



Enterprise Voice Operations & Analytics (EVOA)

Installation Guide

Version 1.10.0

July 2026

Publisher: **MeeraApps Technology**

Classification: **Customer Deliverable**

Copyright and Legal

Copyright © 2026 MeeraApps Technology. All rights reserved.

Enterprise Voice Operations & Analytics (EVOA) and the MeeraApps logo are trademarks of MeeraApps Technology. All other trademarks, service marks, and trade names referenced in this document are the property of their respective owners.

This document is provided "as is" without warranty of any kind. The publisher reserves the right to update the contents of this document without notice. Product features, screenshots, and command examples in this document reflect the release version noted on the cover; subsequent releases may differ.

Neither this document, in whole or in part, nor any of the information it contains may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, without prior written permission of the publisher.

Feedback on this document is welcome: support@meerapps.com.

Document Control

Revision History

Version	Date	Author	Summary of Changes
1.10.0	July 2026	MeeraApps Documentation	Desktop Notifier, Email channel for Emergency Alerts, SignalR reconnect hardening
1.9.0	July 2026	MeeraApps Documentation	SNMP Trap Receiver, Emergency Alerts, ACD Agent Status phone screen
1.8.0	June 2026	MeeraApps Documentation	Phone Display (Mitel 6900) provisioning, licensing, help content
1.5.0	June 2026	MeeraApps Documentation	Queue drill-down, trial license unlock
1.4.0	May 2026	MeeraApps Documentation	Real-Time Wallboards, ACD Supervisor role, backup/restore hardening

Table of Contents

Right-click the TOC below in Word and pick "Update Field" > "Update entire table" to refresh page numbers after any edit.

Copyright and Legal	2
Document Control	3
Revision History	3
Table of Contents	4
About This Guide	7
Purpose	7
Intended Audience	7
Prerequisites for Reading	7
Document Conventions	7
Related Documents	7
System Overview	8
What EVOA Does	8
Component Architecture	8
On-Disk Layout	8
What's New	9
Version 1.10.0 (July 2026)	9
EVOA Desktop Notifier	9
Desktop Channel on Real-Time Alert Rules	9
Push to Desktop Toggle on Caller Tags	9
Desktop Stations Tab	9
Notifier Auto-Update Endpoint	9
Emergency Alert Popup and History Visual Upgrade	9
Email Channel for Emergency Alerts	9
SignalR Reconnect Hardened in the Desktop Notifier	10
Localisation	10
Version 1.9.0 (July 2026)	10
SNMP Trap Receiver and Emergency Alerts	10
Phone-Only Emergency Delivery	10
ACD Agent Status Phone Screen	10
Queue Status Phone Screen Polish	10
Phone Display Reliability Bundle	11
Version 1.8.0 (June 2026)	11
Phone Display	11
Phone Display Licensing	11
Latin-Script Phone Cap	11
Earlier Releases	11
System Requirements	12
Server Operating System	12
Hardware	12
Baseline Hardware by Extension Count	12
Additive Resources per Licensed Module	12
What the Baseline Includes	12
Sizing Assumptions	13
Software Prerequisites	13
Network and Ports	13
Pre-Installation	14

Downloads	14
Step 1a — IIS with ASP.NET Features	14
Windows Server 2019 / 2022 / 2025	14
Windows 10 / 11	14
Step 1b — .NET 10 Hosting Bundle	14
Step 1c — PostgreSQL 17	15
Installation	16
Step 2 — Run the Installer	16
Installer Wizard Pages	16
.....	17
Step 3 — First Login	17
Step 4 — Post-Installation Checklist	18
Real-Time / Contact Center Customers	18
Service Verification	18
Emergency Alerts (v1.9.0+)	18
EVOA Desktop Notifier (v1.10.0+)	18
Accessing EVOA from Other Machines	20
Check Windows Firewall Rules	20
Re-Create Missing Rules	20
Phone Display (Mitel 6900) Setup	21
Verified Hardware	21
License Prerequisite	21
A. AppInfo Configuration Templates	21
B. MiVB Application Info (per Tenant)	22
C. Firewall Requirements	22
D. Network Topology Notes	23
E. Verifying the Push Path	23
F. Softkey URLs (Programmable Keys in MIVB ESM)	23
SNMP / Emergency Alerts Setup	25
A. Windows Service	25
B. MiVB ESM Configuration (per Tenant / per MIVB)	25
C. EVOA Admin Configuration	26
Trap Sources Tab	26
CESID Locations Tab	26
Recipients Tab	26
Test	26
D. Acknowledgement Lifecycle	27
E. Troubleshooting	27
SNMP Trap Receiver Installed but Not Running	27
MIVB Confirmed Sending Traps but EVOA Shows No Events	27
EVOA Receives the Trap but No Phone Shows the Alert	27
Desktop Notifier Setup	28
Purpose Roles	28
Step 1 — Install the Notifier on a PC	28
Step 2 — Approve the Station (Admin)	29
Step 3 — Enable Desktop Delivery on Rules / Tags	30
Network / Firewall	30
Upgrading the Notifier	30
Troubleshooting	30
Upgrade and Reinstallation	32
Standard Upgrade	32
Upgrading from v1.2.x or Earlier	32
Upgrading from v1.3.x through v1.9.x	32
v1.10.0-Specific Notes	32

v1.9.0-Specific Notes	32
v1.8.0-Specific Notes (Applies When Upgrading from 1.7.x or Earlier)	32
Backup Before Upgrading	33
Complete Reinstall	33
Optional Hardening: phx_writer Database Role	34
Troubleshooting	35
Installer Prerequisite Checks	35
Installer shows "MISSING: IIS with ASP.NET features"	35
Installer shows "MISSING: .NET 10 Hosting Bundle"	35
Installer shows "MISSING: PostgreSQL 14 or higher"	35
Database Connectivity	35
Database connection fails during installation	35
Web Layer	35
Login page does not load (http://localhost:8080)	35
API returns 503 or 500 errors	35
Blank page or UI not loading after upgrade	36
App pool crashes immediately after upgrade	36
Collection Service	36
Collection Service not running / not collecting calls	36
Real-Time / Wallboards	36
Real-Time wallboard shows Disconnected or no live data (v1.4.0+)	36
Queue Drill-Down on a digital queue shows an empty table (v1.5.0+)	36
Phone Display	36
Administration > Phone Display page shows "License Required" (v1.8.0+)	36
Phone registers as Pending but never moves to Active (v1.8.0+)	37
Phone shows "Cannot display" instead of an EVOA screen (v1.8.0+)	37
Phone registers + polls fine but never receives any alert (v1.8.0+)	37
Phone displays squares instead of Arabic / Hindi / Chinese text (v1.8.0+)	37
SNMP / Emergency Alerts	37
CallAccountingSnmpReceiver service won't start (v1.9.0+)	37
SNMP traps not reaching EVOA (v1.9.0+)	37
Trap arrives at EVOA but recipient phones don't show alert (v1.9.0+)	38
HTTPS Certificate	38
HTTPS certificate warning in browser	38
Remote Access	38
Cannot connect from another machine	38
Appendix A: File Locations	39
Appendix B: Supported PBX and ACD Systems	40
PBX Systems (CDR / SMDR Collection)	40
ACD / Contact Center Systems (Real-Time, v1.4.0+)	40
Support and Contact	41

About This Guide

Purpose

This guide describes how to prepare a Windows Server host, install Enterprise Voice Operations & Analytics (EVOA) v1.10.0, complete the post-install configuration, and troubleshoot the most common issues encountered during deployment. It is written for the engineer responsible for the initial install and for the administrator who owns the system afterwards.

Intended Audience

- System administrators deploying EVOA on Windows Server 2019, 2022 or 2025
- Voice / telephony engineers configuring the MiVoice Business (MIVB) integration, SNMP Emergency Response feed, or Phone Display module
- Partner deployment engineers running certified installs on customer sites

Prerequisites for Reading

Familiarity with Windows Server administration (Services, IIS Manager, Windows Firewall), PostgreSQL basics (roles, database creation, connection strings), and the MiVoice Business Embedded System Management (ESM) UI where the Phone Display and Emergency Response features are configured.

Document Conventions

UI paths are shown with arrow separators: Administration > Emergency Alerts

Commands and code are shown in a monospaced font on a light shade:

```
iisreset /restart
```

Placeholders in commands and paths are shown in angle brackets: <evoa-host>, <tenantCode>

Callout boxes highlight information that requires special attention:

NOTE General information that clarifies behaviour but is not action-required.

TIP Optional guidance that can save time or improve the deployment.

WARNING A step or configuration that could cause degraded operation if skipped or misapplied.

IMPORTANT A step that must be completed for the install to succeed, or that has safety implications.

Related Documents

- README.txt — short release manifest bundled with the installer package (contents, SHA-256 hash, quick install commands)
- In-app help — accessed from the Help icon in the EVOA browser UI once installed; provides configuration walkthroughs for every admin page in all 8 supported languages
- What's New — opens from the in-app Help menu; details post-1.10.0 release-by-release changes

System Overview

What EVOA Does

Enterprise Voice Operations & Analytics (EVOA) is a unified voice operations platform that combines call accounting, real-time supervisor wallboards, alert delivery, SNMP-driven emergency dispatch, and reporting for every PBX in the environment. A single Windows Server install serves supervisors on the browser, operators on Mitel 6900 phones, TV wallboards in the operations centre, and Windows tray notifiers on individual PCs.

