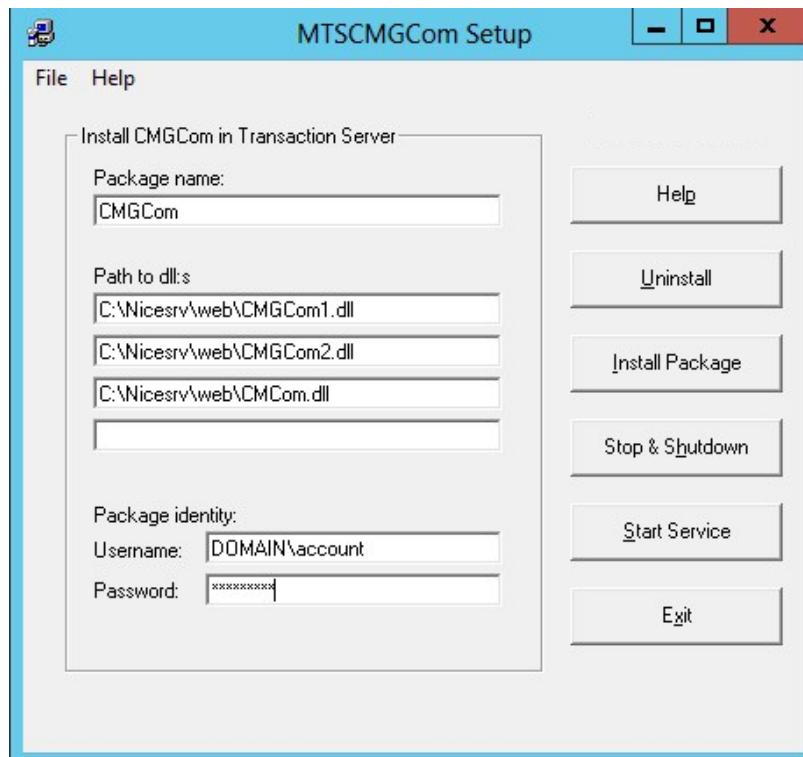


4. If there is a need to run SQL Server Agent on the same account (not valid for SQL Server Express), double-click on the **SQL Server Agent (MSSQLSERVER)** service and change to the domain account. See the following example:

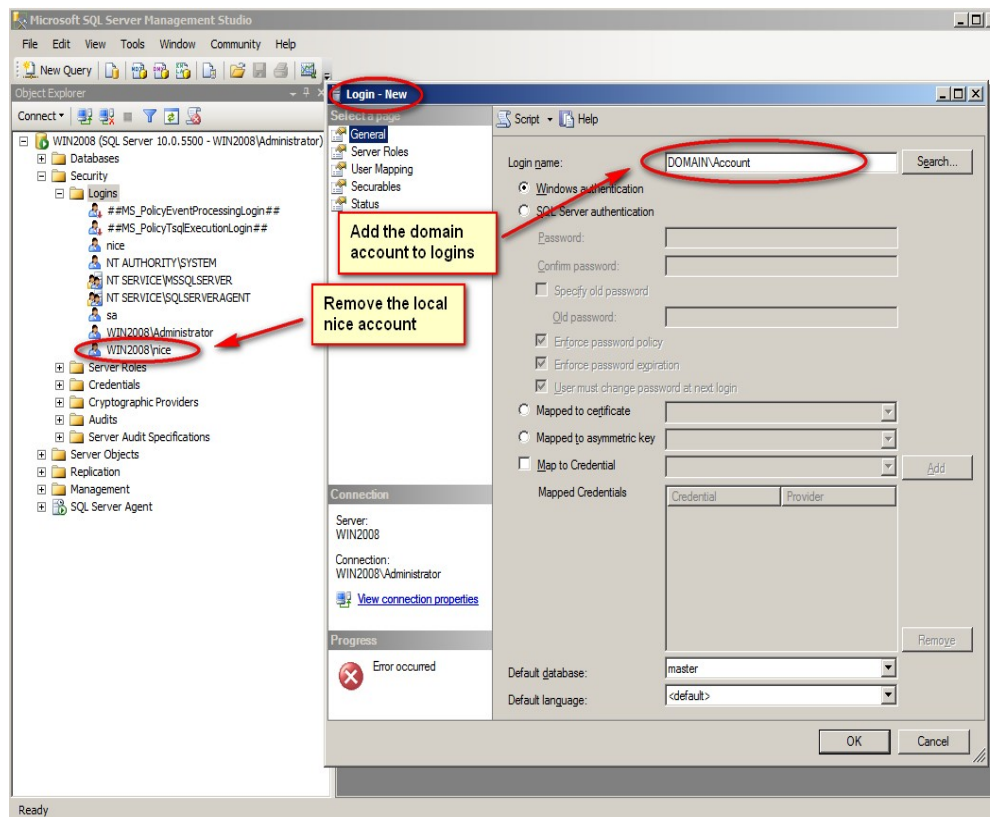


5. Run `\NiceSrv\web\MTSCMGComSetup.exe` to change identity for the CMG Components:



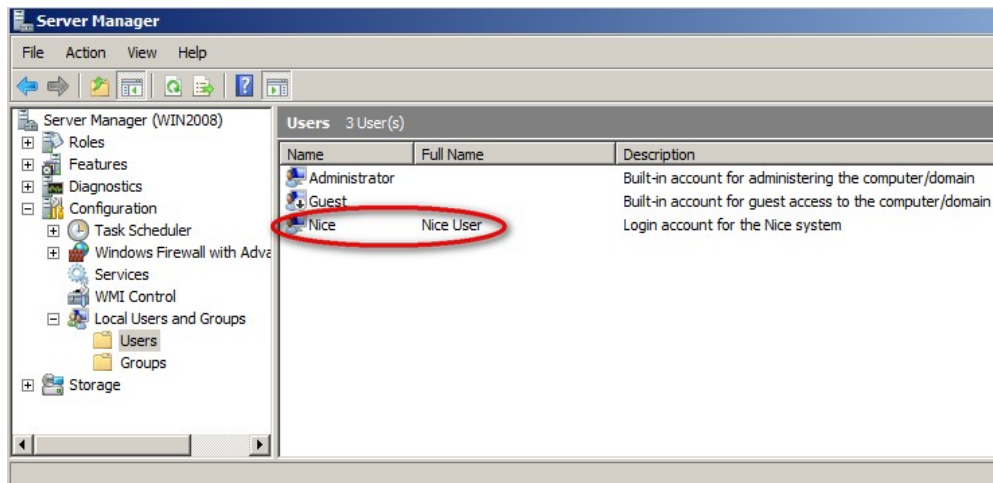


6. Remove the local Windows account nice from SQL logins and add 'DOMAIN\Account'. See the following example:



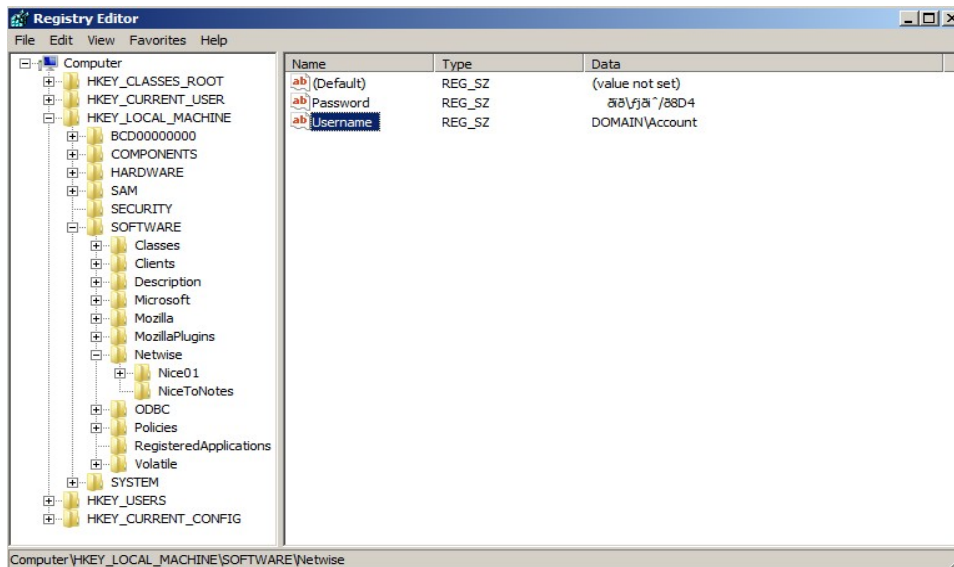
Add **sysadmin** as Server Role for 'DOMAIN\Account'.

7. Remove the local Windows account Nice if there is a need for it. See the following example:

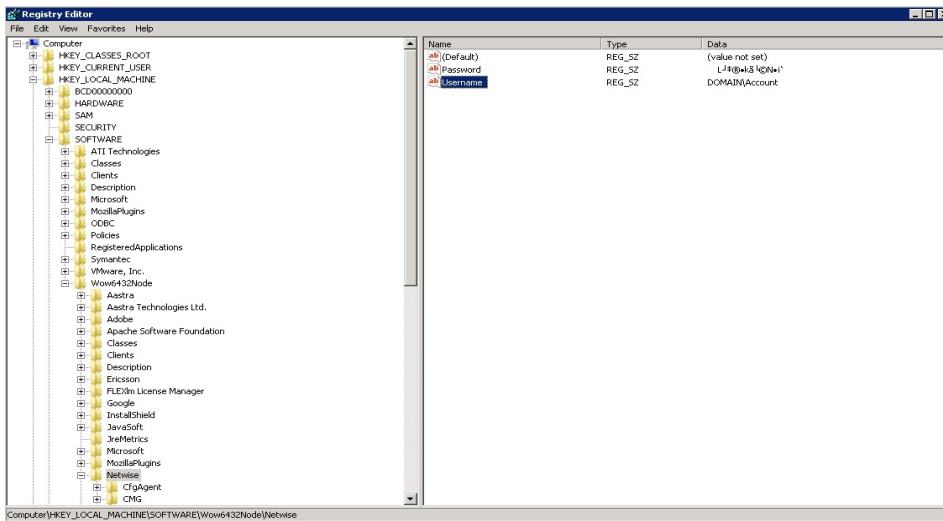


8. Change the registry parameter 'Username':

- a. On a 32-bit Windows, change the value of registry parameter HKEY\_LOCAL\_MACHINE\SOFTWARE\Netwise\Username to 'DOMAIN\Account'. See the following example:



- b. On a 64-bit Windows, Change the value of registry parameter HKEY\_LOCAL\_MACHINE\SOFTWAREWow6432Node\Netwise\Username to 'DOMAIN\Account'. See the following example:



**NOTE:** The screenshots in this appendix are from a CMG installation on Windows 2008 with SQL 2008. If CMG is installed on Windows 2012/R2 with SQL 2012, the examples would look a bit different, but the procedure would be the same.

# Appendix II – Configuring Single Sign-On

This appendix describes how to configure Single Sign-On on a Windows Server.

For Single Sign-On (SSO) to work, both the CMG Server and the CMG users have to belong to the same domain.

**NOTE:** The screenshot examples below are from Windows Server 2008 (32-bit).

## Single Sign-On for CMG Web

To configure Single Sign-On for CMG Web, do the following:

**1. Open CMG Configuration Manager.**

Base path is: CMG Web => Parameters => Windows Authentication

- a. Give the IP or hostname of the AD server to be used for signing on user when windows authentication is needed:

=> Active Directory Server

- b. The LDAP path indicating the part of AD to be used for authentication:

=> Active Directory Path

- c. Username and password for connecting to AD server:

=> Active Directory Username

=> Active Directory Password

- d. Pick a miscfield in the database to hold the login information:

=> Active Directory User Identifier Field

- e. Pick a field in CMG that is unique for a user that is used to match an AD user with a CMG user:

=> CMG User Identifier Field

- f. User authentication type can either be set to CMG or Windows.

