Mitel Technical Configuration Notes – KB000128073

June 22, 2026

MiVB - Configure MiVoice Business 10.5 SP1 with MCX for use with IDgo

Description: This document provides a reference for Mitel Authorized Solutions Providers for configuring MiVoice Business 10.5 SP1 (10.5.1.17) and MCX with IDgo

Environment: MiVoice Business 10.5 SP1 (10.5.1.17), MCX (2.1.0.0), IDgo Cloud Service (SaaS)

NOTICE

TRADEMARKS

Mitel Technical Configuration Notes – Configure MiVoice Business 10.5 SP1 (10.5.1.17) for use with IDgo

June 2026 – KB000128073

Table of Contents

Overview

This document provides a reference for Mitel Authorized Solutions Providers for configuring the MiVoice Business 10.5 SP1 (10.5.1.17) with MCX to Integrate the IDgo Cloud Service. This document covers a basic IDgo Integration.

Interop History

Version	Date	Reason
1	June, 2026	Interop with MiVB 10.5 SP1 (10.5.1.17) with MCX for use with IDgo

Interop Status

The Interop of IDgo has been given a Certification status. This device will be included in the SIP CoE Reference Guide. The status of IDgo achieved is:

	The most common certification which means the IDgo device has been tested and/or validated by the Mitel SIP CoE team. Product support will provide all necessary support related to the interop, but issues unique or specific to the 3rd party will be referred to as the 3rd party as appropriate.

Software & Hardware Setup

The test setup established basic integration between IDgo and MiVB with MCX.

The most common certification which means the IDgo device has been tested and/or validated by the Mitel SIP CoE team. Product support will provide all necessary support related to the interop, but issues unique or specific to the 3rd party will be referred to as the 3rd party as appropriate.

Manufacturer	Tested Variant	Software Version	Additional Applicable Variants
Mitel	MiVoice Business	10.5 SP1 (10.5.1.17)	NA
Mitel	MCX	2.1.0.0	NA
IDgo	IDgo	IDgo Cloud Service (SaaS)	NA

Tested Features

Listed below is an overview of the features tested during the Interop test cycle and not a detailed view of the test cases.

Feature	Feature Description	Issues
Successful IDgo Authentication	Verify end-to-end IDgo authentication and Ignite screen pop	☑
Caller Without IDgo Account	Verify graceful fallback for unregistered callers	☑
Customer Exists but Mobile Unregistered	Verify onboarding flow	☑
Authentication Timeout	Verify timeout handling	☑
Authentication Rejection	Verify user rejection handling	☑
IDgo Service Unavailable	Verify fallback to manual verification	☑

☑ - No issues found X - Issues found, cannot recommend to use ⚠ - Issues found **NA** - Feature Not Supported

Device Limitations

This is a list of problems or not supported features when the IDgo is connected to MiVoice Business and MCX.

Feature	Problem Description
Authentication Timeout/Rejection	No Timeout/Rejected Message **Recommendation:** Please contact IDgo support for more details.

Network Topology

This diagram shows how the testing network is configured for reference.

