# Mitel MiContact Center Enterprise

## MOBILE AND WEB APPLICATIONS CONFIGURATION GUIDE

Release 9.1

## NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

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

MiContact Center Enterprise Mobile and Web Applications
Configuration Guide
Release 9.1 – May 2016

# INTRODUCTION

This document describes how to properly configure the mobile applications and web applications in MiCC Enterprise. It applies to the following applications.

- The **Mobile Agent**, which allows phone agents to log on to MiCC Enterprise, set and view their ready / not ready status, and view real-time information about their service groups.
- The **Web Manager**, which can be used for day-to-day adaptation of the Contact Center parameters based on real-time supervision data.

Common configuration steps are presented, and an entire section is also devoted to accessing these apps from the internet.

## LICENSING

No specific license is associated to the mobile and web applications, which depend on the licenses required for Phone Agents and Real Time Interface usage.

### MOBILE AGENT

Each user of the Mobile Agent application needs the licenses associated to Phone Agents, which are the two following concurrent licenses:

- Number of Connected users,
- Call control.

In addition, the Service Groups information display requires the following site license:

- Real Time Interface.

### WEB MANAGER

The Web Manager application requires the following site license:

- Real Time Interface.

# CONFIGURATION

## BROADCAST INTERFACE

The Mobile Agent application receives Ready and Not Ready status change notifications if the corresponding events are sent to the Broadcast Interface.

This option must be selected using Configuration Manager as follows.

1. In the Contact Center (Tenant) Properties, click Advanced…
2. In the Broadcast Parameters group box of the General tab, check the Send Events for Phone Agents to Broadcast Interface option.

## PERMISSIONS

### MOBILE AGENT

The Mobile Agent application is accessible to Phone Agents, who are users associated with a User Type allowing Answer Service Calls privilege.

### WEB MANAGER

The Web Manager is accessible to users associated with a User Type providing access to the Configuration Manager application (although no Configuration Manager license is consumed by Web Manager users).

To configure the contact center elements, the user's User Type must be defined with the corresponding Manage privileges.  For instance, creating and modifying Service Groups (and changing their skill assignment) requires the Manage Service Group privilege.

## PRIVACY LINK

The Web Manager Logon window supports the display of a privacy link. If enabled, the user can click on the link to view the organization’s privacy policy. You must specify a valid URL for the privacy link in the web.config file.

The web.config file is stored in a sub-folder of the MiCC Enterprise installation directory (e.g., C:\Program Files (x86)\Mitel\MiCC Enterprise\Services\Web\WebApps).

1. Open the web.config file in a text or XML editor.
2. In the appSettings section, specify the URL in the **value** attribute of the **PrivateURL** key element. For example:

   ```
   <add key="PrivacyURL" value="http://www.mitel.com/content/legal-information"/>
   ```

3. Save the web.config file.

**Note**:   Do not make any other changes to the web.config file.

# EXTERNAL AUTHENTICATION

By default, the mobile and web applications authenticate users based on their Logon ID and / or Password (PIN). However, the authentication process can also be delegated to an external service.

Each MiCC Enterprise Tenant can be configured with such a service, thereby enabling Single Sign-On (SSO) for tenant users.

## SUPPORTED PROTOCOL

To be eligible for use with the MiCC Enterprise mobile and web applications, an external authentication service must comply with the **SAML version 2.0** protocol.

In SAML terms, the external authentication service is called *Identity Provider* and the MiCC Enterprise mobile and web applications are called the *Service Provider*.

## SECURE CONNECTIONS TO WEB SERVICES AND APPLICATIONS

Some external Identity Providers require the Service Provider to be accessed through secure connections. In this case, the IIS server hosting the MiCC Enterprise web services must be configured as described on page 10 (IIS 7 secure connections).

Furthermore, the Web Server Location must be specified using the fully qualified domain name of the MiCC Enterprise web server. This is the name that has been associated with the encryption certificate installed on the web server.

- Open the **MiCC Enterprise Setup** Utility.
- Select Web Server Location in the left list.
- Change the Location field to the fully qualified domain name of the MiCC Enterprise web server.
  **Example:** change “`micc-enterprise`” to “`micc-enterprise.somecompany.com`”.