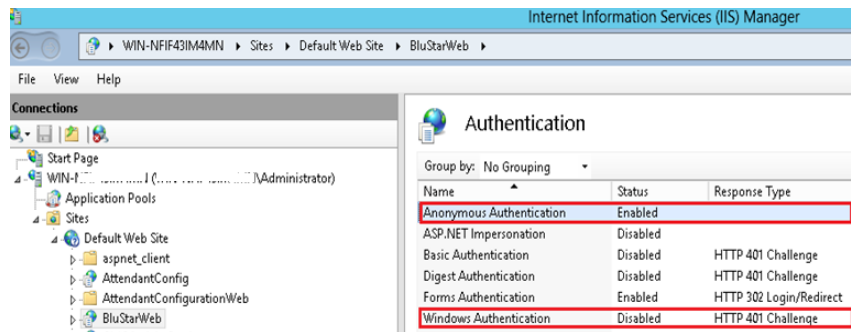
Used when forms authentication is configured in IIS Manager:

=> User Authentication Type

**2. Open CMG Directory Manager.**

- a. Enter information in CMG DM for all users in the newly renamed miscfield, in the format DOMAIN\USERNAME.

**3. Open IIS Manager** and set Anonymous Authentication to “Disabled” and Windows Authentication to “Enabled” for **CMGWeb**:



# SINGLE SIGN-ON FOR CMG WEB USING SAML

Before configuring Single Sign On for SAML, ensure that the IDP has the following setup:

- The default value of Entity ID for CMG Web is set to **MitelBluStarWeb**.
- All the users must have a valid email address in CMG Web which are linked to the user records.
- If the client configuration has multiple CMG Web URLs configured for a single instance, then all the URLs must be configured on the client's IDP.
- The SAML response from client IDP must have a **valid Signature**. For more details on the format for a valid signature, see the section [SAML AUTHENTICATION RESPONSE FROM IDP TO CMG](#).
- CMG Web will be using the POST URL from metadata file to send SAML request.
- The metadata's Name ID format must be –  
`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`

## TO CONFIGURE SINGLE SIGN-ON FOR SAML

1. Open the Install directory of CMG Web, default path is: `C:\inetpub\wwwroot\BluStarWeb`
2. Add the following metadata file configuration:

- a. Create a new folder App\_Data in the below path:

`C:\inetpub\wwwroot\BluStarWeb\`

- b. Copy the IDP metadata file in the **App\_Data** folder, and rename the file as `metadata.xml`.

**NOTE:** You can get the metadata file from the client. For more details on Metadata file format, see the section **Metadata File Format**.

3. To configure the SAML BluStar web.configuration file:

- a. Enter the following key details under the `<appsettings>` tag:

- i. `<add key="MetadataLocation" value="{Path_Of_Metadata_File}"/>`

Enter the path value of the meta data file. The path value is set to `value="~/App_Data/metadata.xml"`

- ii. `<add key="ServiceProviderUrl" value="{Blustarweb_Sign_Page_Url}"/>`

Enter the complete BluStar Web Sign In URL. For example:

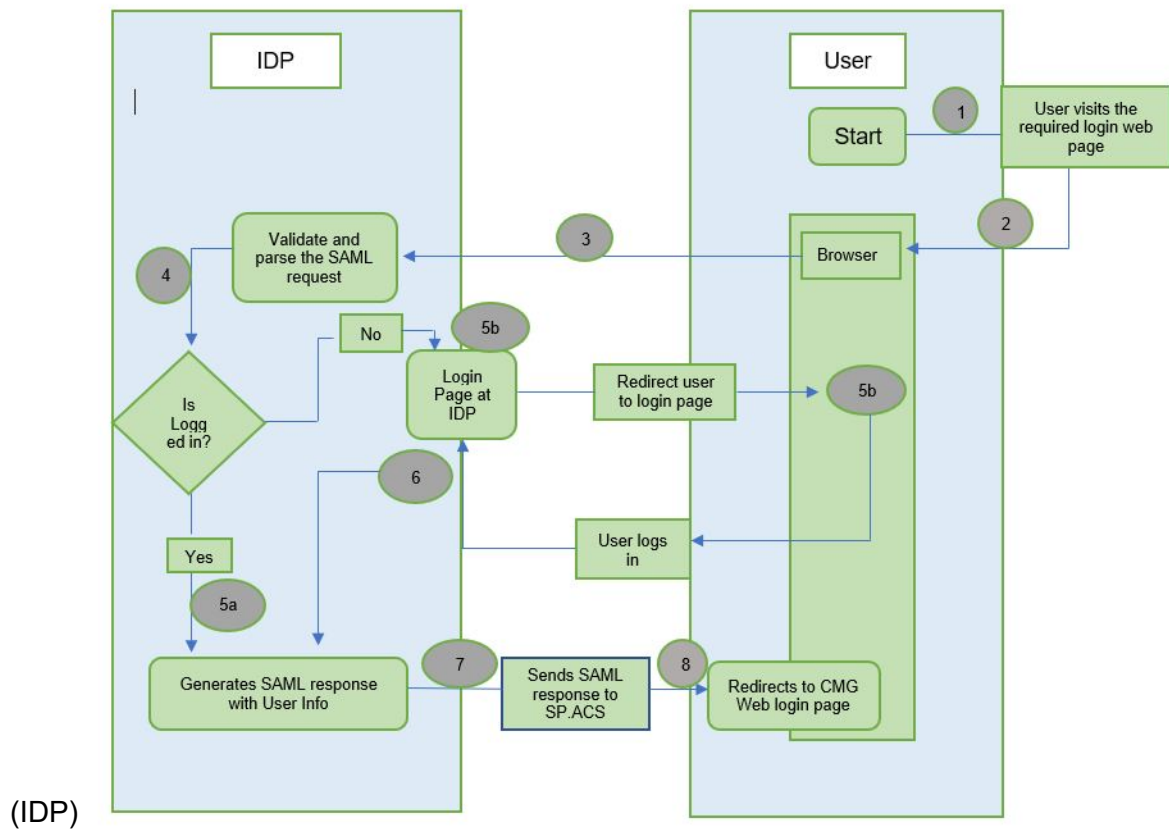
<http://localhost/BluStarWeb/SignIn>

The domain of the URL specified should be a localhost.

- iii. `<add key="STSName" value="{Name_of_The_Provider}" />`

Enter the STS name, that is, the Name of the Provider. By default, the value is External Sign In and the client can change this value.

Figure 8.1: SSO-Login at Identity Provider



## METADATA FILE FORMAT:

The metadata file has attributes value in place of "{}" and requires tags such as X509Certificate, SingleLogoutService, NameIDFormat and SingleSignOnService. The metadata file format is as follows:

```
<?xml version="1.0"?>
<EntityDescriptor
xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="{ }">
  <IDPSSODescriptor
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfoxmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>{}</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
```

```

<SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="{ }"/>

<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>

<SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="{ }"/>

</EntityDescriptor>

```

## SAML REQUEST AND RESPONSE EXPECTATIONS

Ensure that the IDP is compatible with CMG Web's request and response syntax, because BluStarWeb reads SAML token only in the formats given in the following sections:

### SAML AUTHENTICATION REQUEST FROM CMG WEB TO IDP:

1. The SAML authentication request sent to IDP will be in the following format:
2. Here only the **AssertionConsumerServiceURL** and **ID** attribute values would be set when sending a request to IDP.
3. **ID** – This is the Unique Id generated for each request.
4. **AssertionConsumerServiceURL** - This URL is taken from the ServiceProviderUrl parameter.

```

<samlp:AuthnRequest ID="{ }" Version="2.0"
IssueInstant="2017-06-08T10:51:27Z"

ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="{ }"

xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">MitelBluStarWeb</saml:Issuer>

<samlp:NameIDPolicy
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified"
AllowCreate="true" />

<samlp:RequestedAuthnContext Comparison="exact">

<saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>

</samlp:RequestedAuthnContext></samlp:AuthnRequest>

```

### SAML AUTHENTICATION RESPONSE FROM IDP TO CMG:

1. The SAML response that BluStarWeb receives from IDP must be in the following format.
2. The {} curly braces enclose the actual values.

```

<samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="{ }" Version="2.0"

```



```

IssueInstant="2017-06-08T10:30:44Z" Destination="{recipient}"
InResponseTo="{ }">
<saml:Issuer>{ }</saml:Issuer>
<samlp:Status>
<samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:{ }"/>
</samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Version="2.0"
ID="pfx1abc4703-b737-cbc2-bdd5-d35d07edbec6"
IssueInstant="2017-06-08T10:30:44Z">
<saml:Issuer>{ }</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference URI="#pfx1abc4703-b737-cbc2-bdd5-d35d07edbec6">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>{ }</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>{ }</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>{ }</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">{ }</saml:
NameID>
<saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2017-06-08T10:33:44Z"
Recipient="{recipient}"
InResponseTo="_01c34e63-e72d-4b5c-b4c7-575b08a08ada" />
</saml:SubjectConfirmation>

```

```

</saml:Subject>
<saml:Conditions NotBefore="2017-06-08T10:27:44Z"
NotOnOrAfter="2017-06-08T10:33:44Z">
<saml:AudienceRestriction>
<saml:Audience>{audience}</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2017-06-08T10:30:43Z"
SessionNotOnOrAfter="2017-06-09T10:30:44Z"
SessionIndex="_731e7bc0-2e63-0135-39a2-02af1cf39a00">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passwo
rdProtectedTransport</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="last name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">{}</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="company"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">{}</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>

```

## SAMPLE METADATA, REQUEST AND RESPONSE

### Metadata File Sample:

```

<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://app.onelogin.com/saml/metadata/644310">
<IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data</ds:X509Data></ds:KeyInfo></KeyDescriptor>
<SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"

```

```

Location="https://qwert-dev.onelogin.com/trust/saml2/http-redirect/slo/644310"/>
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
<SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://qwert-dev.onelogin.com/trust/saml2/http-redirect/sso/644310"/>
<SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://qwert-dev.onelogin.com/trust/saml2/http-post/sso/644310"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://qwert-dev.onelogin.com/trust/saml2/soap/sso/644310"/>
</IDPSSODescriptor>
</EntityDescriptor>

```

**Authentication Request Sample:**

```

<samlp:AuthnRequest ID="_4fd95a67-8e72-4054-91d5-c7fb3d0c8b9a"
Version="2.0" IssueInstant="2017-06-08T10:51:27Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="http://localhost:58267/SignIn"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">MitelBluStarWeb</saml:Issuer>
<samlp:NameIDPolicy
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified"
AllowCreate="true" />
<samlp:RequestedAuthnContext Comparison="exact">
<saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
</samlp:AuthnRequest>

```

**SAML Response sample:**

```

<samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="R0141a8dfa0ed8f47d0d7034f6e55dde257620ad3" Version="2.0"
IssueInstant="2017-06-08T10:30:44Z" Destination="{recipient}"
InResponseTo="_01c34e63-e72d-4b5c-b4c7-575b08a08ada">
<saml:Issuer>https://app.onelogin.com/saml/metadata/644310</saml:Issuer>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Version="2.0"