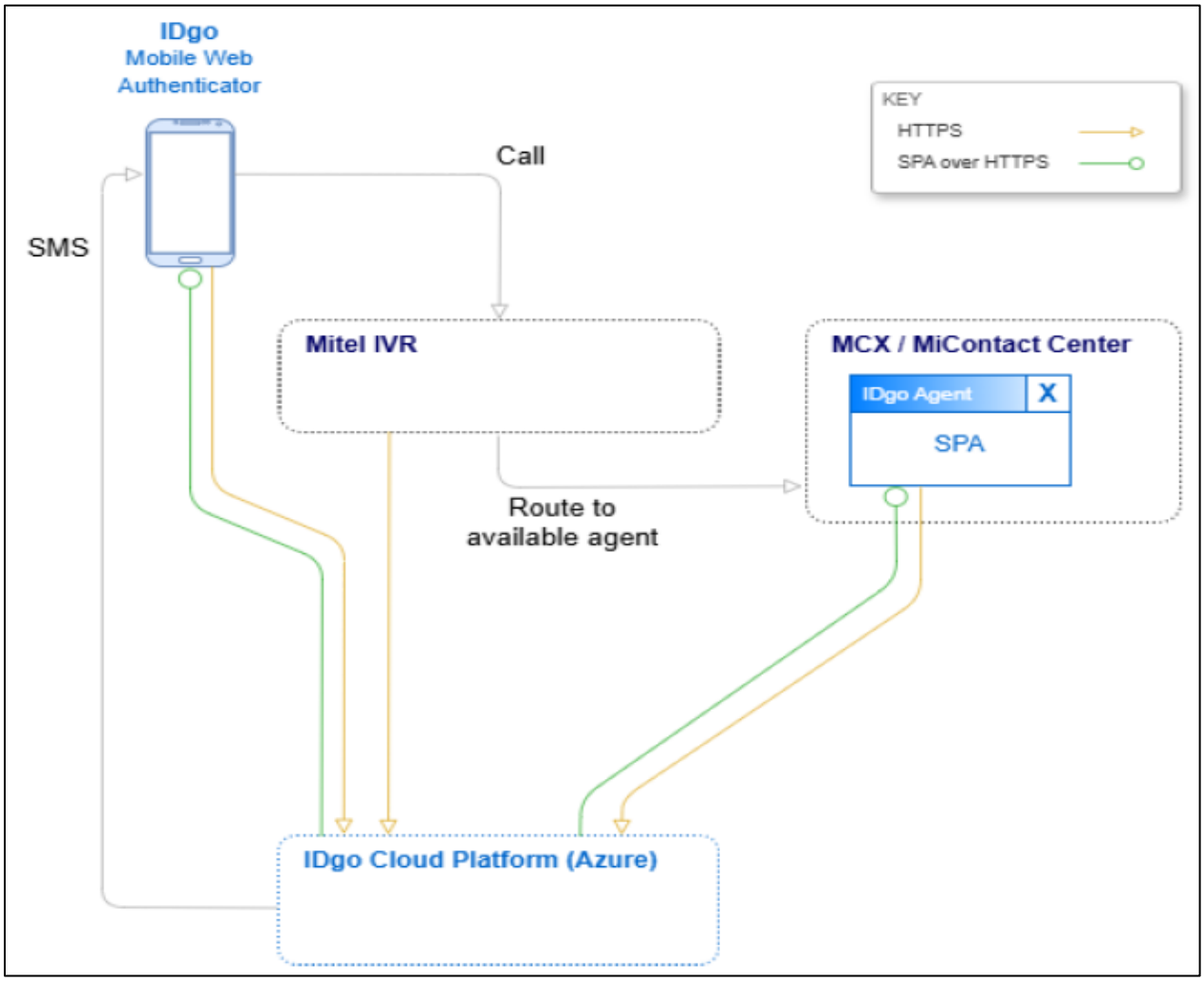

Figure 1 – Network Topology

MiVoice Business - Configuration Notes

The following steps show how to program a MiVoice Business/MCX to connect with the IDgo

Network Requirements

- There must be adequate bandwidth to support the voice over IP. As a guide, the Ethernet bandwidth is approx 85 Kb/s per G.711 voice session and 29 Kb/s per G.729 voice session (assumes 20ms packetization). As an example, for 20 simultaneous SIP sessions, the Ethernet bandwidth consumption will be approx 1.7 Mb/s for G.711 and 0.6Mb/s. Almost all Enterprise LAN networks can support this level of traffic without any special engineering. Please refer to the MiVoice Business Engineering guidelines for further information.
- For high quality voice, the network connectivity must support a voice-quality grade of service (packet loss <1%, jitter < 30ms, one-way delay < 80ms).

Assumptions for the MiVoice Business Programming

- The SIP signalling connection uses UDP on Port 5060.

Software License – Licensing

Ensure that the MiVoice Business is equipped with enough licenses for the connection.

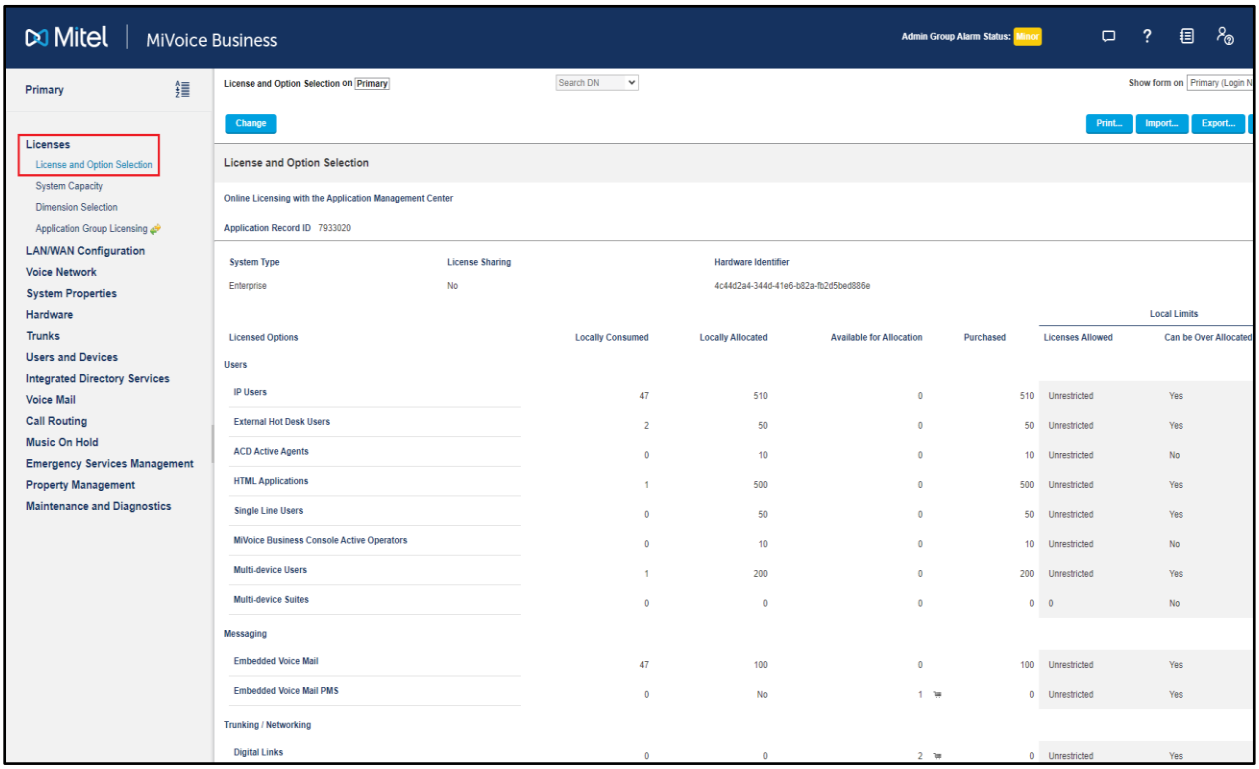

Figure 2 – Software License

Note: Enable ACD and SMDR Options required for MCX integration

DID Mapping to Hunt Group

Create a Hunt Group in either MIVB or MCX and assign a DID number to the Hunt Group. Configure the Hunt Group to route incoming calls to the IVR flow created in MCX.