Component Architecture

The installer deploys four cooperating components on the same Windows Server host by default. Larger deployments may split the API and database tiers across separate hosts.

Component	Type	Purpose
Web API	IIS application	REST + SignalR endpoints for the UI, phones, TV, notifier
Web UI	IIS site (Blazor)	Supervisor and admin browser experience
Collection Service	Windows Service	SMDR / CDR capture from every configured PBX
SNMP Receiver	Windows Service (UDP 162)	Emergency Response trap listener (v1.9.0+)

On-Disk Layout

Data, logs, and the on-disk copy of this guide are stored under the following root, which is created by the installer and retained across upgrades and uninstalls:

```
C:\CallAccountingData\  
C:\CallAccountingData\docs\INSTALLATION-GUIDE.txt (copy of this file)
```

NOTE See the File Locations section in Appendix A for the full path list.

What's New

This section summarises the notable changes in the current and recent releases. For a complete change list, use the What's New page in the in-app Help menu after installation.

Version 1.10.0 (July 2026)

EVOA Desktop Notifier

A lightweight Windows tray application delivers Emergency, VIP, and Real-Time Alert Center notifications to any PC on the network with no browser session required. It connects over SignalR, pops a full-screen alert window on every matching event, and participates in the same full-mesh acknowledgement fabric as the phone and browser surfaces: acknowledging on any one closes the same alert on the other three within a second. See the Desktop Notifier Setup chapter for the full deployment walkthrough.

Desktop Channel on Real-Time Alert Rules

The alert-rule editor exposes a new Desktop channel checkbox alongside Browser, Phone, and TV. Default remains Browser-only, so existing rules do not surprise-fire the notifier until a supervisor opts in. Rules gated on Desktop only reach desktop stations whose Purpose role includes Supervisor.

Push to Desktop Toggle on Caller Tags

Independent from the v1.9.0 Push to Phone flag, so an admin can decide phone-only, desktop-only, or both per VIP entry. Enable at Administration > Caller Tags. Tagged Caller In Queue alert rules inherit from the tag flag (no per-rule Desktop toggle in the editor for that metric).

Desktop Stations Tab

A new tab on the Phone Display admin page provisions notifier PCs. Same shape as the Phones tab: pending stations at the top, approve / edit / reject / delete actions per row, Purpose radio (Supervisor / Supervisor + Emergency / Emergency Only), Site hard ceiling, and an optional assigned user for queue-scope narrowing.

NOTE Initial install distribution: the signed notifier installer ships as a STANDALONE .exe in the customer release package — copy to your internal channel to bypass Windows SmartScreen. Updates propagate silently via the built-in AutoUpdater.

Notifier Auto-Update Endpoint

The `/api/v1/desktop-notifier/version` endpoint lets the notifier client poll for a newer signed installer every 24 hours; when a newer one lands in the server's `wwwroot\downloads\notifier\` folder the client applies it silently. Filename convention `EvoaNotifier-{version}-{platform}.{ext}` is enforced by the catalog endpoint so operators can drop test builds without breaking the catalog.

Emergency Alert Popup and History Visual Upgrade

Emergency popups now use a red-tinted background wash with an oversized title so the operator can read "who + where" from across the room. Per-category tints extend to Alert Center popups (VIP = cyan, Critical = orange, Warning = yellow) and to History rows so surface and severity are distinguishable at a glance.

Email Channel for Emergency Alerts

Emergency Alerts now supports an Email Group recipient type alongside the existing Phone type. On an SNMP emergency event, EVOA renders a branded HTML email (with plain-text fallback) and hands it to the

tenant's SMTP for delivery to every active member of the chosen Recipient Group. Delivery runs on a dedicated Hangfire queue with 3-attempt exponential retry (~7 min self-healing window). Every fan-out writes an audit row to `snmp.EmergencyEmailDeliveries` with SMTP status.

NOTE Notification-only: email cannot acknowledge the alert. Acknowledgement must come from the desk phone, EVOA Desktop Notifier, or dashboard.

SignalR Reconnect Hardened in the Desktop Notifier

Previously the client's built-in reconnect schedule gave up after ~107 seconds, leaving the tray app stuck in "Reconnecting" after longer WebApi restarts (deploy, iisreset). Now, after the built-in schedule exhausts, a perpetual reconnect loop with 5 / 10 / 30 / 60 second exponential backoff rebuilds the HubConnection from scratch until the server is back. Silent recovery without the close-and-reopen workaround.

Localisation

Seven new UI strings shipped in all 8 languages: Desktop channel labels, Push to Desktop toggles, installer download strip header and hint, and the refreshed alert-channel guidance.

Version 1.9.0 (July 2026)

SNMP Trap Receiver and Emergency Alerts

EVOA now listens for SNMP traps from MiVoice Business and surfaces Mitel Emergency Response notifications (911 / 999 dialled) as full-screen alerts on the 6900 phones in the recipient list. A new standalone Windows Service (CallAccountingSnmpReceiver) listens on UDP 162, decodes the trap per the MITEL-ERN MIB, and forwards decoded events to the WebApi. Configured under Administration > Emergency Alerts (trap sources, CESID location map, recipients, event history with ACK lifecycle). See the SNMP / Emergency Alerts Setup chapter for the MiVB ESM configuration checklist.

Phone-Only Emergency Delivery

The v1.9.0 emergency pipeline delivers exclusively to the recipient phones. The v1.10.0 release adds Desktop Notifier and Email channels for emergency events.

ACD Agent Status Phone Screen

Supervisors can browse a live, push-refreshed list of every agent in scope right on the phone: presence (Available / Busy / DND / Away / Offline), ACD work state (Idle / ACD / Hold / NACD / MakeBusy / LoggedOut), Make-Busy reason, time-in-state, and today's per-channel conversation counts. Tiered by phone model:

- 6920 shows name and state
- 6920 shows name and state
- 6930 adds extension, time-in-state, and channels V / C / E
- 6940 shows the full 5-channel breakdown plus MB(reason) inline

Help softkey opens an on-phone legend; Stop softkey unsubscribes. Recommended phone for supervisors: 6940 (7 comfortable rows and a 56-character label budget).

Queue Status Phone Screen Polish

Now refreshes live every 15 seconds via server-push (was snapshot-on-fetch in v1.8.0). New Help and Stop softkeys. New per-row metrics on the wider phones: 6920 unchanged (AG / WT / AB); 6930 adds LW (longest wait); 6940 adds LW / OF (offered today) / HD (handled today) / SL% (service level today). A stale indicator surfaces in the title if the Mitel CX driver hasn't emitted any queue event in five minutes, so supervisors don't trust frozen counters during an outage.

Phone Display Reliability Bundle

The v1.8.0 "Refresh Now" menu row was removed (the underlying /heartbeat endpoint returned 204 No Content, which the firmware misread as "File Not Found"). Disconnect detection: a new PhoneStalenessWatcher flips Active phones to Unreachable when LastSeenAt is older than five minutes, and a push-failure counter on PhonePushSender catches the outbound direction. Test-Push UI now reports the real outcome instead of always-success. New Extension / DN column in the admin grid. Per-phone poll metrics now populate via ON CONFLICT upsert.

Version 1.8.0 (June 2026)

Phone Display

Mitel 6900-series IP phones (6915, 6920, 6930, 6940 on firmware 03.02.00.022 verified) become live operations surfaces for the call centre. Phones show the same VIP-Waiting screen, alert takeovers, and queue status the supervisor sees on the browser dashboard and TV wallboard. Acknowledging an alert from any surface clears it from all three in sync. Configured under Administration > Phone Display. See the Phone Display (Mitel 6900) Setup chapter for the MiVB AppInfo and firewall checklist.

Phone Display Licensing

Chargeable per-seat add-on (CA-PD-PHN). Order quantity = number of phones in Active status simultaneously. Pending / Disabled / Unreachable phones do not consume a seat. The feature flag is auto-granted whenever the per-seat order quantity is > 0; no separate add-on SKU needed. Trial licenses include 5 phone seats by default. Settings > License surfaces both the ceiling and the live count.

Latin-Script Phone Cap

The Mitel 6900 firmware font covers Latin-1 and Latin Extended-A, which renders English, German, Spanish, French, and Turkish fully. Arabic, Hindi, and Chinese codepoints have no glyphs in the firmware font, so EVOA automatically falls back to English on the phones for those tenants. Admin UI and TV wallboard remain in the chosen language.

Earlier Releases

Detailed change logs for v1.7.0 (Caller Tags / VIP), v1.6.0 (Real-Time Alerts, Agent Recognition), v1.5.0 (Queue Drill-Down per Agent), and v1.4.0 (Real-Time Wallboards) are available in the in-app What's New page after login: Help icon > What's New.

System Requirements

Server Operating System

- Windows Server 2019, 2022, or 2025 (recommended for production)
- Windows 10 or 11 Professional / Enterprise (supported for lab and pilot deployments)

Hardware

Sizing is driven by extension count, with additive resources per licensed EVOA module. The baseline column is what a Call Accounting-only deployment needs on a single host; add the columns to the right for each module the customer has licensed. All figures include Windows Server, PostgreSQL, IIS, and every EVOA component co-hosted on the same box.

