ORINEX

Workspace

Installation Guide

Version 3.8.2.17

September 2026

Enterprise Google Workspace Administration

ORINEX Systems LLC

Table of Contents

Before You Begin: System Requirements

1. Installing and Configuring GAM
2. Installing ORINEX Workspace
3. First Run Setup Wizard
4. Setting Up Additional Admin Machines
5. Application Settings
6. Updating the Application
7. Troubleshooting Common Issues

Before You Begin: System Requirements

Before installing ORINEX Workspace, verify that your environment satisfies all of the following prerequisites. The application is designed exclusively for Windows and relies on GAM to communicate with Google Workspace APIs.

Operating System

ORINEX Workspace runs only on Windows. Supported versions include Windows 10 (64-bit) and later, as well as Windows Server 2016 and later. The application depends on PyInstaller packaging, Windows system-tray integration, and Windows-specific process management, so Linux and macOS are not supported.

GAM

ORINEX Workspace communicates with Google APIs through GAM. Two builds work, and they share the same code base: GAM7 (the GAM-team project) and GAMADV-XTD3 (the taers232c fork). GAM7 is the continuation of GAMADV-XTD3 -- identical commands, the same gam.cfg, and the same credentials -- so an existing GAMADV-XTD3 installation works unchanged and does not need to be migrated.

For a new installation, use GAM7. GAMADV-XTD3 was retired by its author in favour of GAM7 and its final release (7.05.08, March 2025) is unsigned; GAM7 is still updated and its Windows binaries are code-signed, which makes antivirus and endpoint-protection software far less likely to quarantine it. GAM must be installed separately and fully authorized with OAuth credentials and a service account before ORINEX Workspace can function. Complete GAM setup instructions appear in Chapter 1.

Google Workspace Edition

The following Google Workspace editions are supported. You must hold Super Admin access to the domain you intend to manage. Delegated admin accounts with limited privileges will not have sufficient API access for most operations.

Edition	Support Level
Education Standard / Plus	Fully supported
Education Fundamentals	Supported, except device approval
Business Starter / Standard	Supported, except device approval
Business Plus	Fully supported
Enterprise Standard / Plus	Fully supported
Nonprofits	Supported, except device approval
Essentials	Supported, except Gmail features

Mobile device approval is part of Google's advanced mobile management, which Google includes with Education Standard and Plus, Business Plus, and Enterprise. Blocking a device, remote account wipe, and the

device inventory work on every edition. Essentials has no Gmail, so mailbox features do not apply. Beyond that, what ORINEX Workspace can report follows what your edition exposes through Google's Admin SDK.

Web Browser

ORINEX Workspace presents its interface through a local web server, reached over HTTPS at https://workspace.orinexsystems.com. Any modern browser will work:

- Google Chrome 90 or later (recommended)
- Microsoft Edge 90 or later
- Mozilla Firefox 90 or later

Warning: *Internet Explorer is not supported. JavaScript must be enabled.*

Hardware Recommendations

ORINEX Workspace is lightweight, but it holds all cached Google data in memory, so memory use scales with the size of your domain. The figures below are total system resources, not headroom left over after the operating system.

Resource	Minimum	Recommended (500+ users)
CPU	2 cores	4 cores
RAM	4 GB system memory	8 GB system memory
Disk	2 GB free	5 GB free

Program files take about 55 MB and GAM about another 55 MB. What grows is the audit database. Core installs collect no audit events and it stays empty. Compliance installs on a large domain add roughly 50-100 MB per month, bounded by retention - admin and login events are purged after 90 days, drive events after 30 - so it settles at a few hundred MB. Allow 5 GB free for Compliance, and 10 GB on domains over 5,000 users.

Two things need free space beyond the database itself: compacting it rebuilds the file and temporarily needs free space roughly equal to its finished size, and the application raises a storage warning whenever free space on the volume drops below 2 GB.

Network Requirements

The web server binds to port 443 by default, falling back to port 5000 if another service already holds 443. A Workstation install listens on this machine only; a Server install accepts connections from the local network, so allow inbound traffic on that port to the server. GAM communicates outbound with Google APIs over HTTPS (port 443). The following domains must be reachable:

- accounts.google.com
- oauth2.googleapis.com
- www.googleapis.com
- admin.googleapis.com

- chromedevicemanagement.googleapis.com
- cloudresourcemanager.googleapis.com

> ***Warning:*** *If your organization uses a web proxy or firewall, allow the domains listed above. GAM may fail silently or produce authorization errors when it cannot reach Google APIs.*

If you operate behind a corporate proxy, set the HTTPS_PROXY and HTTP_PROXY environment variables before launching the application:

```
set HTTPS_PROXY=http://your-proxy-server:port
set HTTP_PROXY=http://your-proxy-server:port
```

1. Installing and Configuring GAM

ORINEX Workspace delegates all Google Workspace API communication to GAM. This chapter walks through installing GAM, creating a Google Cloud project, authorizing OAuth credentials, and configuring domain-wide delegation for the service account.

Two builds of GAM work with ORINEX Workspace and they share the same code base: GAM7 (the GAM-team project) and GAMADV-XTD3 (the taers232c fork). GAM7 is the continuation of GAMADV-XTD3, so the commands, the gam.cfg file, and the credentials are identical. This chapter uses GAM7, which is the recommended build for a new installation. If you already run GAMADV-XTD3, everything below applies unchanged -- substitute your own install path for C:\GAM7.

> ***Note:*** *If GAM is already installed and authorized (you can successfully run "gam info domain"), skip ahead to Chapter 2.*

> ***Tip:*** *Set aside about forty minutes and do the whole chapter in one sitting. Several steps hand off between a Command Prompt window and a browser, and one step waits on Google to propagate a change. Work through it in order and it is straightforward; skip ahead and you will be unpicking it later.*

Step 1 is the hardest part and it comes first. It deals with Google Cloud permissions and takes about five minutes. Everything after it is mostly clicking Next and pasting values that GAM prints for you. If Step 1 looks like more than you signed up for, that is a fair reaction -- but it is also the step that prevents the failure most people hit, which is why it is not last.

Step 1 -- Prepare Your Google Workspace

Four settings in the Google Admin Console decide whether the rest of this chapter will work. All four are quick to check, and when one is wrong the failure message you eventually see does not name the real cause. Check them first.

Sign in to admin.google.com as a Super Admin, then go to **Apps** then **Additional Google services**:

1. Find **Google Cloud Platform** in the service list. Its Service status must be **ON**.
2. Open that same Google Cloud Platform entry, expand **Cloud Resource Manager API settings**, and confirm **Allow users to create projects** is turned on.
3. Back on the Additional Google services page, confirm **Access to additional services without individual control** is **On**.

If your Workspace is an Education edition, two more settings apply. Neither exists on a business Workspace, and both will stop project creation:

4. The Super Admin account you are about to use must sit in an organizational unit labelled **18 or older**. An administrator whose account lives in a student OU cannot create Google Cloud projects.

Go to **Account** then **Account settings** then **Age-based access settings**, choose the organizational unit your admin account belongs to from the tree on the left, and set **Age label** to **All users in this group or org unit are 18 or older**. Changes take a few minutes to apply.

> ***Note:*** *Your organization type sets the default for this, so an Education tenant will often have org units labelled under-18 without anyone having chosen that. Check the org unit your admin account sits in rather than assuming.*

5. Under **Apps** then **Google Workspace** then **Classroom**, expand **Data access** and confirm **Users can authorize apps** is checked.

Allow Service Account Key Uploads

> ***Warning:*** *This is the single most common reason GAM setup fails, and it is switched on by default in current Google Cloud organizations. Doing it now takes five minutes. Discovering it later means unpicking a half-configured project.*

GAM authenticates as a service account, and to do that it must upload a key to Google. A Google Cloud organization policy called **iam.disableServiceAccountKeyUpload** blocks exactly that. Until it is turned off, GAM will create your project, enable every API, generate a key -- and then fail on the last step with a constraint violation.

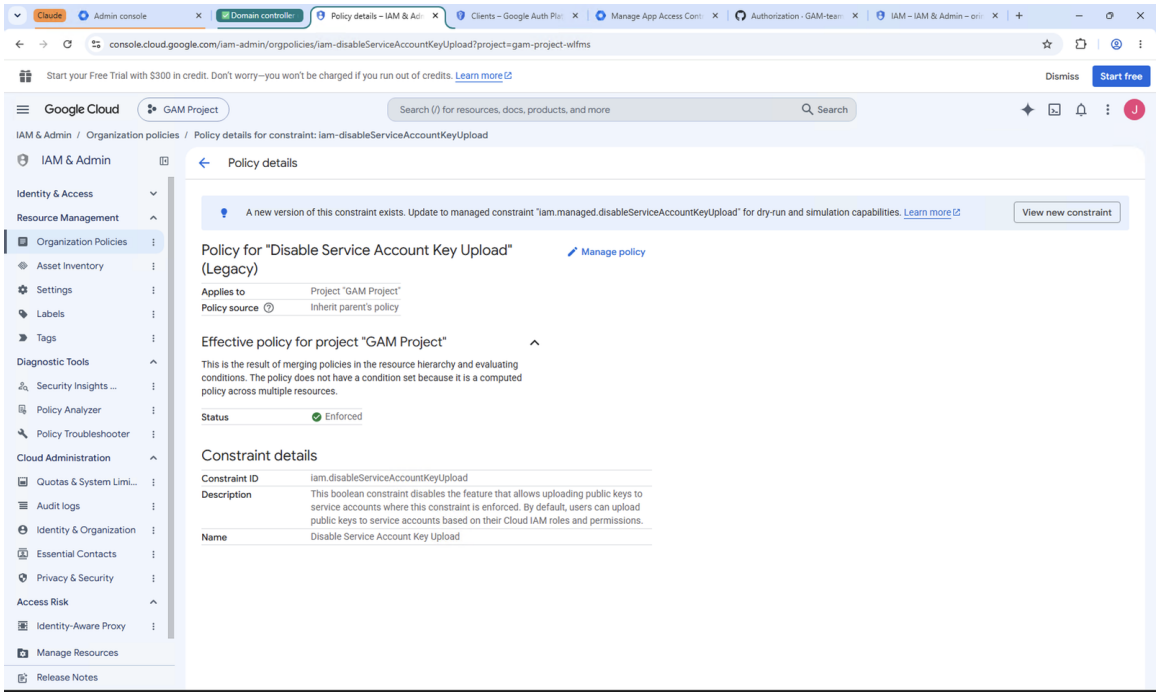
First, give yourself permission to change organization policies. Being a project owner is not enough:

1. Open console.cloud.google.com and go to **IAM & Admin** then **IAM**.
2. Click the resource selector at the top of the page and switch it from your project to your **organization**. The page heading must read "Permissions for organization", not "Permissions for project". This is easy to get wrong and nothing later will warn you about it.
3. Click **Grant access**, enter your admin address as the principal, and in the role filter type **orgpolicy.policyAdmin**. Select **Organization Policy Administrator** and save.