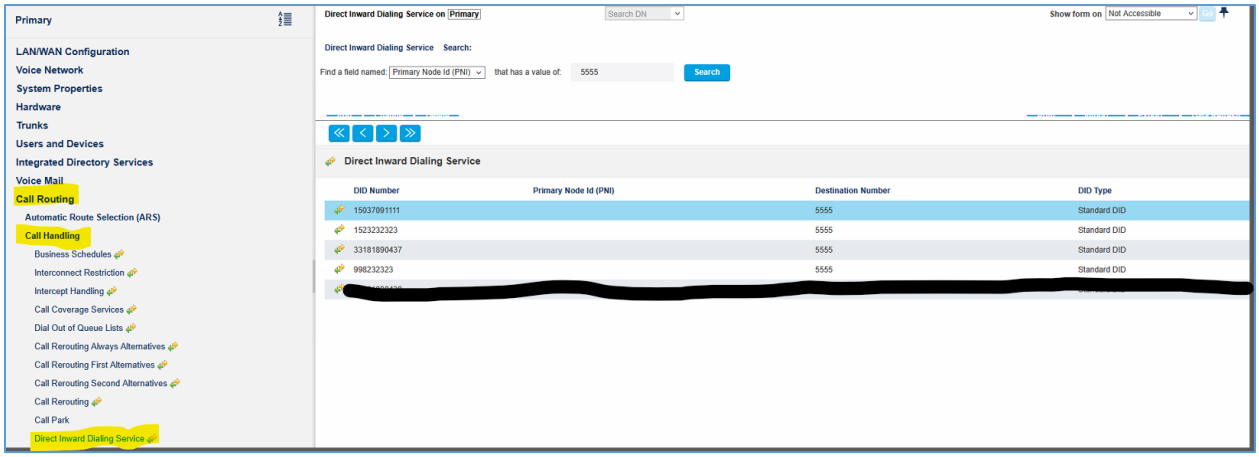

Figure 3 – DID Mapping

MCX Configuration Notes

This document doesn't intend to provide detailed instructions on installing, configuring, and Integrating MCX

All relevant Agent Queues are already configured properly in MCX to receive Voice Calls. Workflows are required to integrate IDgo with MCX. COS need to be properly configured.

In our lab environment, the following setup was used for validation and testing:

Voice Media Server

- Media Server Name: MIVB95
- Type: ICP3300 with MiTAI
- Site: Default Site
- IP Address: 192.168.10.95
- Telephone System Version: 21.5.1.17