Baseline Hardware by Extension Count

Tier	Extensions	Baseline (Call Accounting only)
Small	Up to 500	2 vCPU · 12 GB RAM · 250 GB SSD · single host
Medium	500 - 2,500	4 vCPU · 16 GB RAM · 500 GB SSD · single host
Large	2,500 - 10,000	8 vCPU · 32 GB RAM · 1 TB SSD · single host (or DB split)
Enterprise	10,000+	16+ vCPU · 64+ GB RAM · 2+ TB SSD · split DB tier recommended

Additive Resources per Licensed Module

Add these on top of the baseline for every module the deployment uses. Modules the customer has not licensed contribute zero.

Tier	+ Real-Time (Mitel CX / MIVB-ACD)	+ Phone Display + Desktop Notifier	+ Emergency Alerts (SNMP + Email)
Small	+1 vCPU · +4 GB RAM	+1 vCPU · +2 GB RAM	negligible (+1 GB)
Medium	+2 vCPU · +8 GB RAM	+1 vCPU · +4 GB RAM	negligible (+2 GB)
Large	+4 vCPU · +16 GB RAM	+2 vCPU · +8 GB RAM	+1 vCPU · +4 GB RAM
Enterprise	+8 vCPU · +32 GB RAM (dedicated CX host recommended)	+4 vCPU · +16 GB RAM	+2 vCPU · +8 GB RAM

What the Baseline Includes

The RAM figures above are the total single-host allocation. A rough breakdown for the Small tier (12 GB total) illustrates the split:

- Windows Server (OS + services): ~3 GB
- PostgreSQL 17 (base + shared_buffers ~25% of RAM): ~3 GB
- IIS worker processes (WebAPI + BlazorUI app pools): ~1.5 GB
- Collection Service + SNMP Receiver: ~0.5 GB
- Headroom for query bursts, report generation, WAL replay: ~4 GB

Sizing Assumptions

- 30 calls per extension per day average, 22 working days per month
- 24-month CDR retention baseline (adjust storage proportionally for longer retention)
- Phone Display and Desktop Notifier load scales with device count (60-second phone heartbeats, one SignalR connection per station), not extension count directly
- SNMP Trap Receiver and Emergency email delivery are event-driven and use negligible resources at baseline

NOTE Split-DB deployments (recommended at 10,000+ extensions): subtract roughly 25% of RAM and 40% of disk from the app host, then provision the database host at that reduced size. Combined total is unchanged.

TIP For a full parametric sizing (custom retention, calls-per-extension override, backup policy, reports volume), use the Capacity Planning Calculator provided by the MeeraApps partner team.

Software Prerequisites

- IIS with ASP.NET features (installed as a Windows Feature; see chapter Pre-Installation)
- .NET 10 Hosting Bundle for IIS integration
- PostgreSQL 14 or higher; PostgreSQL 17 is recommended and used in the examples in this guide

Network and Ports

Port	Protocol	Direction	Purpose
8080	TCP	Inbound	Default HTTP port for the EVOA UI and API (configurable at install)
443	TCP	Inbound	HTTPS for UI and API; self-signed certificate created by installer
162	UDP	Inbound	SNMP trap receiver for MiVB Emergency Response (v1.9.0+)
80	TCP	Outbound	EVOA WebApi to Mitel 6900 phones for XML push (v1.8.0+)
5432	TCP	Local	PostgreSQL default port (loopback for co-located deployments)

Pre-Installation

The installer checks for all three prerequisites and will NOT proceed if any are missing. Install them in the order below.

Downloads

The two downloadable prerequisites (IIS is a built-in Windows role):

- **.NET 10 Hosting Bundle:** <https://dotnet.microsoft.com/download/dotnet/10.0>
- **PostgreSQL 17 (Windows x64):** <https://www.enterprisedb.com/downloads/postgres-postgresql-downloads>
- **IIS installation reference:** <https://learn.microsoft.com/en-us/iis/install/>

Step 1a — IIS with ASP.NET Features

Windows Server 2019 / 2022 / 2025

Open Server Manager > Manage > Add Roles and Features. Under Server Roles > Web Server (IIS), include:

- Web Server > Common HTTP Features (all)
- Web Server > Application Development > ASP.NET 4.8
- Web Server > Application Development > .NET Extensibility 4.8
- Web Server > Application Development > ISAPI Extensions
- Web Server > Application Development > ISAPI Filters
- Web Server > Application Development > WebSocket Protocol
- Management Tools > IIS Management Console
- Management Tools > IIS Management Scripts and Tools

Windows 10 / 11

Control Panel > Programs > Turn Windows features on or off. Enable the following:

- Internet Information Services > Web Management Tools > IIS Management Console
- World Wide Web Services > Application Development Features (.NET Extensibility 4.8, ASP.NET 4.8, ISAPI Extensions, ISAPI Filters, WebSocket Protocol)
- World Wide Web Services > Common HTTP Features (Default Document, Directory Browsing, HTTP Errors, Static Content)
- World Wide Web Services > Security > Request Filtering

TIP Verify: open <http://localhost> in a browser. The IIS default page should appear.

IMPORTANT WebSocket Protocol is REQUIRED. Without it, SignalR real-time updates used by v1.4.0+ wallboards will fall back to long-polling or stall completely.

Step 1b — .NET 10 Hosting Bundle

Download the latest 10.0.x Hosting Bundle from dotnet.microsoft.com/download/dotnet/10.0 (choose ASP.NET Core Runtime 10.0.x > Hosting Bundle > Windows).

IMPORTANT Install the Hosting Bundle, NOT just the runtime. The Hosting Bundle includes the ASP.NET Core Module for IIS.

Run the installer and accept the defaults. After installation, restart IIS as Administrator:

```
iisreset /restart
```

Or restart the computer. This is required for IIS to detect the new ASP.NET Core module.

Verify:

```
dotnet --list-runtimes
```

You should see a line similar to:

```
Microsoft.AspNetCore.App 10.0.x [C:\Program Files\dotnet\shared\...]
```

NOTE If you are upgrading from a previous version that used the .NET 8 Hosting Bundle, install the .NET 10 Hosting Bundle alongside it. Both can coexist; the .NET 8 bundle does not need to be uninstalled first.

Step 1c — PostgreSQL 17

Download the Windows x86-64 installer from enterprisedb.com/downloads/postgres-postgresql-downloads (choose Version 17).

During installation:

- Set the postgres superuser password to Admin@123! (the installer expects this as the default; you may use a different password and enter it during EVOA install)
- Leave port at 5432
- Leave locale at Default locale
- pgAdmin 4 and Stack Builder are optional (useful for troubleshooting)

WARNING Do NOT change the default data directory unless you have a specific reason. The default is C:\Program Files\PostgreSQL\17\data\.

Verify from an elevated Command Prompt:

```
"C:\Program Files\PostgreSQL\17\bin\psql.exe" -U postgres -c "\l"
```

Enter Admin@123! when prompted. You should see a list of default databases (postgres, template0, template1).

Installation

Step 2 — Run the Installer

Right-click CallAccountingSetup-1.10.0.exe > Run as administrator. Administrator rights are required to create IIS sites and install Windows services.

IMPORTANT The SNMP Trap Receiver (v1.9.0+) binds to UDP port 162. If another SNMP listener is already running on this host (Windows SNMP Trap Service, third-party SNMP manager, etc.), the EVOA receiver will start but log "address in use" and not receive traps. Stop or reconfigure the conflicting listener BEFORE running the installer:

```
Get-Service "SNMPTRAP" | Stop-Service ; Set-Service "SNMPTRAP" -StartupType Disabled
```

Installer Wizard Pages

1. Welcome — click Next
2. License agreement — accept and click Next
3. Database configuration:
 - Database Host: localhost (change if PostgreSQL is on another server)
 - Port: 5432
 - Database Name: CallAccounting (created automatically)
 - Username: postgres
 - Password: Admin@123! (or your postgres superuser password)

NOTE The installer tests the database connection before proceeding. If the connection fails, verify PostgreSQL is running via services.msc > postgresql-x64-17 > Status: Running.

4. Web server port — 8080 recommended (avoids conflict with IIS Default Web Site); 80 works if IIS Default Web Site is stopped or removed. A self-signed HTTPS certificate is also created on port 443.
5. Application language — choose the default language for the web interface. Users can change this at any time from the top menu bar after login. Available: English, Arabic, French, Spanish, German, Turkish, Hindi, Chinese.
6. Click Install. The installer will:
 - Copy application files to IIS folders and Program Files
 - Drop a copy of this guide at C:\CallAccountingData\docs\
 - Create and configure IIS application pools and site
 - Generate a self-signed HTTPS certificate (port 443)
 - Install and start the Collection Windows Service
 - Install and start the SNMP Trap Receiver Windows Service
 - Create the PostgreSQL database and run migrations
 - Open firewall ports (HTTP port, 443, and UDP 162 for SNMP)
7. Click Finish when complete.

TIP Installation logs are written to C:\CallAccountingData\install-iis.log and install-setup.log. Check these first if anything goes wrong.

Database Configuration
Enter the PostgreSQL connection details for the EVOA database.

Database Host:

Port:

Database Name:

Username:

Password:

change only if you installed PostgreSQL with a different password.

Installation wizard

Step 3 — First Login

Open a browser and navigate to:

`http://localhost:8080` (HTTP - or whichever port you chose)
`https://localhost` (HTTPS - accept the self-signed certificate warning)

Default credentials:

Username	admin
Password	Admin@123!

IMPORTANT Change the admin password immediately after first login via Settings > Account.

MeeraApps
Enterprise Voice Operations & Analytics
 Real-Time Wallboards · ACD Analytics · AI Insights

Username:

Password:

Version 1.10.0

EVOA login page (localhost:8080)

Step 4 — Post-Installation Checklist

Work through the following list top-to-bottom. Items marked with a version tag are only relevant when you have licensed those features.