> ***Warning: Organization Administrator*** *is a different role and will not work. Its own description gives it away: it says it can view organization policies. You need the role that can set them.*

Now turn the constraint off. Open the policy directly:

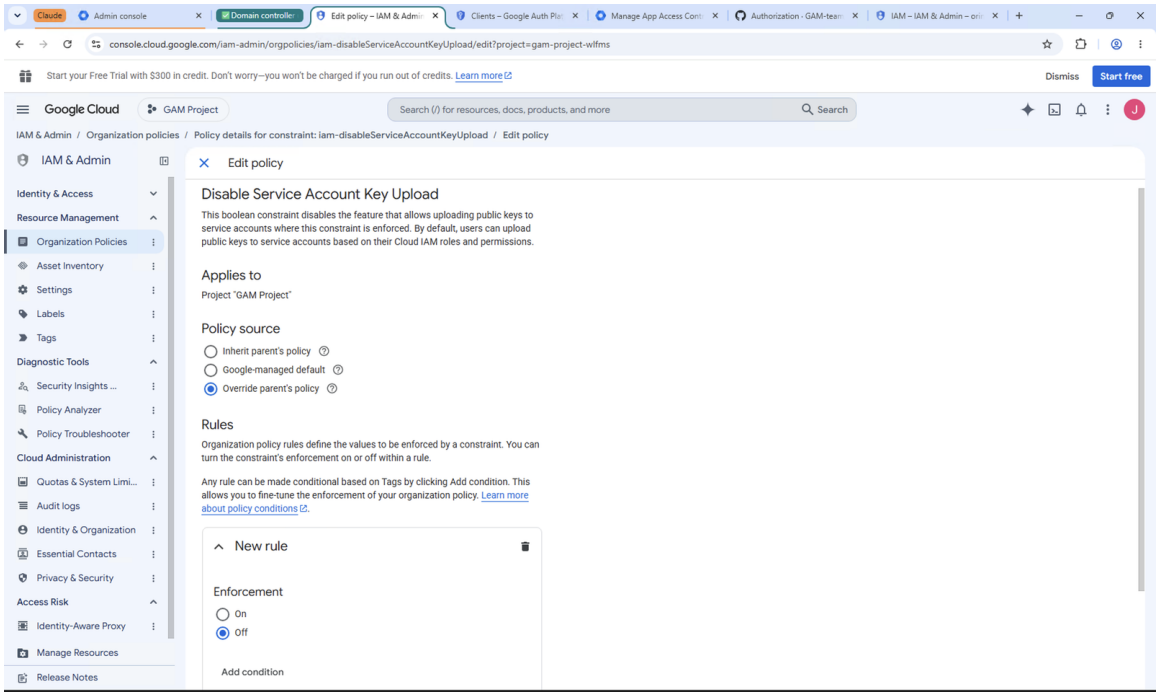
```
https://console.cloud.google.com/iam-admin/orgpolicies/
iam-disableServiceAccountKeyUpload
```



Before: the policy is inherited from the organization and Status reads Enforced. In this state GAM cannot complete setup.

1. Click **Manage policy**. If that link is greyed out, your role grant has not propagated yet -- wait a minute and reload the page.

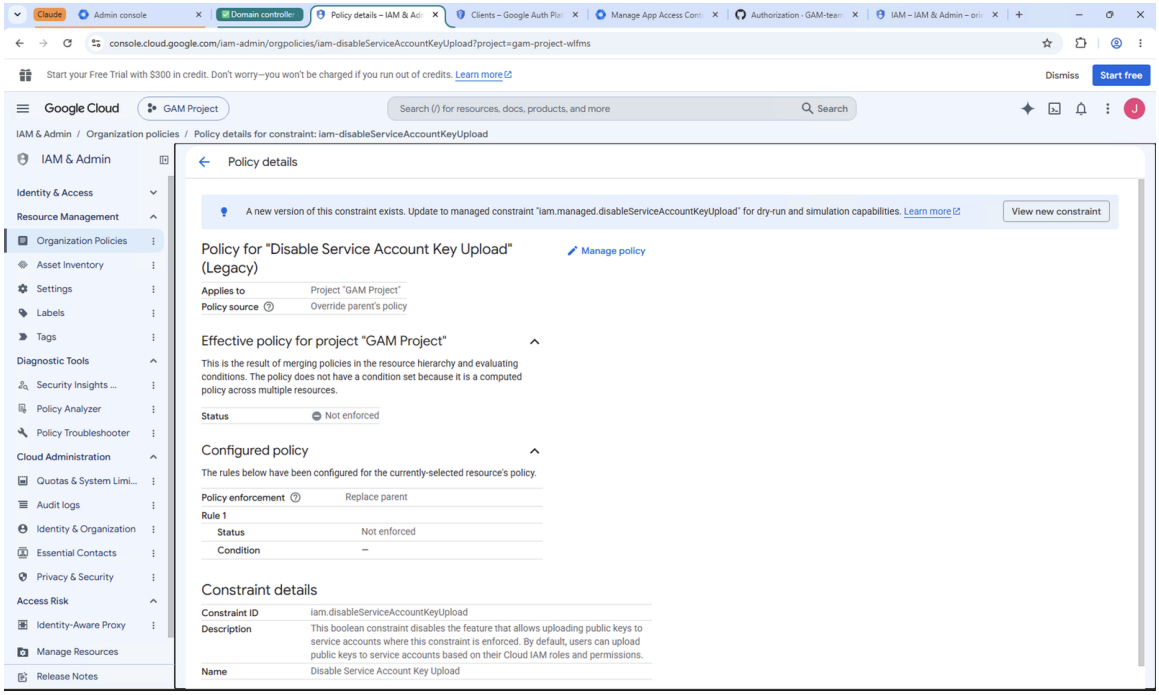
2. Choose **Override parent's policy**, then set the rule's Enforcement to **Off** and save. Some organizations already have an explicit rule here, in which case you are simply switching it from On to Off.



Policy source set to Override parent's policy, with rule Enforcement set to Off.

3. Reload the page and check two fields: **Policy source** should read "Override parent's policy" and **Status** should read **Not enforced**.

> ***Warning:*** *Do not trust the confirmation message. The console displays "Policy updated. It may take a few minutes for these changes to become active" even when the change did not save -- for example if you did not yet hold the role. Reload the page and read Policy source and Status. Those two fields are the only reliable confirmation.*



After: Policy source now reads Override parent's policy and Status reads Not enforced. This is what a successful change looks like.

> ***Note:*** *Filtering the policy list for "disableServiceAccountKeyUpload" returns two entries: iam.disableServiceAccountKeyUpload and iam.managed.disableServiceAccountKeyUpload. Google is migrating between them and both can be active. Override whichever one your error message names. If the error returns after you have changed one, change the other as well.*

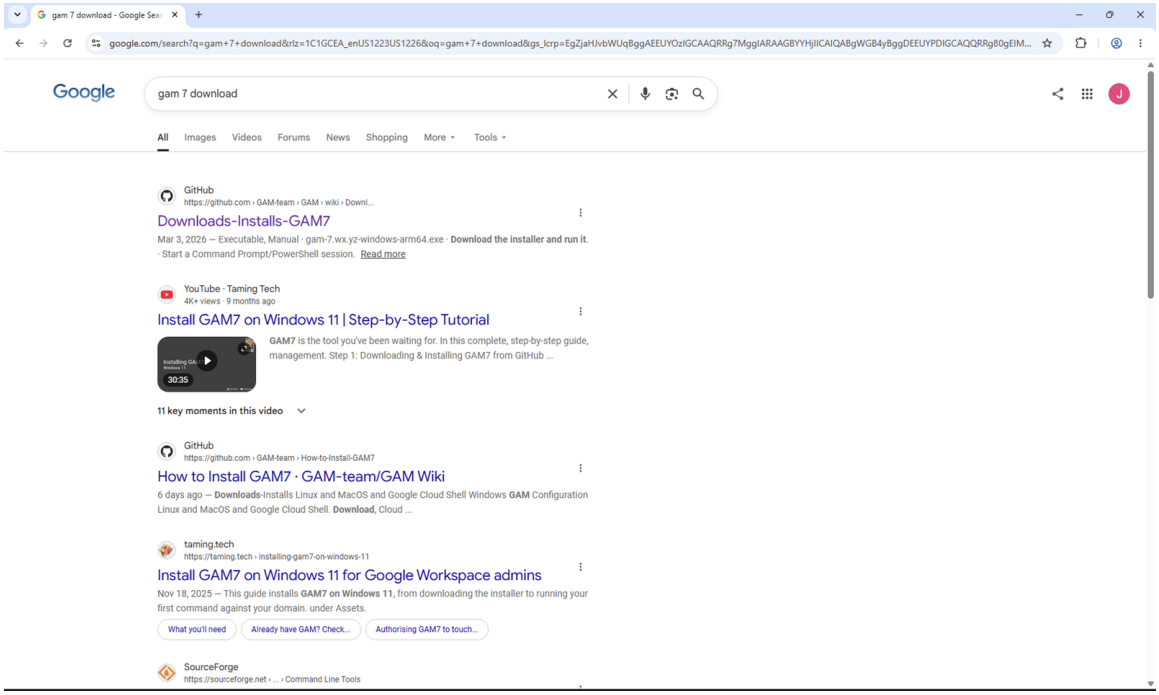
> ***Note:*** *Setting this at the organization level covers every project you will ever create. Setting it on a single project is narrower and is the better choice if your district reviews security changes -- but a project-scoped override is deleted along with the project, so it has to be re-applied if you ever start over.*

Step 2 -- Install GAM

Download GAM only from the official GitHub releases page:

```
https://github.com/GAM-team/GAM/releases
```

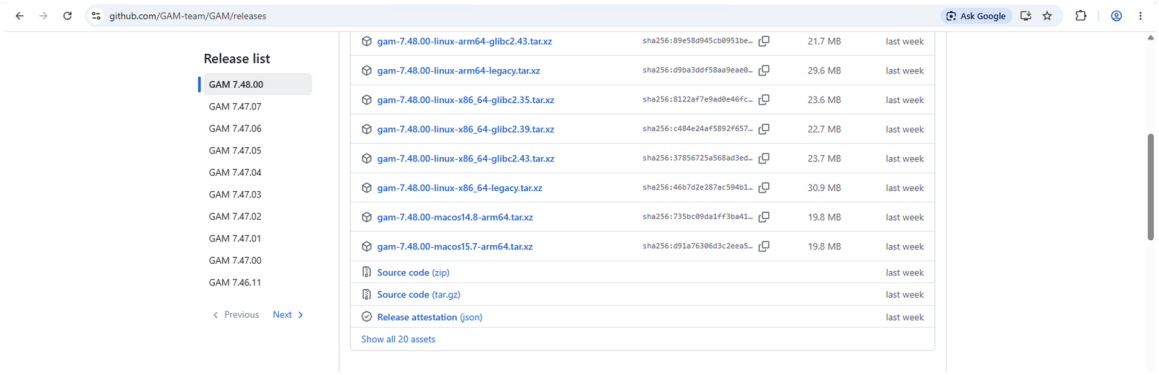
> ***Warning:*** *Searching the web for "GAM download" also returns a SourceForge page. That is the original legacy GAM, not GAM7 -- a different tool with different commands. Use the GitHub releases page above.*



Search results for GAM 7. The GitHub wiki and releases entries are correct; the SourceForge result is the wrong tool.