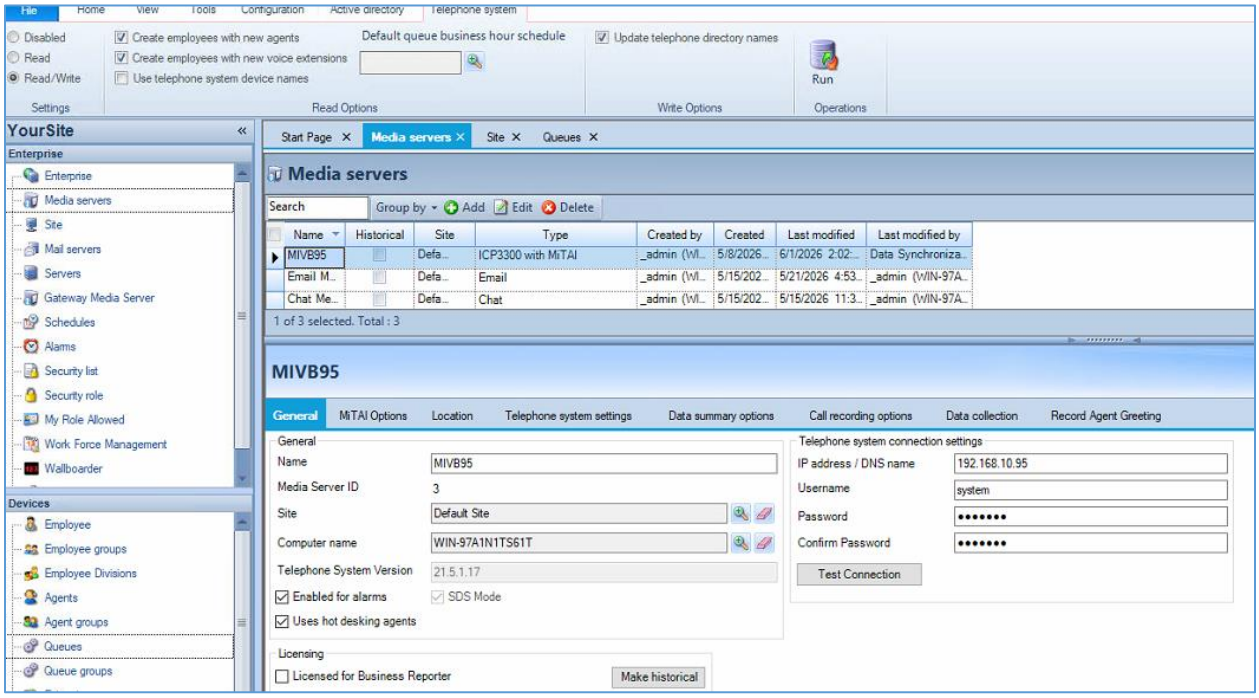

Figure 4 – Media Server

Employee

Employees are assigned to the appropriate queues and media types

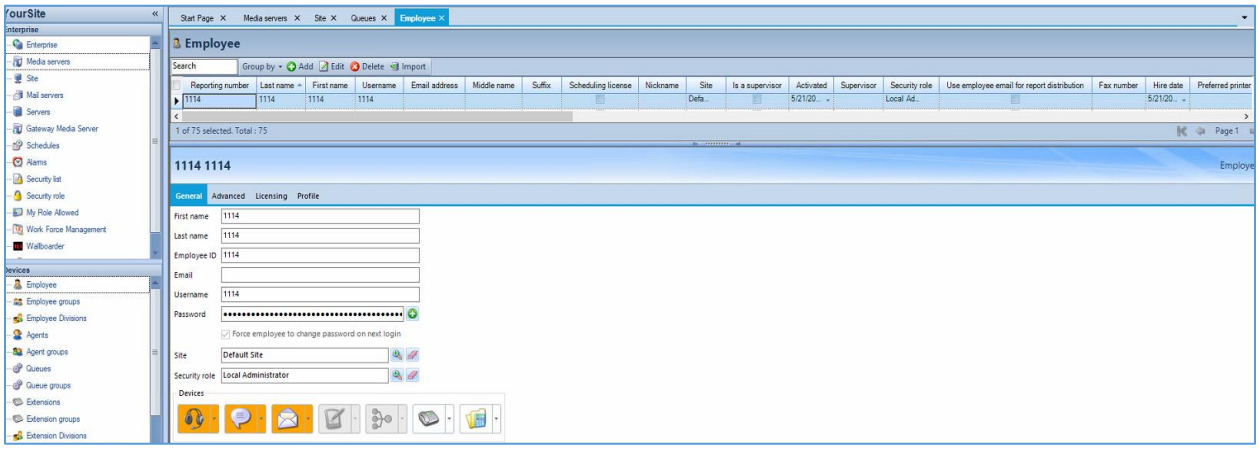

Figure 5 – Agent

Agent Group

Employees are assigned to the required Agent Groups. Agent Groups are configured as members of the corresponding Voice, Email, and Chat queues.

