



How to Use a Google Account
with an App Password
for a SMTP relay in Jamf Pro





We recommend that you integrate your Jamf Pro server with an SMTP (Simple Mail Transport Protocol) server. According to the Jamf Pro Administrator Guide, this allows you to do the following:

- Send email notifications to Jamf Pro users when certain events occur.
- Send enrollment invitations via email.
- Send mass emails to end users.

If your organization uses Google accounts (Gmail or G Suite) you can use Google's SMTP service at smtp.google.com as an SMTP relay (the Jamf Pro web admin interface refers to this as an SMTP server, but you may also see it referred to as an SMTP relay, because it relays mail from your Jamf Pro service to the SMTP service of the email recipient).

In general, we recommend that you consider deploying "2-Step Verification" for your Google accounts. But if you turn on 2-Step Verification, you need to perform some additional configuration in order to use Google as an SMTP relay for Jamf Pro. You'll create what Google calls an "app password" that allows Jamf Pro, which doesn't support 2-Step Verification, to use the Gmail SMTP server.

The additional configuration consists of:

- configuring your Google domain to use something called "less secure applications" (LSAs)
- configuring a specific Google account that uses 2-Step Verification to have an additional password that's used for a specific application, in this case, Jamf Pro.

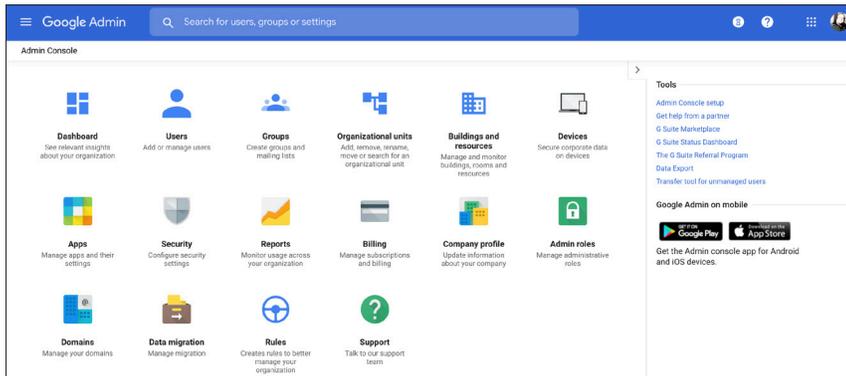
Be aware that, there are some changes coming that will require "less secure applications" (LSAs) to use something called OAuth in order to use Google as an SMTP relay, but that's not until June 15, 2020 for accounts that haven't yet been configured to use LSAs. And after February 15, 2021, "Access to LSAs will be turned off for all G Suite accounts," according to Google.

<https://gsuiteupdates.googleblog.com/2019/12/less-secure-apps-oauth-google-username-password-incorrect.html>

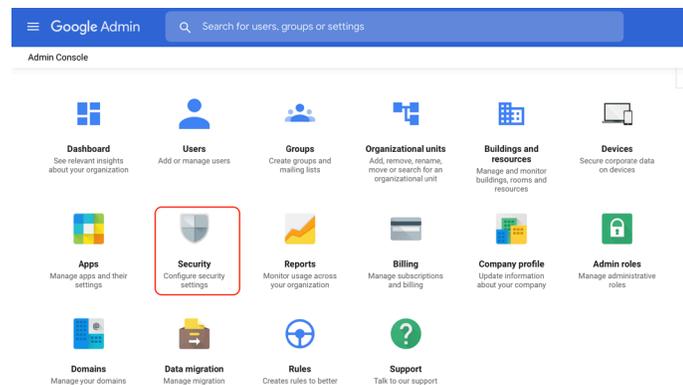
For more information, see Google's support article, "Send email from a printer, scanner, or app," at <https://support.google.com/a/answer/176600> in the "Gmail SMTP server" option.