- Browse to <http://localhost:8080> and confirm the login page loads
- Log in with admin / Admin@123!
- Change the admin password (Settings > Account)
- Go to Administration > License to activate your license (or use the 30-day Trial that ships with Real-Time and AI Analytics enabled for up to 5 agents)
- Add Sites (Administration > Sites)
- Add PBX Systems and configure CDR collection (Administration > PBX Systems)

Real-Time / Contact Center Customers

- Administration > Real-Time Settings: configure the Mitel CX or MIVB-ACD feed per site and verify the status pill shows Connected
- Administration > ACD Systems: register the ACD system, queues, agents, and agent groups
- Call Center > Sync Health: confirm all systems report Connected
- Call Center > My Dashboards: open a live dashboard and use Queue Members on a queue tile to view the per-agent drill-down

Service Verification

Confirm both Windows services are running (services.msc):

- CallAccountingCollection — Status: Running
- CallAccountingSnmpReceiver — Status: Running (v1.9.0+)

Confirm UDP 162 is bound by the receiver (v1.9.0+):

```
Get-NetUDPEndpoint -LocalPort 162 | Select OwningProcess
Get-Process -Id <pid> # should be CallAccounting.SnmpReceiver
```

Emergency Alerts (v1.9.0+)

Under Administration > Emergency Alerts:

8. Add at least one Trap Source (the MIVB controller's IP)
9. Map at least one CESID to a human-readable location label
10. Add at least one Phone recipient with a phone in Active status
11. (v1.10.0+, optional) Add one or more Email Group recipients:
 - Create a Recipient Group at Administration > Recipient Groups
 - In Emergency Alerts > Recipients tab, add a row with Type = "Email Group" and pick the group
 - Verify tenant SMTP is configured at Administration > Settings > Email

See the SNMP / Emergency Alerts Setup chapter for the MiVB ESM configuration.

EVOA Desktop Notifier (v1.10.0+)

12. Extract EvoaNotifier-{version}-win-x64.exe from the release package and copy it to your internal distribution channel
13. Install as Administrator on each operator PC
14. Complete the first-run wizard on the PC (server URL, tenant code) — the station appears as Pending

15. In the admin UI go to Administration > Phone Display > Desktop Stations, approve the row, pick the Purpose role, and optionally an assigned user
16. Enable the Desktop channel on any alert rules or caller tags that should reach the notifier

See the Desktop Notifier Setup chapter for the full deployment checklist.

Finally:

- Make a test call and verify it appears in Call Records within a few seconds

Accessing EVOA from Other Machines

From another machine on the same network:

```
http://<server-ip>:8080  
https://<server-ip>
```

The firewall rules for the HTTP port, 443, and UDP 162 (SNMP) are added automatically by the installer. If access is still blocked:

Check Windows Firewall Rules

```
netsh advfirewall firewall show rule name="CallAccounting HTTP"  
netsh advfirewall firewall show rule name="CallAccounting HTTPS"  
netsh advfirewall firewall show rule name="CallAccounting SNMP Trap"
```

Re-Create Missing Rules

Run as Administrator if any of the above rules are missing:

```
netsh advfirewall firewall add rule name="CallAccounting HTTP" dir=in action=allow  
protocol=TCP localport=8080  
netsh advfirewall firewall add rule name="CallAccounting HTTPS" dir=in action=allow  
protocol=TCP localport=443  
netsh advfirewall firewall add rule name="CallAccounting SNMP Trap" dir=in  
action=allow protocol=UDP localport=162
```

NOTE Check any network or hardware firewalls between the client and EVOA. The SNMP path is one-way (MIVB -> EVOA, UDP 162); make sure that direction is permitted on every hop between the MIVB and EVOA.

Phone Display (Mitel 6900) Setup

The Phone Display module turns Mitel 6900 IP phones into live operations surfaces driven by the EVOA WebApi. This chapter is needed **ONLY** if you intend to provision phones; the rest of the system runs without it. (Feature introduced in v1.8.0.)

Verified Hardware

Mitel 6915, 6920, 6930, and 6940 on firmware 03.02.00.022. The 6915 uses the same AppInfo configuration as the 6920 (identical XML rendering capabilities on this firmware). Older 6800-series phones and softphones are **NOT** supported in this release.

License Prerequisite

Your EVOA license must include CA-PD-PHN with quantity $\geq$ number of phones you plan to set to Active simultaneously. Trial licenses ship with 5 phone seats. Without the seats, the Administration > Phone Display page renders a "License Required" panel.

A. AppInfo Configuration Templates

The installer ships four pre-built AppInfo configuration files that tell each Mitel 6900 phone where to find the EVOA WebApi and how often to heartbeat. They land at:

```
C:\CallAccountingData\Templates\PhoneXml\  
AppInfo-6915.cfg  
AppInfo-6920.cfg  
AppInfo-6930.cfg  
AppInfo-6940.cfg
```

Each file is identical except for the filename — the per-model naming exists because MiVB Phone Application Manager uploads are scoped per model, so having one file per model lets you upload and assign without renaming. The 6915 file is a copy of the 6920 file; they render EVOA content identically on the current supported firmware.

Open each .cfg in a text editor and replace the three placeholders:

<EVOA_HOST>	Public hostname or FQDN of the EVOA server (the phone must resolve this via its DNS). Example: evoa.contoso.local
<EVOA_HOST_IP>	The same server's IP address. Used by the phone to allow-list inbound XML pushes. Example: 10.20.30.40
<TENANT_CODE>	The customer tenant's code from EVOA (Administration > Tenants > Tenant Code). Example: ACME

The default "https validate certificates : 0" line allows EVOA's self-signed certificate to be accepted. If your EVOA is fronted by a publicly trusted cert, change 0 to 1 for strict validation.

The default poll interval of 60 seconds is enough for Pending detection within ~30 seconds and keeps the bandwidth footprint trivial. Lower it if you need faster provisioning during a roll-out.

B. MiVB Application Info (per Tenant)

In the MiVoice Business System Administration:

17. Open Phone Application Manager.
18. Create an Application Info entry with this URL pattern:
`https://<evoa-host>/api/phone-xml/{tenantCode}/menu`

where <evoa-host> is the public hostname or IP of the EVOA server (must be reachable from the phone subnet on port 443) and {tenantCode} is the customer's tenant code from EVOA (Administration > Tenants > Tenant Code).

IMPORTANT The field labelled "Application Info URL" is the one EVOA reads. The older "Application URL" field is for a different feature; leave it blank.

19. Open the Phone Application Update form, select the matching per-model file from Section A (AppInfo-6915.cfg / AppInfo-6920.cfg / AppInfo-6930.cfg / AppInfo-6940.cfg), and upload it. MiVB delivers it to each phone of that model on the next TFTP fetch.
20. Assign the AppInfo entry to the phones that should join EVOA.
21. Reboot the phones (or wait for the next polling cycle).

Within ~30 seconds the phones appear in EVOA at Administration > Phone Display with status "Pending". An admin then approves each phone and assigns either a user-bound scope (Shape A) or an explicit device scope (Shape B). See the in-app help for the full assignment-shape walkthrough.

The screenshot shows the 'Phone Display' interface in the EVOA system. At the top, it says 'Provision and manage Mitel MiNET phones (6900 series). Phones auto-register on first contact and wait here for admin approval.' There are 3 pending phones. Below this is a search bar and a list of tabs: 'Phones' (selected), 'Desktop Stations', and 'Telephone Directory'. The main table lists the following data:

PHONE	EXT	MODEL	FW	STATUS	SITE	ASSIGNMENT	LAST SEEN	LAST IP	ACTIONS
14:00:E9:0C:62:49	—	MitelMINET_6940w	03.02.00.022-162582	Pending	-	Click Approve to assign	26/06/2026 10:44	10.140.9.212	Approve Delete
06:00:0F:8D:82:0F	—	MitelMINET_6940	03.02.00.022-162582	Pending	-	Click Approve to assign	26/06/2026 10:44	10.140.9.236	Approve Delete
06:00:0F:81:64:E9	—	MitelMINET_6920	03.02.00.022-162582	Pending	-	Click Approve to assign	24/06/2026 02:37	10.140.9.218	Approve Delete

Below the table, it says 'Administration > Phone Display: pending phones list'.

C. Firewall Requirements

Phone Display uses TWO independent network paths that must BOTH work:

- Phone > EVOA WebApi on TCP 443 (inbound HTTPS poll)
- EVOA WebApi > Phone on TCP 80 (outbound MiNET push callback)

Path 1 is initiated by the phone — most enterprise networks allow it trivially. Path 2 is initiated by the EVOA server toward the phone's IP address — this is the path most often missed when phones are not on the same subnet as the server.

Run on the EVOA server (PowerShell):

```
New-NetFirewallRule -DisplayName "EVOA Phone Display Push" `
                    -Direction Outbound `
                    -Protocol TCP `
                    -RemotePort 80 `
                    -Action Allow
```

And ensure the inter-VLAN ACL or hardware firewall between the EVOA server subnet and the phone subnet(s) allows the same TCP 80 server-to-phone path.