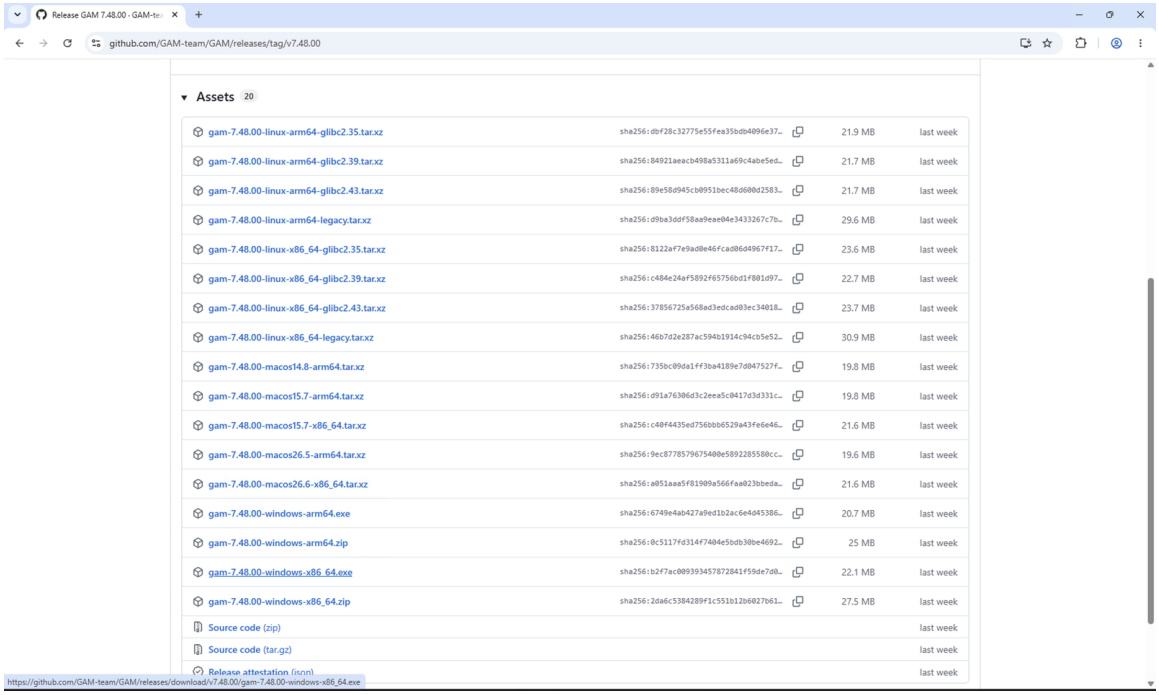
1. On the latest release, scroll to **Assets** and click **Show all assets**.

> ***Warning:*** *GitHub hides most of the file list by default and shows only the Linux and macOS builds. If you do not expand the list you will conclude there is no Windows download. There is -- it is behind that link.*



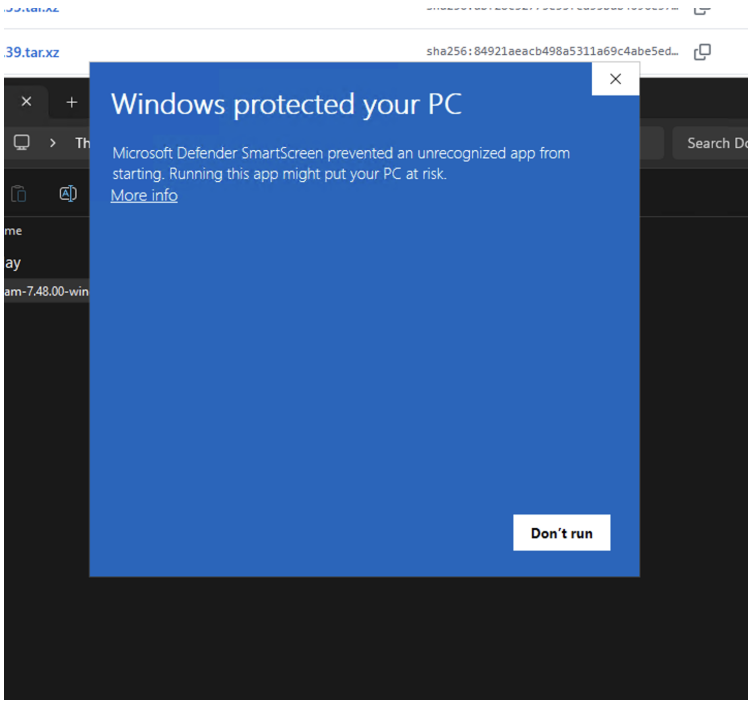
This is what you land on: twelve files, none of them Windows. Click Show all assets.

2. Download **gam-x.xx.xx-windows-x86_64.exe**. Take care with the choice: there are four Windows files. You want **x86_64** rather than arm64 for a standard PC, and the **.exe** installer rather than the .zip archive.



The expanded asset list. Each file also publishes a SHA256 you can check the download against.

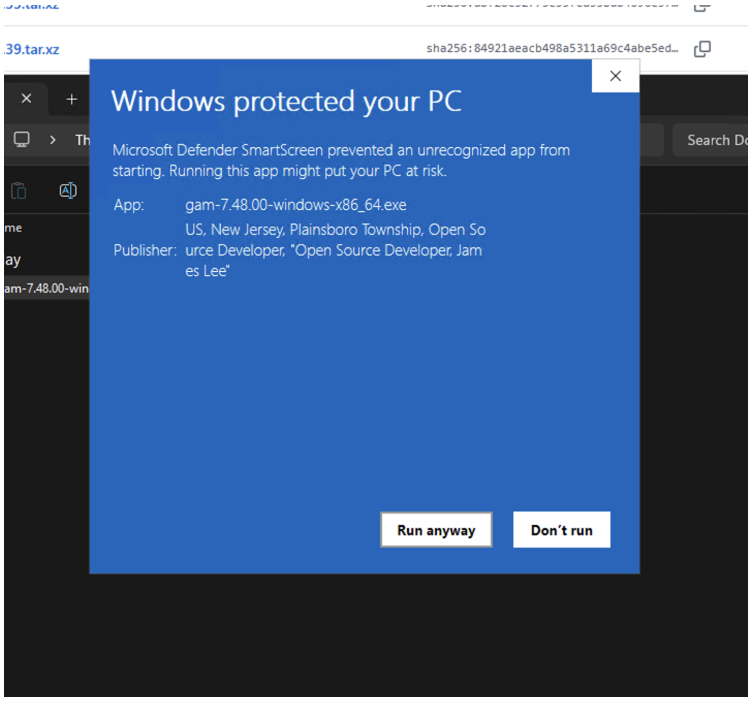
3. Run the installer. Windows will show "Windows protected your PC" and offer only a Don't run button. Click **More info**, then **Run anyway**.



SmartScreen initially hides the option to continue. Click More info.

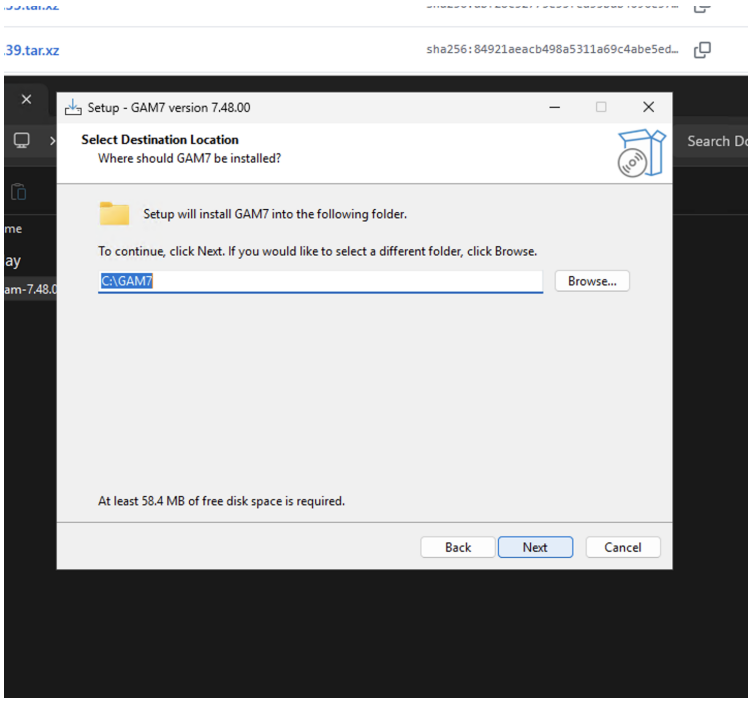
The publisher then reads as an individual open-source developer rather than a company. That is expected: GAM is signed with an open-source developer certificate belonging to its original author. If your security team

needs assurance, compare the SHA256 published beside the download on the releases page against the file you received.



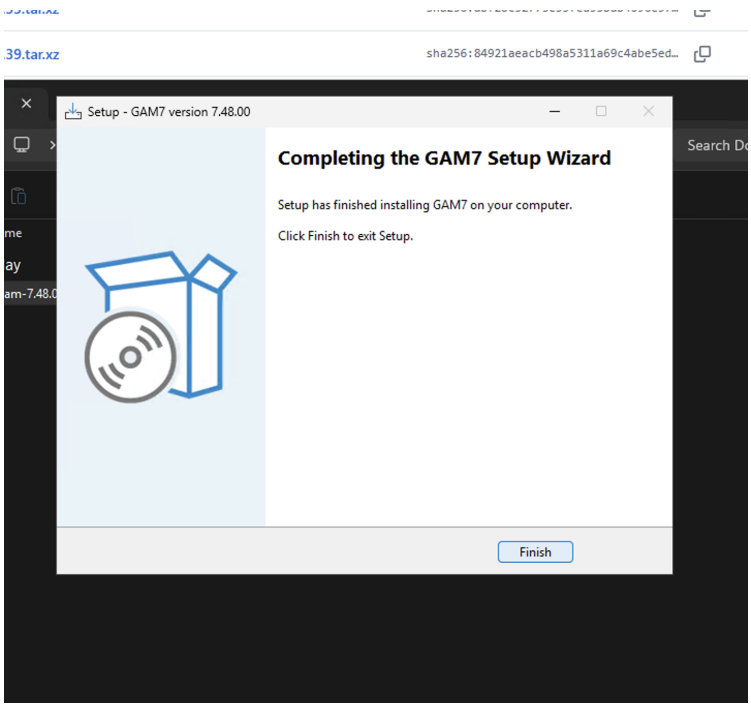
After clicking More info the publisher and a Run anyway button appear.

4. Accept the licence, then accept the default install location of **C:\GAM7**.



The default install location. Any path works; only gam.exe inside it matters.

5. Finish the installer. C:\GAM7 now contains gam.exe and gam-setup.bat.



Installation complete.

Where GAM Keeps Its Files

GAM stores gam.cfg, client_secrets.json, oauth2service.json, and oauth2.txt together in one configuration directory. Left alone it uses C:\Users\<username>\.gam. You can move that somewhere more durable by creating a folder such as C:\GAMConfig and setting a system environment variable named **GAMCFGDIR** to point at it. Keeping credentials outside the program folder means a future GAM upgrade cannot overwrite them.