Configure your Google domain to use "less secure applications"

1. Log in to your Google Admin portal at <https://admin.google.com>.

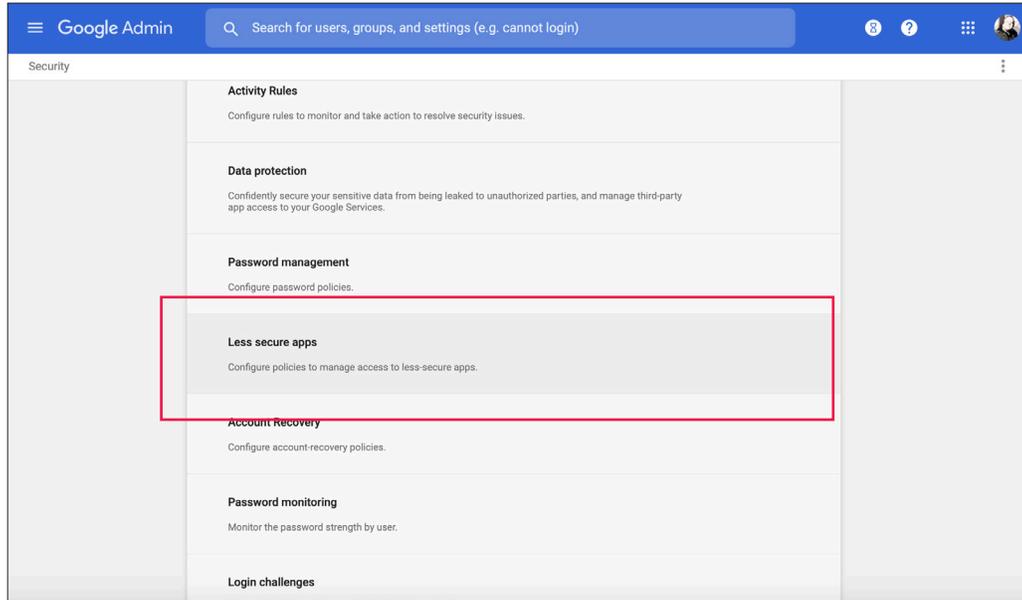


2. Select Security.

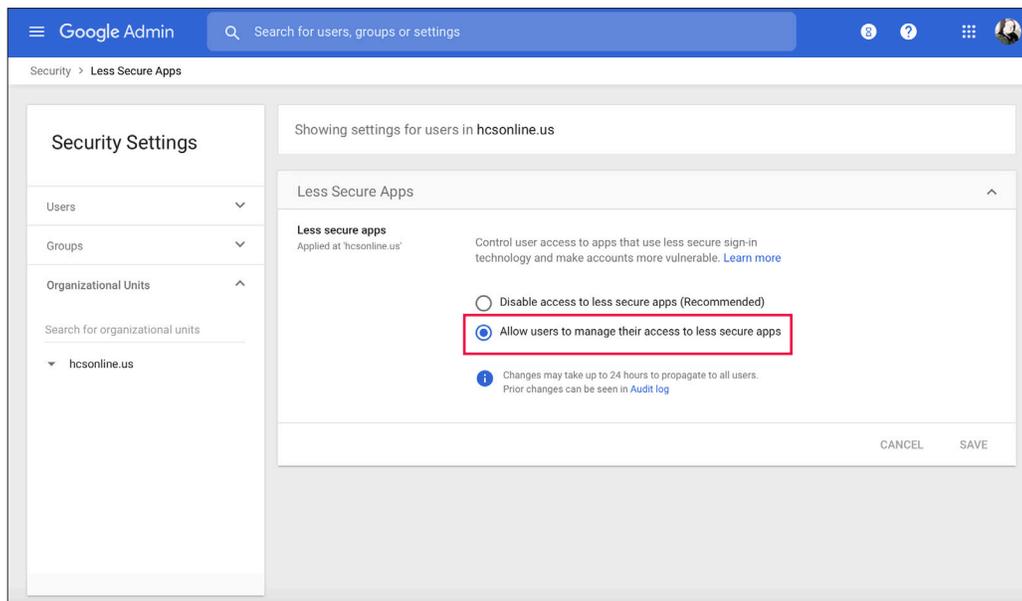




3. Select Less Secure Apps.



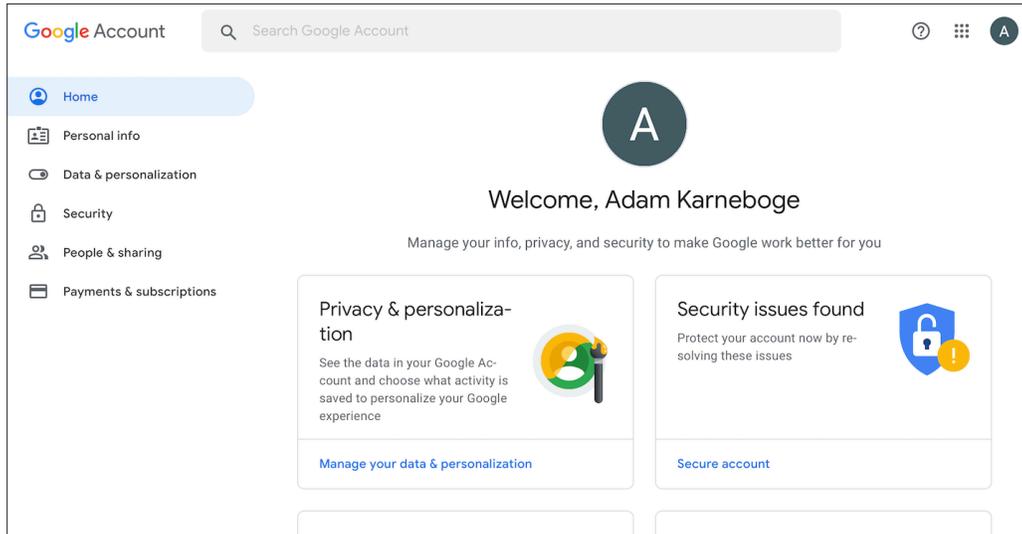
4. If the option "Allow users to manage their access to less secure