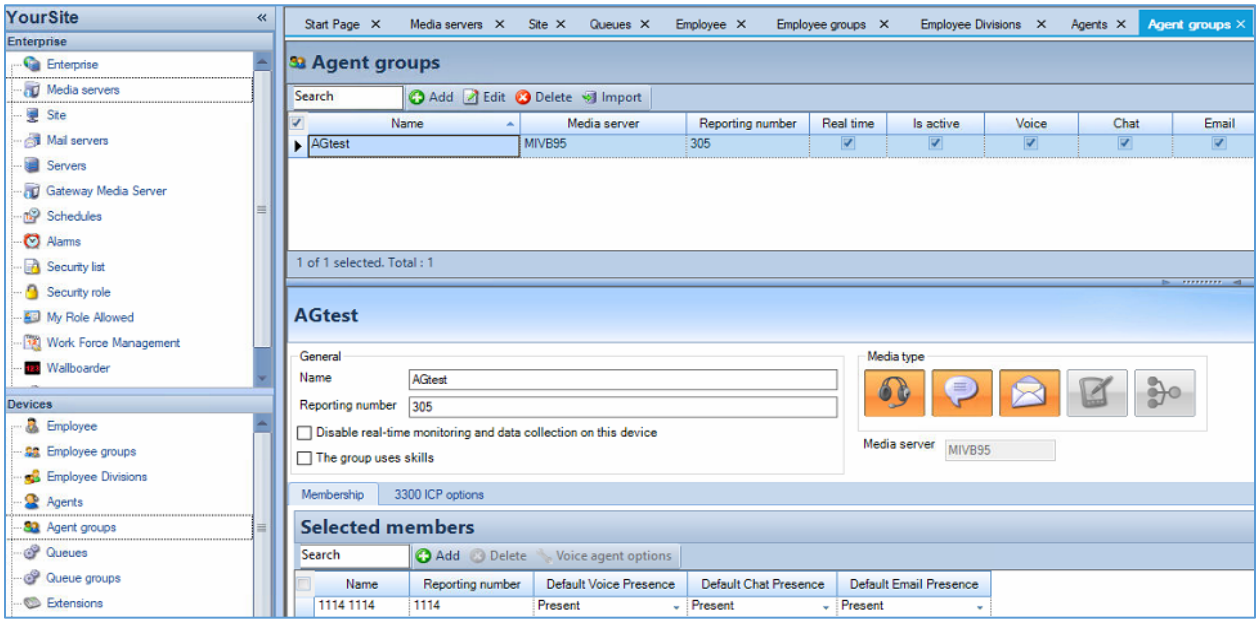

Figure 6 – Agent Group

Queues

Queues are configured to handle

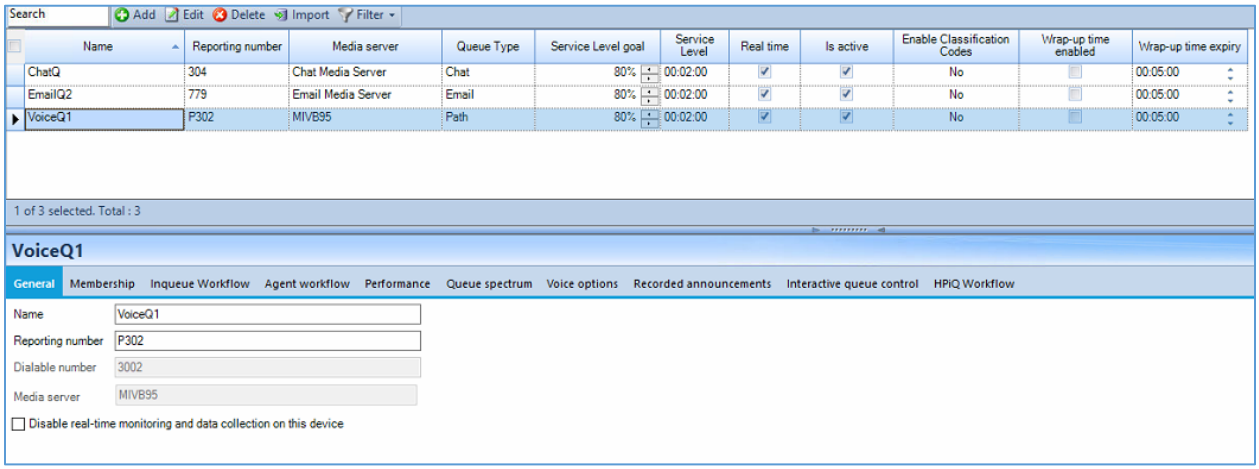

Figure 7 – Voice Queues

Hunt Groups

IVR Routing calls are answered by Voice Hunt group in the workflows

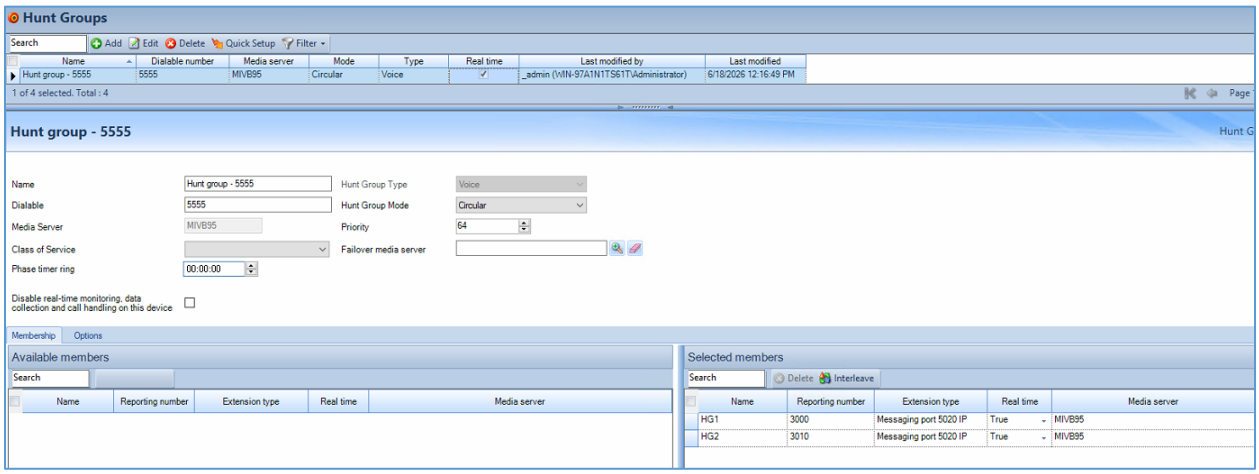

Figure 8 – Voice Queues

IVR Routing – Workflows

This section provides a detailed, step-by-step explanation of the validated IDgo_IVR workflow, and the specific Mitel configuration screenshots from the lab environment.

