

Microsoft 365 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 Microsoft 365 using Microsoft Graph API and OAuth 2.0 authentication. This integration allows ilminate to:

- Monitor incoming emails in real-time
- Analyze messages for threats using APEX detection engines

- Move suspicious emails to quarantine folders
- Provide detailed threat reports and analytics

Key Benefits:

- No MX record changes required
- Email flow remains unchanged
- Reversible actions (no permanent deletions)
- Full audit trail of all actions
- Works with Exchange Online, Outlook, and Office 365

Integration Method: Microsoft Graph API with OAuth 2.0 application permissions

Prerequisites

Before starting the integration, ensure you have:

Required Access

- **Global Administrator** or **Exchange Administrator** role in Microsoft 365
- Access to Microsoft 365 Admin Center (`admin.microsoft.com`)
- Access to Azure AD Portal (`portal.azure.com`)

Required Information

- Microsoft 365 tenant ID (found in Azure AD → Overview)

- Primary domain name
- List of mailboxes/users to protect (optional for initial setup)

Technical Requirements

- Microsoft 365 subscription (Business Standard or higher recommended)
- Modern authentication enabled (default for most tenants)
- Network access to Microsoft Graph API endpoints

Pre-Integration Checklist

- ☐ Verify Global Admin access
 - ☐ Note your tenant ID
 - ☐ Identify pilot group (recommended: 5-10 mailboxes)
 - ☐ Review current email security settings
 - ☐ Ensure no 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 "Microsoft 365" platform card

2. Request Setup Link

- Click "Start Microsoft 365 Setup" button
- Fill out contact form with:
 - Your name and email
 - Company name
 - Microsoft 365 tenant domain
 - Preferred contact method

3. Receive Personalized Setup Link

- ilminate will send you a secure, personalized OAuth consent link
- This link is unique to your tenant and includes necessary parameters
- Link format: `https://login.microsoftonline.com/{tenant-id}/adminconsent?...`

Step 2: Grant Admin Consent

1. Open the Setup Link

- Click the link provided by ilminate
- You'll be redirected to Microsoft's admin consent page

2. Sign In

- Sign in with your **Global Administrator** account
- Use the account that has permission to grant tenant-wide consent

3. Review Permissions

You'll see the following permissions requested:

Application Permissions:

- `Mail.Read` - Read mail in all mailboxes
- `Mail.ReadWrite` - Read and write mail in all mailboxes
- `offline_access` - Maintain access to data

Why These Permissions?

- `Mail.Read` : Allows ilminate to evaluate email content and metadata
- `Mail.ReadWrite` : Enables moving threats to quarantine folders
- `offline_access` : Ensures continuous operation without re-authentication

4. Grant Consent

- Review the permissions carefully
- Click **"Accept"** or **"Consent on behalf of your organization"**
- You'll see a confirmation page: "You have successfully granted permissions"

5. Confirmation

- After consent, you'll be redirected back to ilminate
- You should see: "Microsoft 365 connection successful"

Step 3: Configure Mailbox Selection

1. **Access ilminate Dashboard**

- Log in to your ilminate portal
- Navigate to **Settings** → **Integrations** → **Microsoft 365**

2. **Choose Protection Scope**

Option A: Pilot Group (Recommended)

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

Option B: Department/Group

- Select specific Microsoft 365 groups
- Choose departments (e.g., Finance, HR, Sales)
- Apply to administrative units
- **Why:** Phased rollout reduces risk

Option C: Entire Organization

- Select all mailboxes
- Apply to all users
- **Why:** Immediate full protection (use after pilot validation)

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

- Exclude specific mailboxes if needed
- Set up inclusion/exclusion rules

- Apply to shared mailboxes (optional)

Step 4: 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" folder
- **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 banners 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 folder name: `ilminate - Quarantine` (default)
- Configure retention period (default: 30 days)
- Set up release workflow
- Enable user notifications

Step 5: Verify Integration

1. Check Connection Status

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

2. Send Test Email

- Send a test phishing email to a protected mailbox
- 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 Mailbox**

- Log in to protected mailbox
 - Verify "ilminate – Quarantine" folder exists
 - Check that test email is in quarantine (if applicable)
-

Configuration Options

Mailbox Selection Options

By User:

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

By Group:

- Select Microsoft 365 security groups
- Select distribution groups
- Best for: Department-based protection

By Administrative Unit:

- Apply to entire administrative units
- Best for: Large organizations with structured AD

By License Type:

- Filter by license (e.g., E3, E5)
- Best for: License-based deployment

Protection Modes Explained

Observe Mode:

Email Arrives → ilminate 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 → ilminate Analyzes → Threat Detected →
Moved **to** Quarantine Folder

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

Tag Mode:

Email Arrives → ilminate Analyzes → Warning **Added** →
Email Delivered with **Banner**

- 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

Retention Policies:

- Quarantine retention period (default: 30 days)
 - Auto-delete after retention period
 - Archive old threats
-

Verification & Testing

Initial Verification Checklist

- ☐ OAuth consent granted successfully
- ☐ Connection status shows "Connected"
- ☐ Mailboxes appear in ilminate dashboard
- ☐ Quarantine folder created in test mailbox
- ☐ 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 folder (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 mailbox
3. Review quarantined email
4. Release email back to inbox
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 Microsoft Graph API status
 - Check for throttling or rate limits
 - Verify connection stability
-