apps" is not already selected, select the radio button "Allow users to manage their access to less secure apps," then click Save.



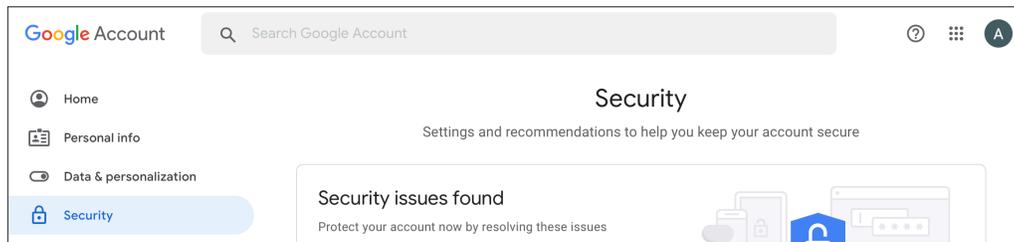


Configure an account to use a less secure password for your Jamf Pro server to use for SMTP.

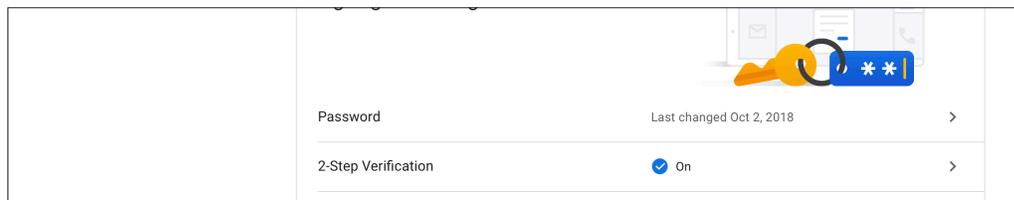
1. Log in to your Google account at <https://myaccount.google.com>.



