

Google Workspace Integration Guide

Complete Step-by-Step Instructions for ilminate Integration

Table of Contents

1. [Overview](#)
 2. [Prerequisites](#)
 3. [Step-by-Step Integration](#)
 4. [Configuration Options](#)
 5. [Verification & Testing](#)
 6. [Troubleshooting](#)
 7. [Security & Permissions](#)
 8. [Advanced Configuration](#)
-

Overview

ilminate integrates with Google Workspace using Gmail API and OAuth 2.0 authentication with domain-wide delegation. This integration allows ilminate to:

- Monitor incoming emails in real-time
- Analyze messages for threats using APEX detection engines
- Move suspicious emails to quarantine labels
- Provide detailed threat reports and analytics

Key Benefits:

- No MX record changes required
- Email flow remains unchanged
- Works with Gmail and Google Workspace
- Reversible actions (no permanent deletions)
- Full audit trail of all actions

Integration Method: Gmail API with OAuth 2.0 service account and domain-wide delegation

Prerequisites

Before starting the integration, ensure you have:

Required Access

- **Super Administrator** role in Google Workspace
- Access to Google Admin Console (`admin.google.com`)
- Access to Google Cloud Console (`console.cloud.google.com`)

Required Information

- Google Workspace domain name
- Organization unit (OU) structure (if using OUs)
- List of users to protect (optional for initial setup)

Technical Requirements

- Google Workspace subscription (Business Standard or higher)
- API access enabled for your domain
- Network access to Google APIs

Pre-Integration Checklist

- ☐ Verify Super Admin access
 - ☐ Note your domain name
 - ☐ Identify pilot group (recommended: 5-10 users)
 - ☐ Review current email security settings
 - ☐ Ensure API access is enabled
 - ☐ Check for conflicting email security policies
-

Step-by-Step Integration

Step 1: Contact ilminate to Begin Setup

1. Navigate to Integration Page

- Go to `https://www.ilminate.com/integration`

- Select "Google Workspace" platform card

2. Request Setup Link

- Click "Start Google Workspace Setup" button
- Fill out contact form with:
 - Your name and email
 - Company name
 - Google Workspace domain
 - Preferred contact method

3. Receive Setup Instructions

- ilminate will send you setup instructions
- Includes service account details
- Contains domain-wide delegation configuration

Step 2: Configure Domain-Wide Delegation

Domain-wide delegation allows ilminate's service account to access user data on behalf of your organization.

1. Access Google Cloud Console

- Go to `https://console.cloud.google.com`
- Sign in with your Super Admin account
- Select your organization's project (or create one)

2. Create Service Account (if not already created by ilminate)

- Navigate to **IAM & Admin** → **Service Accounts**
- Click **"Create Service Account"**
- Name: `ilminate-email-security`
- Description: `Service account for ilminate email security integration`
- Click **"Create and Continue"**

3. Grant Domain-Wide Delegation

- In Service Account details, click **"Show Domain-Wide Delegation"**
- Check **"Enable Google Workspace Domain-wide Delegation"**
- Note the **Client ID** (you'll need this)

4. Configure OAuth Scopes in Google Admin Console

- Go to `https://admin.google.com`
- Navigate to **Security** → **API Controls** → **Domain-wide Delegation**
- Click **"Add new"**
- Enter the **Client ID** from step 3
- Enter OAuth Scopes:

```
https://www.googleapis.com/auth/gmail.readonly
https://www.googleapis.com/auth/gmail.modify
https://www.googleapis.com/auth/gmail.settings.basic
```

- Click **"Authorize"**

5. Share Service Account Details with ilminate

- Provide ilminate with:
 - Service account email address
 - Client ID
 - Confirmation that delegation is configured

Step 3: Grant Initial Authorization

1. Receive Authorization Link from ilminate

- ilminate will provide a Google OAuth authorization link
- This link initiates the consent flow

2. Sign In and Authorize

- Click the authorization link
- Sign in with your **Super Admin** account
- Review requested permissions:
 - View and manage Gmail messages
 - Modify Gmail settings

- Click **"Allow"** or **"Authorize"**

3. **Confirm Authorization**

- You'll see: "Authorization successful"
- You'll be redirected back to ilminate
- Connection status should show "Connected"

Step 4: Configure User Selection

1. **Access ilminate Dashboard**

- Log in to your ilminate portal
- Navigate to **Settings** → **Integrations** → **Google Workspace**