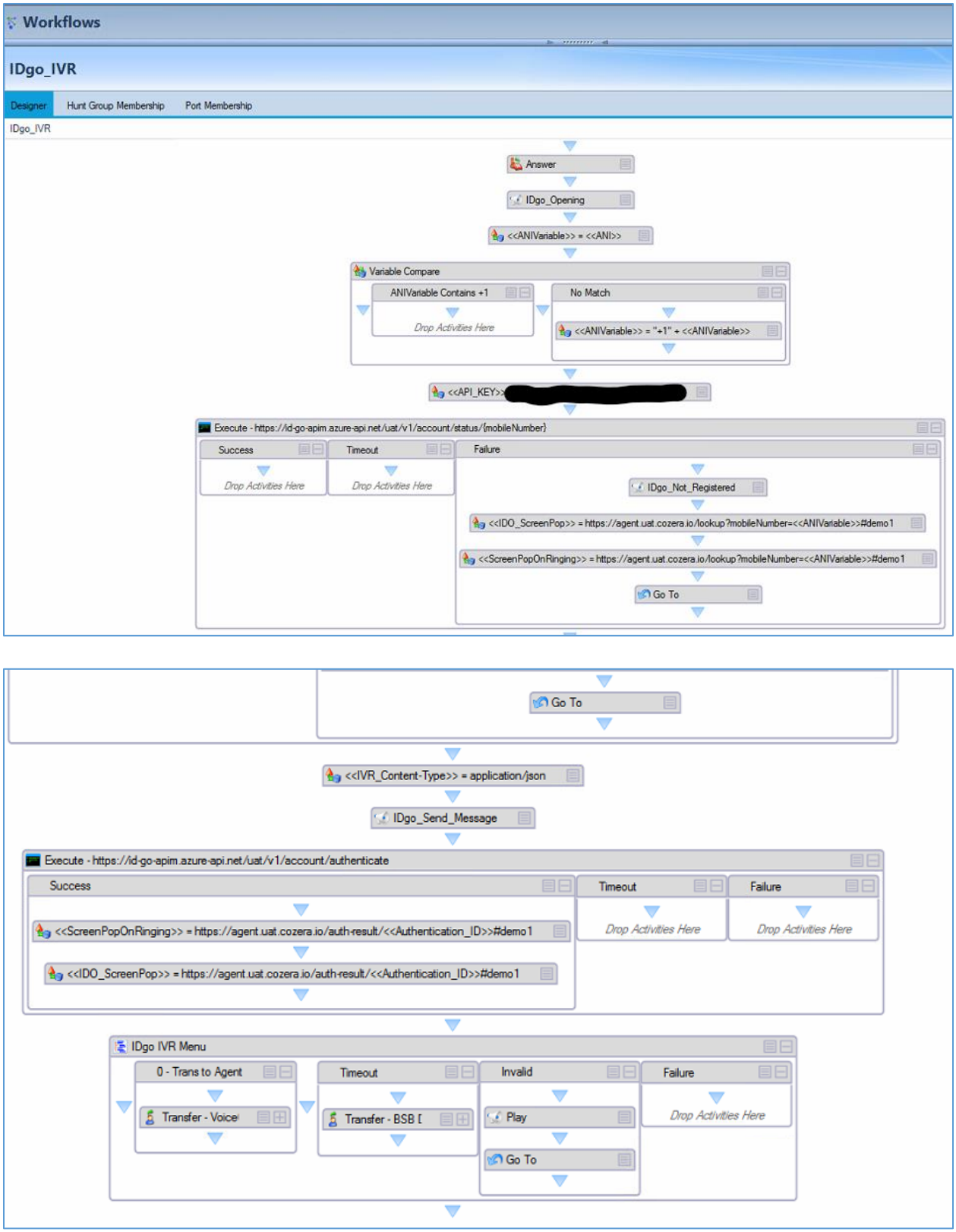

Figure 9 – Workflows

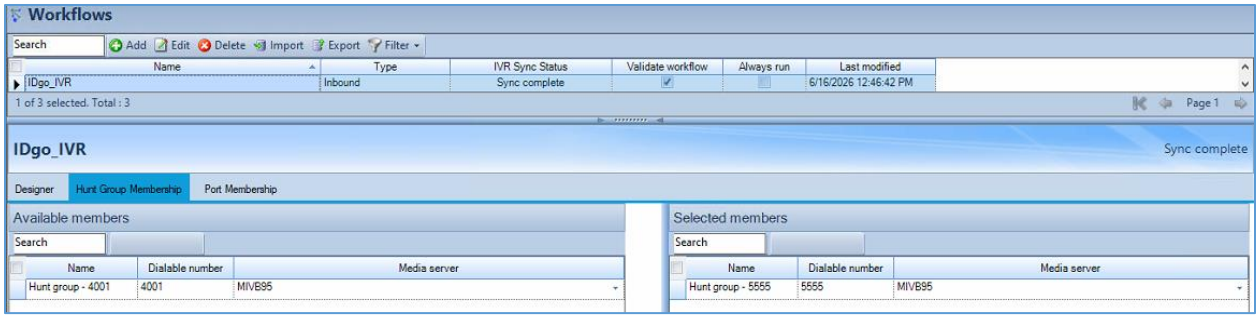

Figure 10 – Workflows Hunt Group Membership

Variables

Create the following IVR variables (IVR Routing > Variables). Only the most critical ones (bold in lab) need 'Send to agent desktop' enabled for screen pop / toaster context:

Variable Name	Type	Purpose / Notes	Send to Desktop?
ANIVariable	Custom	Stores the caller phone number (ANI) throughout the flow	Yes
API_KEY	Custom	Stores the IDgo x-api-key for reuse in REST headers	
canAuthenticate	Custom	Output from enrollment status REST; indicates if caller can proceed with auth	
enrollmentComplete	Custom	Output from enrollment status REST; true if caller is already enrolled with IDgo	
Authentication_ID	Custom	Stores the 'id' returned from /authenticate POST; used in auth-result screen pop URL	
IDO_ScreenPop	Custom	Holds the full IDgo lookup or auth-result URL for non-enrolled / enrolled paths	Yes

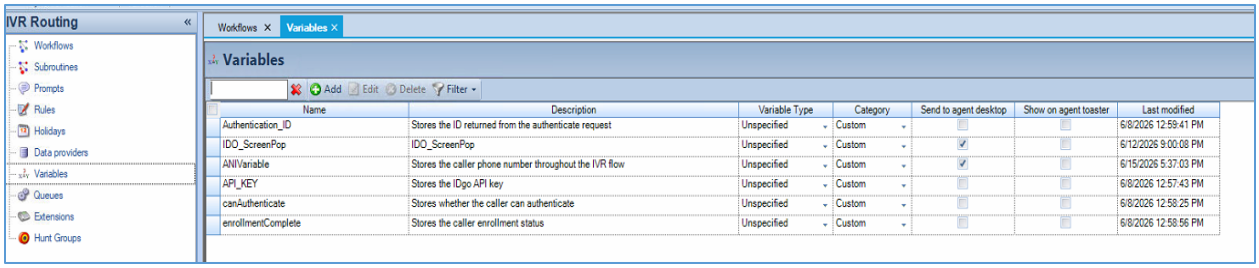

Figure 11 – Variables

Assumptions:

- MiVB IVR / Auto Attendant is operational and can invoke the IDgo_IVR workflow on inbound calls.
- Active IDgo API key (x-api-key) obtained during client onboarding.
- IDgo agent portal subdomain configured for the tenant (used in #demo1).
  Note: demo1 should be update to your subdomain
- Variables named exactly as shown (or adjusted to your Mitel naming standards); bold/important ones are sent to agent desktop.

1. ANI Formatting (E.164 Compliance)

Many mobile APIs (including IDgo) expect numbers in strict international format, if not required this tab can be removed for E.164. The lab workflow includes a Variable Compare activity:

- Compare ANIVariable 'Contains' '+1' (adjust country code as needed, e.g. '+91' for India)
- If Match (already formatted): Drop / continue
- If No Match: Set ANIVariable = '+1' + <<ANIVariable>> (or your country code)

This ensures the mobileNumber parameter sent to IDgo is always correctly formatted.

2. Check Caller Enrollment Status (REST GET)

After ANI formating and API_KEY assignment, execute a REST webhook to determine enrollment:

Setting	Value
Method	GET
Type	REST
Endpoint(s)	**UAT**: https://id-go-apim.azure-api.net/uat/v1/account/status/{mobileNumber} **Production**: https://id-go-apim.azure-api.net/v1/account/status/{mobileNumber}
Header: x-api-key	<<API_KEY>>
Input Param: mobileNumber	<<ANIVariable>>

Output Mappings (from response JSON):

- canAuthenticate → canAuthenticate variable
- enrollmentComplete → enrollmentComplete variable

Documentation: https://id-go-apim.developer.azure-api.net/api-details#api=id-go-api&operation=get-v1-account-status

On Success: Proceed to branch logic (enrolled vs non-enrolled). On Timeout/Failure: Treat as non-enrolled path (play message + screen pop).