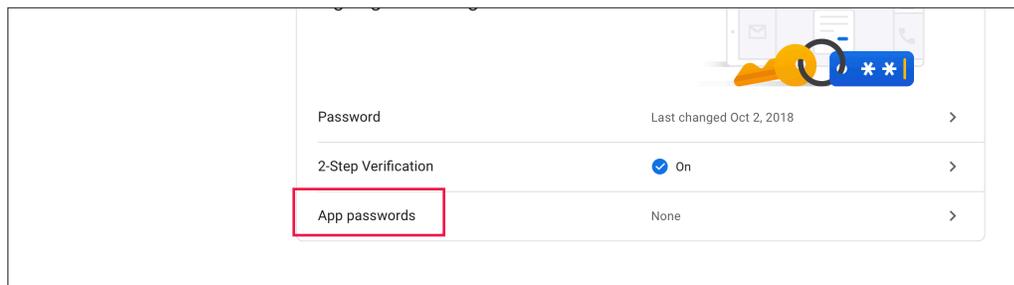
2. In the sidebar, click Security.



3. Confirm that "2-Step Verification" is displayed in the "Signing in to Google" section. If you haven't yet turned on 2-Step Verification for your Google account, turn it on now using the steps outlined here: https://support.google.com/accounts/answer/185839?hl=en&ref_topic=2954345



4. Click "App passwords." If you recently enabled the "Less secure apps" option in step 4, you may need to wait up to 24 hours for your portal to display the "App passwords" option.





5. Authenticate at the prompt.
6. From the “Select app” menu, chose Other (Custom name).

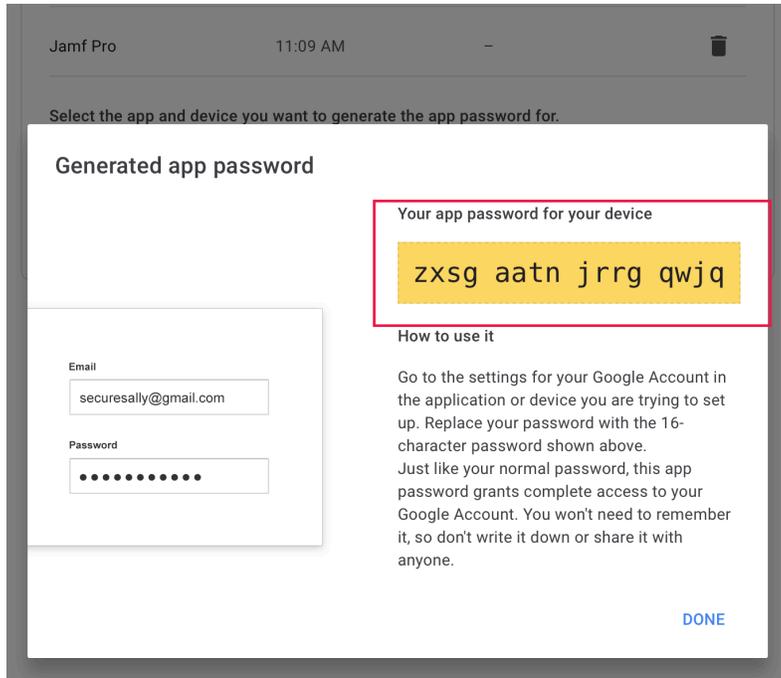
A screenshot of the 'App passwords' settings page. At the top, there is a back arrow and the title 'App passwords'. Below this, a paragraph explains that app passwords allow signing into a Google Account from apps that don't support 2-Step Verification. The main content area contains the text 'You don't have any app passwords.' followed by the instruction 'Select the app and device you want to generate the app password for.'. There are two dropdown menus: 'Select app' and 'Select device'. The 'Select app' dropdown is open, showing a list of options: Mail, Calendar, Contacts, YouTube, and 'Other (Custom name)'. The 'Other (Custom name)' option is highlighted with a red rectangular box. A 'GENERATE' button is visible to the right of the dropdown menus.