> ***Note:*** *If you set GAMCFGDIR, do it* ***before*** *running the setup wizard in Step 3, or the credentials will be written to the default location instead.*

> ***Note:*** *If you plan to install ORINEX Workspace in Server mode, use C:\ProgramData\GAM as your GAMCFGDIR -- a machine-wide install needs GAM's credentials somewhere every Windows account on the server can reach. You can also simply install ORINEX Workspace first and let it set the variable for you. Workstation installs are unaffected.*

Step 3 -- Start the Setup Wizard

GAM ships a wizard that runs the whole configuration in order. Open a Command Prompt and run:

```
C:\GAM7\gam-setup.bat
```

1. The first question asks whether to **u**pgrade or set up as **n**ew. Answer **n**.

> ***Warning:*** *Answering* ***u*** *does nothing except print "setup complete" and exit. It is meant for copying credentials from a machine you have already configured. On a first install it looks like success and leaves you with nothing.*

2. Answer **y** to setting up a Google API project, then enter your Super Admin email address.

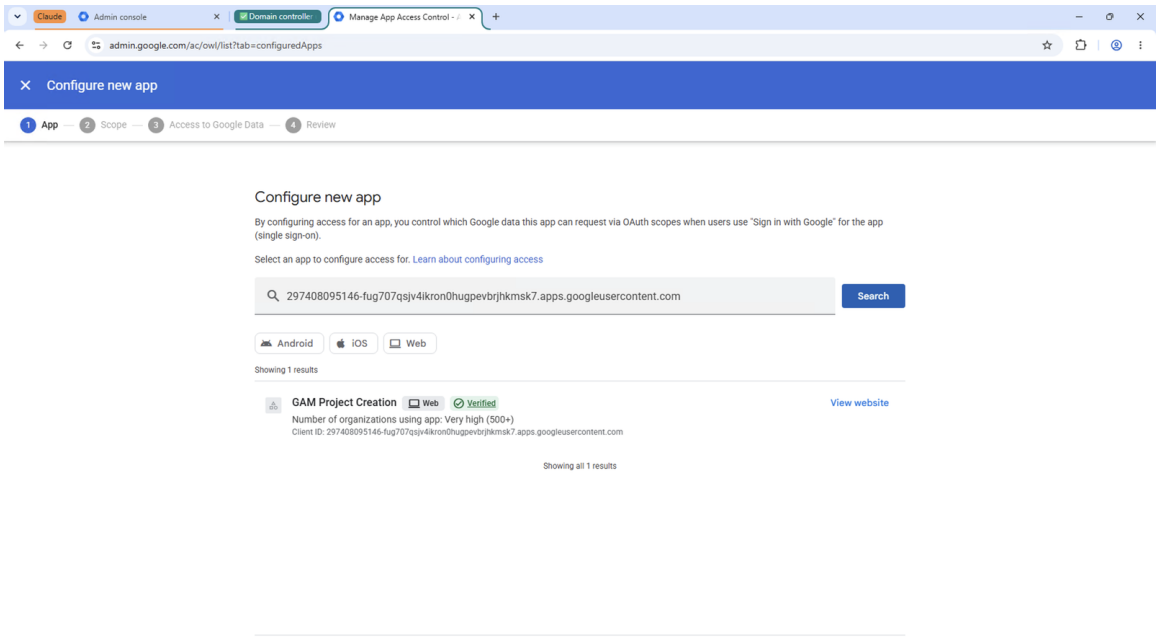
> ***Note:*** *Two warnings about oauth2.txt and oauth2service.json not being found are normal at this point. GAM has not created them yet.*

Trust the GAM Client ID

The wizard pauses and asks you to mark GAM's own Client ID as trusted in the Admin Console. It cannot continue until you do. In the Admin Console go to **Security** then **Access and data control** then **API controls** then **App access control**, and open **Configured apps**:

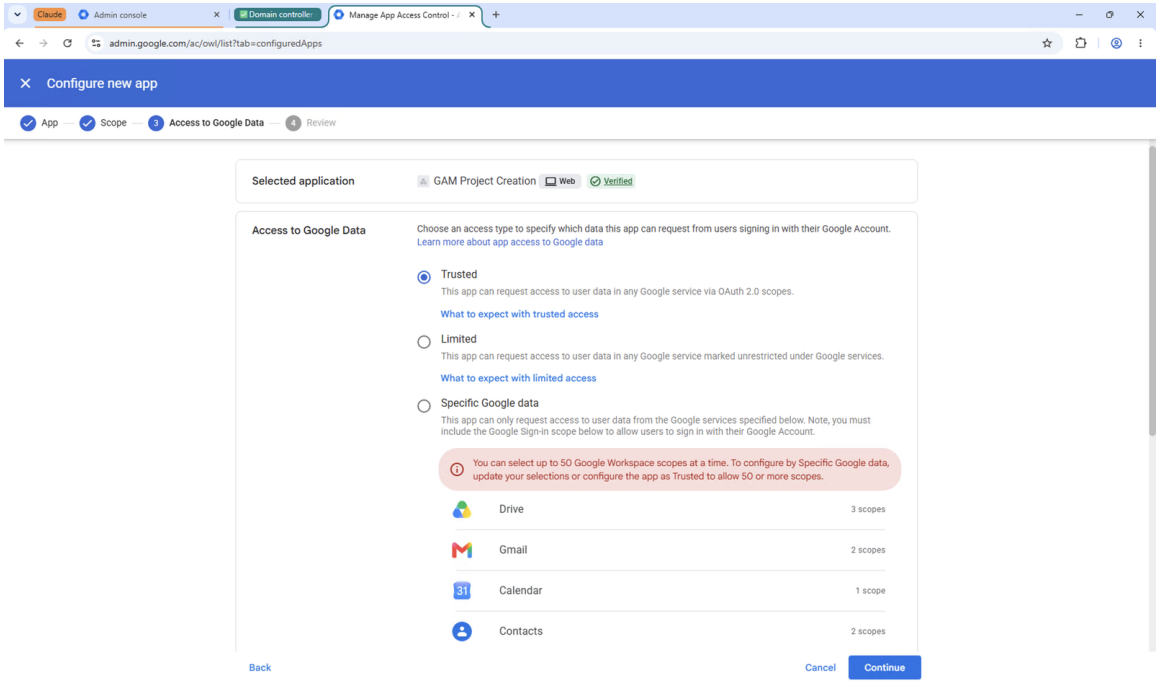
```
https://admin.google.com/ac/owl/list?tab=configuredApps
```

1. Click **Configure new app**, paste the Client ID the wizard printed into the search box, and click **Search**.
2. Select the **GAM Project Creation** result.



Searching by Client ID finds the app. It is published by Google as Verified and shows high organization usage.

3. Leave the scope on your whole organization, click Continue, choose **Trusted**, then Continue and Finish.



Set the access level to Trusted.

4. Return to the Command Prompt and press Enter.

> ***Note:*** *This Client ID is the same for every GAM installation everywhere -- it belongs to the GAM project itself, not to your domain. Copy it from your terminal rather than retyping it.*

5. A browser window opens. Sign in as your Super Admin and click **Allow**. GAM then creates the project and enables around forty APIs, which takes a minute or two.

> ***Tip:*** *If the machine is signed in to more than one Google account, do this in a new Incognito window and pick the Super Admin account deliberately. Silently authorizing as the wrong account is a common and confusing failure.*

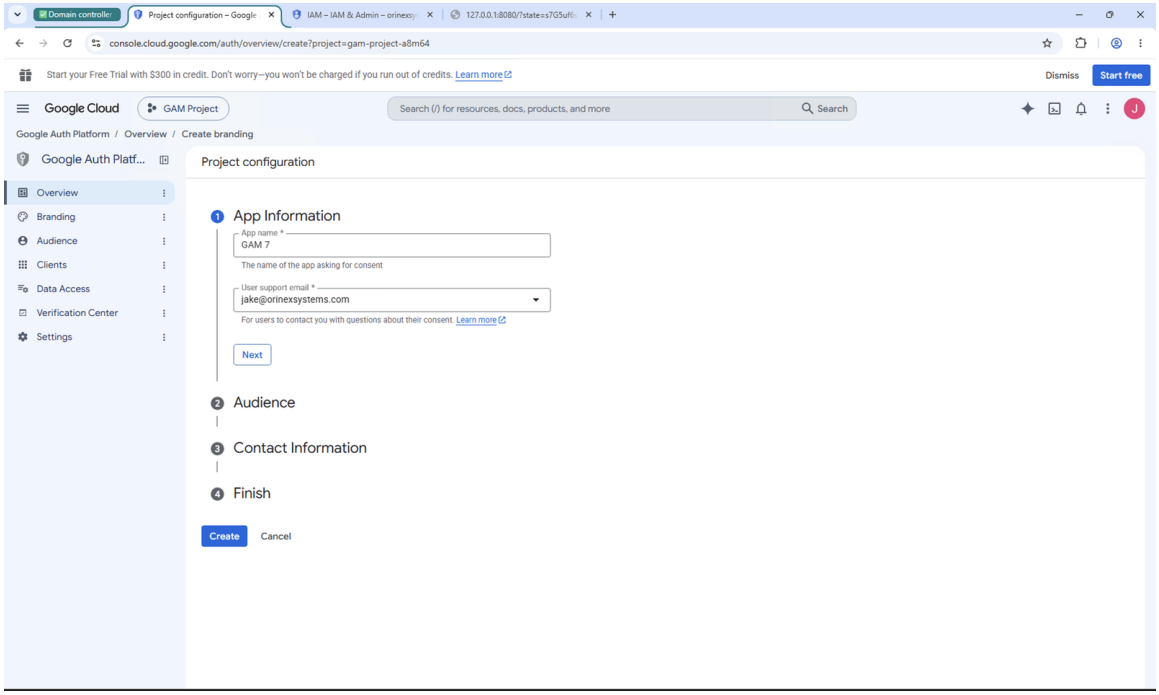
Step 4 -- Create the OAuth Client

The wizard now prints a long list of numbered steps and waits at an "Enter your Client ID" prompt. This part is done by hand in the Google Cloud console, using the link the wizard gives you. If the Clients page already offers a Create client button, skip straight to creating the client.