2. **Choose Protection Scope**

Option A: Pilot Group (Recommended)

- Select 5-10 users for initial testing
- Choose users from different departments
- Include executives and regular users
- **Why:** Allows you to verify functionality before full deployment

Option B: Organizational Unit (OU)

- Select specific OUs in Google Workspace
- Choose departments (e.g., Finance, HR, Sales)
- Apply to entire OUs
- **Why:** Phased rollout reduces risk

Option C: Entire Organization

- Select all users in domain
- Apply organization-wide
- **Why:** Immediate full protection (use after pilot validation)

3. **Configure User Filters** (Optional)

- Exclude specific users if needed
- Set up inclusion/exclusion rules
- Apply to groups (if using groups)

Step 5: Set Protection Mode

1. **Navigate to Protection Settings**

- Go to **Settings** → **Protection Mode**

2. **Choose Initial Mode**

Mode 1: Observe (Recommended for First Week)

- **What it does:** Logs threats but doesn't move emails
- **Use case:** Testing and validation
- **Duration:** 1-2 weeks recommended
- **Benefits:**
 - See what would be blocked
 - Verify detection accuracy
 - No impact on email delivery

- Build confidence in the system

Mode 2: Quarantine

- **What it does:** Moves suspicious emails to "ilminate – Quarantine" label
- **Use case:** Active protection
- **When to use:** After Observe mode validation
- **Benefits:**
 - Automatic threat removal
 - Users can review quarantined items
 - Reversible actions

Mode 3: Tag

- **What it does:** Adds warning labels to risky emails
- **Use case:** User awareness without blocking
- **When to use:** For low-risk items or user training
- **Benefits:**
 - Users see warnings
 - Emails still delivered
 - Educational value

3. Configure Quarantine Settings

- Set quarantine label name: `ilminate – Quarantine` (default)
- Configure label color (recommended: Red or Orange)
- Set up release workflow

- Enable user notifications

Step 6: Verify Integration

1. Check Connection Status

- In ilminate dashboard, verify "Connected" status
- Check last sync time (should be recent)
- Verify user count matches your selection

2. Send Test Email

- Send a test phishing email to a protected user
- Use ilminate's test email generator (if available)
- Or send from external address with suspicious characteristics

3. Verify Detection

- Check ilminate dashboard for threat detection
- Verify email appears in quarantine (if Quarantine mode enabled)
- Review threat details and reason codes

4. Check Gmail

- Log in to protected user's Gmail
- Verify "ilminate – Quarantine" label exists
- Check that test email has quarantine label (if applicable)

Configuration Options

User Selection Options

By Individual User:

- Select specific users from directory
- Manually add/remove users
- Best for: Small teams, specific individuals

By Organizational Unit (OU):

- Select OUs from Google Workspace structure
- Apply to entire OUs
- Best for: Department-based protection

By Group:

- Select Google Groups
- Apply to group members
- Best for: Team-based deployment

By License Type:

- Filter by Google Workspace license
- Best for: License-based deployment

Protection Modes Explained

Observe Mode:

Email Arrives → illuminate Analyzes → Threat Logged →
Email Delivered **Normally**

- No email movement
- Full logging and reporting
- Zero impact on users
- Best for: Initial testing

Quarantine Mode:

Email Arrives → illuminate Analyzes → Threat Detected →
Label Applied → Moved to Quarantine

- Automatic threat removal
- User can review and release
- Reversible actions
- Best for: Production protection

Tag Mode:

Email Arrives → illuminate Analyzes → **Warning Label** Added
→ Email Delivered **with Label**

- Visual warnings for users
- No email movement
- Educational value

- Best for: Low-risk items, training

Advanced Settings

Threat Thresholds:

- Configure confidence levels for automatic quarantine
- Set different thresholds for different threat types
- Example: Quarantine BEC at 85% confidence, phishing at 90%

Notification Settings:

- Email alerts for admins
- User notifications for quarantined items
- Daily/weekly summary reports

Label Configuration:

- Customize quarantine label name
 - Set label color and visibility
 - Configure label permissions
-

Verification & Testing

Initial Verification Checklist

- [] Domain-wide delegation configured
- [] OAuth authorization granted successfully

- [] Connection status shows "Connected"
- [] Users appear in illuminate dashboard
- [] Quarantine label created in test user's Gmail
- [] Test email detected and logged/quarantined
- [] Dashboard shows threat details correctly

