A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise

Web Applications Configuration Guide

Release 9.8
Document Version 1.0

August 2025

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**

The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

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

INTRODUCTION

This document describes how to configure the following web applications in MiCC Enterprise:

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

This document describes how to access these applications from the internet, and includes common configuration procedures.

LICENSING

MOBILE AGENT

Each Mobile Agent user must have the following licenses (associated with Phone Agents):

- Number of Connected users
- Call control

Real-time information display requires the following site license:

- Real Time Interface

WEB MANAGER

Each Web Manager user must have a Web Manager license, which is a concurrent usage license.

The Web Manager application also requires the following site license:

- Real Time Interface

CONFIGURATION

REAL TIME INTERFACE

The RTI interface must be enabled and All (or at least relevant) Service Groups, Service Accesses and Agents need to be monitored.

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.

CALL DETAIL DATA

Some reports available in Web Manager, such as the Performance and Transfers reports on Agents, Service Groups and Agent Groups, show values that are computed from Call Detail Records (CDR). It is thus necessary to save the CDR in the database.

This must be enabled using Configuration Manager as follows.

1. Open the Contact Center (Tenant) Properties.
2. On the Report tab, check the Log Call Detail Data 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.

CALL MANAGER RESOURCES

On systems configured with Telephony Application Service (TAS), Web Manager can be used to configure Call Manager resources: BVDs, Languages and Play Messages. Audio files corresponding to Sound Media Objects can then be uploaded or generated using the Google Cloud Text-to-Speech API.

Note: A Play Message list cannot be configured for multiple languages. To support multiple languages, create a separate Play Message list for each language.

UPLOAD PATH FOR SOUND FILES

Management of Call Manager Resources is only enabled if the **UploadPathPrefix** is properly configured in the web.config file.

1. Create a directory (or a symbolic link to a network folder using the mklink /d command).

2. Grant Modify permission on this directory or link to IIS_IUSRS.

3. In web.config set the **UploadPathPrefix** value to the path of this folder or link. Example:

```
<add key="UploadPathPrefix" value="C:\Tools\MediaServerPrompts" />
```

4. Create subfolders in this directory, named after the **Prompt path** of each **Language** defined in any Call Manager.

Note: on multi-tenanted or multi-TAS systems the same upload path prefix is used for all Tenants and Call Managers.

TEXT-TO-SPEECH

The generation of Sound Media Object audio files using Text-to-Speech requires setting up a Google Cloud Platform project.

1. Open the Google Cloud Text-to-Speech documentation and follow the instructions under Quick Start > Using the command line > Before you begin.

2. Save the downloaded service account key file on the MiCC Enterprise web server and grant Read permission on this file to IIS_IUSRS.

3. In web.config, set the **GCPServiceAccountFilePath** value to the path of this key file. Example:

```xml
<add key="GCPServiceAccountFilePath" value="C:\Tools\Google\mitel-srv-accnt-590212a47e8e.json" />
```

4. Set the Text-to-Speech synthesis parameters to the desired values in web.config. Example:

```xml
<!-- Text to Speech voice gender: Male | Female | Neutral -->
<add key="SsmlVoiceGender" value="Female" />
<!-- Text to Speech voice name.  If not set, the service will choose a voice.
See https://cloud.google.com/text-to-speech/docs/voices -->
<add key="VoiceName" value="sv-SE-Wavenet-A" />
<!-- Speaking rate/speed, in the range [0.25, 4.0] -->
<add key="SpeakingRate" value="0.5"/>
<!-- Speaking pitch, in the range [-20.0, 20.0] -->
<add key="Pitch" value="-5.0"/>
<!-- Volume gain (in dB), in the range [-96.0, 16.0]. -->
<add key="VolumeGainDb" value="8.0"/>
```

5. Download and install the FFmpeg audio/video conversion tool on the MiCC Enterprise server.

6. Grant Execute permission on ffmpeg.exe to IIS_IUSRS.

7. In web.config, set the FFmpegExePath value to the path of ffmpeg.exe. Example:

```xml
<add key="FFmpegExePath" value="C:\Tools\ffmpeg-4.2.1-win64-static\bin\ffmpeg.exe"/>
```

WHITE LABELLING AND CUSTOMIZATION

MOBILE AGENT

The Mobile Agent application can be displayed in the following modes.

- **Default**: supervision of Service Groups + agent status in drop-down menu.
- **Left** and **Right Sidebar**: supervision of Service Groups + agent status in sidebar.
- **Mini**: agent status only.

White labeling settings control the displayed product name, application name and login label.

Custom styling can also be applied on some user interface elements.