D. Network Topology Notes

Topology	Result
Same subnet as EVOA server	Works trivially.
Different VLAN, routable	Works as long as the inter-VLAN ACL allows server > phone-subnet:80.
Remote office over VPN	Works if VPN routes both directions (server's reply path back to the phone subnet must be in the VPN's route table).
Phone behind NAT (branch with port-forwarding to one phone)	BROKEN by default. The recorded LastIp is the NAT gateway, not the phone. Workaround: 1:1 NAT for each phone, or place phones in a directly-reachable subnet.
Server > phone blocked at the firewall	SILENTLY BROKEN. The phone registers and polls fine but no alert ever reaches the screen.

E. Verifying the Push Path

After approving a phone, click Test Push on its row in the admin page. EVOA sends a one-shot test screen. If the phone displays it, path 2 is healthy. If not:

22. From the EVOA server, run:

```
Test-NetConnection -ComputerName <phone-ip> -Port 80
```

Expected: TcpTestSucceeded : True

23. Check the phone's Last IP column in Administration > Phone Display; if it's a NAT gateway, see the NAT note above.

24. Inspect the phx.PushHistory table for the phone — every push attempt is logged with its status and any error message. A run of "connection refused" or "timeout" entries points to path 2 routing/firewall.

F. Softkey URLs (Programmable Keys in MIVB ESM)

The Application Info URL configured in Section B is what the phone loads at boot to discover EVOA. For DIRECT access to specific EVOA screens, you can program additional softkeys in MIVB ESM (System > Devices and Feature Codes > User and Device Configuration > Edit phone > Keys / Programmable Keys). Each softkey carries one URL of type "XML Application" pointing at the matching EVOA endpoint.

All URLs share the prefix `https://<evoa-host>/api/phone-xml/{tenantCode}/...`. Recommended softkey assignments:

Label	Endpoint	Purpose
EVOA	/menu	Home menu. Opens the supervisor's hub which lists VIP Waiting, Interactions Waiting, Queue Status, and Refresh in one navigable TextMenu. One softkey covers everything if programmable-key space is tight.
VIP	/vip-queue	Jumps straight to the VIP Waiting takeover (filtered to tagged callers currently in the phone's scope). Empty list shows "All VIPs handled."
Waiting	/interactions-waiting	Lists every interaction currently in queue for the phone's scope (not just tagged). Useful for a backlog snapshot without alert noise.
Status	/idle-status	Per-queue summary (waiting count + longest wait) for every queue the phone is allowed to see. Equivalent to glancing at the wallboard's queue tiles.

Label	Endpoint	Purpose
WARNING Do NOT program softkeys for internal endpoints (/heartbeat, /alert-ack, /vip-queue/ack, /noop, /pending). The phone calls them automatically; mapping them to a softkey causes confusing behaviour.		

To verify a softkey URL is reachable from your network, open <https://<evoa-host>/api/phone-xml/<tenantCode>/menu> in a browser. You should see the XML payload inline. "Pending Configuration" means the tenant code is wrong; a 404 means the WebApi is not reachable.

SNMP / Emergency Alerts Setup

The SNMP module turns EVOA into a trap receiver for Mitel ER (Emergency Response) notifications. When MIVB detects an emergency dial pattern (typically 911 / 999 / 112), it emits an SNMP trap; EVOA decodes the trap and pushes a full-screen alert to every Phone Display in the configured recipient list. From v1.10.0, EVOA also fans out to Email Group recipients and Desktop Notifier stations whose Purpose includes Emergency.

A. Windows Service

Service name	CallAccountingSnmpReceiver
Display name	Call Accounting SNMP Trap Receiver
Binary	C:\Program Files\CallAccounting\SnmpReceiver\CallAccounting.SnmpReceiver.exe
Listens on	UDP 162 on all interfaces (0.0.0.0)
Account	LocalSystem (required to bind a privileged port)
Startup	Automatic, with crash-recovery (restart after 60s twice, then 5 min; reset count daily)
Config	C:\Program Files\CallAccounting\SnmpReceiver\appsettings.json
Logs	C:\Program Files\CallAccounting\SnmpReceiver\logs\snmp-receiver-<date>.log

The installer pre-populates appsettings.json with the WebApi ingest URL (`http://localhost:<http-port>/api/v1/snmp/emergency`) using the HTTP port chosen during install. The AllowedSources array is intentionally EMPTY — the receiver is up but accepts nothing until the admin populates the allow-list (see step C below).

B. MiVB ESM Configuration (per Tenant / per MIVB)

In the MiVoice Business Embedded System Management UI:

25. Open Shared System Options > Emergency Response.
26. Set "Trap IPAddress/FQDN for ER Notification" to the IP of the EVOA server (NOT a hostname — the MIVB form accepts an FQDN but the most reliable behaviour is the raw IP). Example: 10.20.30.40.

IMPORTANT This field rejects host:port syntax. MIVB always sends ER traps to UDP 162; you cannot redirect to a high port.

27. Set "Trap Community String" to a non-default value (e.g., evoa-traps) for at least a minimum level of source attribution. The receiver does not gate on community string alone — the allow-list (step C) is the real authorisation layer — but a custom community helps you spot stray traps from misconfigured devices in the receiver log.
28. Configure dial patterns: System Properties > System Feature Settings > Emergency Response > Emergency Numbers. Add the codes that should trigger a trap (911, 999, 112, etc.) and the corresponding CESID per phone or per zone.
29. Save. MIVB will emit a trap whenever a configured emergency number is dialled by a phone with a known CESID.

Reference MIB	MITEL-ERN.mib (Mitel Emergency Response Notification)
----------------------	---

Trap OID

1.3.6.1.4.1.1027.4.1.1.401 (notification 401)

C. EVOA Admin Configuration

In EVOA: Administration > Emergency Alerts.

Trap Sources Tab

Add one row per MIVB controller IP that should be accepted. Sources NOT in this list are silently dropped, regardless of community string. This is the defensive default for fresh installs.

Emergency Alerts
Configure PBX SNMP trap sources and the recipients (security, supervisors, phones, TVs) that receive emergency-call alerts. Independent from ACD real-time alerts.

Configuration

Events 200

Trap Sources 1

SOURCE IP	DESCRIPTION	ACK BACK TO PBX	ENABLED
192.168.2.2	EXDemo		Enabled

Phone Recipients 2

Mitel 6900 phones that receive the full-screen emergency takeover — typically security desks, reception, and dedicated response stations. Delivered 24/7 while the phone is Active.

TARGET	SCOPE	ENABLED
Guest Room 3002 — Ext 3002 — Guestroom 3002 — 08:00:0F:88:A8:62	192.168.2.2	Enabled
Guest Room 3001 — Ext 3001 — Guestroom 3001 — 08:00:0F:05:E1:79	192.168.2.2	Enabled

Email Group Recipients 1

Off-station stakeholders who receive a branded HTML email — site managers, external security company, on-call rotations, insurance contacts. Independent from Phone Recipients. Notification-only: email cannot acknowledge an alert.

RECIPIENT GROUP	SCOPE	ENABLED
Emergency Group (1 members)	192.168.2.2	Enabled

CESID Locations 1

Maps the CESID digits MIVB emits in the trap to a human-readable location. Without this, the emergency alert reads '5001' instead of '3F Reception'.

CESID	LOCATION LABEL	NOTES
5001	EXDemo	Testing

Enterprise Voice Operations & Analytics v1.10.0 | © 2026 MeeraApps Technology. All rights reserved.

Administration > Emergency Alerts > Trap Sources tab

CESID Locations Tab

Map each CESID code emitted by the MIVB to a human-readable label that supervisors will see on the alert screen:

CESID 5001 -> "3F Reception"

CESID 5012 -> "Fire Marshal Office"

Unmapped CESIDs render as the raw digits — functional but less useful in an emergency.

Recipients Tab

Add one row per phone that should receive emergency alerts. Phone-only delivery: pick from the list of Active phones in Administration > Phone Display. Per-source scoping is supported: leave Trap Source blank to receive alerts from ANY configured source, or pin to a specific source for multi-MIVB sites with separate security teams.

(v1.10.0+) Email Group recipients are added the same way — pick Type = Email Group and select the group; ensure tenant SMTP is configured under Administration > Settings > Email.

Test

MIVB ESM > Emergency Response > "Send Test Trap" (if available on your MIVB build) OR dial a configured emergency number from a phone with a CESID. A successful trap appears on every configured recipient phone within 2-3 seconds and in the Events tab of the Emergency Alerts admin page.

D. Acknowledgement Lifecycle

When an emergency alert appears on a recipient phone, the supervisor presses the Acknowledge softkey:

- The alert dismisses on THAT phone immediately
- The acknowledge propagates to every OTHER recipient phone — the alert dismisses on them too (with a brief "Acknowledged by <name>" status)
- The event row in Administration > Emergency Alerts > Events gets AckedAt / AckedBy / AckChannel populated for the audit trail

The Events tab is the long-term compliance record (E911 reporting, security incident review). Events are append-only — never deleted by the application.

E. Troubleshooting

SNMP Trap Receiver Installed but Not Running

Check it's not blocked by a UDP 162 port conflict:

```
Get-NetUDPEndpoint -LocalPort 162 | Select OwningProcess
Get-Process -Id <pid>
```

If the owning process is NOT CallAccounting.SnmpReceiver, stop the conflicting service:

```
Get-Service "SNMPTRAP" | Stop-Service ; Set-Service "SNMPTRAP" -StartupType Disabled
```

Check logs at C:\Program Files\CallAccounting\SnmpReceiver\logs\.