After these steps, the URLs used to access the mobile and web applications become

https://<Fully Qualified Server Name>/webapps/agent

https://<Fully Qualified Server Name >/webapps/contactcenter

# CONFIGURATION GUIDELINES

## CONFIGURATION OF THE IDENTITY PROVIDER

Before accepting authentication requests, the Identity Provider must be configured with data about the Service Provider (MiCC Enterprise mobile and web applications).

- **Entity ID**: this is a URI that uniquely identifies the Service Provider. Some Identity Providers refer to this Entity ID as “Audience” or “Recipient”.

  On a properly configured MiCC Enterprise installation, the Entity ID is the following:

  https://<Fully Qualified Server Name >/webapps/AuthServices

  **Note:** the correct case must be used when setting this property in the Identity Provider. When in doubt, check this value in the `entityID` attribute of the `EntityDescriptor` element in the MiCC Enterprise metadata file (see location below).

- **Assertion Consumer Service (ACS) URL**: this is the location to which the Identity Provider will redirect clients (web browsers) after they have been successfully authenticated. The ACS should be set to

  https://<Fully Qualified Server Name >/webapps/AuthServices/Acs

The Identity Provider may be able to configure a Service Provider from its metadata, which is an XML document containing the Entity ID and ACS URL. After configuring a MiCC Enterprise system as described previously, the metadata document that must be sent to the Identity Provider is accessible from the following location:

https://<Fully Qualified Server Name >/webapps/AuthServices

(Following the general convention, this location is identical to the Entity ID.)

## CONFIGURATION OF A MICC ENTERPRISE TENANT

The association between a Tenant and an external Identity Provider must be configured as follows.

- In Configuration Manager, open the **Properties** dialog of the Tenant (or the system Properties dialog on a non-tenanted installation).
- Select the **Authentication** tab.
- Set the **Name** field to any value of your choice. This name will appear on the users’ login page in the mobile and web applications.
- Set the **Entity ID** field to the unique identifier of the Identity Provider. This Entity ID may have been assigned during (or after) configuration of the Identity Provider. It can be found in its metadata document.
- Set the **Metadata Location** field to the URL or local path to the metadata document of the Identity Provider. This location must be accessible from the MiCC Enterprise web server.

- Depending on the Identity Provider type, it may be necessary to deselect the **Check signature** option for proper decoding of SAML assertions.

## ASSOCIATION OF MICC ENTERPRISE USERS TO THEIR EXTERNAL LOGIN

When MiCC Enterprise users authenticate via an external Identity Provider for the first time, they have to register by specifying their Logon ID. This one-time operation assigns the **External Login** property of these users so that they are immediately identified later on.

It is also possible to set the External Login of users from Configuration Manager or Web Manager, by editing their properties.

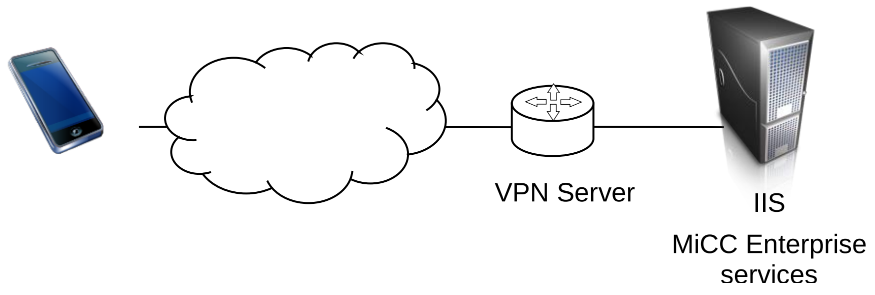
# INTERNET ACCESS

## ARCHITECTURES

Phone agents, supervisors and managers may use the mobile and web applications from outside the company's network (LAN). For this purpose, servers and network appliances can be organized in several ways.