All these settings can be set in the web.config file.

```xml
<!-- Application display mode (applies to Mobile Agent only).
Supported values (case sensitive): Default, LeftSideBar, RightSideBar, Mini.
Empty value is equivalent to Default. -->
<add key="DisplayMode" value="Default" />

<!-- Product name (applies to Mobile Agent only).
Empty value is replaced by localized ProductName entry in Agent.*.resx. -->
<add key="ProductName" value="" />

<!-- Product name (applies to Mobile Agent only).
Empty value is replaced by localized ApplicationName entry in Agent.*.resx. -->
<add key="AgentApplicationName" value="" />

<!-- Product name (applies to Mobile Agent only).
Empty value is replaced by localized LogInUsingMiccEnterprise entry in
Supervisor.*.resx. -->
<add key="AgentLoginLabel" value="" />

<!-- CSS color for Mobile Agent application background. -->
<add key="AgentAppBackgroundColor" value="" />

<!-- CSS color for Mobile Agent application foreround. -->
<add key="AgentAppForegroundColor" value="" />

<!-- CSS color for Mobile Agent title bar background. -->
    <add key="AgentTitleBarBackgroundColor" value="" />

<!-- CSS color for Mobile Agent title bar foreground. -->
<add key="AgentTitleBarForegroundColor" value="" />

<!-- Additional CSS rules for Mobile Agent application. -->
<add key="AgentCustomCSS" value="" />
```

These settings can be overridden by registry values, which persist across upgrades.

Values are obtained from the following sources if they exist (named after the web.config keys), in the following order:

1. Tenant-specific registry values under HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mitel\SeC\Common\Parameters\Services\WebApps\Tenants\<Tenant Name>

2. Global registry values under HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mitel\SeC\Common\Parameters\Services\WebApps

3. Web.config appSettings values

WEB MANAGER

Each tenant can use a custom logo in the Web Manager application.

Web Manager can obtain the tenant logo file from the **\MiCC Enterprise\Services\SeCLogo** folder. If no tenant logo file is available, Web Manager uses the default Mitel logo (located at **MiCC Enterprise\Services\Web\WebApps\Areas\ContactCenter\Img**).

DATA SOURCE DRIVERS

Some data sources used in Web Manager to configure Wall Display panels depend on a specific driver to transfer data between Microsoft Office System files and non-Microsoft Office applications. This is required for panels that are configured with a Microsoft Excel (.XLSX) ODBC or OLE DB connection string.

This driver is available from the following location.

https://www.microsoft.com/en-us/download/details.aspx?id=13255

Download the **32-bit version** ("AccessDatabaseEngine.exe" file) and follow the installation instructions.

MOBILE AGENT CALL MANAGER SELECTION

On systems configured with Telephony Application Service (TAS), Mobile Agent by default uses load balancing to select the least used call manager for connection. To override this and allow the agent to select the call manager from the list of configured call managers, modify Web.config and set the **ShowCallManagers** value to "true".

Example:

```
<add key="ShowCallManagers" value="true" />
```

Note: This setting only applies if there are multiple call managers in the MiCC-E system. For multi-site systems, this setting should always be set to "true".

AUTOMATIC LOGOUT FROM WEB MANAGER

To automatically log the user off from Web Manager after a period of inactivity, modify the in Web.config file or Windows registry and set the **AutoLogoutTimeoutSeconds** value to the duration in seconds after which the session should be closed.

When this value is set to 0, automatic logout is disabled.

Example (1800 seconds = 30 minutes):

```
<add key="AutoLogoutTimeoutSeconds" value="1800"/>
```

EXTERNAL AUTHENTICATION USING SAML 2.0

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.

- In order for Web Manager to let users authenticate with SSO, an internet connection is required.

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 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 14 (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.

1. Open the **MiCC Enterprise Setup** Utility.

2. Select Web Server Location in the left list.

3. 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 URL used to access the web applications becomes:

http//<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).

4. **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:

   http://<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).

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

   http://<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:

   http://<Fully-Qualified-Server-Name>/webapps/AuthServices

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

CONFIGURATION OF A MICC ENTERPRISE TENANT

In Configuration Manager, the Tenant authentication uses OpenID Connect for single sign-on. In addition, Web manager has the ability to override these parameters and enable SAML 2.0 for Single Sign-on.

To configure the association between a Tenant and an external Identity Provider, the below values must be set in the web.config file.

```
<!—Used to enable SAML 2.0 Authentication. If set to true, Web Manager will use
the SAML Authentication by overriding any OpenID configuration made for that
tenant on CM-->
<add key="EnableSAML" value="True" />

<!-- Set the SamlIDPEntityID field to the unique identifier of the Identity
Provider. This SamlIDPEntityID may have been assigned during (or after)
configuration of the Identity Provider.  It can be found in its metadata document-
-->
```

```
<add key="SamlIDPEntityID" value="" />

<!-- Set the Name field to any value of your choice.  This name will appear on the
user's login page in the mobile and web applications. -->
<add key="SamlIDPName" value="" />

<!-- Set the SamlIDPMetadataLocation 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. -->
<add key="SamlIDPMetadataLocation" value="" />

<!-- Depending on the Identity Provider type, it may be necessary to set
SamlSignatureCheck value to false, to disable Check Signature option for proper
decoding of SAML assertions. -->
<add key="SamlSignatureCheck" value="false" />

<!-- Above SAML keys can be configured to be tenant specific by appending tenantID
to the key. Example:<add key="SamlIDPEntityID:1" value="" />; where 1 is the
tenantID-->
```

These settings can be overridden by registry values, which persist across upgrades.