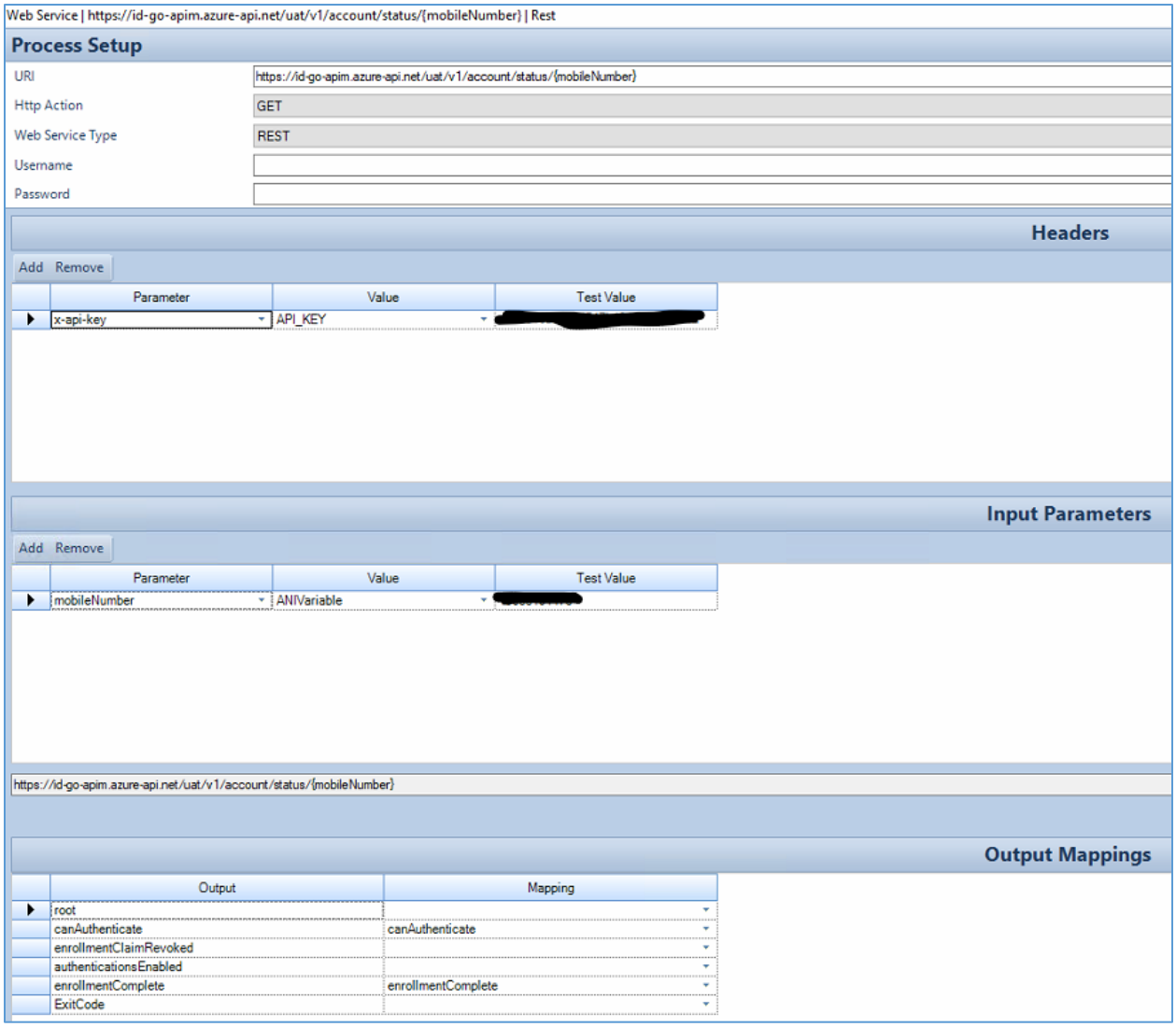

Figure 12 – Account Status Validate Process

3. Non-Enrolled / Failure Path Handling

If the caller is not enrolled (or the status call fails), the workflow:

1. Plays an announcement: e.g., 'You are not currently registered with our verification service.'

2. Sets the screen pop URL variable(s) to the lookup endpoint with the caller's mobile number: https://agent.uat.cozera.io/lookup?mobileNumber=<<ANIVariable>>#demo1 (replace demo1 with your tenant subdomain)

3. Triggers the agent desktop (Ignite) to open the lookup page or show a toaster, allowing the agent to assist with enrollment or handle the call manually.

4. Continues to standard IVR routing, menu, or transfers back to queue (Transfer-Voice or Transfer-BSB).

Note: In the lab implementation, the 'Failure' output branch of the REST activity is reused for the non-enrolled scenario. For production clarity, consider adding an explicit decision step on enrollmentComplete == false.

4. Enrolled Caller – Send Authentication Request (REST POST)

If enrollmentComplete is true (or canAuthenticate allows), the workflow proceeds to initiate

- Play prompt: 'Your number has been recognized. An SMS verification message is being sent to your mobile.'
- Execute REST POST to authentication endpoint

Setting	Value
Method	POST
Type	REST
Endpoint(s)	**UAT**: https://id-go-apim.azure-api.net/uat/v1/account/authenticate **Production**: https://id-go-apim.azure-api.net/v1/account/authenticate
Header: x-api-key	<<API_KEY>>
Header: Content-Type	application/json (or <<Content_Type>> variable)
Input Param: mobileNumber	<<ANIVariable>>
Input Param: channel	Ivr
Input Param: pollForResponse	True
Input Param: timeoutSec	55