Otherwise click **Get started** and complete the four short pages with these values:

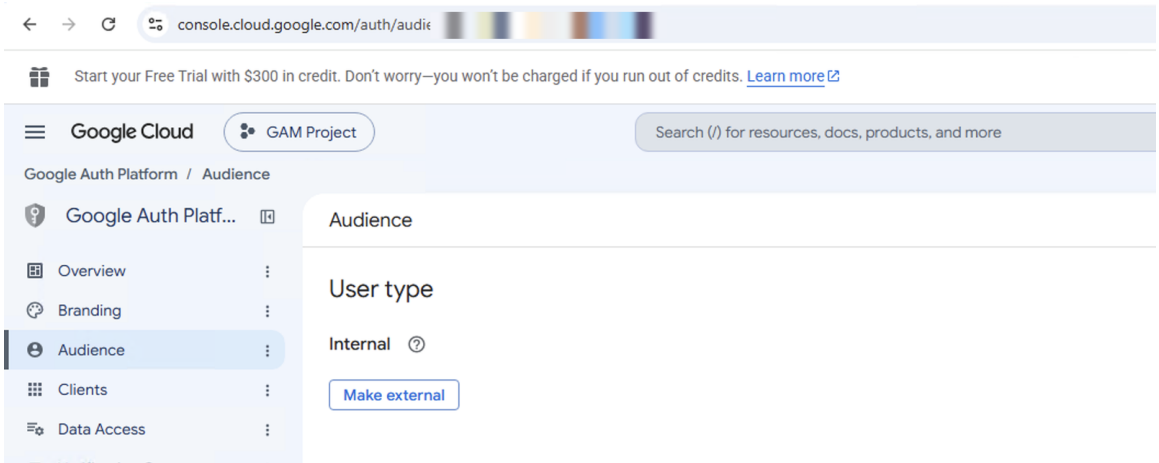
Field	Value
App name	GAM
User support email	Your Super Admin address
Audience	Internal
Contact email	Your Super Admin address

> ***Warning:*** *Choose* ***Internal*** *for Audience. Choosing External puts your app into Google's verification queue, which is a review process you do not need and cannot easily back out of.*



The App Information page. The remaining pages ask for the audience type, a contact address, and agreement to Google's API user data policy.

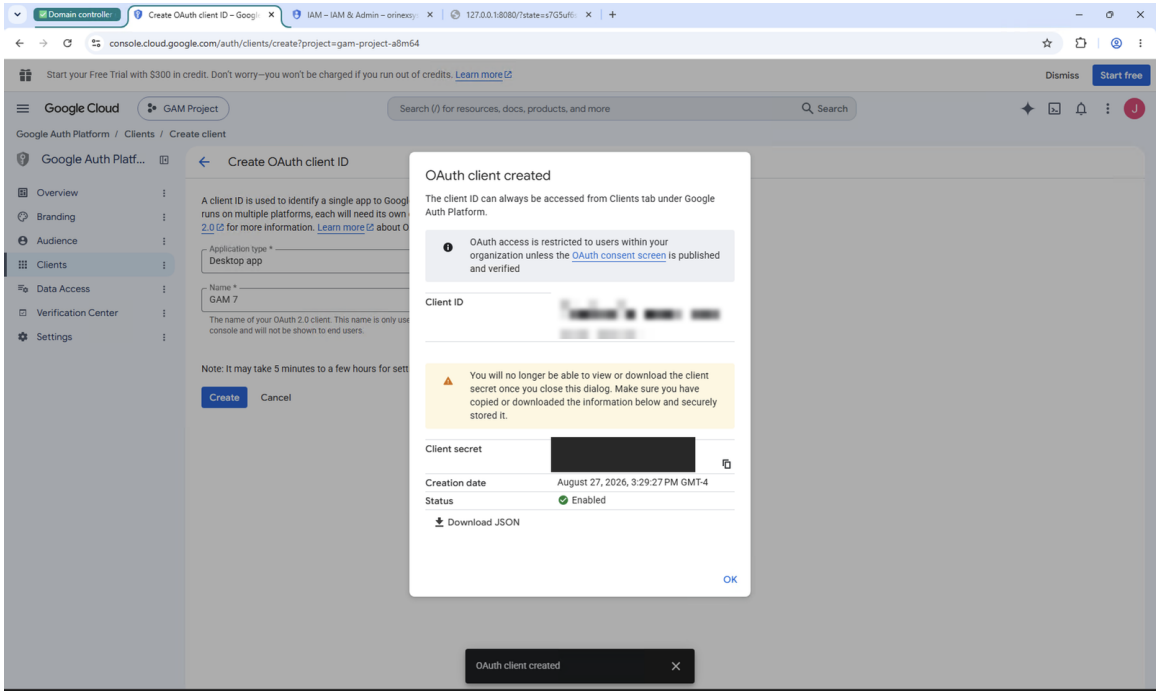
Once the four pages are done, open **Audience** in the left column and confirm it reads **Internal**. If it says External, click Make internal before going any further.



This check is worth doing -- the audience setting decides whether Google puts your app into a verification review.

Then create the client itself:

1. Open **Clients** in the left column and click **Create client**.
2. Set Application type to **Desktop app**, give it the name **GAM**, and click Create.
3. Copy the **Client ID** into the terminal prompt and press Enter, then copy the **Client secret** into the next prompt and press Enter.

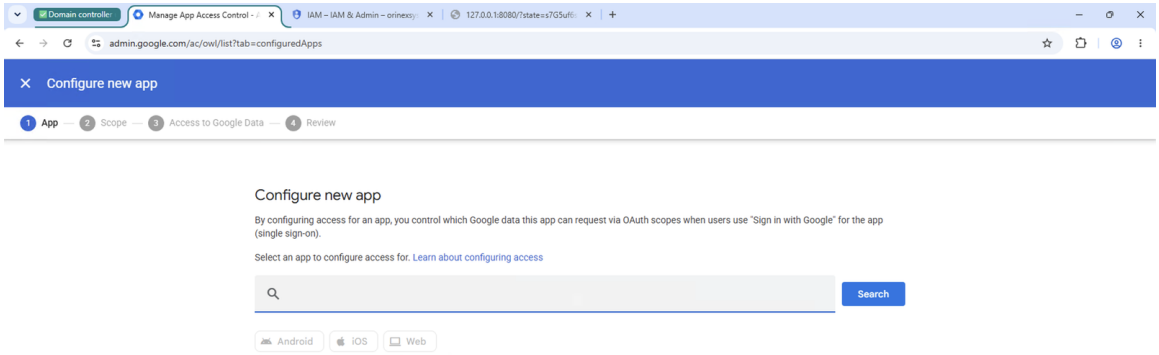


The client is created as a Desktop app. The Client ID and secret shown here are unique to your domain and are obscured in this guide.

> ***Warning:*** *The client secret is displayed only once. If you close the dialog before copying it, delete the client and create a new one.*

Step 5 -- Trust Your Own Client ID

The wizard now asks you to trust a second Client ID -- this time the one you just created. The steps are identical to Step 3, but the Client ID is different and is specific to your domain.



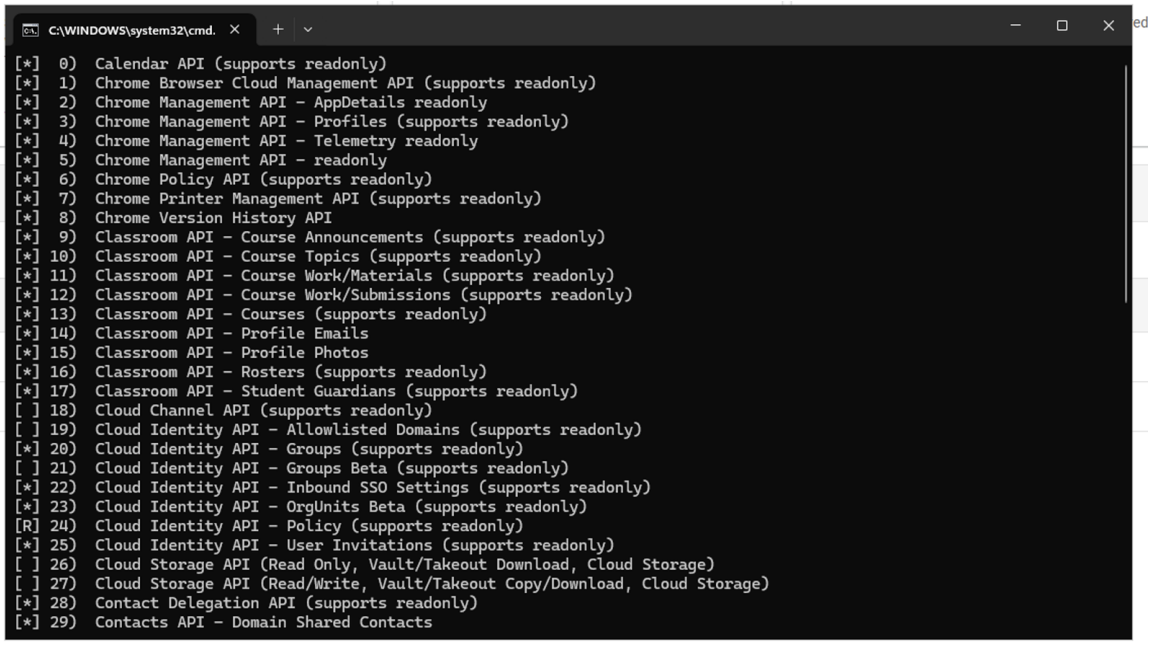
Searching Configured apps for your own Client ID. Unlike GAM's shared client, your client will not carry a Verified badge -- that is normal for an internal app.

> ***Note:*** *Three different Client IDs appear across this chapter and they are handled three different ways. GAM's shared client and your own OAuth client are both marked Trusted in App access control. The service account Client ID, which appears in Step 7, goes to domain-wide delegation instead.*

Step 6 -- Authorize Your Admin Account

Answer **y** when the wizard asks whether to authorize GAM to perform Google Workspace management operations. GAM displays a numbered menu of API scopes with sensible defaults already selected.

1. Type **c** to continue with the default selection. Do not select every scope; that can trigger a Google authorization error.



The scope menu. Entries marked with an asterisk are selected by default and cover what ORINEX Workspace needs.

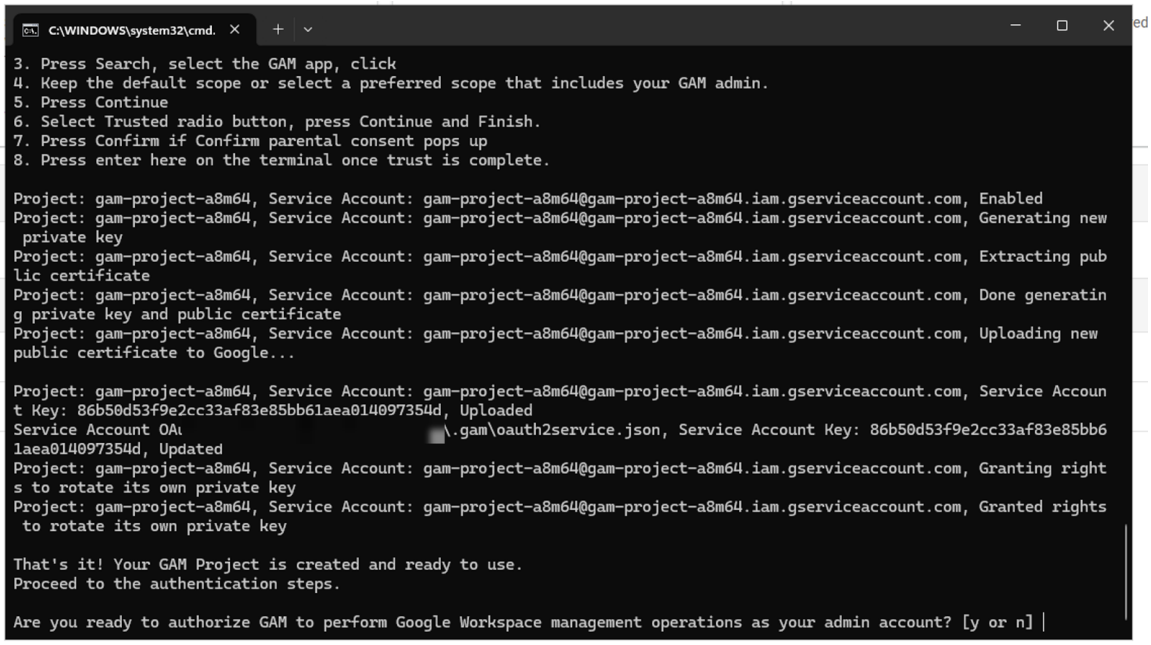
> ***Note:*** *The defaults grant more than ORINEX Workspace uses. That is the documented path and it works, but if your district reviews API grants, the GAM Permissions article in the Help Center lists exactly which scopes are used, cites the code that calls them, and explains how to narrow the grant safely.*

2. A browser window opens. Sign in as your Super Admin and grant consent.

3. The browser lands on a local page reading "The authentication flow has completed." Close it and return to the terminal.