MIVB Confirmed Sending Traps but EVOA Shows No Events

30. Capture inbound UDP 162 at the EVOA NIC (PowerShell as admin):

```
netsh trace start capture=yes scenario=NetConnection tracefile=C:\Temp\snmp.etl
# wait, send a test trap, then:
netsh trace stop
```

Open the .etl in Wireshark; the trap should appear with source = MIVB IP, dest port 162.

31. If the capture shows no inbound traffic, the trap is being dropped by an intermediate hop (firewall, ACL, NAT). Verify with Test-NetConnection (UDP probe; on Windows this is best-effort but useful):

```
Test-NetConnection -ComputerName <evoa-ip> -Port 162 -InformationLevel Detailed
```

32. If the capture shows traps but no events appear, check the source-IP allow-list in Administration > Emergency Alerts > Trap Sources. Traps from un-listed sources are silently dropped (intentional security default).

EVOA Receives the Trap but No Phone Shows the Alert

33. The receiver forwards to the WebApi at `http://localhost:<http-port>/api/v1/snmp/emergency`. Check the receiver log — a 200 OK means the WebApi accepted it. A 4xx/5xx points at the WebApi (check C:\inetpub\wwwroot\CallAccounting\api\logs\).

34. From the WebApi, the alert pushes to every recipient phone via the existing Phone Display push pipeline. Check the phx.PushHistory table for the recipient phones — failed pushes log the exact connection error.

35. Common gotcha: a recipient is configured but its assigned phone is in Pending or Unreachable status. Only Active phones receive emergency pushes.

Desktop Notifier Setup

The EVOA Desktop Notifier is a Windows tray application that delivers Emergency, VIP, and Real-Time Alert Center notifications to any PC on the network. It runs quietly in the system tray, connects to the EVOA server over SignalR, and pops a full-screen alert window on every matching event. Acknowledging from the desktop instantly closes the same alert on every other surface (phone, browser, TV) — and vice versa. (Feature introduced in v1.10.0.)

Purpose Roles

Purpose roles decide which alert types a station receives:

Purpose	What the station receives
Supervisor	Real-Time Alert Center + VIP tag alerts. No emergency channel.
Supervisor + Emergency	Everything a Supervisor receives, PLUS SNMP-driven Emergency Alerts.
Emergency Only	ONLY Emergency Alerts. Ideal for security desks that shouldn't be interrupted by ACD supervisor notifications.

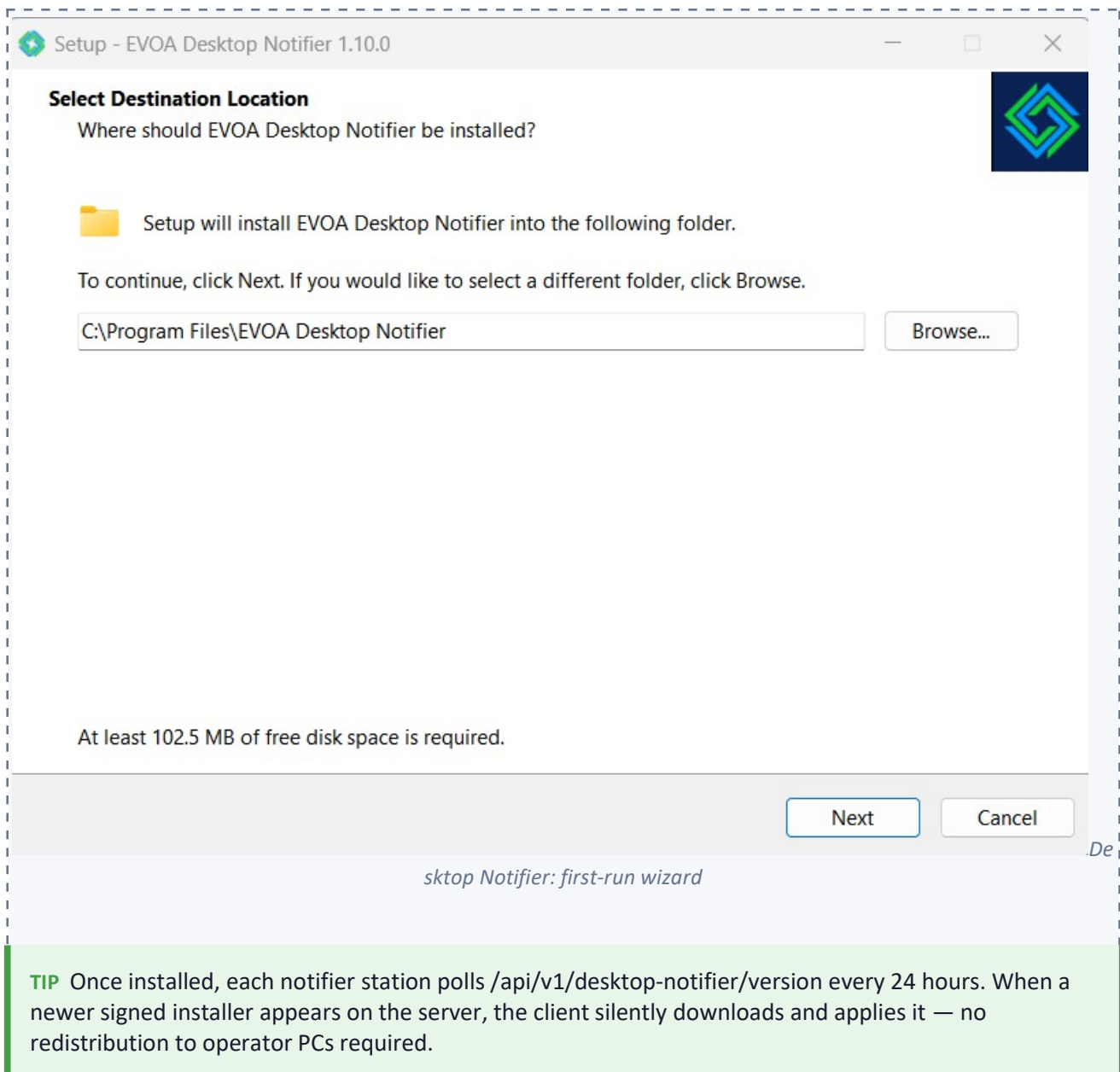
Step 1 — Install the Notifier on a PC

The notifier installer (EvoaNotifier-{version}-win-x64.exe) ships as a STANDALONE file inside the customer release package (CallAccountingSetup-{version}-Package.zip), alongside the server installer, INSTALLATION-GUIDE.txt, and README.txt.

NOTE Why not a download link from the admin UI: browser-initiated .exe downloads trigger Windows Defender SmartScreen's "not commonly downloaded" reputation warning until the Certum SA cert accumulates enough public download volume. Files distributed via trusted INTERNAL channels (network share, SCCM, Intune, email) do not carry Mark-of-the-Web and therefore skip SmartScreen entirely — that is the customer-friendly path.

36. Copy EvoaNotifier-{version}-win-x64.exe from the release package to your internal distribution channel: a network share readable by operator PCs, Microsoft Endpoint Manager (Intune) app package, SCCM / MDT deployment collection, or an email attachment for one-off installs.
37. On the target PC, run the installer as Administrator. Accept the defaults: install to C:\Program Files\EVOA Desktop Notifier, create a Start Menu shortcut, and (optionally) a Desktop icon. Leave "Launch EVOA Desktop Notifier" ticked on the final page so the tray icon appears immediately.
38. On first launch a wizard opens automatically. Enter:
 - Server URL: https://<evoa-host> (or http://<host>:8080)
 - Tenant code: your tenant code exactly (case-sensitive)

Click Register. The tray tooltip flips to "waiting for administrator approval".



Step 2 — Approve the Station (Admin)

39. Return to Administration > Phone Display > Desktop Stations in the browser UI. The new station appears at the top with Pending status. Click Approve.

40. Fill in:

- Contact name: "Front Desk PC", "Guard Room 2"
- Location: "Lobby", "Warehouse Loading Bay"
- Role (Purpose): Supervisor / Supervisor + Emergency / Emergency Only
- Site (hard ceiling): caps effective scope; leave "Any" for multi-site supervisors
- Assigned user: optional; narrows Alert Center rule fires to that user's dashboard scope. Leave blank for tenant-wide alerts (subject to Site ceiling).

41. Save. Status flips to Active and the tray notifier's status switches to Connected within seconds.

[Screenshot placeholder]*Administration > Phone Display > Desktop Stations: approve dialog*

Step 3 — Enable Desktop Delivery on Rules / Tags

Adding a station registers the client but does not automatically wire it into every alert. Two independent knobs:

- Alert Center rules: Administration > Real-Time Alerts, edit a rule, tick the Desktop channel checkbox alongside Browser / Phone / TV. Default remains Browser-only.
- VIP caller tags: Administration > Caller Tags, edit the tag, enable Push to Desktop (independent from Push to Phone).

Emergency Alerts (SNMP-driven) go to every station whose Purpose includes emergency — no per-event toggle.

Network / Firewall

Notifier PC to EVOA server:

Port	Protocol	Purpose
443	TCP	HTTPS — REST API + SignalR hub
8080	TCP	HTTP alternate if HTTPS is not in use

The notifier polls /api/v1/desktop-notifier/version on a periodic cadence for auto-update checks.

Upgrading the Notifier

Shipping a new client build:

42. Build and sign the notifier installer at C:\EvoaNotifier\installer\Output\EvoaNotifier-{version}-win-x64.exe (use sign-binaries.bat notifier and sign-binaries.bat notifier-installer with the Certum card).
43. Run sync-to-production.bat — the pre-mirror step stages every *.exe from the notifier Output folder into wwwroot\downloads\notifier so the next EVOA installer bundles it.
44. Existing installations pick up the new version automatically via the client's auto-update check — no need to visit each PC.