Testing Scenarios

Test 1: Basic Detection

1. Send email with obvious phishing characteristics
2. Verify detection in dashboard
3. Check quarantine label (if enabled)
4. Review threat details and reason codes

Test 2: BEC Detection

1. Send email impersonating executive
2. Verify BEC detection
3. Check for executive impersonation reason code
4. Verify quarantine action (if enabled)

Test 3: False Positive Check

1. Send legitimate business email
2. Verify it's NOT flagged
3. Check it arrives in inbox normally
4. Confirm no false positive in dashboard

Test 4: Release Workflow

1. Quarantine a test email
2. Log in to user's Gmail
3. Review quarantined email
4. Remove quarantine label
5. Verify release action logged

Performance Verification

Check Processing Time:

- Monitor dashboard for detection latency
- Verify emails processed within seconds
- Check for any delays or backlogs

Check API Health:

- Review Gmail API status
 - Check for throttling or rate limits
 - Verify connection stability
-

Troubleshooting

Common Issues and Solutions

Issue 1: "Domain-Wide Delegation Failed"

Symptoms:

- Error: "Access denied" or "Insufficient permissions"
- Service account cannot access user data
- Authorization fails

Solutions:

1. **Verify Delegation Configuration:**

- Google Admin Console → Security → API Controls → Domain-wide Delegation
- Verify Client ID is correct
- Check OAuth scopes are exactly as specified
- Ensure "Authorize" button was clicked

2. **Check Service Account:**

- Google Cloud Console → IAM & Admin → Service Accounts
- Verify service account exists
- Check domain-wide delegation is enabled
- Verify Client ID matches Admin Console

3. **Verify Super Admin:**

- Ensure you're using Super Admin account
- Check account has necessary permissions
- Try signing out and back in

Issue 2: "Authorization Failed" or "Consent Denied"

Symptoms:

- Error when authorizing
- "Access denied" message
- Cannot complete OAuth flow

Solutions:

1. Check Admin Permissions:

- Verify Super Admin role
- Check account is not suspended
- Ensure account has API access

2. Review OAuth Scopes:

- Verify requested scopes are authorized
- Check domain-wide delegation scopes match
- Ensure no conflicting policies

3. Clear Browser Cache:

- Clear cookies and cache
- Try incognito/private mode
- Use different browser

Issue 3: "Connection Failed" or "Cannot Connect"

Symptoms:

- Dashboard shows "Disconnected" status

- Error: "Unable to connect to Google Workspace"
- API errors in logs

Solutions:

1. **Verify Network Connectivity:**

- Check firewall rules allow Google APIs
- Verify proxy settings (if applicable)
- Test connectivity to `gmail.googleapis.com`

2. **Check API Access:**

- Google Admin Console → Security → API Controls
- Verify "Gmail API" is enabled
- Check API access settings for your domain

3. **Verify Service Account:**

- Check service account is active
- Verify credentials are valid
- Check for expired keys

Issue 4: "Users Not Appearing"

Symptoms:

- No users listed in dashboard
- Selected users don't show up
- "No users found" message

Solutions:

1. Check User Selection:

- Verify users have Gmail enabled
- Check users are not suspended
- Ensure users are in correct OU (if using OUs)

2. Verify Permissions:

- Check domain-wide delegation scopes
- Verify service account has access
- Check for organizational unit restrictions

3. Refresh Sync:

- Click "Refresh" or "Sync Now" in dashboard
- Wait for sync to complete (may take several minutes)
- Check sync status and errors

Issue 5: "Emails Not Being Detected"

Symptoms:

- Test emails not showing in dashboard
- No threats detected
- Quarantine label not applied

Solutions:

1. Verify Protection Mode:

- Check protection mode is enabled
- Verify users are selected
- Confirm protection scope includes test user

2. **Check Email Flow:**

- Verify emails are arriving in Gmail
- Check Gmail filters and rules
- Ensure no other security products intercepting

3. **Review Detection Settings:**

- Check threat thresholds
- Verify detection engines are enabled
- Review detection logs for errors

Issue 6: "Quarantine Label Not Created"

Symptoms:

- Quarantine mode enabled but no label
- Emails not being labeled
 - "Label not found" errors

Solutions:

1. **Manual Label Creation:**

- Log in to user's Gmail
- Create label: "ilminate – Quarantine"