> ***Note:*** *If you authorized on a different computer to the one running GAM, that page will instead fail to load. This is expected -- copy the whole URL out of the address bar and paste it at the terminal prompt.*

GAM then generates the service account key and uploads it to Google. Because you cleared the organization policy in Step 1, this succeeds:



The service account key uploads and GAM reports the project is ready. Without the Step 1 policy change, this is where setup fails.

Step 7 -- Domain-Wide Delegation

The service account lets ORINEX Workspace act on user mailboxes and files in the background without an interactive sign-in. Domain-wide delegation is what grants it that access, and it is the one step Google requires you to perform by hand.

1. Answer **y** when the wizard offers to authorize user data access, then enter the address of an **ordinary user** -- not your Super Admin.

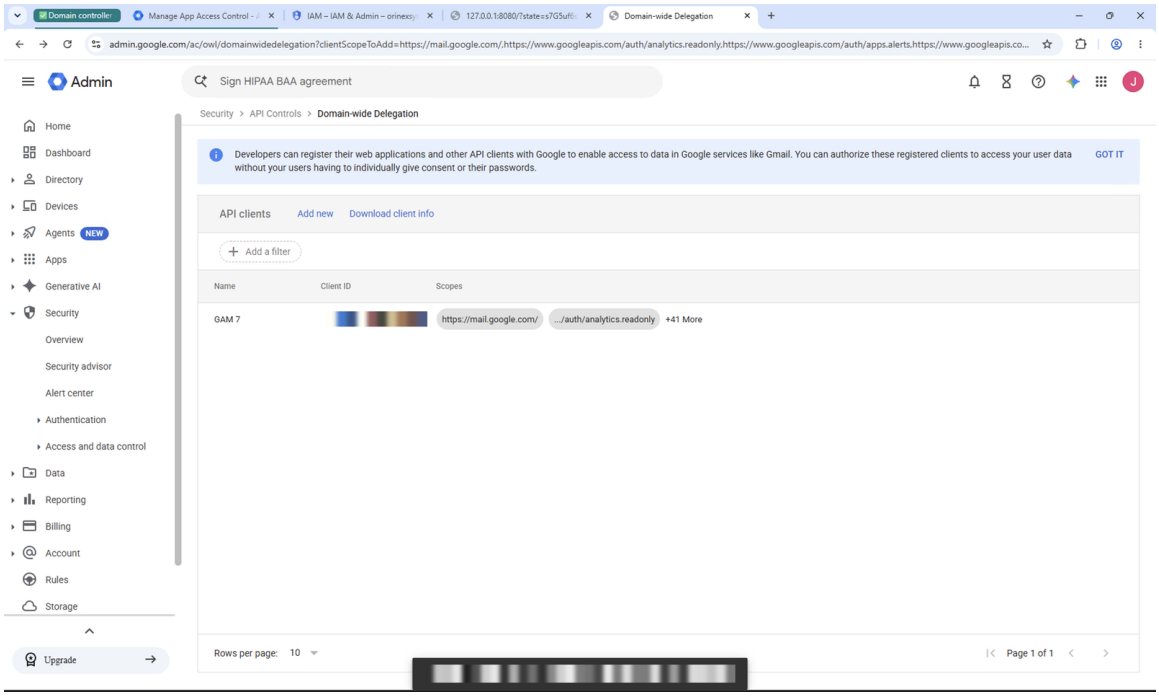
> ***Warning:*** *Use a regular staff mailbox here. GAM's own reference calls for "a non-Google Workspace administrator". Delegation works by impersonating users, so testing against an ordinary account is what actually proves it works.*

2. The check runs and every scope reports **FAIL**. This is expected and the wizard says so -- delegation has not been granted yet.

```
C:\WINDOWS\system32\cmd.

lassroom.guardianlinks.students%20https://www.googleapis.com/auth/classroom.courseworkmaterials%20https://www.googleapis
.com/auth/admin.directory.device.chromebrowsers%20https://www.googleapis.com/auth/userinfo.email%20openid&authuser=0&hd=
orinexsystems.com&prompt=consent HTTP/1.1" 200 91

The authentication flow has completed.
Client OAuth2 File:                                    th2.txt, Created

Are you ready to authorize GAM to manage Google Workspace user data and settings? [y or n] y

Please enter the email address of a regular Google Workspace user: jake@orinexsystems.com
Great! Checking service account scopes. This will fail the first time. Follow the steps to authorize and retry. It can t
ake a few minutes for scopes to PASS after they've been authorized in the admin console.
System time status
  Your system time differs from admin.googleapis.com by less than 1 second  PASS
Service Account Private Key Authentication
  Authentication                                                            PASS
Service Account Private Key age; Google recommends rotating keys on a routine basis
  Service Account Private Key age: 0 days                                   PASS
Domain-wide Delegation authentication:, User: jake@orinexsystems.com, Scopes: 42
  https://mail.google.com/                                                  FAIL (1/42)
  https://www.googleapis.com/auth/analytics.readonly                        FAIL (2/42)
  https://www.googleapis.com/auth/apps.alerts                               FAIL (3/42)
  https://www.googleapis.com/auth/calendar                                  FAIL (4/42)
  https://www.googleapis.com/auth/chat.admin.delete                         FAIL (5/42)
  https://www.googleapis.com/auth/chat.admin.memberships                    FAIL (6/42)
  https://www.googleapis.com/auth/chat.admin.spaces                         FAIL (7/42)
  https://www.googleapis.com/auth/chat.customemojis                         FAIL (8/42)
  https://www.googleapis.com/auth/chat.delete                               FAIL (9/42)
  https://www.googleapis.com/auth/chat.memberships                          FAIL (10/42)
```

The first check always fails. The system time and key authentication checks above it should pass.

3. GAM prints a link. Open it. It leads to the Domain-wide Delegation page with your service account's Client ID and the full scope list already filled in -- click **Authorize** and you are done.



The delegation entry after authorizing, with its scope count. GAM pre-fills this for you; there is no need to paste scopes by hand.

> ***Warning:*** *Delegation changes can take up to fifteen minutes to propagate through Google's systems. A scope that still fails immediately after authorizing is almost always propagation rather than a mistake.*

4. Wait, then answer **y** to retry the check.

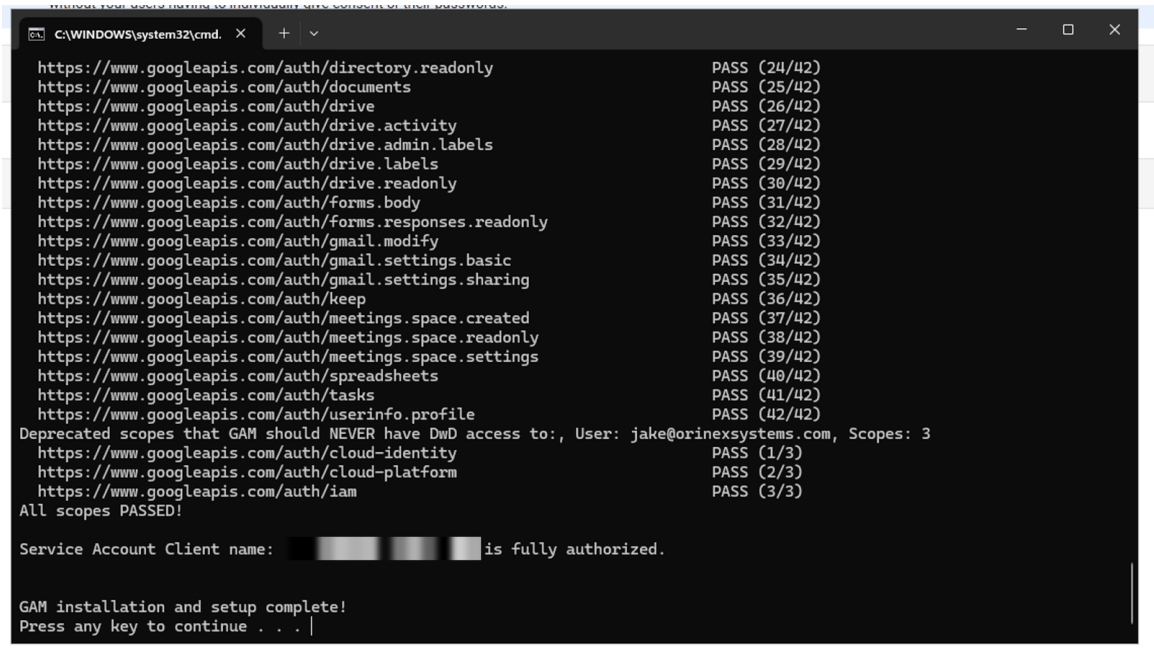
Configuring Delegation by Hand

If the pre-filled link does not open, the same thing can be done manually. Go to **Security** then **Access and data control** then **API controls**, and under Domain-wide delegation choose **Manage Domain Wide Delegation**. Click **Add new**, enter the service account's numeric Client ID, paste the comma-separated scope list GAM printed, and click Authorize.

> ***Note:*** *Use the numeric Client ID, not the service account email address. Entering the email address is the most common mistake here. You can also read the value from the client_id field of oauth2service.json.*

Step 8 -- Confirm It Works

Every scope should now report **PASS** and the wizard finishes.



All scopes pass and the service account is reported as fully authorized. GAM is now configured.

As a final independent check, run:

```
C:\GAM7\gam.exe info domain
```

You should see your domain name, admin email address, user count, and other domain details. Once that works, GAM is ready and you can install ORINEX Workspace.

> ***Note:*** *If some scopes still fail after fifteen minutes, confirm that the Client ID in the delegation entry matches the one GAM printed, and that the scope list was pasted complete. Chapter 7 covers the remaining failure messages.*

2. Installing ORINEX Workspace

ORINEX Workspace is distributed as a Windows installer built with Inno Setup. The procedure below covers downloading, installing, and verifying the application.