```

```

ID="pfx1abc4703-b737-cbc2-bdd5-d35d07edbec6"
IssueInstant="2017-06-08T10:30:44Z">
<saml:Issuer>https://app.onelogin.com/saml/metadata/644310</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference
URI="#pfx1abc4703-b737-cbc2-bdd5-d35d07edbec6"><ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>WqKsIdUb9/p41184UaTxsB2jS+I=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue> ==</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds: >
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">qwert@te
st.com</saml:NameID>
<saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2017-06-08T10:33:44Z"
Recipient="{recipient}"
InResponseTo="_01c34e63-e72d-4b5c-b4c7-575b08a08ada" />
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2017-06-08T10:27:44Z"
NotOnOrAfter="2017-06-08T10:33:44Z">
<saml:AudienceRestriction>
<saml:Audience>{audience}</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2017-06-08T10:30:43Z"
SessionNotOnOrAfter="2017-06-09T10:30:44Z"
SessionIndex="_731e7bc0-2e63-0135-39a2-02af1cf39a00">

```

```
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passwo
rdProtectedTransport</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="last name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Qwert</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">qwert@test.com</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="first name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Qwert</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="phone"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">1000</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="company"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">wipro</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

# Appendix III – Using Import Export Configuration Tool

This appendix describes how to use the Import Export Configuration tool, which is used to configure the Import and Export jobs in CMG.

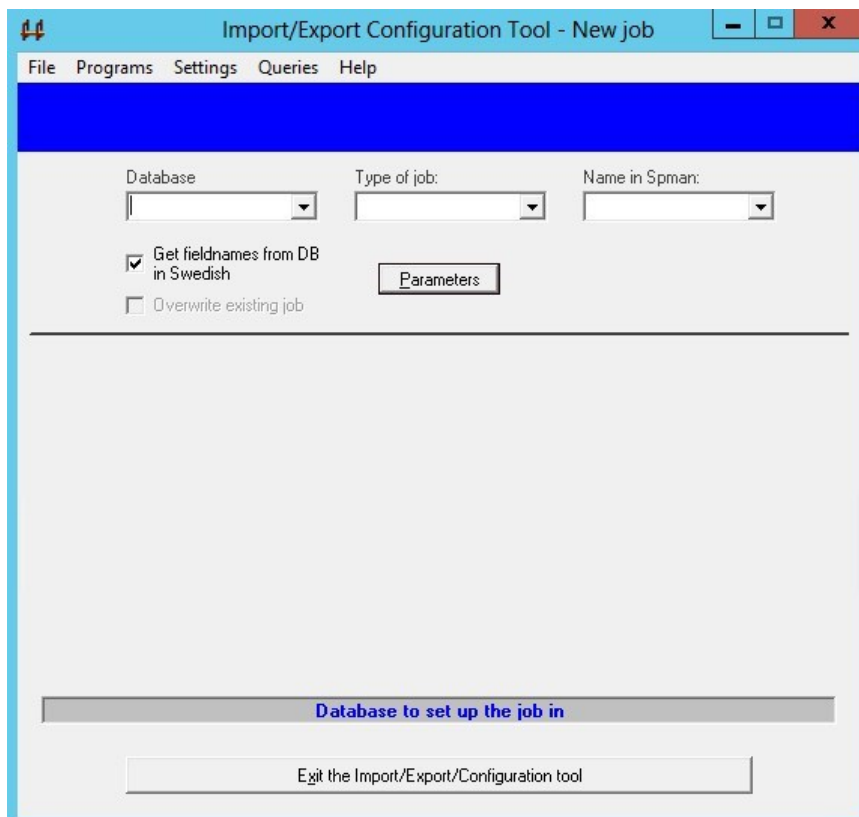
The Import Export Configuration tool is located in the <drive:>\NiceSrv\pgm directory and is called ImpExpCfg.

## Export Configuration

This section describes how to do an export configuration.

Do the following:

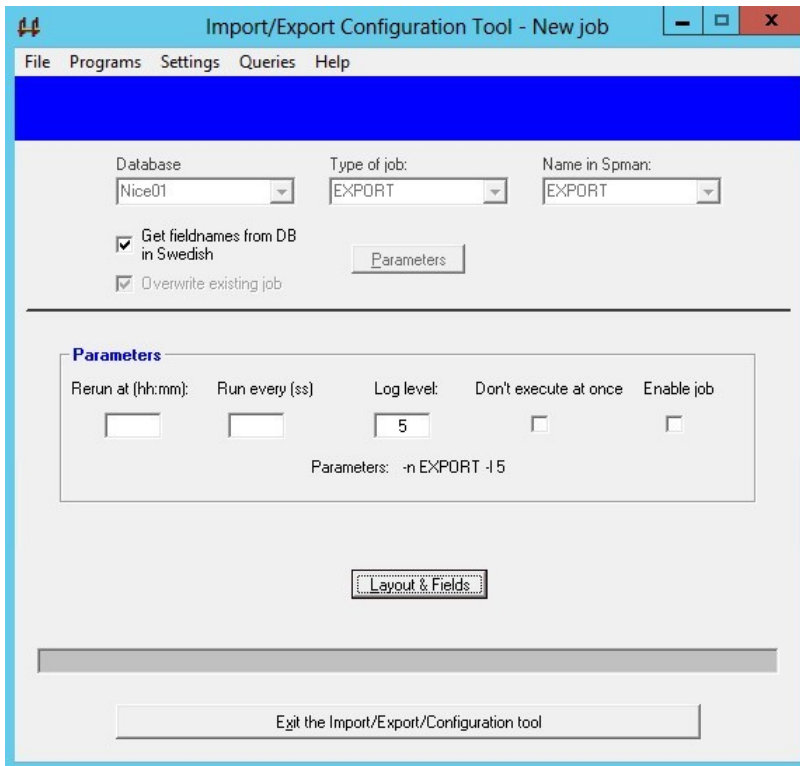
1. Open the **Import/Export Configuration Tool**.
2. On the start screen, click **File** and then select **New** (or **Open** or **Delete**) to display the **New job** dialog:



The title bar shows the kind of operation being performed (in this case New job).

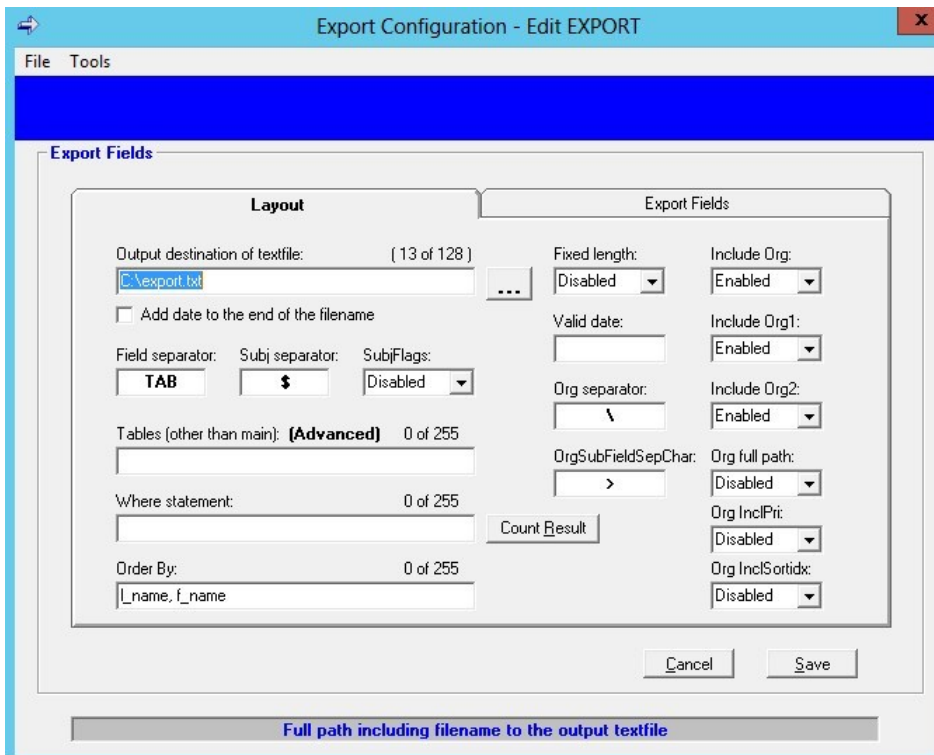
3. Select the **Database**, the **Type of job** and the **Name in Spman**, then click **Parameters**.

A new section (**Parameters**) appears in the dialog.



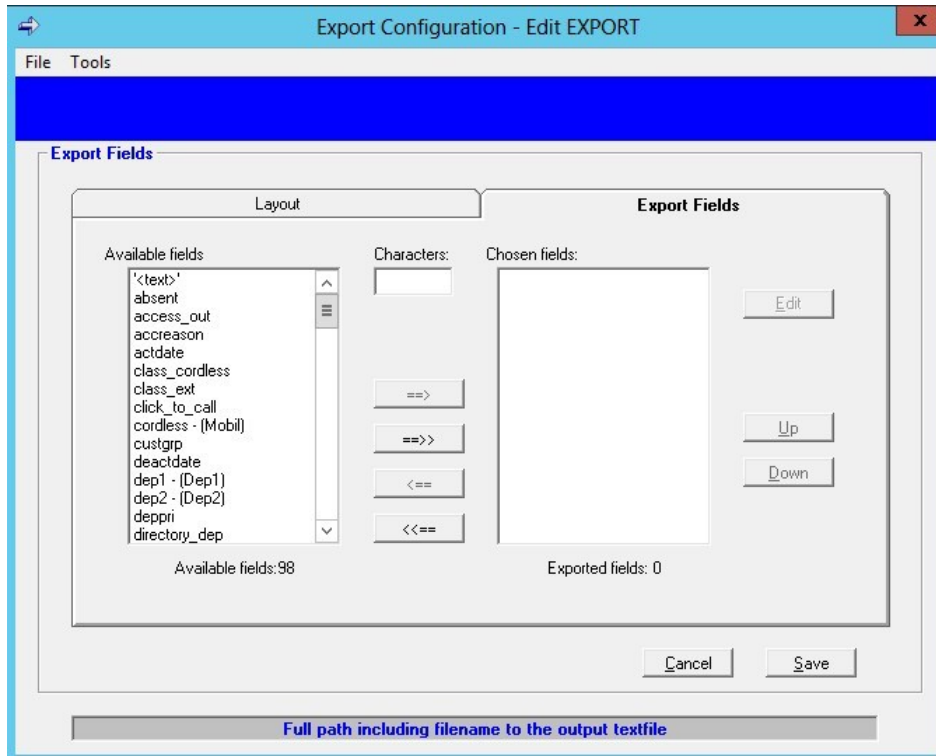
4. Type when and how often the job should run, then click Layout & Fields.

The following dialog is displayed:



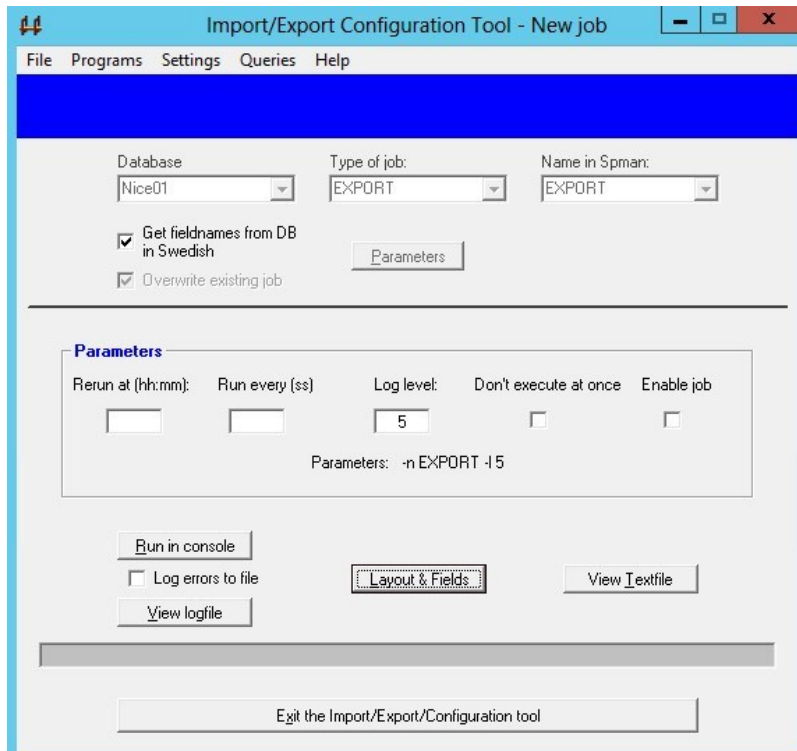
The title bar shows the name of the job being edited.

5. Define the Export text file (see example in the previous dialog) and click on the **Export Fields** tab. The following dialog is displayed:



6. Select the fields to be exported from **Available fields**, and then click **Save**.

The following dialog is displayed:





From this dialog, the job can be tested and the exported text file can be viewed.

## Import Configuration

This section describes how to import a configuration. The Import configuration process is similar to Export configuration, except that there are three tabs to configure.

### Layout Tab

The Import text file is specified on the **Layout** tab.

The screenshot shows the 'Import Configuration - Edit IMPORT' dialog box with the 'Layout' tab selected. The 'Input destination of textfile' is set to 'C:\KPN\_Beheer\import.txt'. The 'Field separator' is set to ';'. The 'Subj separator' is set to '!', which is highlighted with a red box. The 'Function code' is set to '1'. The 'Rename file' is set to 'Disabled'. The 'Append subject' is set to 'Disabled'. The 'OrgUnits' section has 'OrgUseOnlyDesc' selected, and 'OrgDescIsFullPath' is checked. The 'Fixed length' is set to 'Disabled'. The 'DeleteDelay' is set to '10'. The 'Org separator' is set to '/'. The 'KeepSign' is set to 'Disabled'. The 'OrgPriIncluded' is set to 'Disabled'. The 'SubjFieldRemoveLeadingSpace' is set to 'Enabled'. The 'MultipleRecordMode' is set to 'Disabled'. The 'DefaultSQLTime' is set to '||'. The 'Number of milliseconds for the query execution' is shown at the bottom.

Ensure the imported data field values do not include any of the following permanently restricted characters.

<		;	"	&#
---	--	---	---	----

**NOTE:** "&#" as a combination is not allowed. "&" and "#" as single characters are still allowed.

There are some other special characters that are not allowed in DM 8.5 version by default. But, you can choose to allow these characters or restrict it in CMG CM application.

To configure the list of allowed and restricted characters, go to **CMG Directory Manager > Parameters > ExceptionCharactersList**.

Parameter	Value	Description
ActiveXOrgtreeIncluded	ENABLED	Defines whether or not ActiveX component for Administrative Orgtree is included.
autoCapitalizeName	no	Defines whether or not the name fields will be capitalized automatically. Can be overridden by the user.