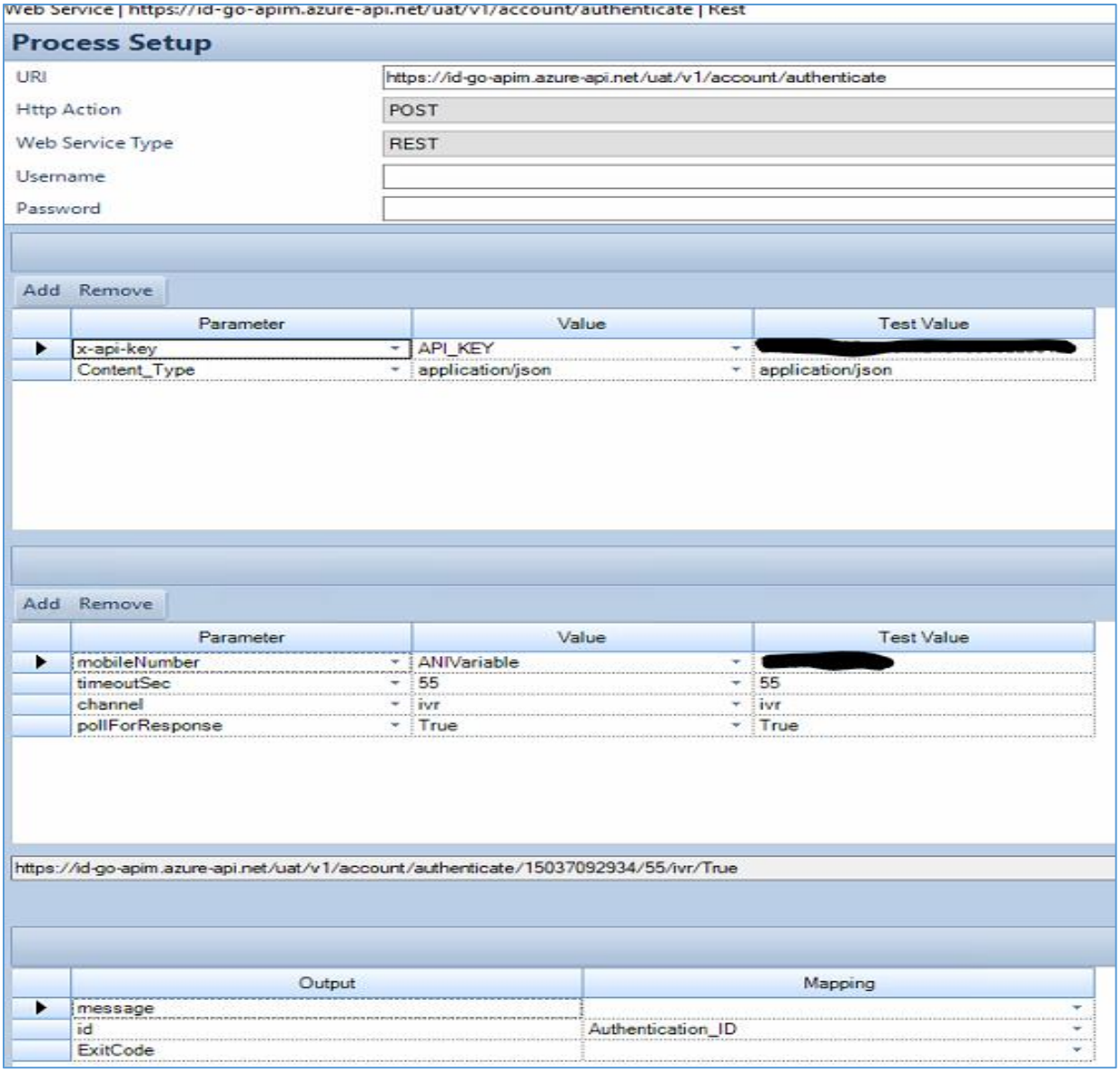

Figure 13 – Account Authentication

Output Mapping: id → Authentication_ID variable

The pollForResponse=true parameter makes the IVR wait (up to timeoutSec) for the authentication result / SMS interaction to complete before continuing.

Documentation: https://id-go-apim.developer.azure-api.net/api-details#api=id-go-api&operation=post-v1-account-authenticate

5. Present Authentication Results to Agent (Screen Pop)

After successful authentication request:

- Set screen pop variable(s) to the auth-result URL including the returned ID: https://agent.uat.cozera.io/auth-result/<<Authentication_ID>>#demo1
  Note: **demo1** should be update to your subdomain
- This opens the IDgo auth-result page (or Ignite URL tab) showing the caller's verification status, allowing the agent to see whether authentication succeeded.

Two common options in Mitel environments:

- Screen Pop On Ringing – Opens browser tab/window on call presentation to agent
- URL Tab Assignment in Ignite – Displays inside the Mitel agent desktop tab

6. IDgo IVR Menu & Transfer Options (Post-Auth)

After the authentication flow (or in parallel for non-enrolled), present a menu to the caller:

Option / Branch	Action / Activity	Notes
0 - Trans to Agent	Transfer – Voice	Transfers to configured voice queue / agent group in MCX. Agent already has screen pop context.
Timeout	Transfer – BSB	Transfers to BSB destination (configure as needed; may be a specific hunt group or service).
Invalid	Play prompt + Go To menu	Error message, then return to menu for retry.
Failure	Drop / error handling	Log and end call or route to fallback queue.

This menu gives the caller control while the agent is already informed via screen pop.

Workflow Summary Flow (End-to-End)

1. Caller dials → Answer + Play opening prompt
2. Capture & format ANI to +E.164
3. Set API_KEY and Content-Type

4. REST GET enrollment status → map canAuthenticate / enrollmentComplete
5. If not enrolled / Failure branch: Play message → Set lookup screen pop URL → Transfer or continue routing
6. If enrolled: Play recognition + SMS announcement → REST POST authenticate (poll) → Map Authentication_ID
7. Set auth-result screen pop URL with Authentication_ID
8. Present IVR Menu → Caller chooses transfer (0) or other options; agent already has full context via screen pop

All key variables are passed to the agent desktop for a seamless agent experience.

IDgo Configuration Notes

Contact IDgo Support for any guidance on Configuration of Accounts/Admin and Agent Portals

Glossary

MiVoice Business	MiVB
Mitel Customer Experience	MCX
MiNET Interface	MiNET
Mitel Technology Network	MTN
Class of Service	COS