Troubleshooting

Symptom	Resolution
Status stuck on Pending	An admin has not yet approved the station. Check Desktop Stations for the row and click Approve.
Status shows Reconnecting for more than a minute	SignalR hub connection cannot be established. Verify the PC can reach the EVOA server over TCP 443 (or 8080 if HTTP). Corporate proxies that strip WebSocket upgrade headers will cause the same

Symptom	Resolution
	symptom.
No alerts arriving despite Connected status	Verify (a) the rule / tag has the Desktop channel enabled, (b) the station's assigned user's queue scope overlaps the rule's queue scope, (c) the Site ceiling doesn't exclude the source site, (d) the alert wasn't already acked from another surface.
Emergency alerts not arriving on a Supervisor-only station	Emergency channel is gated by Purpose. Edit the station and change Purpose to Supervisor + Emergency or Emergency Only.
First-run wizard didn't reopen after Disconnect	Close the tray app fully (right-click > Exit) and start it again. Disconnect wipes the local config; the wizard opens on next launch when no server URL or tenant is set.
Installer download strip empty on Desktop Stations page	Server's wwwroot\downloads\notifier folder has no EvoaNotifier-{version}-{platform}.{ext} files. Check the catalog endpoint at /api/v1/desktop-notifier/downloads returns a non-empty platforms array.

Upgrade and Reinstallation

Standard Upgrade

45. Run the new installer — it will detect existing components and update in-place (existing configuration and data are preserved).
46. The Collection Service AND the SNMP Trap Receiver are stopped, binaries updated, and restarted.
47. Database migrations are re-run automatically (safe to run on existing DB).
48. IIS application pools are recycled automatically.

Upgrading from v1.2.x or Earlier

v1.3.0 and later require the .NET 10 Hosting Bundle. If you are upgrading from a version that used .NET 8, install the .NET 10 Hosting Bundle BEFORE running this installer (see Pre-Installation > Step 1b). The .NET 8 Hosting Bundle does NOT need to be removed.

Upgrading from v1.3.x through v1.9.x

Direct upgrade to v1.10.0 is supported from any v1.3+ release. No prerequisite changes between 1.3 through 1.10 (all use the .NET 10 Hosting Bundle + PostgreSQL 14+). Existing dashboards, wallboard tokens, ACD Supervisor scope assignments, real-time settings, alert rules, alert assets, agent recognition history, caller tags, and phone provisioning are all preserved.

v1.10.0-Specific Notes

- Emergency Alerts gains an "Email Group" recipient type. The new `snmp.EmergencyEmailDeliveries` audit table and `RecipientGroupId` column on `snmp.EmergencyRecipients` are added by the `AddEmergencyEmailChannel` migration on first start. No manual step needed. Idempotent IF NOT EXISTS SQL — safe to re-run.
- EVOA Desktop Notifier client update: rerun the standalone `EvoaNotifier-*.exe` installer on each operator PC (or wait for the built-in AutoUpdater to pick up the newer signed installer from the server's `wwwroot/downloads/notifier/` folder within 24 hours).

v1.9.0-Specific Notes

- The new "snmp" schema (Emergency Alert tables: `TrapSources`, `CesidLocations`, `EmergencyRecipients`, `EmergencyEvents`) is created automatically by the EF migration on first start. No manual DB step needed.
- Five additional `phx.*` migrations also run automatically. They are all idempotent IF NOT EXISTS SQL — safe to re-run.
- The SNMP Trap Receiver is a NEW Windows Service. The installer registers it, opens UDP 162 in the Windows Firewall, and starts the service. If you previously had the Windows built-in SNMP Trap Service (SNMPTRAP) running on this host, you MUST stop and disable it before installation — both services cannot bind UDP 162 simultaneously.
- The Administration > SNMP Emergency page (v1.8.0 SNMP preview) is now Administration > Emergency Alerts. Existing trap-source and recipient rows are preserved by the upgrade; the navigation label and help-content slug are renamed.

v1.8.0-Specific Notes (Applies When Upgrading from 1.7.x or Earlier)

- The "phx" schema (Phone Display tables: Phones, PushHistory, PollMetrics) is created automatically by the EF migration on first start.
- Existing licenses do NOT have the Phone Display add-on. To enable phones, customers need a license re-issuance from the License Manager including CA-PD-PHN with the appropriate qty. Until then, the Administration > Phone Display page renders a "License Required" panel.
- The default language for the Phone Display surface comes from the tenant's Default Language (Tenants > Edit > Default Language).

Backup Before Upgrading

Take a configuration backup at Administration > Maintenance > Backup > New Backup (use Config Export or Portable Export).

IMPORTANT Sensitive credentials (SMTP password, OAuth client secret, AI API key, PBX/ACD passwords, Mitel CX OAuth credentials) are stripped from export files for security; you will need to re-enter them after a cross-server restore. The Backup dialog lists exactly what is and is not included.

Complete Reinstall

49. Control Panel > Programs > Uninstall > Enterprise Call Accounting System. This stops the service, removes IIS site and app pools, and removes firewall rules — but does NOT delete data in C:\CallAccountingData\ or the PostgreSQL database.
50. Run the new installer.

NOTE Uninstalling does NOT delete your database or collected data. To fully clean up, manually delete the PostgreSQL database "CallAccounting" (via pgAdmin or psql) and the C:\CallAccountingData\ folder.

Optional Hardening: phx_writer Database Role

The phone-XML endpoints under `/api/phone-xml/{tenantCode}/...` are reached by Mitel phones WITHOUT a JWT cookie (the phones can't run a browser). The endpoints are scoped to the `phx.*` schema (Phones, PushHistory, PollMetrics) and never touch the call records or alert history tables.

In production deployments where defence-in-depth matters, you can run the WebApi under a reduced-privilege Postgres role (`phx_writer`) instead of the default postgres superuser. This limits the blast radius of any hypothetical SQL-injection or auth bypass on the phone endpoints.

NOTE As of v1.8.0 the WebApi still uses ONE connection string for all operations. This hardening is OPTIONAL today — a future release may split the connection per surface. For now, apply this only if your security policy requires sub-database privilege separation.

To create the role (run as postgres superuser):

```
-- Create the writer role
CREATE ROLE phx_writer WITH LOGIN PASSWORD '<strong-password>';

-- Apply to EACH tenant database (repeat for every tenant)
\c CallAccounting_<TenantCode>

-- Read everywhere (the WebApi still needs to query AcAgents,
-- AcQueues, RealtimeAlertRules, etc. when serving phone XML)
GRANT USAGE ON SCHEMA public TO phx_writer;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO phx_writer;
ALTER DEFAULT PRIVILEGES IN SCHEMA public
    GRANT SELECT ON TABLES TO phx_writer;

-- Write only on phx.*
GRANT USAGE, CREATE ON SCHEMA phx TO phx_writer;
GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA phx
    TO phx_writer;
GRANT USAGE, SELECT ON ALL SEQUENCES IN SCHEMA phx TO phx_writer;
ALTER DEFAULT PRIVILEGES IN SCHEMA phx
    GRANT SELECT, INSERT, UPDATE, DELETE ON TABLES TO phx_writer;
ALTER DEFAULT PRIVILEGES IN SCHEMA phx
    GRANT USAGE, SELECT ON SEQUENCES TO phx_writer;
```

When ready to switch the WebApi over, update the connection string in `appsettings.json` with the `phx_writer` credentials and restart the CallAccounting API app pool. Run the EF migrations under the original superuser BEFORE switching (`phx_writer` cannot CREATE/ALTER tables).

Troubleshooting

Each entry below lists the symptom followed by the corrective steps. Work through them in order.

Installer Prerequisite Checks

Installer shows "MISSING: IIS with ASP.NET features"

Complete Pre-Installation > Step 1a and re-run the installer. Make sure WebSocket Protocol is enabled under Application Development (required for SignalR real-time updates from v1.4.0 onwards).

Installer shows "MISSING: .NET 10 Hosting Bundle"

Download and install the .NET 10 Hosting Bundle from <https://dotnet.microsoft.com/download/dotnet/10.0>. After installing, run:

```
iisreset /restart
```

Then re-run the installer. A reboot may be needed if iisreset does not resolve it. Verify with `dotnet --list-runtimes` — you should see Microsoft.AspNetCore.App 10.0.x.

Installer shows "MISSING: PostgreSQL 14 or higher"

Install PostgreSQL 17 (Pre-Installation > Step 1c) and ensure the service is running:

```
Get-Service postgresql* | Select Name,Status
```

If installed but not detected, ensure the PostgreSQL bin directory is in the system PATH, or restart the computer after installation.

Database Connectivity

Database connection fails during installation

51. Verify PostgreSQL service is running (services.msc)
52. Verify the password is correct:

```
"C:\Program Files\PostgreSQL\17\bin\psql.exe" -U postgres
```
53. Check PostgreSQL is listening on port 5432:

```
netstat -an | findstr 5432
```
54. Check pg_hba.conf allows local connections (default does).