ExceptionCharacterList		Defines list of Special Characters that should be allowed in DM Application Entries. By Default all these Special Characters are not allowed.
maxFormPrefetchCount	4	Defines number of subscriber main forms to be prefetched once the search is completed or when a form is opened.
maxOrgFetchCount	300	Defines the maximum number of organizational units to fetch first after login.
maxSubjectFetchCount	20	Defines the maximum number of keywords to fetch when searching for keywords.
QuickInfoIncluded	yes	Defines whether or not Quick Info Manager is included.
ReceptionMisc	DISABLED - Not in Use	Defines the field containing the reception information.

**NOTE:** If these restricted characters are included in any of the imported data fields, then the import will fail to CMG and this will be logged in the import log file.

## Default Values Tab

The default values for fields that are not imported are configured on the **Default Values** tab.

Import Configuration - Edit IMPORT

File Tools

Import Fields

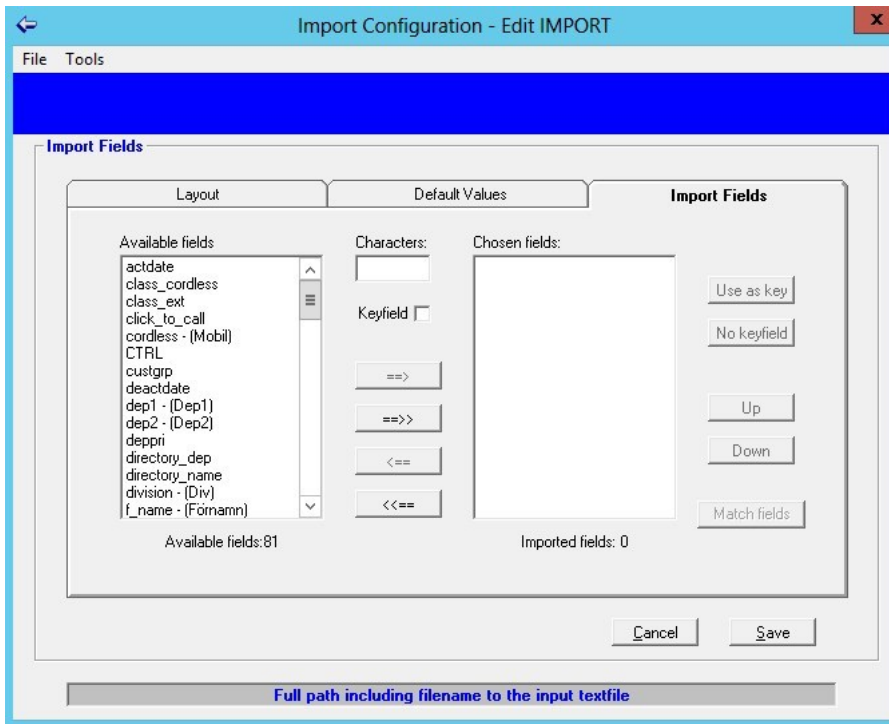
Layout	Default Values	Import Fields
Default custgroup: 1 View CMG	DefaultSearch_Name <input checked="" type="checkbox"/>	DefaultVisitorHostEnabled <input type="checkbox"/>
DefaultDepri: 500	DefaultSearch_office <input checked="" type="checkbox"/>	DefaultSubjectFlags <input type="checkbox"/> T - Operators <input type="checkbox"/> K - Phonebook <input type="checkbox"/> S - Subject index <input type="checkbox"/> O - Office users
DefaultPbxid: 1 View CMG	DefaultDirectory_name <input checked="" type="checkbox"/>	
DefaultTimeZone: NULL View CMG	DefaultDirectory_dep <input checked="" type="checkbox"/>	
DefaultProfileLevel: 4	DefaultClass_ext <input type="checkbox"/>	
	DefaultClass_Cordless <input type="checkbox"/>	
	DefaultMessage_wait <input checked="" type="checkbox"/>	
	DefaultSecretary <input type="checkbox"/>	
	DefaultTelnoPri <input checked="" type="checkbox"/>	
	DefaultShowlist <input type="checkbox"/>	
	DefaultFixedPhoneExists <input type="checkbox"/>	

Cancel Save

Full path including filename to the input textfile

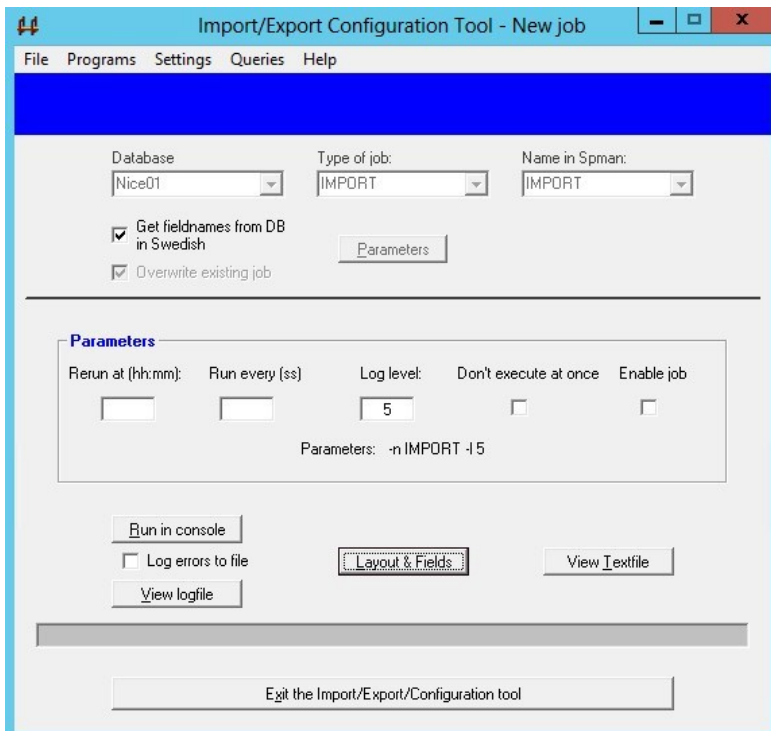
## Import Fields Tab

The fields into which data has to be imported are selected on the **Import Fields** tab.



## Importing the Text File

When all values have been specified and saved, the following dialog is displayed:

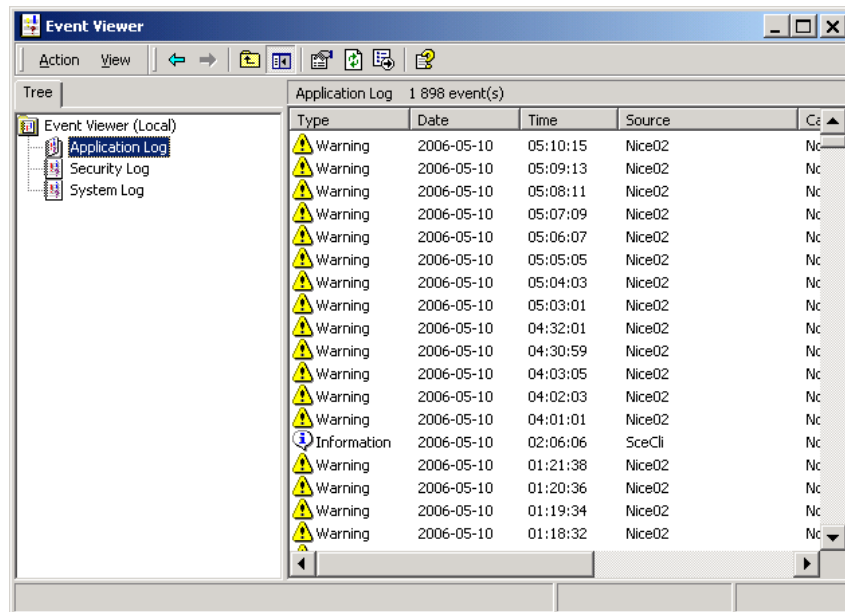


From this dialog, the job can be tested and the import text file can be viewed.

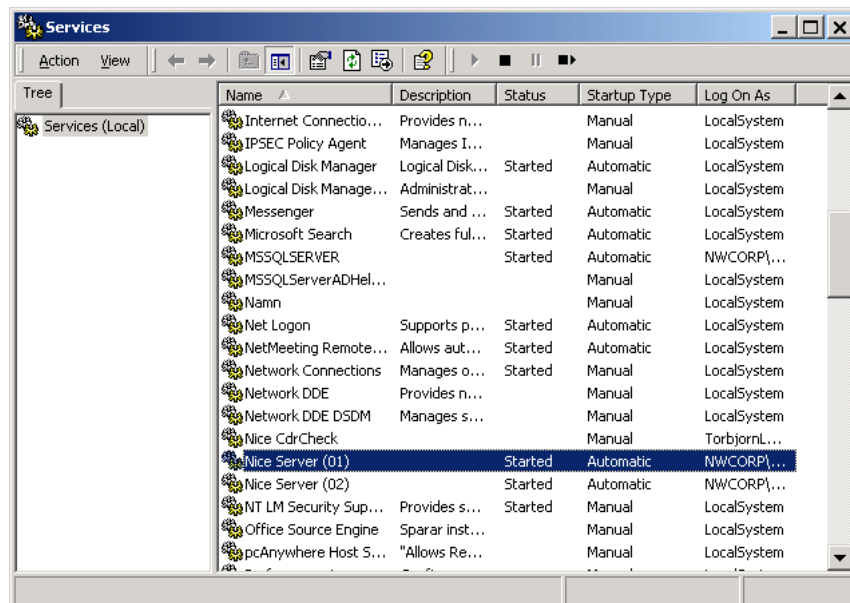
If anything goes wrong, use the **Windows Event Viewer** to check for errors. In this case, the job has to be restarted from **Spmann tool**.

## Event Viewer

Event Viewer is launched from the menu **Programs > Event Viewer**.



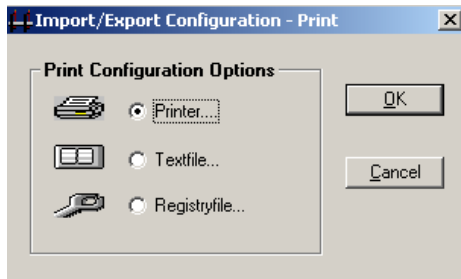
Sometimes, Nice Service stops after an Export or Import. If this happens, start it again from **Windows Services**. Services can be started from the menu **Programs > Services**.



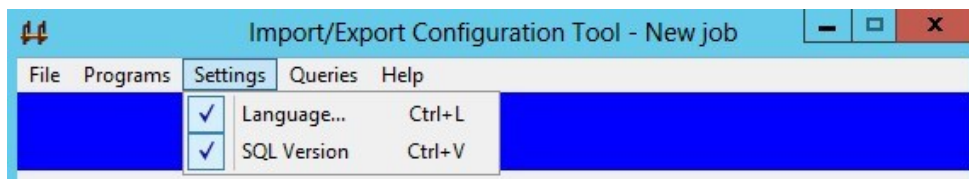
## Printing Import/Export Configuration

If Import/Export is successful and you want to implement it somewhere else, the configuration can be printed out from the menu **File > Print Import/Export Conf.**

If Import/Export is not successful, you can save it as a text file and send to Mitel Support for investigation.



## Settings



If supporting a CMG System in another language, fields that can be re-named can also be displayed in any supported language. Choose menu **Settings > Language**

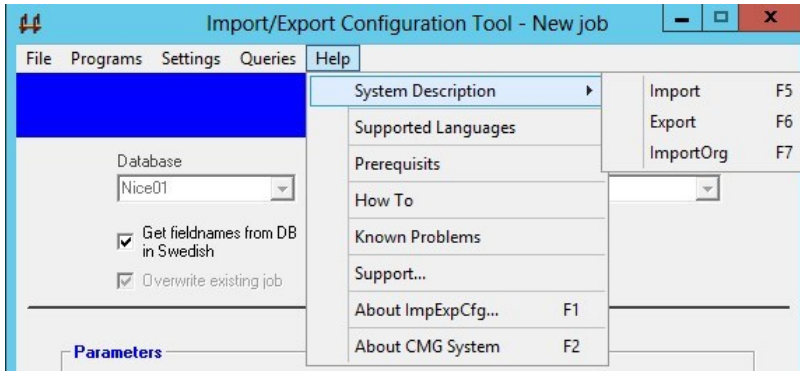


To be able to display the re-named fields in the selected language, the correct version of SQL has to be specified. Click **Settings**, select **SQL Version**, and type the number corresponding to the SQL version.

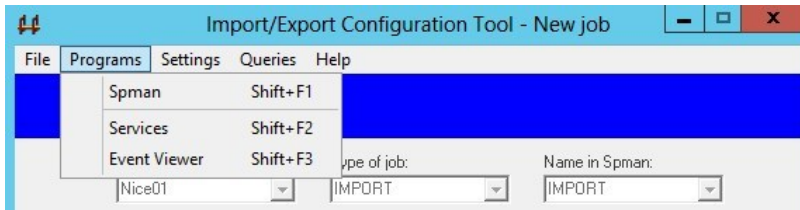


## Additional Information

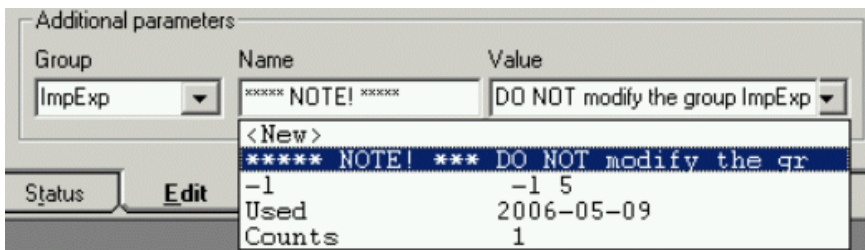
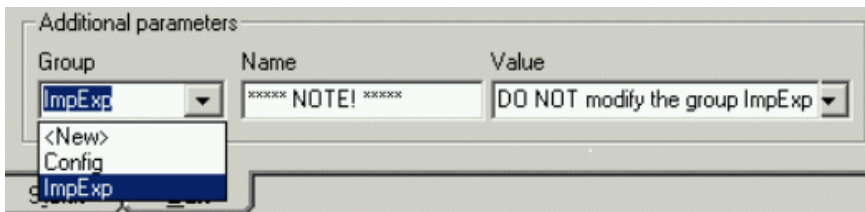
The **Help** menu contains other options, as shown in the following figure:



Programs can be started from the menu Programs as shown in the following figure:

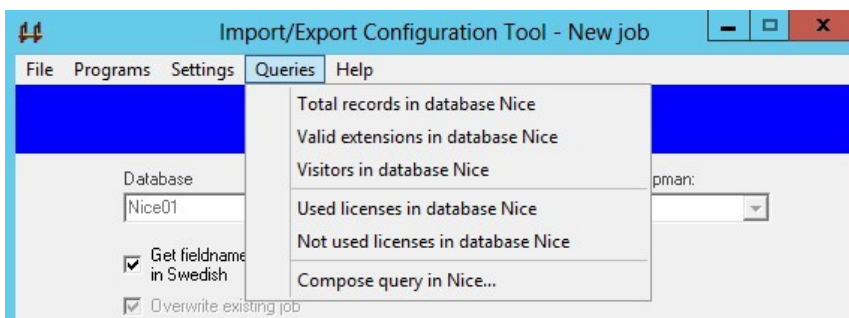


**NOTE:** Spman tool will get a new branch in the registry where statistics are located. Do not edit this branch.

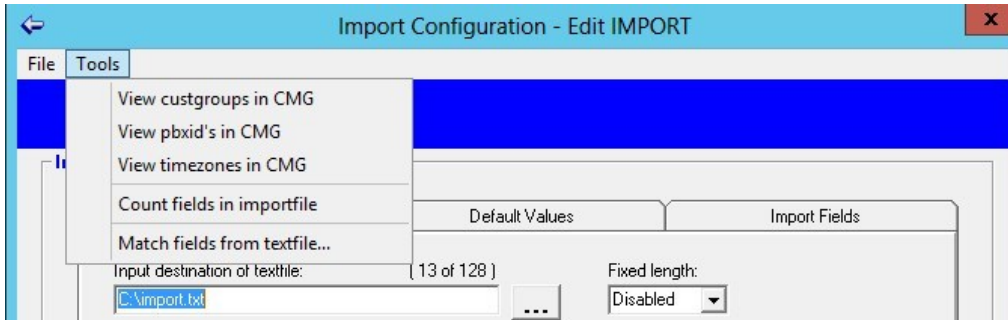


## Queries

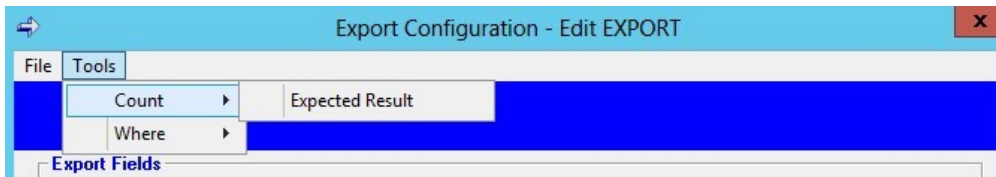
You can use the configuration tool to get answers about records in the database.



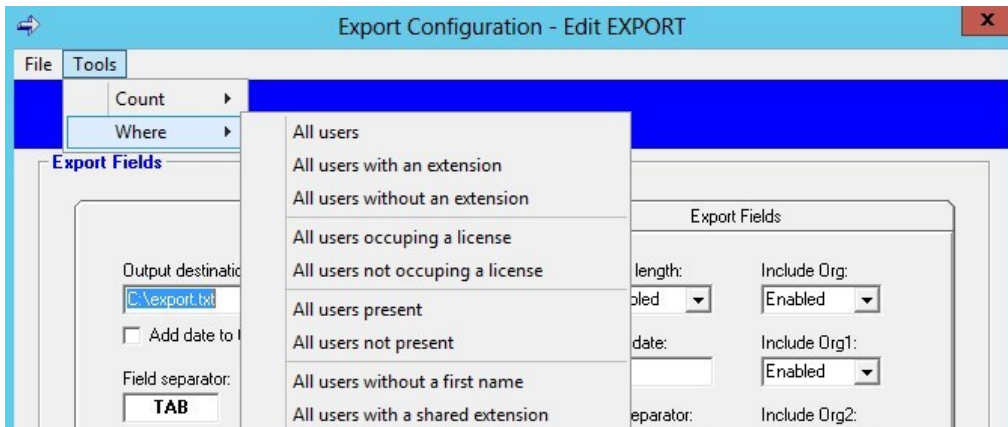
You can use the configuration tool to determine what alternatives you can enter in the fields. Check the import text file for errors. Match fields from a post towards the configuration to see where the data will go.



You can use the configuration tool to find out what you can expect from an export of data.



You can use the configuration tool to get help when filtering records for an export.



## Support

If you encounter any trouble regarding the configuration tool, do the following:

1. Go to **Help > Support** and click **Copy to clipboard**.
2. Attach the info from the clipboard to the error report.



**Support** [X]

When opening a call, the following parameters need to be known. Click "Copy to clipboard" and paste the text into an e-mail. Send e-mail to:

Hostname:

CMG-Version:

Export:  Import:  Importorg:  ImpExpCfg:

SQL-Server:

User:

Password:

SQL-Version:

Language fieldnames:

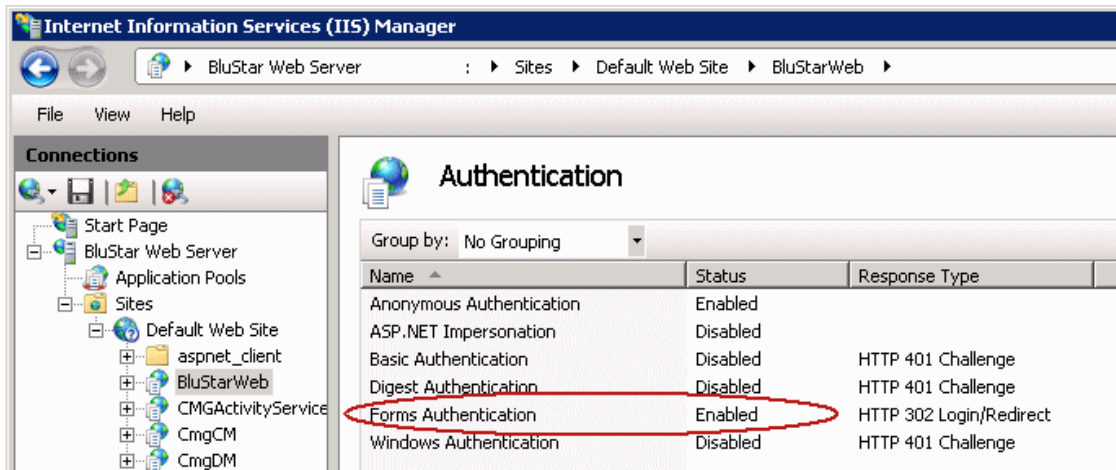