Troubleshooting

Common Issues and Solutions

Issue 1: "Consent Failed" or "Permissions Denied"

Symptoms:

- Error message when granting consent
- "Insufficient privileges" error
- Consent page shows errors

Solutions:

1. Verify Admin Role:

- Ensure you're using Global Administrator account
- Check Azure AD → Roles → Global Administrator
- Try signing out and back in

2. Check Consent Settings:

- Azure AD → Enterprise Applications → User Settings
- Verify "Users can consent to apps" is enabled (if needed)
- Check "Admin consent requests" settings

3. Try Direct Consent:

- Azure AD → App Registrations → Find ilminate app
- Go to API Permissions → Grant admin consent
- Manually grant each permission

Issue 2: "Connection Failed" or "Cannot Connect"

Symptoms:

- Dashboard shows "Disconnected" status
- Error: "Unable to connect to Microsoft 365"
- API errors in logs

Solutions:

1. Verify Network Connectivity:

- Check firewall rules allow Microsoft Graph API
- Verify proxy settings (if applicable)
- Test connectivity to `graph.microsoft.com`

2. Check API Permissions:

- Azure AD → App Registrations → ilminate app

- Verify all permissions granted
- Check for expired permissions

3. **Verify Service Principal:**

- Azure AD → Enterprise Applications
- Find ilminate application
- Verify it's enabled and not disabled

Issue 3: "Mailboxes Not Appearing"

Symptoms:

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

Solutions:

1. **Check Mailbox Selection:**

- Verify mailboxes have Exchange Online licenses
- Check mailboxes are not hidden from address list
- Ensure mailboxes are not on hold or archived

2. **Verify Permissions:**

- Check Mail.Read permission is granted
- Verify application has access to selected mailboxes
- Check for conditional access policies blocking access

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 4: "Emails Not Being Detected"

Symptoms:

- Test emails not showing in dashboard
- No threats detected
- Quarantine folder empty

Solutions:

1. **Verify Protection Mode:**

- Check protection mode is enabled
- Verify mailboxes are selected
- Confirm protection scope includes test mailbox

2. **Check Email Flow:**

- Verify emails are arriving in mailbox
- Check Exchange Online mail flow 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 5: "Quarantine Folder Not Created"

Symptoms:

- Quarantine mode enabled but no folder
- Emails not moving to quarantine
- "Folder not found" errors

Solutions:

1. Manual Folder Creation:

- Log in to Outlook/OWA
- Create folder: "ilminate – Quarantine"
- Set folder permissions if needed

2. Check Permissions:

- Verify Mail.ReadWrite permission granted
- Check application has folder creation rights
- Review mailbox permissions

3. Retry Folder Creation:

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

Getting Help

ilminate Support:

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

Microsoft Support:

- Microsoft 365 Admin Center → Support
 - Azure AD Support (for permission issues)
 - Microsoft Graph API Documentation
-

Security & Permissions

Permissions Explained

Mail.Read

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

Mail.ReadWrite

- **Purpose:** Read and modify emails

- **Scope:** All selected mailboxes
- **What it does:** Moves threats to quarantine
- **Security:** Limited to moving emails, no deletion

offline_access

- **Purpose:** Maintain access without re-authentication
- **Scope:** Application-level
- **What it does:** Continuous monitoring
- **Security:** Uses refresh tokens securely

Security Best Practices

1. Least Privilege:

- Only grant necessary permissions
- Scope to specific mailboxes when possible
- Use administrative units for large deployments

2. Conditional Access:

- Restrict access by IP address
- Require device compliance
- Use location-based policies

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
- Tasks
- Notes
- OneDrive files

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

Conditional Access Policies

Create Policy:

1. Azure AD → Security → Conditional Access
2. New Policy → Name: "ilminate API Access"
3. Users: Select ilminate service principal
4. Conditions: IP address location
5. Access Controls: Grant access
6. Enable policy

Benefits:

- Restrict API access by location
- Require specific IP addresses
- Add device compliance requirements

Administrative Units

Setup:

1. Azure AD → Administrative Units
2. Create new unit (e.g., "Pilot Group")
3. Add users to unit
4. Assign ilminate permissions to unit

Benefits:

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

Service Principal Configuration

View Service Principal:

1. Azure AD → Enterprise Applications
2. Find "ilminate" application
3. Review properties and permissions

Configure:

- Assign owners
- Set expiration policies
- Configure certificate authentication (if used)

API Throttling & Limits

Microsoft Graph Limits:

- 10,000 requests per 10 minutes per app
- 1,000 requests per 10 seconds per user
- eliminate handles throttling automatically

Monitoring:

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

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 mailboxes after pilot validation

- Roll out to additional departments
- Consider full organization deployment

4. **Training:**

- Train users on quarantine folder
- 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`
 - **Microsoft Graph API Docs:** `https://docs.microsoft.com/graph`
 - **Microsoft 365 Admin Center:** `admin.microsoft.com`
 - **Azure AD Portal:** `portal.azure.com`
 - **Support:** `support@ilminate.com` | 910 760-3146
-

Document Version: 1.0

Last Updated: November 2024

Maintained By: ilminate Technical Team