Values are obtained from the following sources if they exist (named after the web.config keys), in the following order:

1. Tenant-specific registry values under
   HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mitel\SeC\Common\Parameter s\Services\WebApps\Tenants\<Tenant Name>

2. Global registry values under
   HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mitel\SeC\Common\Parameter s\Services\WebApps

3. Web.config appSettings values:

   - On a tenanted installation, the above-mentioned keys can be configured to be tenant specific by appending tenantID to each key separated by a colon symbol (no empty spaces).

   - Example:<add key="SamlIDPEntityID:1" value="" />; where 1 is the tenantID

   - if there is no TenantID specified with the key, those values would be considered common configuration items and would apply to all tenants.
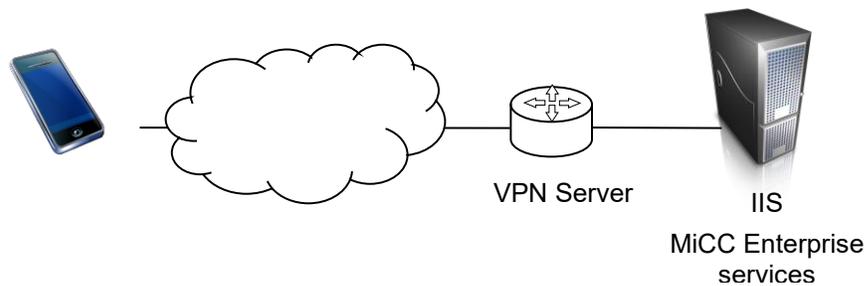
INTERNET ACCESS

ARCHITECTURES

Phone agents, supervisors and managers may use the 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.

VPN Server

IIS

MiCC Enterprise services

MICC ENTERPRISE WEB APPICATIONS 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.

Firewall

IIS
Web Apps

Firewall

MiCC
Enterprise
services

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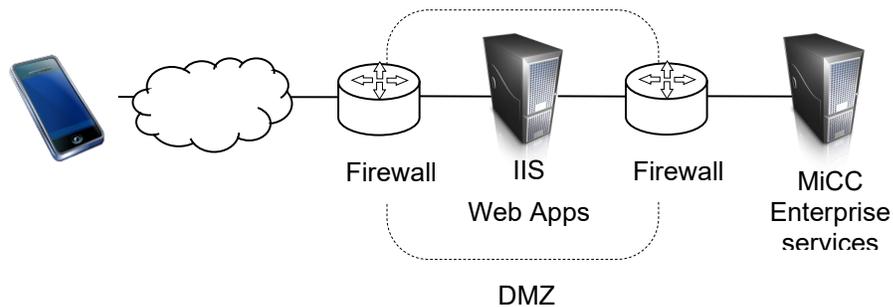
In this architecture however, multiple connections must be allowed between this server and the other MiCC Enterprise server(s) located in the LAN.

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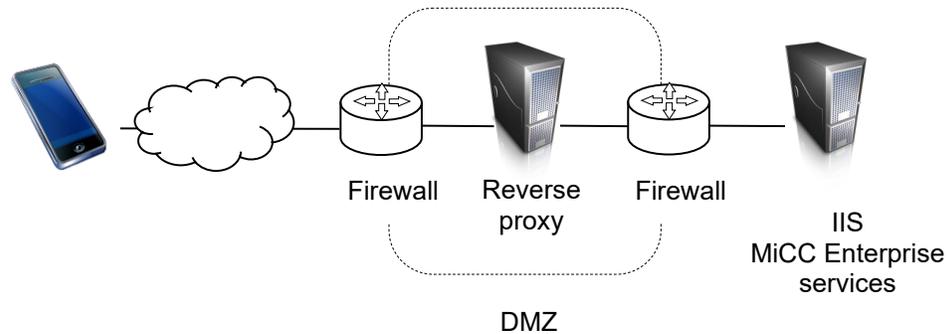
In addition to forwarding client requests and returning server responses, the reverse proxy may also provide additional functionality.

- **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 web 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 Setting up a Reverse Proxy using IIS, URL Rewrite and ARR for more details.

PROGRESSIVE WEB APP ADAPTATION

The Mobile Agent application can be used as a Progressive Web App (PWA), making it close to a native app on mobile devices.

INSTALLATION

When the Mobile Agent app is loaded in the main web browser on the mobile device, it can be installed (sent to the Home screen) as follows:

Chrome browser on Android devices: on the right of the address bar, tap More ⋮ > Add to home screen > Install.

Safari browser on iOS devices: press the Share ⬆ button; select Add to Home Screen; confirm by pressing Add.

As a result, a shortcut will be available to launch full-screen, as a native application.