# Appendix IV - Setting up User Authentication

There are multiple ways of authenticating users in CMG Web:

- CMG user authentication using Forms Authentication with Extension and password, the same as in Office Web. This is the default authentication setting after installation.
- Windows authentication using Forms Authentication with Windows user and password. LDAP is used to fetch a user unique field to match to a CMG user.
- IIS Windows authentication with automatic logon, Windows authentication performed in IIS. If the Windows account information is not provided by the browser, the user is prompted for credentials in a separate dialog.
- Automatic Windows authentication with Forms Authentication if Windows authentication fails. If the browser does not provide the correct Windows user credentials, the Forms Authentication is offered to the user. The Forms Authentication can be either CMG user authentication or Windows authentication based on the configuration.
- ADFS authentication

## CMG Forms Authentication

In **IIS Manager**, change **Authentication - Forms Authentication** to Enabled and leave the **Anonymous Authentication** set to Enabled for the CMG Web Website.



If no authentication is required in order to perform a search in the CMG Web GUI, then you can set the parameter "DirectoryPageRequireAuthentication" to "false" in Application Settings Application Settings for the CMG Web in IIS Manager.

## Windows Forms Authentication

1. Add the server running the CMG Server to the Windows domain.
2. In **IIS Manager**, change **Authentication - Forms Authentication** to Enabled for the **CMG Web** Website.

3. Set up the parameters for Windows Authentication in **CMG Configuration Manager**. Do the following:
  - a. Open **CMG Configuration Manager** and expand **CMG Web** in the sidebar. Select **Parameters** and navigate to **Windows Authentication**.
  - b. Set up the Active Directory access parameters to access AD through LDAP.
  - c. Set User **Authentication Type** to Windows.
  - d. Enter the correct values in the fields **Active Directory User Identifier Field** and **CMG User Identifier Field**. These fields are used to match the Windows user to a CMG user and the values have to be user unique and matched. The e-mail address is used default to match the user.

## Windows Authentication in IIS

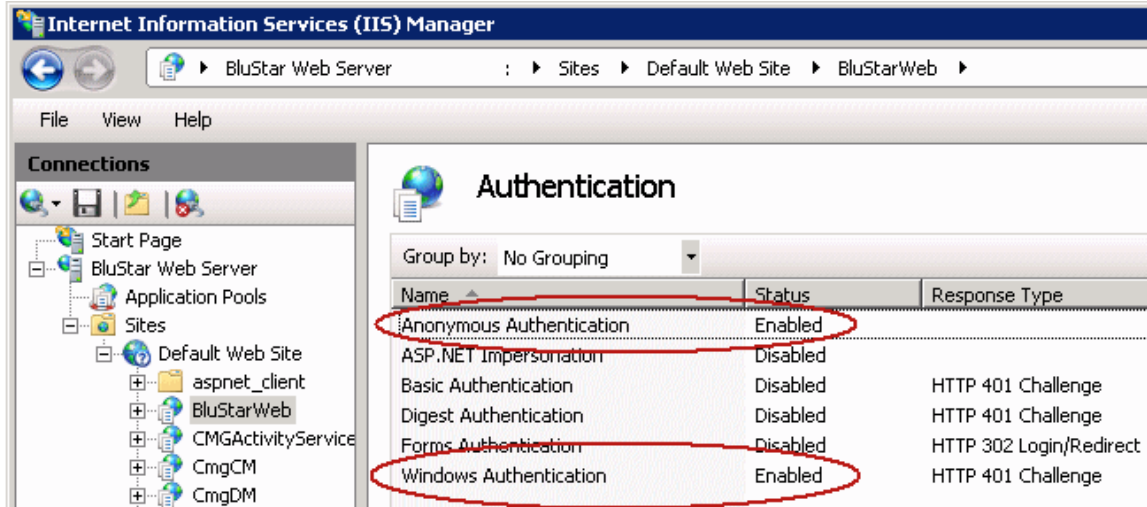
1. Add the server running the CMG Server to the Windows domain.
2. In IIS Manager, change **Authentication - Windows Authentication** to Enabled and all the other authentication options set to Disabled for the CMG Web Website.



3. In **IIS Manager** check **Providers** for **Windows Authentication** so that NTLM is the enabled provider.
4. Set up the parameters for Windows Authentication in **CMG Configuration Manager**. Do the following:
  - a. Open **CMG Configuration Manager** and expand **CMG Web** in the sidebar. Select **Parameters** and navigate to **Windows Authentication**.
  - b. Set up the Active Directory access parameters to access AD through LDAP.
  - c. Enter the correct values in the fields **Active Directory User Identifier Field** and **CMG User Identifier Field**. These fields are used to match the Windows user to a CMG user and the values have to be user unique and matched. The email address is used by default to match the user.

## Automatic Windows Forms Authentication

1. Add the server running the CMG Server to the Windows domain.
2. In IIS Manager, change **Authentication - Anonymous Authentication** and **Windows Authentication** to Enabled to for the CMG Web Website.



3. In **IIS Manager** check **Providers** for **Windows Authentication** so that NTLM is the enabled provider.
4. Set up the parameters for Windows Authentication in **CMG Configuration Manager**. Do the following:
  - a. Open **CMG Configuration Manager** and expand **CMG Web** in the sidebar. Select **Parameters** and navigate to **Windows Authentication**.
  - b. Set up the AD access parameters to access AD through LDAP.
  - c. Set **User Authentication Type** to CMG or Windows, depending on what type of authentication is to be offered in the Forms Authentication.
  - d. Enter the correct values in the fields **Active Directory User Identifier Field** and **CMG User Identifier Field**. These fields are used to match the Windows user to a CMG user and the values have to be user unique and matched. The e-mail address is used default to match the user.

## Active Directory Federation Services (ADFS) Authentication

Active Directory Federation Services (ADFS) simplifies access to systems and applications using a claims-based access (CBA) authorization mechanism to maintain application security. For more information, please refer to: <http://technet.microsoft.com/en-us/windowsserver/dd448613.aspx>

1. In the C:\inetpub\wwwroot\CMGWeb directory:
  - a. Delete the existing web.config file.
  - b. Rename the web.adfs.config file to web.config.
2. In the new web.config file, configure <appSettings>:
  - a. Set the value of UserClaimType to an ADFS claim type, which contains the information to match with a CMG field (typically a claim type that contains the e-mail address of the users), see step 6.
  - b. Set a value of Claim<x> to filter on, for example, a group or a company.
3. Make sure that your ASP.NET application's URL and port number match the values in the audienceUris entry, for example,