- Set label color (recommended: Red)
- Verify label is visible

2. **Check Permissions:**

- Verify gmail.modify permission granted
- Check service account has label creation rights
- Review API permissions

3. **Retry Label Creation:**

- Disable and re-enable quarantine mode
- Trigger manual sync
- Check for label creation errors in logs

Getting Help

ilminate Support:

- Email: `support@ilminate.com`
- Phone: `910 760-3146`
- Portal: `apex.ilminate.com`

Google Support:

- Google Workspace Admin Help Center
 - Google Cloud Support (for API issues)
 - Gmail API Documentation
-

Security & Permissions

Permissions Explained

gmail.readonly

- **Purpose:** Read email content and metadata
- **Scope:** All selected users
- **What it does:** Evaluates emails for threats
- **Security:** Read-only access, no modifications

gmail.modify

- **Purpose:** Read and modify emails
- **Scope:** All selected users
- **What it does:** Applies labels and moves threats
- **Security:** Limited to labeling, no deletion

gmail.settings.basic

- **Purpose:** Access Gmail settings
- **Scope:** All selected users
- **What it does:** Creates labels and filters
- **Security:** Label management only

Security Best Practices

1. **Least Privilege:**

- Only grant necessary scopes
- Scope to specific users when possible
- Use organizational units for large deployments

2. **Service Account Security:**

- Use service account keys securely
- Rotate keys regularly
- Store keys in secure key management system

3. **Monitoring:**

- Review audit logs regularly
- Monitor for unusual API activity
- Set up alerts for permission changes

4. **Regular Reviews:**

- Review permissions quarterly
- Remove unused access
- Update scopes as needed

Data Handling

What ilminate Accesses:

- Email headers (From, To, Subject, Date)
- Email body content
- Attachments (scanned, not stored)
- Metadata (message ID, thread ID)

What ilminate Does NOT Access:

- Calendar items
- Contacts
- Drive files
- Chat messages
- Meet recordings

Data Storage:

- Threat metadata stored securely
- Email content not stored long-term
- Processing happens in-region when possible
- Full audit trail maintained

Data Retention:

- Threat logs: 90 days (configurable)
 - Quarantined emails: 30 days (configurable)
 - Audit logs: 1 year (compliance requirement)
-

Advanced Configuration

Organizational Units (OUs)

Setup:

1. Google Admin Console → Directory → Organizational Units

2. Create or select OU
3. Assign users to OU
4. Apply ilminate settings to OU

Benefits:

- Scope permissions to specific groups
- Easier management for large organizations
- Gradual rollout capability

Google Groups

Using Groups:

1. Create Google Group for pilot users
2. Add users to group
3. Apply ilminate protection to group
4. Manage protection via group membership

Benefits:

- Easy user management
- Dynamic membership
- Group-based policies

API Quotas & Limits

Gmail API Limits:

- 1,000,000 quota units per day

- 250 quota units per user per 100 seconds
- ilminate handles throttling automatically

Monitoring:

- Check dashboard for quota warnings
- Review API usage metrics
- Adjust if needed

Service Account Key Management

Best Practices:

- Use key rotation (every 90 days recommended)
- Store keys securely (not in code)
- Use Google Cloud Secret Manager
- Limit key access

Key Rotation:

1. Create new service account key
2. Update ilminate with new key
3. Verify connection works
4. Delete old key after verification

Next Steps

After successful integration:

1. **Monitor Dashboard:**

- Review threats daily for first week
- Check for false positives
- Verify detection accuracy

2. **Tune Settings:**

- Adjust threat thresholds if needed
- Configure notifications
- Set up reporting schedules

3. **Expand Protection:**

- Add more users after pilot validation
- Roll out to additional OUs
- Consider full organization deployment

4. **Training:**

- Train users on quarantine label
- Explain release workflow
- Share threat awareness resources

5. **Ongoing Management:**

- Review monthly reports
 - Update protection settings as needed
 - Stay informed about new threats
-

Additional Resources

- **ilminate Dashboard:** `apex.ilminate.com`
 - **Gmail API Docs:** `https://developers.google.com/gmail/api`
 - **Google Admin Console:** `admin.google.com`
 - **Google Cloud Console:** `console.cloud.google.com`
 - **Support:** `support@ilminate.com` | 910 760-3146
-

Document Version: 1.0

Last Updated: November 2024

Maintained By: ilminate Technical Team