Disabling Less Secure Apps:

In the coming weeks, we will be disabling the "Less secure apps" access function from all campus Gmail accounts. Less secure apps allows authentication without modern security standards.   Prior to disabling Less secure apps, please confirm that all existing known clients will still be able to authenticate following this change. Before the system-wide disablement, we request all local system admins test their mail client versions prior to the change. Local system admins can test by disabling Less secure apps and testing their clients devices. *Please note if you have MFA enabled on your account, Less secure apps is already disabled, and you should consider using a functional account to test.

Clients affected by this change include:

- Non-Google Android mail clients (Samsung Email, Blue Mail, etc.)
- iOS Mail
- Apple Mail (MacOS)
- Microsoft Outlook (when not using GWSMO, and 2013 or earlier)
- Mozilla Thunderbird (when not using OAuth2)
- Printers, Scanners, Copiers*

*These devices will work when using SMTP, such as the MTA service. If not, please confirm the device is using modern authorization.

To disable Less secure apps:

1. Go to https://myaccount.google.com/lesssecureapps
2. Login to your Google account
3. Toggle Allow less secure apps: OFF

To test mail clients with Less secure apps disabled:

Less secure app	**Alternative**
Apple Mail configured with POP3	Re-add your Google Account to Apple Mail and configure it to use IMAP with OAuth2. This automatically initiates the connection with OAuth2.
iOS Mail	Continue using iOS Mail as long as you have iOS 6.0 or later. OAuth2 support is automatically included in iOS 6.0 and later when you add an account using the Google option.
Outlook for Windows via password-based POP or IMAP	Google Workspace Sync for Microsoft Outlook (GWSMO). Web-based or latest version of Outlook. About Google Workspace Sync for Microsoft Outlook
Mozilla Thunderbird	Re-add your Google Account to Thunderbird and configure it to use IMAP with OAuth2. This automatically initiates the connection with OAuth2.
Legacy office devices Examples: scanners and multifunctional printers that send email	Continue using legacy office devices with SMTP. Other protocols (such as POP3 and IMAP) will be blocked unless they use OAuth. Adding these to the MTA service is preferred.
Any other app	Request that the app developer update the app to use OAuth 2.0

The transition to More secure apps access will help keep our campus accounts safe. For this reason, we are limiting password-based programmatic sign-ins.

Note: When the 2-step verification or MFA is turned on for an account, the goal for all campus applications, access to Less secure apps is automatically disabled.

If you would like assistance with testing, please contact the Messaging & Collaboration team by opening a ticket at ithelp.ucsb.edu.

If you require technical assistance, please contact:

For problems or time sensitive requests:

IT Core Services - Service Desk: (805) 893-5000 or X5000

For all other services:

Submit a self-service request at: ithelp.ucsb.edu

Services provided by Enterprise Technology Services
Include level agreements for Response and
Resolution Time. Our commitment to your technical needs