Running the Installer

1. Unblock the installer first. Windows marks every file downloaded through a browser, and SmartScreen reacts to that mark until a publisher has built up install history -- our installer is code-signed, but the warning still appears. Right-click the downloaded file, choose **Properties**, tick **Unblock** at the bottom of the General tab, then **OK**. Doing this before you run it avoids the warning entirely.

2. Launch the installer. Double-click the OrinexWorkspace_Setup executable. Administrator privileges are required. If you skipped the unblock step and SmartScreen appears, choose **More info** then **Run anyway** -- confirm the publisher reads **ORINEX Systems LLC** before you do.

3. License agreement. Read and accept the ORINEX Systems license agreement.

4. Installation directory. The default path is C:\Program Files\ORINEX Workspace. You may change this to any location you prefer.

5. Optional tasks. The installer offers two optional settings: a desktop shortcut and automatic startup when you log in to Windows. Select the options you want and proceed.

6. Installation type. Choose Workstation or Server. This choice is permanent for the life of the installation -- to change it later you must uninstall and reinstall. See the table below.

7. Install. The installer writes the application executable and its supporting files. This typically takes under a minute.

8. Launch. When the installer finishes, check the option to launch ORINEX Workspace and click Finish. The application starts as a system tray icon near the clock, and your default browser opens to https://workspace.orinexsystems.com.

Installation Type: Workstation or Server

The installation type determines where ORINEX Workspace keeps its data and how it is reached over the network. It is set once, on the installer's Installation Type page, and is locked on subsequent upgrades.

	Workstation (default)	Server
Intended for	One administrator on a personal workstation	Multiple administrators connecting through a browser
Data directory	%APPDATA%\ORINEX Workspace\	%PROGRAMDATA%\ORINEX Workspace\
Network access	This computer only	Reachable across the local network
Idle timeout	4 hours	30 minutes
Two-factor authentication	Optional; browsers can be trusted for 14 days	Required; every sign-in is challenged
IP allowlist	Not applicable	Available in Settings

> ***Warning:*** *Do not uninstall before an upgrade. Uninstalling clears the deployment-mode marker, and a Server installation reinstalled from scratch will look for its data in the per-user location instead of the machine-wide one. Run the new installer directly over the existing installation.*

Installed Components

Item	Description
OrinexWorkspace.exe	Self-contained executable. The Python runtime, the HTML templates, and the CSS/JavaScript/imag
LICENSE.txt	The ORINEX Systems license agreement
docs\	The Help Center articles served inside the application
static\docs\	The downloadable Administrator Guide and Installation Guide PDFs

Application data -- configuration, databases, and log files -- is stored separately from the program files, in %APPDATA%\ORINEX Workspace\ on a Workstation install or %PROGRAMDATA%\ORINEX Workspace\ on a Server install. That directory holds app_config.json, auth.db, history.db, audit.db, license.json, and log output.

How the Application Runs

ORINEX Workspace operates as a Windows system tray application. The executable starts a local Flask web server (served by Waitress) and fronts it with HTTPS. A tray icon appears near the system clock; right-click it for options such as opening the browser or quitting. Everything runs locally on your machine -- no cloud hosting is involved.

The installer adds a workspace.orinexsystems.com entry to the Windows hosts file pointing at this machine, and installs a matching certificate, so the application opens at https://workspace.orinexsystems.com with no certificate warning. ORINEX Workspace serves on port 443 by default. If another service on the machine already holds port 443, it falls back automatically to port 5000 (https://workspace.orinexsystems.com:5000). The port can be changed in Settings.

Auto-Start on Login

If you selected "Start ORINEX Workspace when you sign in to Windows", a shortcut is placed in your Windows Startup folder. To change this later, press Win+R, type shell:startup, and press Enter. Add or remove the ORINEX Workspace shortcut from that folder. This option runs ORINEX Workspace inside your Windows session: it starts when you sign in and closes when you sign out.

Running as a Background Service (Server installations)

On a server, signing in to Windows is not something you want to depend on. The second startup option, "Run at system startup, independent of user sign-in", registers ORINEX Workspace as a Windows scheduled task that starts about two minutes after the machine boots, before anyone signs in, and keeps running after everyone signs out. Choose this if administrators reach ORINEX Workspace over the network rather than at the console, or if you use Scheduled actions, which need the application running at the scheduled time.

This option appears on Server installations only. On a Workstation installation the application's data is stored per-user, which a service running as the system account cannot read, so the option has no effect there.

Because the service runs outside your session, it cannot display a tray icon of its own. When you sign in, ORINEX Workspace places an icon in the notification area that connects to the running service rather than starting its own copy. Right-click it to open the console, check whether the service is running, start or stop the service (Windows will ask for administrator approval), or close the icon. Closing the icon closes the icon only; the service keeps running.

Stopping the service stops it for everyone using that server, and scheduled actions will not run until it starts again. It restarts automatically at the next system startup, or immediately using Start Background Service.

Verifying the Installation

1. Confirm the ORINEX Workspace icon is visible in the system tray.
2. Open a browser and navigate to https://workspace.orinexsystems.com.
3. You should see the First Run Setup Wizard (on first launch) or the login page.

If the page does not load, verify the application is running, then check whether port 443 is occupied by another process (netstat -ano | findstr :443). If it is, ORINEX Workspace will have fallen back to port 5000 -- try https://workspace.orinexsystems.com:5000 instead. Review the error log at error.log inside your data directory (%APPDATA%\ORINEX Workspace\ on a Workstation install, %PROGRAMDATA%\ORINEX Workspace\ on a Server install).

Uninstalling

Use Add or Remove Programs in Windows Settings, or run the uninstaller from the Start Menu entry. The uninstaller removes the application files, removes the workspace.orinexsystems.com entry from the hosts file, and removes the ORINEX certificate from the Windows Trusted Root store.

> ***Note:*** *Your data is preserved by default so that a reinstall picks up where you left off -- administrator accounts, activity history, audit events, settings, and the license activation all survive. The uninstaller offers a prompt to remove all data from the computer; it defaults to keeping the data, and a silent uninstall never removes it. Choose the wipe only when decommissioning the machine.*

3. First Run Setup Wizard

The first time you open ORINEX Workspace in a browser, an eight-step wizard guides you through the initial configuration. It detects your GAM installation, identifies your Google Workspace domain, activates your license, and creates your first local admin account.

> ***Note:*** *The wizard appears automatically when no completed configuration exists (app_config.json with setup_complete set to true). If setup has already been completed, you will see the login page instead.*

Step 1 -- Welcome

A welcome screen outlines what the wizard will set up and confirms the two prerequisites: an authorized GAM installation and a Google Workspace super-admin account. Click Next to begin.

Step 2 -- GAM Path Detection

The wizard searches common Windows locations for a valid GAM installation: C:\GAM7, C:\GAM, C:\GAMADV-XTD3, C:\Program Files\GAM, and C:\Program Files\GAM7; bin\gam and bin\gamadv-xtd3 under your user profile; any extracted gamadv-xtd3* or GAM7* folder in your Downloads; and any location on your system PATH. If GAM is found, the wizard displays the detected path, version, and configuration directory. Confirm the path is correct and click Next, or click Browse to select the gam.exe binary manually if auto-detection chose the wrong one.

> ***Warning:*** *If the wizard cannot find GAM at all, return to Chapter 1 and complete the GAM installation before proceeding.*

Step 3 -- Domain Detection

The wizard invokes GAM to query your Google Workspace domain (equivalent to running gam info domain). It displays the detected domain name, organization, Customer ID, and total user count. Verify the information is correct and click Next. If the domain shown is incorrect, you can type the correct domain name before proceeding.

> ***Note:*** *A working internet connection is required for this step because GAM contacts Google APIs to retrieve domain information.*

Step 4 -- Deployment Mode

The wizard shows the Workstation or Server choice you made on the installer's Installation Type page. It is displayed here read-only and cannot be changed -- switching modes requires a reinstall. See Chapter 2 for what each mode means.

Server installs get one additional, optional field here: a Server Network Address. Leave it blank -- the default -- and ORINEX Workspace accepts connections on every network interface. Pin it to a specific IP only when the server has multiple network cards and you want ORINEX Workspace to use just one of them. Which workstations may connect is controlled separately, by the IP allowlist in Settings.

Step 5 -- License Activation

Enter the license key that was emailed to the administrator who purchased ORINEX Workspace, then click Validate & Activate. You cannot continue past this step until activation succeeds.

The key is bound to your Google Workspace domain at the time it is issued, so keys cannot be shared between organizations. Activation also binds the key to this machine's fingerprint, consuming one of your seats. Stale seats can be released later from Settings, under Subscription.

> ***Note:*** *Activation requires an internet connection, because the wizard contacts the ORINEX licensing service to validate the key.*

Step 6 -- Admin Account Creation

Create your first ORINEX Workspace admin account. This is your sign-in for the ORINEX Workspace web interface, and it is entirely separate from your Google Workspace account. There are three fields:

Field	Description
Username	Login username for the ORINEX Workspace web interface
Password	Must be at least 12 characters and include at least 3 of the 4 character types: uppercase, lowerca
Confirm Password	Re-type the password to confirm

A live checklist under the password field shows each requirement turning green as you satisfy it, so you can see exactly what is still missing.

> ***Warning:*** *Save this password somewhere secure. There is no self-service password reset. For account recovery, add a second super-admin from the Admins page once you have signed in -- they can reset your password if you lose it.*

Step 7 -- Two-Factor Authentication

The wizard offers to enroll two-factor authentication on the account you just created. Choosing Set up 2FA now displays a QR code to scan with an authenticator app (Google Authenticator, Authy, 1Password, and similar), asks you to verify a code, and then shows your backup codes once. Save the backup codes at that moment -- they are not shown again.

Installation type	2FA at setup	Trusted browsers
Workstation	Optional -- a Skip for now button is offered	A browser can be marked trusted for 14 days
Server	Required -- no skip option is shown	Not available; every sign-in is challenged

> ***Note:*** *If you skip 2FA on a Workstation install you can enable it at any time from My Account.*

Step 8 -- Completion

The wizard saves your configuration and confirms that setup is complete. Click Continue to go straight to the dashboard -- the wizard signs you in automatically, so no separate login is needed the first time.

> ***Note:*** *On a Server install, ORINEX Workspace restarts itself at this point. The network address chosen in Step 4 cannot take effect without a restart, so the wizard triggers one and waits for the application to come back up before handing you the Continue button. No manual quit-and-relaunch is needed.*

After the Wizard

Once you log in, the dashboard appears. The application begins its initial data sync automatically in the background, populating user, device, group, and license data from Google Workspace. A sync indicator appears in the header while this is in progress. Depending on domain size, the initial sync may take several minutes.

From the dashboard you can view domain statistics, manage users and devices, manage groups and organizational units, and export data to CSV.

Changing Settings After Setup

The setup wizard runs only once. To change configuration afterward, open the Settings page from the navigation menu. To completely reset the application, quit ORINEX Workspace from the tray icon, delete app_config.json and auth.db from your data directory, and start it again -- the wizard will reappear. The data directory is %APPDATA%\ORINEX Workspace\ on a Workstation install and %PROGRAMDATA%\ORINEX Workspace\ on a Server install.