```
<audienceUris>
```

```
<add value="http://localhost/CMGWeb" />
```

```
</audienceUris>
```

4. Set a trusted issuer, for example:

```
<trustedIssuers>
```

```
<add thumbprint=" 1234567890ABCDEF GHIJKLMNOPQRSTUVWXYZ1234 "  
name="YourSTSName" />
```

```
</trustedIssuers>
```

It is possible to have several `<trustedIssuers>` elements.

5. Make sure that the `issuer` value fits your Security Token Service (STS) URL and that your ASP.NET application's URL and port number match the values in the `realm` attribute of the `<wsFederation>` element:

```
<wsFederation passiveRedirectEnabled="true"
```

```
issuer="http://localhost:13922/wsFederationSTS/Issue/"
```

```
realm="http://localhost/CMGWeb" requireHttps="true" />
```

6. Open CMG Configuration Manager and expand **CMG Web** in the sidebar. Select **Parameters** and navigate to **Windows Authentication**.

- a. Enter the correct values in the field **CMG User Identifier Field**. This field is used to match the domain user to a CMG user, and should indicate which CMG field that contains the information to match with the content of the claim type specified in step 2. The setting should typically be set to MSGID to indicate that the e-mail address of the user in CMG should match the content of the claim type from ADFS.

**NOTE:** When setting up ADFS and IIS you need to configure the IIS site (BSW) application pool to set the Process model -> load user profile to 'true'.

# Appendix V - CMG Web Multi-Server Deployment

Multiple CMG Web sites can be deployed using the same CMG Web Service. The CMG Web sites can use different authentication methods and the application settings can be configured individually for each site.

## Configure Server Address for CMG Web Service

To connect CMG Web to CMG Web Service on another server, the following configuration has to be done in IIS:

1. Open **IIS Manager**, then select **Application Settings**.
2. In the **Application Settings** window, update the **CMGWebServiceBaseUrl** setting with the address of the other server.

## Configure CMG Web Service

If CMG Web Service is deployed on another server than the CMG Server, the configuration file `CMGWebServiceConfig.xml`, located in the folder of CMG Web Service, has to be modified.

Set the following parameters, where the CMG Server, AnA and CWI web services are assumed to be installed on a server named `cmgsrv`:

```
<CmgDatabaseConnectionString>
server=cmgsrv;database=nice;User ID=nice;Password=thepassword
</CmgDatabaseConnectionString>
<CmgUserInfoServiceUrl>
http://cmgsrv/CMGUserInfoService/CMGUserService.asmx
</CmgUserInfoServiceUrl>
<CmgActivityServiceUrl>
http://cmgsrv/CMGActivityService/CMGActivityService.asmx
</CmgActivityServiceUrl>
<AnAServiceUrl>
http://cmgsrv/nwAna/AnAService.asmx
</AnAServiceUrl>
```

# Appendix VI - Connecting to the PBX

## Connecting to Mitel TSW (serial)

This appendix describes the common installation and configuration procedure for the communication between a CMG Server and one Mitel TSW with serial interface.

This description has to be used only when the serial interface from the PBX is connected directly to the COM port of the CMG Server.

### Before the Installation

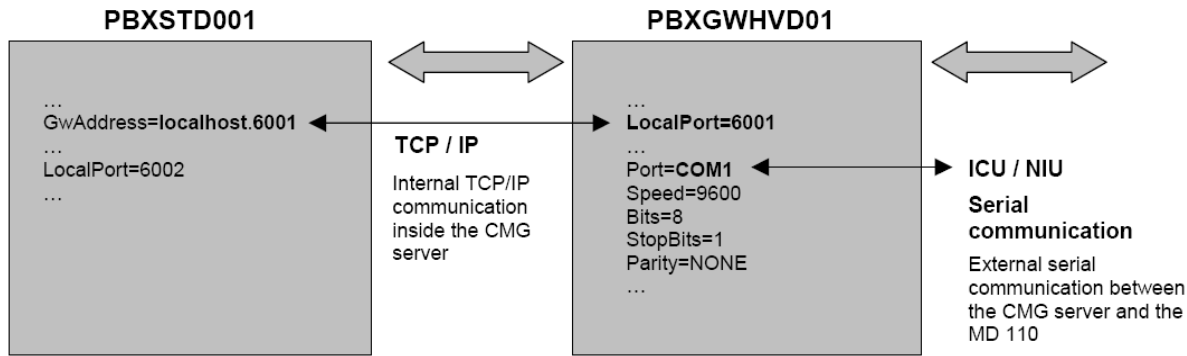
Before starting the configuration, note the following considerations:

- Available com port(s) at the CMG Server
- Speed and parity of the serial device/interface from the PBX. For example:
  - Speed = 2400
  - Parity = 8
  - Bits = 1
  - StopBits = None
- ExtLth of the PBX. If the internal phone numbers are within the interval 1000 – 9999 then, normally the ExtLth = 4, 10 000 – 99 999 then the ExtLth = 5, and so on.
- What to name the PBX in the CMG system.

The serial communication between the CMG Server and Mitel TSW requires one com port. The interface communicates to the IDP-unit in the Mitel TSW through the NIU2 board.

### Installation Steps

1. Connect the cable from the PBX to a COM port in the CMG Server.
2. Open **CMG Configuration Manager**.
3. Choose **PBX's/Flash Clients** in the left frame.
4. As you will see, PBX number 1 is already installed by default with ExtLth=4.  
Change the type and values to fit your system and save.
5. Highlight the PBX. Extensions 1000-9999 are added as default.  
Change the values to fit your system and save.
6. Start **Spman tool**.
7. Highlight the pre-configured PBXSTD001 process and control the settings.
8. The picture below describes the relationship between the key processes. Control and – if necessary – modify the settings for the PBXSTD001 and PBXGWHVD01 process. These processes are pre-configured in Spman tool.



9. If you have edited the processes, highlight PBXSTD001 and PBXGWHVD01 and choose **Stop**, then **Start** and then **Refresh**.
10. If the processes started without any errors, it is recommended that you also refresh the following processes: DBtoPBX, IRTIMER, DELIR, MRTIMER, NICESRV, and the process for the IVR (if there is one).

## Verify Call Forwarding on New Activity

1. Open **CMG Directory Manager**.
2. Choose **New record** in the left frame. Add a test individual and type the extension number to a telephone that is nearby. Be sure to give the record the correct PBX id or PBX name. Save the record.
3. Start CMG Web or the InAttend client and add a new current activity for your test individual.
4. Check the telephone whose extension you used for the test record. Verify that forwarding is enabled on the phone, for example to the operator or the IVR system.
5. Delete the activity.
6. Add a new activity using the telephone (\*23\*...).
7. Check on the telephone that it is forwarded.
8. Check in CMG Web or the InAttend client that the activity has been entered.

## Connecting to Mitel TSW (with NIU2 board)

This is a description of the common way to install and configure the communication between a CMG Server and Mitel TSW with NIU2 (Network interface unit) board.

### Before the Installation

Before starting the configuration, note the following considerations:

- Available IP-ports at the CMG Server.
- IP address for the CMG Server.
- IP port of the PBX.

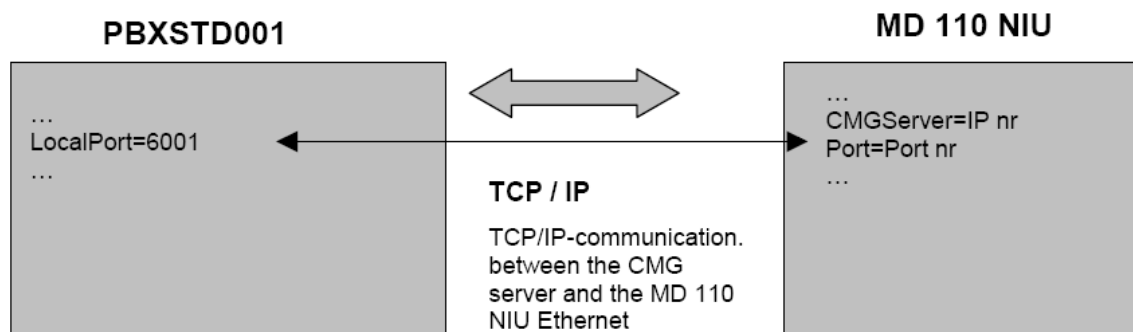


- ExtLth of the PBX. If the extension numbers are within the interval 1000 – 9999 then, normally the ExtLth = 4, 10 000 – 99 999 then the ExtLth = 5, and so on.
- What to name the PBX in the CMG system

The interface from the PBX to the CMG Server requires that the correct IP no for the CMG Server is properly set in the PBX. At the CMG Server you only need to set the right IP port number to/from the PBX.

## Installation Steps

1. Open **CMG Configuration Manager**.
2. Choose **PBX's/Flash Clients** in the left frame.
3. PBX number 1 is already installed by default with ExtLth=4. Change the type and values to fit your system and save.
4. Highlight the PBX. Extensions 1000-9999 are added as default. Change the values to fit your system and save.
5. Start **Spman tool**.
6. The picture below shows the relationship between the key processes. Control and – if necessary – modify the settings for the PBXSTD001 process. This process is pre-configured in Spman.



7. If you have edited the process, highlight PBXSTD001 and choose Stop, then Start and then Refresh.
8. If the process started without any errors, it is recommended to also refresh the following processes: DbToPBX, IRTIMER, DELIR, MRTIMER, NICESRV, and the process for the IVR (if there is one).

## Verify Call Forwarding on New Activity

1. Open **CMG Directory Manager**.
2. Choose **New record** in the left frame. Add a test individual and type the extension number to a telephone that is nearby. Make sure you give the record the correct PBX id or PBX name. Save the new record.
3. Start CMG Web or the InAttend client and add a new current activity for your test individual.
4. Check the telephone whose extension you used for the test record. Verify that forwarding is enabled on the phone, for example to the operator or the IVR system.
5. Delete the activity.

6. Add a new activity using the telephone (\*23\*...).
7. Check on the telephone that it is forwarded.
8. Check in CMG Web or the InAttend client that the activity has been entered.

## Connecting to MiVoice MX-ONE

This section describes the common way to install and configure the communication between a CMG Server and MiVoice MX-ONE.

### Before the Installation

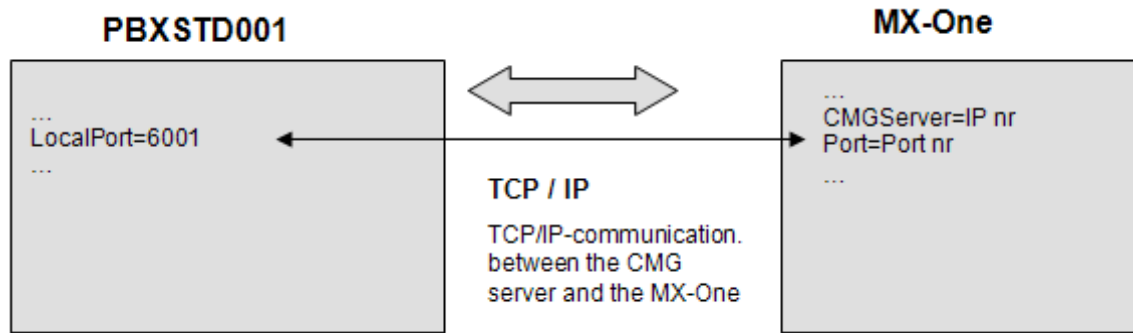
Before starting the configuration, note the following considerations:

- Available IP ports at the CMG Server.
- IP address for the CMG Server.
- IP port of the PBX.
- ExtLth of the PBX. If the extension numbers are within the interval 1000 – 9999 then, normally the ExtLth = 4, 10 000 – 99 999 then the ExtLth = 5, and so on.
- What to name the PBX in the CMG system.

The interface from the PBX to the CMG Server requires that the correct IP address for the CMG Server is properly set in the PBX. At the CMG Server you only need to set the right IP port number to/from the PBX.

### Installation Steps

1. Open **CMG Configuration Manager**.
2. Choose **PBX's/Flash Clients** in the left frame.
3. PBX number 1 is already installed by default with ExtLth=4. Change the type and values to fit your system and save.
4. Highlight the PBX. Extensions 1000-9999 are added as default. Change the values to fit the system and save.
5. Start **Spman tool**.
6. The picture below shows the relationship between the key processes. Control and – if necessary – modify the settings for the PBXSTD001 process. This process is pre-configured in Spman.



7. If you have edited the process, highlight PBXSTD001 and choose **Stop**, then **Start** and then **Refresh**.
8. If the process started without any errors, it is recommended that you also refresh the following processes: DbToPBX, IRTIMER, DELIR, MRTIMER, NICESRV, and the process for the IVR (if there is one).

**NOTE:** If adding more PBXs, this is done manually. You need to add a new PBX from Configuration Guide - CMG.

## How to add PBXSTD for multiple PBXs.

To add PBXSTD for multiple PBXs, follow the below steps:

1. First, launch the **Spman** > Click the **Edit** tab.

The screenshot shows the Spman application window with the title bar 'Server: WIN-0RKISRQJC6Q DBID: 01'. The menu bar includes 'File', 'Command', 'WinTools', and 'Help'. The main window is divided into several sections:

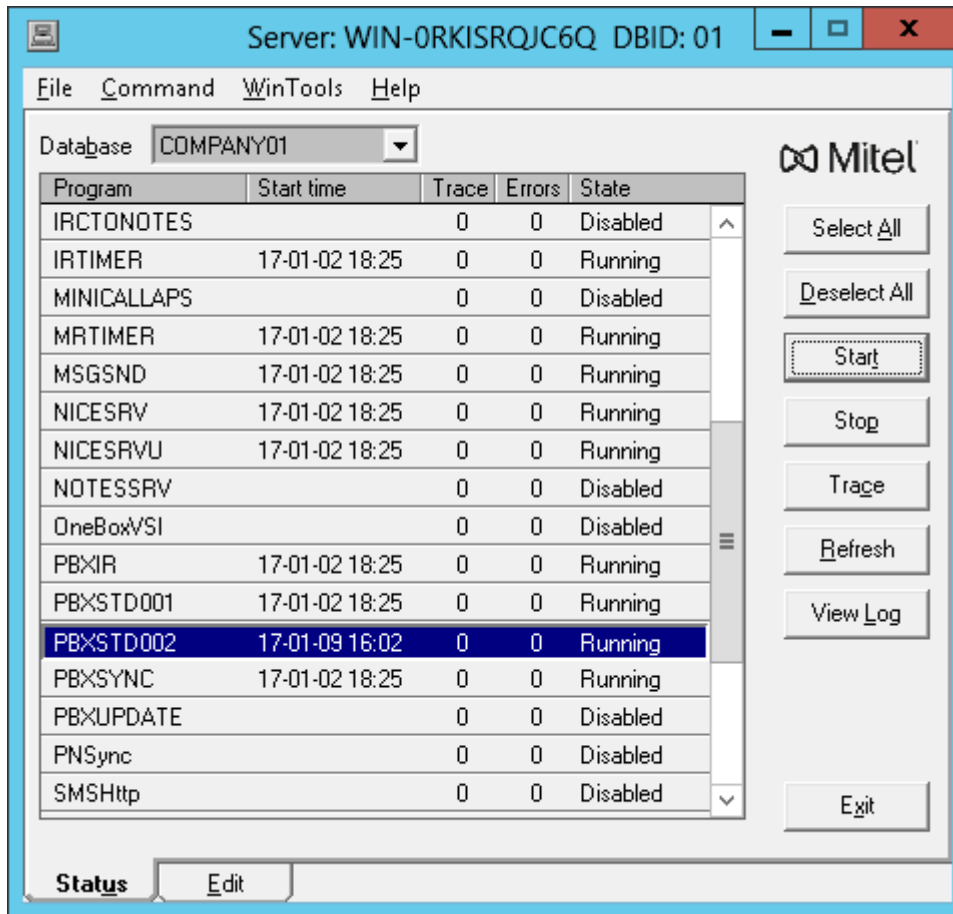
- Program Configuration:**
  - Program: PBXSTD002
  - Program path: pbxstdniu.exe
  - Parameters: | -5
  - Wait: 0
  - Max restarts: 3
  - Start order: 0
  - Enabled: ☒
  - Desktop: ☐
- Buttons:** Save, New, Delete, Previous, Next.
- Status Section:**
  - State: Not running
  - Start time: (empty field)
  - Errors: 3
- Additional parameters:**

Group	Name	Value
Config	ExternalSys	Disabled
- Bottom Tabs:** Status, Edit.

2. Select **New** button.
3. Type the desired **Program name** (Ex: PBXSTD002).
4. Enter the **Program Path** as "pbxstdniu.exe".