Web Layer

Login page does not load (<http://localhost:8080>)

55. Open IIS Manager > Sites > CallAccounting > Browse
56. Check both app pools are Started: CallAccountingUI, CallAccountingAPI
57. If app pools are Stopped, check install-setup.log for errors
58. Run: `iisreset /restart` (as Administrator)
59. Check C:\inetpub\wwwroot\CallAccounting\api\logs\ for errors

API returns 503 or 500 errors

60. Check CallAccountingAPI app pool is Started in IIS Manager
61. Check API logs: C:\inetpub\wwwroot\CallAccounting\api\logs\

62. Verify PostgreSQL is running: Get-Service postgresql* | Select Name,Status
63. Verify the connection string in appsettings.json is correct

Blank page or UI not loading after upgrade

64. Clear browser cache: Ctrl+Shift+Delete > Cached images and files
65. Hard refresh: Ctrl+F5
66. Blazor WASM files may be cached — clearing cache resolves this

App pool crashes immediately after upgrade

67. Ensure the .NET 10 Hosting Bundle is installed
68. Run: iisreset /restart after installing the bundle
69. Check the Windows Event Viewer > Application log for ANCM errors
70. Verify with: dotnet --list-runtimes (should list 10.0.x)

Collection Service

Collection Service not running / not collecting calls

71. Open Services (services.msc) > CallAccountingCollection > Start
72. Check service logs in C:\CallAccountingData\
73. Verify PBX system is configured: Administration > PBX Systems
74. Check PBX connection status shows Connected in the UI
75. Check raw SMDR files: C:\CallAccountingData\RawSmdr\

Real-Time / Wallboards

Real-Time wallboard shows Disconnected or no live data (v1.4.0+)

76. Administration > Real-Time Settings: confirm the per-site URL, auth method (password grant or client credentials grant), and credentials are correct, and click Test Connection.
77. The status pill should show Connected within a few seconds. If it shows Error, expand the SignalR event log on that page.
78. Confirm the IIS WebSocket Protocol feature is enabled — without it SignalR falls back to long-polling and may stall on some networks.
79. Call Center > Sync Health: confirm ACD systems report Connected and watermark badges are green.

Queue Drill-Down on a digital queue shows an empty table (v1.5.0+)

80. The drill-down resolves agents in this order: designer mapping intersected with override, then override alone, then live presence.
81. Administration > Dashboards: open the dashboard, edit the queue widget, and assign one or more agent groups to the queue under the Mapping section. Save and reload the wallboard.

Phone Display

Administration > Phone Display page shows "License Required" (v1.8.0+)

82. The CA-PD-PHN seat product is missing from the license. Administration > Settings > License: confirm "Phone Display Devices" row exists with a non-zero ceiling.
83. If missing, request a license re-issuance from the License Manager with CA-PD-PHN qty = number of phones to license.

84. Upload the new .lic via Settings > License > Upload.
85. Trial licenses ship with 5 phone seats by default.

Phone registers as Pending but never moves to Active (v1.8.0+)

86. This is normal until an admin approves the phone. Administration > Phone Display > click the Pending row, pick an assignment shape (user-bound or explicit device), then Save.
87. If approval fails with "License limit reached: N/M": you've hit the licensed seat ceiling. Either disable an existing Active phone (frees a seat) or order more CA-PD-PHN seats.

Phone shows "Cannot display" instead of an EVOA screen (v1.8.0+)

88. This is Mitel 6900 firmware 03.02.00.022's response to malformed XML or an unsupported element.
89. Check Content-Type header: EVOA sends "text/xml". A reverse proxy rewriting this to "application/xml" trips the firmware.
90. If a custom integration is sending FormattedTextScreen, that element silently fails on this firmware (HTTP 200 followed by "Cannot display"). EVOA itself does not use it.

Phone registers + polls fine but never receives any alert (v1.8.0+)

91. Almost always a server > phone:80 connectivity issue. The phone-to-server inbound (TCP 443) works because the phone initiates it; the server-to-phone push (TCP 80) requires routing + firewall in the OTHER direction.
92. From the EVOA server: Test-NetConnection -ComputerName <phone-ip> -Port 80 . Expected: TcpTestSucceeded : True
93. If the phone is behind NAT, EVOA pushes to the NAT gateway, not the phone. Give the phone a 1:1 NAT entry or place phones in a directly-reachable subnet.
94. Inspect the phx.PushHistory table for the phone — failed pushes log the exact connection error.

Phone displays squares instead of Arabic / Hindi / Chinese text (v1.8.0+)

By design. The Mitel 6900 firmware font covers Latin-1 + Latin Extended-A only. EVOA automatically falls back to English on the phone for tenants configured to those languages. If you still see squares after the v1.8.0 deploy, restart the WebApi app pool — the Latin-only cap is applied at runtime by the PhoneLocale resolver. The admin UI and TV wallboard remain in the chosen language (they use full OS fonts with complete Unicode coverage).

SNMP / Emergency Alerts

CallAccountingSnmpReceiver service won't start (v1.9.0+)

95. Check who owns UDP 162: Get-NetUDPEndpoint -LocalPort 162 | Select OwningProcess ; Get-Process -Id <pid>
96. If it's the built-in Windows SNMP Trap Service: Get-Service SNMPTRAP | Stop-Service ; Set-Service SNMPTRAP -StartupType Disabled ; Start-Service CallAccountingSnmpReceiver
97. If it's a third-party SNMP manager, stop / reconfigure it to a different port. UDP 162 is hard-coded in MIVB ESM.
98. Check the SNMP Receiver log for the bind error: C:\Program Files\CallAccounting\SnmpReceiver\logs\

SNMP traps not reaching EVOA (v1.9.0+)

99. Confirm the EVOA firewall rule exists: netsh advfirewall firewall show rule name="CallAccounting SNMP Trap"
100. From the MIVB controller, test UDP 162 to the EVOA server. If you can, send a hand-crafted SNMPv2c trap and watch the receiver log.

101. Confirm the MIVB IP is in Administration > Emergency Alerts > Trap Sources. Traps from unlisted sources are silently dropped.
102. Inter-VLAN ACLs / hardware firewalls between MIVB and EVOA must permit UDP 162 in the MIVB > EVOA direction.

Trap arrives at EVOA but recipient phones don't show alert (v1.9.0+)

103. Check Administration > Emergency Alerts > Events for the incoming trap. If the event row is there but with no recipient pushes, the recipient list is empty or all recipients are inactive.
104. Confirm each recipient's assigned phone is in Active status. Only Active phones receive emergency pushes.
105. Check phx.PushHistory for the recipient phone(s) — a "connection refused" or "timeout" points at the server > phone:80 path.

HTTPS Certificate

HTTPS certificate warning in browser

This is normal for the self-signed certificate. In Chrome / Edge: click Advanced > Proceed to <hostname> (unsafe). To suppress permanently, export the certificate from the server and import it into Trusted Root on client machines. For production, replace with a CA-signed certificate in IIS Manager.

Remote Access

Cannot connect from another machine

106. Verify firewall rules (see Accessing EVOA from Other Machines)
107. From the client machine: telnet <server-ip> 8080
108. Check if the server has multiple NICs — IIS binds to all IPs by default

Appendix A: File Locations

Web API binaries	C:\inetpub\wwwroot\CallAccounting\api\
Web UI binaries	C:\inetpub\wwwroot\CallAccounting\ui\
Collection Service	C:\Program Files\CallAccounting\CollectionService\
SNMP Receiver (v1.9)	C:\Program Files\CallAccounting\SnmpReceiver\
Data and backups	C:\CallAccountingData\Backups\
Raw SMDR data	C:\CallAccountingData\RawSmdr\
Reports	C:\CallAccountingData\Reports\
Documentation	C:\CallAccountingData\docs\
API logs	C:\inetpub\wwwroot\CallAccounting\api\logs\
SNMP Receiver logs	C:\Program Files\CallAccounting\SnmpReceiver\logs\
Install logs	C:\CallAccountingData\install-iis.log and install-setup.log

Appendix B: Supported PBX and ACD Systems

PBX Systems (CDR / SMDR Collection)

Vendor	System	Collection Method
Mitel	MiVoice Business (MX / 3300)	TCP Push / TCP Pull
Mitel	MiVoice MX-One	TCP Push / TCP Pull
Mitel	MiVoice Office 400	TCP Push
Unify	OpenScape Voice	TCP Push / SFTP
Unify	OpenScape 4000	TCP Push / TCP Pull
Unify	OpenScape Business	TCP Push
Avaya	Avaya Aura CM	TCP Push
Avaya	Avaya IP Office	TCP Pull
Alcatel-Lucent	OmniPCX Enterprise (OXE)	TCP Push
Alcatel-Lucent	OmniPCX Office (OXO)	TCP Push
Alcatel-Lucent	OpenTouch	TCP Push
Alcatel-Lucent	Alcatel 4400	TCP Push
Cisco	CUCM (Unified CM)	SFTP
Cisco	CME / CUBE	TCP Push (Syslog)

ACD / Contact Center Systems (Real-Time, v1.4.0+)

Vendor	System	Integration
Mitel	Mitel CX (Classic / SIP)	REST + SignalR
Mitel	MIVB-ACD	MSA / MTN SDK (planned, deferred — awaiting MTN partnership)

For PBX-specific configuration details, refer to the in-app help (Administration > Help) or contact MeeraApps Technology support.

Support and Contact

For product support, licensing questions, and technical enquiries:

Publisher	MeeraApps Technology
Email	support@meerapps.com
Website	www.meerapps.com

When opening a support case, please include: the EVOA version (Settings > About in the UI), the Windows Server version, the relevant install log excerpt if the issue occurred at install time, and a clear description of the symptom with the steps to reproduce it.