### VPN

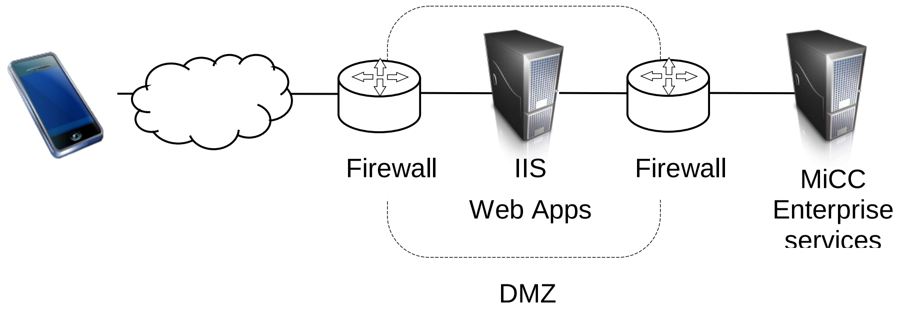
In a VPN-based configuration, mobile users establish a VPN connection to the LAN in which their device is thus temporarily included.



### MICC ENTERPRISE WEB APPS IN DMZ

Company servers accessible from the internet are generally grouped in a DMZ area isolated from the LAN.

By installing the MiCC Enterprise web services on a server in the DMZ, they can be reached from mobile devices.

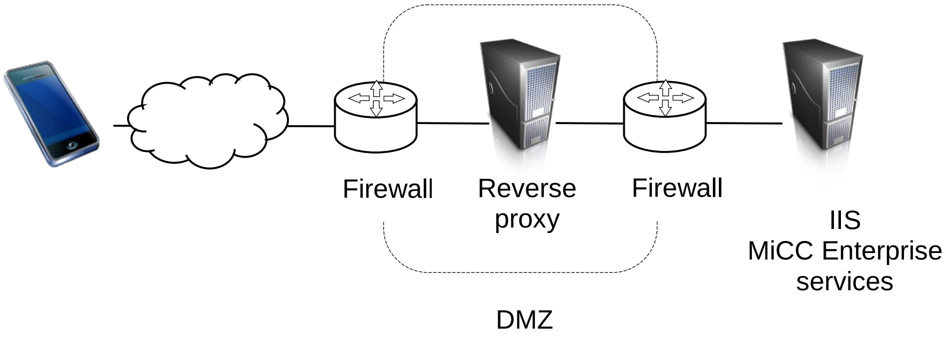


In this architecture however, multiple connections must be allowed between this server and the other MiCC Enterprise server(s) located in the LAN.

## REVERSE PROXY IN DMZ

It is possible to avoid making MiCC Enterprise web services directly accessible from the internet and to minimize the number of connections between the DMZ and MiCC Enterprise servers by using a **reverse proxy**.

Located in the DMZ, the reverse proxy acts as an intermediary component between client devices and MiCC Enterprise web services.  HTTP is the only protocol that needs to be allowed between the DMZ and the LAN.



In addition to forwarding client requests and returning server responses, the reverse proxy may also provide additional functionality.

- **URL rewriting**, allowing the web apps to be accessed from another URL than the default one.
- **SSL offloading**, forwarding HTTPS requests over HTTP to the MiCC Enterprise web services.
- **Caching** of static resources such as HTML, JavaScript and CSS files.

As an independent system, the reverse proxy is not limited to Microsoft Internet Information Server. Other software packages and operating systems can be chosen such as Nginx or Apache on Linux.

# IIS 7 SECURE CONNECTIONS

The MiCC Enterprise mobile applications use Basic HTTP authentication. Since this protocol does not encrypt user credentials, it is recommended to enhance security by enabling HTTPS on the internet-facing server (either the reverse proxy server or the IIS server hosting the MiCC Enterprise web services, depending on the chosen architecture).

## INTERNET SERVER CERTIFICATES

To be accepted by web browsers, HTTPS connections require an Internet server certificate to be installed on the web server. Such certificates are issued by a public certification authority (CA). To obtain an Internet server certificate, a request must be sent to the CA and then the Internet server certificate sent from the CA must be installed.

The following steps describe how to request a server certificate from IIS 7.