5. Provide the below details for the remaining parameters:
  - a. Parameters = "| -5"
  - b. Wait = "0"
  - c. Max restarts = "3"
  - d. Start Order = "0"
6. Check the **Enabled** check box.
7. Click **Save** to save the changes made.

To start the new PBXSTD program, toggle to **Status** tab from Spman.

- Select the new program name that was given above.  
(in this example, it is PBXSTD002)
- Click the **Start** button.



The new PBXSTD program is added and started.

## Verify Call Forwarding on New Activity

1. Open **CMG Directory Manager**.
2. Choose **New record** in the left frame. Add a test individual and type the extension number to a telephone that is nearby. Ensure that you give the record the correct PBX id or PBX name. Save the new record.
3. Start CMG Web or the InAttend client and add a new current activity for your test individual.
4. Check the telephone whose extension you used for the test record. Verify that forwarding is enabled on the phone, for example to the operator or the IVR system.
5. Delete the activity.
6. Add a new activity via the telephone (\*23\*...).
7. Check on the telephone that it is forwarded.
8. Check in CMG Web or the InAttend client that the activity has been entered.

# Connecting to BusinessPhone

This section describes the common way to install and configure the communication between a CMG Server and a BusinessPhone.

## Before the Installation

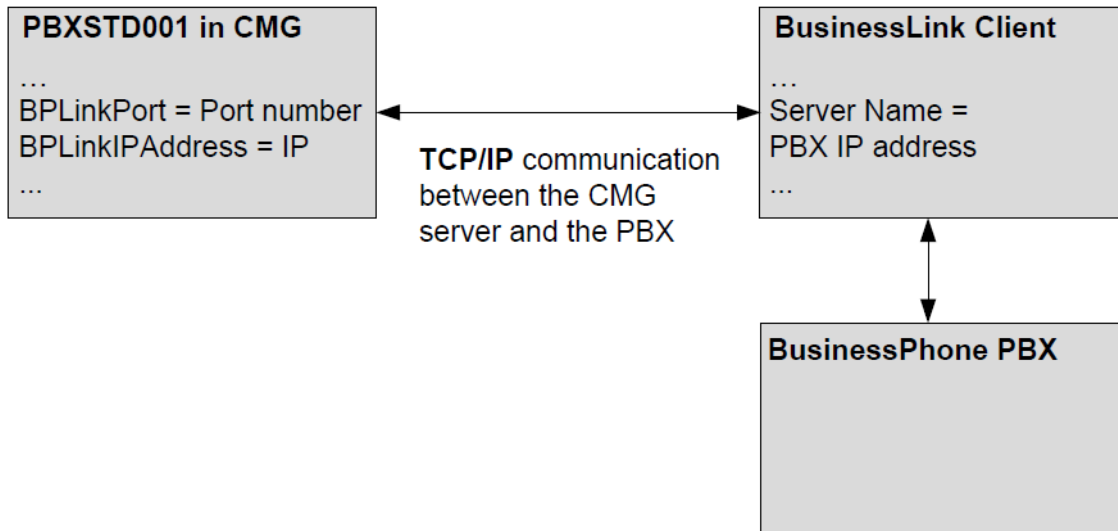
Before starting the configuration, note the following considerations:

- Available IP ports at the CMG Server.
- IP address for the CMG Server.
- IP port on the PBX (default 2555).
- What to name the PBX in the CMG system.

The interface from the PBX to the CMG Server requires that the BusinessLinkClient is installed on the CMG Server.

## Installation Steps

1. Open **CMG Configuration Manager**.
2. Choose **PBX's/Flash Clients** in the left frame.
3. PBX number 1 is already installed by default with ExtLth=3.  
Change the type and values to fit your system and save.
4. Highlight the PBX. Extensions 100–999 are added as default.  
Change the values to fit the system and save.
5. Start **Spman tool**.
6. The picture below shows the relationship between the key processes.  
Control and – if necessary – modify the settings for the PBXSTD001 process. This process is pre-configured in Spman.
7. Start the PBXSTD001 process.



8. If you have edited the process, highlight PBXSTD001 and choose Stop, then Start and then Refresh.
9. If the process started without any errors, it is recommended that you also refresh the following processes: DbToPBX, IRTIMER, DELIR, MRTIMER, NICESRV, and the process for the IVR (if there is one).

## Verify Call Forwarding on New Activity

1. Open **CMG Directory Manager**.
2. Choose **New record** in the left frame. Add a test individual and type the extension number to a telephone that is nearby. Ensure you give the record the correct PBX id or PBX name. Save the new record.
3. Start CMG Web or the InAttend client and add a new current activity for your test individual.
4. Take a look at the telephone you chosen. Check if the phone is forwarded, for example to the operator or the IVR system.
5. Delete the activity.
6. Add a new activity via the telephone (\*23\*...).
7. Check on the telephone that it is forwarded.
8. Check in CMG Web or the InAttend client that the activity has been entered.

# Appendix VII – Connecting to the E-mail System

## Connecting to E-mail System using SMTP

Consider the following prerequisites:

- A connection to a customer's e-mail server using SMTP
- An e-mail account that is allowed to send e-mail

### Installation Steps

1. Configure the e-mail server registry parameters.  
Start **Spmman tool** and configure **SMTPSRV**.  
See CMG Server System Process Description [5] for configuration information.

The screenshot shows the Spman tool configuration window for the process SMTPSRV. The window title is "Server: TBWIN200881N DBID: 01". The menu bar includes File, Command, WinTools, and Help. The configuration fields are as follows:

- Program: SMTPSRV
- Program path: mailsrv.exe
- Parameters: -c 3 -n smtpsrv -l 5
- Wait: 0
- Max restarts: 16
- Start order: 0
- Enabled: ☒
- Desktop: ☐
- State: Running
- Start time: 15-10-12 12:42
- Errors: 0
- Additional parameters table:
 

Group	Name	Value
Config	MailUserName	Mail address @ company

Buttons on the right side include Save, New, Delete, Previous, and Next. At the bottom, there are Status and Edit buttons.

Set the following values:

"MailUserName" = [cmg.system@customer.com](#) (Example of mail user name)

"MailUserPwd" = \*\*\*\*\* (Password for the above mail user)

"MailHost" = MailServerAddress (IP address or host name to the receiving email server)



"MailFrom" = `cmg.system@customer.com` (normally be equal to the MailUserName above)

"MailPort" = (Can be empty)

"IsSSEnabled" = "0" (0 for disabled, 1 for enabled)

"TLSVersion"=(Empty when IsSSEnabled=0 but 1.0, 1.1 or 1.2 when IsSSEnabled=1)

**NOTE:** Depending on the specific customer environment, a certificate might be needed on the CMG server.

## Configuration of the E-mail Connection in CMG CM

1. Open **CMG Configuration Manager**.
2. Select **Message Systems** in the sidebar. Some settings are optional. The default program name, e-mail, relates to the MAPISRV-process in Spman default.
3. Change program MAPISRV to SMTPSRV.
4. Leave rest of parameters with default values.

## Verify the E-mail Function

1. When the parameters and configuration are completed, start Spman tool, and restart MSGSND and SMTPSRV.
2. Start the InAttend client and pick up your "Test individual".
3. Choose the right message System.
4. Choose "New Message".
5. Add a manual timestamp and a relevant text in the body and send it.  
Example: "Test nr 1, Time 15:31"
6. Verify that the mail was successfully delivered.

## Troubleshooting

1. Start process with log level 6:  
`Spman - SMTPSRV -parameters -c 1 -n smtpsrv -l 6`
2. Make sure that the used IP address or host name is correct.
3. Check that SMTP is enabled on the e-mail server.
4. Check that the CMG Server has user rights to connect on port 25.
5. Check if there is any software or hardware firewall blocking port 25.
6. Check the Spman parameter mailfrom. This user must have access to send e-mail.

# Appendix VIII – Change Nice Password in SQL Server

If you want to change the password in SQL for the database user nice or qmuser, use the tool **ChangeNicePwd**, which will update registry and necessary tables in SQL, and in the SQL Server.

## ChangeNicePwd.exe Usage

Start `\nicesrv\pgm\ChangeNicePwd.exe` and do the following:

1. Select the database user to be changed (nice).
2. Enter the password (the current password for the nice account).
3. Check for access to the registry and to the database.
4. Change in files, registry, and database, and in SQL.
5. Reboot the server if password is changed in SQL.
6. After the steps 1 – 4 are executed, all the servers involved have to be rebooted (CMG/CMG Speech/CMG Speech Telephony/BluStar Server).
7. Copy “ChangeNicePwd.exe” to any of the folder among the servers involved (CMG/CMG Speech/CMG Speech Telephony/BluStar Server).
8. The file “UMSCoder.exe” also needs to be copied to the same folder as ChangeNicePwd on the server containing BluStar Server.

Change password for nice and qmuser

File Tools Help

Database User: (1)  
nice

Passwords for db user (2)  
Old password: [format2007] New password:   
☐ Current password for db user in SQL ☐ Current password for db user in SQL

Test for access to (3)  
   
☐ - Not tested ☐ - Not tested

Change password for nice (4)  
 ?  
☐ - Not changed  
 ?  
☐ - Not changed  
 ?  
☐ - Not changed

Change password for qmuser (4)  
 ?  
☐ - Not changed

Change password in SQL (5)  
 ?  
☐ - Not changed for nice  
☐ - Not changed for qmuser

Installed Applications  
☒ CMG  
☒ CMG Visit  
☒ CMG Speech  
☐ CMG Speech Telephony (Standalone Server)  
☒ CMG Speech Attendant  
☐ InAttend  
☐ Quality Manager  
☐ Quality Manager Wallboard

# Technical Assistance

Mitel provides [www.mitel.com](http://www.mitel.com) as a starting point for technical assistance regarding all products, including CMG. From here, partners can obtain online documentation, FAQs, latest software updates and request further technical assistance.

# References

- [1]CMG System Overview
- [2]CMG Installation Guide
- [3]CMG Quick Installation Guide
- [4]Calendar Connection Configuration Guide
- [5]CMG Server System Process Description