> ***Warning:*** *Resetting this way discards your admin accounts. Audit events (audit.db) and the admin action log (history.db) are left untouched, and your license activation (license.json) survives, so the wizard will not ask for the key again.*

> ***Warning:*** *Resetting the application deletes all local accounts and saved settings. GAM credentials and your Google Workspace data are not affected.*

4. Setting Up Additional Admin Machines

When other administrators need to run GAM or ORINEX Workspace from their own workstations, you do not need to repeat the full Google Cloud project and delegation setup. Instead, copy the existing credentials and have each admin authorize their own OAuth token.

Procedure

1. Install GAM on the new machine following Step 1 from Chapter 1.

2. Copy the following three files from your GAM configuration directory (C:\GAMConfig if you followed Chapter 1) into the new machine's configuration directory:

- client_secrets.json
- oauth2service.json
- gam.cfg

Warning: *Do not copy oauth2.txt. That file is the personal access token created by your own authorization, and each administrator must hold their own -- step 4 below generates it for them.*

3. Open gam.cfg on the new machine and update any paths inside it so they point at that admin's directories rather than yours -- drive_dir in particular.

4. Run **gam oauth create** on the new machine so the administrator can authorize with their own Super Admin account. This generates a personal OAuth token while reusing the shared project and service account.

5. Verify with **gam info domain** to confirm the setup is working.

6. Install ORINEX Workspace on the new machine using the standard installer (Chapter 2) and complete the First Run Setup Wizard (Chapter 3).

Note: *The Google Cloud project, service account, and domain-wide delegation are shared across all machines. Each admin only needs their own OAuth token.*

5. Application Settings

The Settings page provides configuration options for GAM integration, data synchronization, email alerts, and operational monitoring. Only administrators can access this page.

General Configuration

Setting	Description
GAM Executable Path	Full path to your gam.exe binary
Default OU	Default Organizational Unit used for queries (usually /)
Command Timeout	Maximum seconds to wait for a GAM command to complete
Max Results	Maximum number of results returned by GAM list commands
Sync Interval	How often (in minutes) cached data is refreshed automatically (range: 5-120, default: 15)

Tip: *For large environments, set the command timeout to 300-600 seconds. Operations such as listing all users or transferring Drive files in a large domain may need the additional time.*

Note: *The sync interval setting takes effect immediately after saving. No restart is required.*

Sync Behavior

ORINEX Workspace caches Google Workspace data in memory for fast access. Three sync mechanisms keep the data current:

- **Initial sync** -- triggered automatically on first launch or when the cache is empty.
- **Periodic sync** -- after the initial sync, the system checks elapsed time on every cache-status poll (every 5 seconds) and starts a new sync when the configured interval has elapsed.
- **Manual sync** -- click the Sync button in the header bar to trigger an immediate full refresh at any time.

Email Alert Settings

Configure SMTP settings to enable email notifications for security alerts from the audit module.

Setting	Description
SMTP Host	Hostname of your SMTP server (e.g., smtp.gmail.com)
SMTP Port	Port number (587 for TLS, 465 for SSL)
SSL/TLS	Enable SSL/TLS encryption
SMTP Auth	Enable authentication (reveals username/password fields)
SMTP Username	Authentication username

Setting	Description
SMTP Password	Authentication password
From Email	Sender address for outgoing notifications
Default Notify Email	Default recipient for alert notifications
Enable email alerts	Master on/off switch for all alert emails; per-rule toggles pick which rules send, and any severity is

After saving SMTP settings, click Send Test Email to verify the configuration. A test message is sent to the configured recipient. If the test fails, an error message describes the issue (connection refused, authentication failed, and so on).

> ***Warning:*** *If SMTP is not configured or the test fails, email notifications will not be delivered. Alerts will still appear within the application interface.*

GAM Status and Data Cache

The Settings page includes a GAM status panel indicating whether GAM is connected (green) or not found (red), along with the detected version. A Data Cache panel shows the current status for each data type (users, devices, OUs, groups, mobile, licenses), including item counts and last-refresh timestamps. Individual Refresh buttons allow re-fetching a specific data type, and Refresh All triggers a full cache refresh.

Command History

The Settings page displays the 20 most recent GAM commands executed by the application, including timestamp, command string, and success/failure status. This is useful for troubleshooting failed operations and auditing administrative actions.

6. Updating the Application

This chapter covers updating ORINEX Workspace to a new version while preserving your configuration, local accounts, and audit history.

Before You Update

Always back up your data files before applying an update. Your data directory is %APPDATA%\ORINEX Workspace\ on a Workstation install, or %PROGRAMDATA%\ORINEX Workspace\ on a Server install. Copy these:

- app_config.json -- settings
- auth.db -- administrator accounts
- history.db -- activity log and undo history
- audit.db -- audit events and alert rules
- license.json -- licence activation

```
set DATA_DIR=%APPDATA%\ORINEX Workspace
copy "%DATA_DIR%\app_config.json" "%DATA_DIR%\app_config.json.backup"
copy "%DATA_DIR%\auth.db" "%DATA_DIR%\auth.db.backup"
copy "%DATA_DIR%\audit.db" "%DATA_DIR%\audit.db.backup"
```

Warning: *Do not skip the backup step. If the update introduces a schema change, you may need these files to roll back.*

Standard Update Procedure

1. **Exit the running application.** Right-click the ORINEX Workspace icon in the system tray and select Exit.
2. **Run the new installer.** Double-click the new setup executable. It detects the existing installation, upgrades the files in place, and preserves your deployment mode, settings, accounts, and history automatically.
3. **Launch the application.** Start ORINEX Workspace from the Start Menu or desktop shortcut. It will automatically pick up your existing configuration and databases.

Warning: *Do NOT uninstall before updating. Uninstalling clears the deployment-mode marker, and a Server installation reinstalled from scratch looks for its data in the per-user location instead of the machine-wide one -- so its administrator accounts, licence activation, and audit history all appear to have vanished. Run the new installer straight over the existing installation.*

What Is Preserved During Updates

Item	Location	Preserved?
Application settings	app_config.json in the data directory	Yes
Local user accounts	auth.db in the data directory	Yes
Activity log and undo history	history.db in the data directory	Yes
Audit events and alert rules	audit.db in the data directory	Yes
Licence activation	license.json in the data directory	Yes
Deployment mode	Set by the installer, locked on upgrade	Yes
In-memory cached data	RAM	No (rebuilt on next sync)
GAM configuration and tokens	GAM installation directory	Yes

Verifying the Update

After launching the updated application, perform these checks:

1. Log in with your admin account to confirm auth.db was preserved.
2. Open Settings and verify GAM path, SMTP configuration, and sync interval.
3. Check the dashboard for user counts, device counts, and GAM health.
4. Navigate to the activity log and confirm historical entries are present.
5. Send a test alert email from Settings to verify SMTP connectivity.
6. Perform a low-impact action (search for a user, view a group) to confirm normal operation.

Rolling Back

If the update causes problems, quit ORINEX Workspace from the tray icon, uninstall the new version, install the previous one, and restore app_config.json, auth.db, history.db, audit.db, and license.json from your backup copies. Launch the application and verify everything works as expected.

> ***Warning:*** *Rolling back is the one case where you do uninstall, and it clears the deployment-mode marker. If this is a Server installation you must re-select Server on the Installation Type page when installing the older version -- the page otherwise defaults to Workstation, which points the application at the per-user data location and hides everything it had.*

7. Troubleshooting Common Issues

WinError 87: The parameter is incorrect

This error can appear in server logs when GAM commands fail intermittently. It is a known interaction between PyInstaller's --noconsole build mode and Windows subprocess handling. The application handles this automatically through the _safe_run() and _safe_popen() functions, which catch WinError 87 and retry the subprocess call without the problematic flags. No action is typically required.

If the error occurs repeatedly without recovery, verify the GAM executable path in Settings is correct, confirm the GAM installation is not corrupted by running gam version from a command prompt, and ensure only one instance of ORINEX Workspace is running.

Error 403: Insufficient Permission

This error means the OAuth tokens used by GAM do not include the required API scopes. Re-authorize GAM by running gam oauth create, selecting the default scopes, and completing the authorization flow with a Super Admin account. Restart ORINEX Workspace after re-authorizing.

unauthorized_client

This error indicates that domain-wide delegation has not been configured for the GAM service account. Open the Google Admin Console, navigate to Security > Access and data control > API controls > Domain-wide Delegation. Add the service account's numeric Client ID with the required scopes. Wait two to five minutes for propagation, then verify with gam user admin@yourdomain.com check serviceaccount.

charmap codec can't decode

This Unicode error occurs when GAM output contains non-ASCII characters (such as accented names) and the Windows system encoding is not UTF-8. To resolve it, set the PYTHONUTF8 environment variable to 1 at the system level:

1. Open System Properties > Environment Variables.
2. Under System variables, click New.
3. Set Variable name to PYTHONUTF8 and Value to 1.
4. Restart ORINEX Workspace.

database is locked

This SQLite error arises when multiple threads or processes compete for write access. Verify that WAL mode is enabled on the database (it should be by default). Ensure only one instance of ORINEX Workspace is running by checking the system tray for duplicate icons. Both databases have busy_timeout configured, so transient lock contention usually resolves automatically. If the database appears permanently locked, exit the application, delete the -wal and -shm files from %APPDATA%\ORINEX Workspace\, and restart.

Command timed out

Operations may time out during initial sync or when listing large datasets. Increase the command timeout in Settings (300-600 seconds is recommended for large environments, or 900+ seconds for domains with over 50,000 users). The initial cache population is the slowest operation; subsequent requests are served from the in-memory cache.

GAM not found

If ORINEX Workspace reports that GAM is not found or the health indicator shows red, verify that GAM works from the command line (gam version). Update the GAM path in Settings to the full path of the executable and save. The health indicator should turn green.

Data is loading

This message appears while the initial sync is still in progress. After startup, ORINEX Workspace needs to fetch all data from Google Workspace before the interface is fully populated. Wait for the sync to complete -- progress is shown on the dashboard. If the message persists for more than ten minutes, check the GAM health indicator, review the error log, and try clicking the Sync button in the header to force a manual refresh.

Error 429: Rate Limit Exceeded

Google imposes API rate limits (1,500 queries per 100 seconds for the Directory API, 600 per minute for Chrome OS). GAM includes built-in retry logic with exponential backoff, so transient 429 errors usually resolve on their own. If the errors persist, increase the sync interval in Settings, avoid triggering multiple simultaneous syncs, and stagger large bulk operations.

Quick Reference

Error	Likely Cause	Quick Fix
WinError 87	PyInstaller noconsole issue	Handled automatically
403: Insufficient Permission	Missing OAuth scopes	gam oauth create
unauthorized_client	No domain-wide delegation	Configure in Admin Console
charmap codec error	Windows encoding	Set PYTHONUTF8=1
database is locked	Multiple instances	Ensure single instance; check WAL
Command timed out	Timeout too low	Increase in Settings
GAM not found	Wrong path	Set correct path in Settings
Data is loading	Sync incomplete	Wait for sync to finish
429: Rate Limit	Too many API calls	Increase sync interval