1. Open IIS Manager and navigate to the server level.
2. In Features View, double-click Server Certificates.
3. In the Actions pane, click Create Certificate Request.
4. On the Distinguished Name Properties page of the Request Certificate Wizard, fill in the requested information, and then click Next.
5. On the Cryptographic Service Provider Properties page, select either Microsoft RSA SChannel Cryptographic Provider or Microsoft DH SChannel Cryptographic Provider from the Cryptographic service provider drop-down list. By default, IIS 7 uses the Microsoft RSA SChannel Cryptographic Provider.
6. In the Bit length drop-down list, select a bit length that can be used by the provider. By default, the RSA SChannel provider uses a bit length of 1024. The DH SChannel provider uses a bit length of 512. A longer bit length is more secure, but it can affect performance. Click Next.
7. On the File Name page, type a file name in the Specify a file name for the certificate request text box, or click the browse button (…) to locate a file, and then click Finish.
8. Send the certificate request to a public CA.

Once the server certificate has been received from the CA, install it as follows.

1. Open IIS Manager and navigate to the server level.
2. In Features View, double-click Server Certificates.
3. In the Actions pane, click Complete Certificate Request.
4. On the Complete Certificate Request page, in the File name that contains the certification authority's response text box, type the path of the file that contains the response from the CA, or click the browse button (…) to search for the file.
5. Type a friendly name for the certificate in the Friendly name text box, and then click OK.

## SSL BINDING

Once an Internet server certificate has been installed, SSL can be enabled for encryption (and authentication of the web server’s identity).

1. Open IIS Manager and select the web site to configure.

2. Click **Bindings...** in the **Actions** pane.
3. Click **Add...** to add your new SSL binding to the site.
4. Select **https** in the **Type** drop-down list, and select the server certificate installed previously from the **SSL Certificate** drop-down list.
5. Click **OK**.

# IIS 7 REVERSE PROXY

If the IIS 7 web server is used as the reverse proxy in the architecture described in section 0, it must be configured as described below.

(Other reverse proxies can be used, as specified in section 0, but we do not document their configuration here.  Please refer to their documentation for help.)

## APPLICATION REQUEST ROUTING

To configure a reverse proxy in IIS 7, the Application Request Routing (ARR) extension must be installed first.

This extension can be downloaded from the Microsoft IIS.net web site.

## REVERSE PROXY

Once the ARR extension is installed, enable proxy support as follows.

1. Open IIS Manager and click the server node in the tree view.
2. Double click **Application Request Routing Cache**.
3. Select the **Server Proxy Settings…** task in the Actions panel.
4. Check the **Enable Proxy** option.

Then follow these steps to configure the reverse proxy.

5. Open IIS Manager and select the web site to configure.
6. From the **Actions** pane, click **Add Rule(s)…**
7. Double-click **Reverse Proxy** in the templates list.
8. In the **Outbound Rules** frame, leave the **Rewrite the domain names of the links in HTTP responses** option unchecked.
9. In the first text box of the **Inbound Rules** frame, enter the name or IP address of the LAN server hosting the MiCC Enterprise web services.
10. Leave the **Enable SSL Offloading** option checked, so that incoming HTTPS requests are forwarded over HTTP to the MiCC Enterprise web services.

At this point, the mobile and web applications can be reached at the following locations.

http://<Reverse Proxy Server>/webapps/agent

http://<Reverse Proxy Server>/webapps/contactcenter

If SSL has been enabled on the reverse proxy server, the applications are also accessible at the following addresses.

https://<Reverse Proxy Server>/webapps/agent

https://<Reverse Proxy Server>/webapps/contactcenter

The MiCC Enterprise web services may not be installed on the reverse proxy server.

More advanced URL rewriting rules can be setup using ARR, allowing for instance the mobile applications to be accessible from another location than the default “WebApps” folder.

Be aware that for outbound rewriting rules to work properly the corresponding inbound rule must clear the Accept-Encoding HTTP header so that responses are not compressed by the IIS hosting the MiCC Enterprise web services.  See the following article for more details.

Setting up a Reverse Proxy using IIS, URL Rewrite and ARR

Mitel®

Powering connections

mitel.com