7. Enter **Jamf Pro**, then click Generate.

A screenshot of the 'App passwords' settings page, showing the next step. The 'Select app' dropdown menu is now closed, and the text 'Jamf Pro' has been entered into the input field. A blue underline is visible under the text, and a small 'X' icon is to its right. The 'GENERATE' button, which was previously greyed out, is now highlighted with a red rectangular box and is a solid blue color with white text.



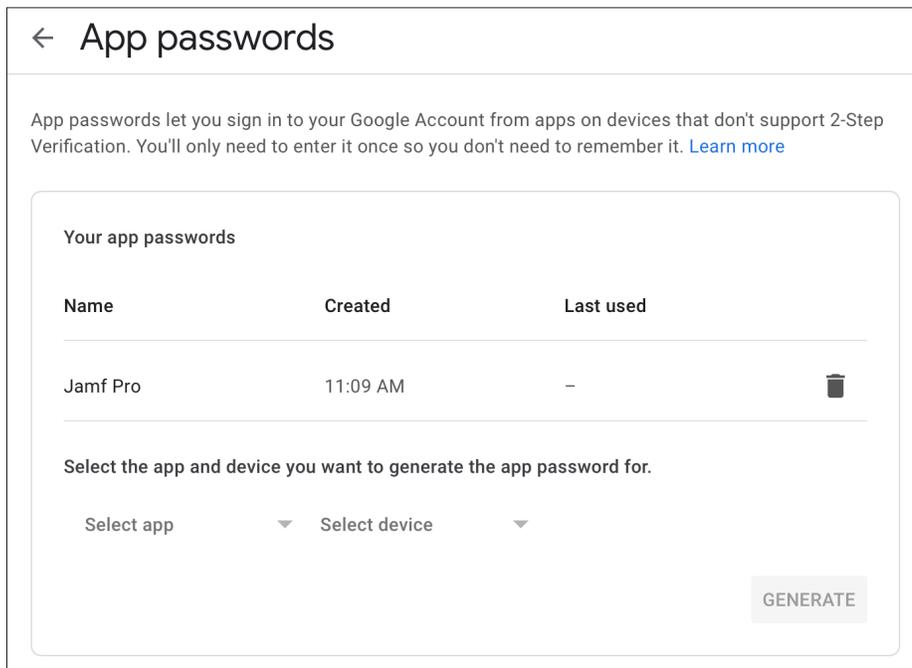
- Your browser will display the generated app password only one time, so select the displayed password and copy it to your clipboard now.



You will not be able to view the app password after you click Done on this screen.

- Click Done.

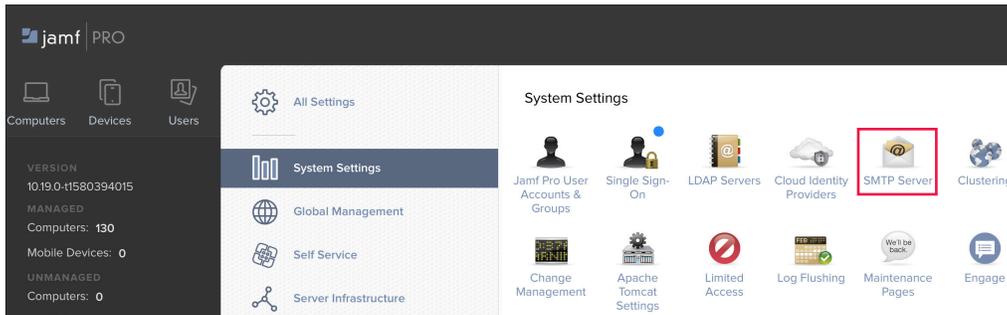
- Confirm that your portal displays something similar to the following figure.



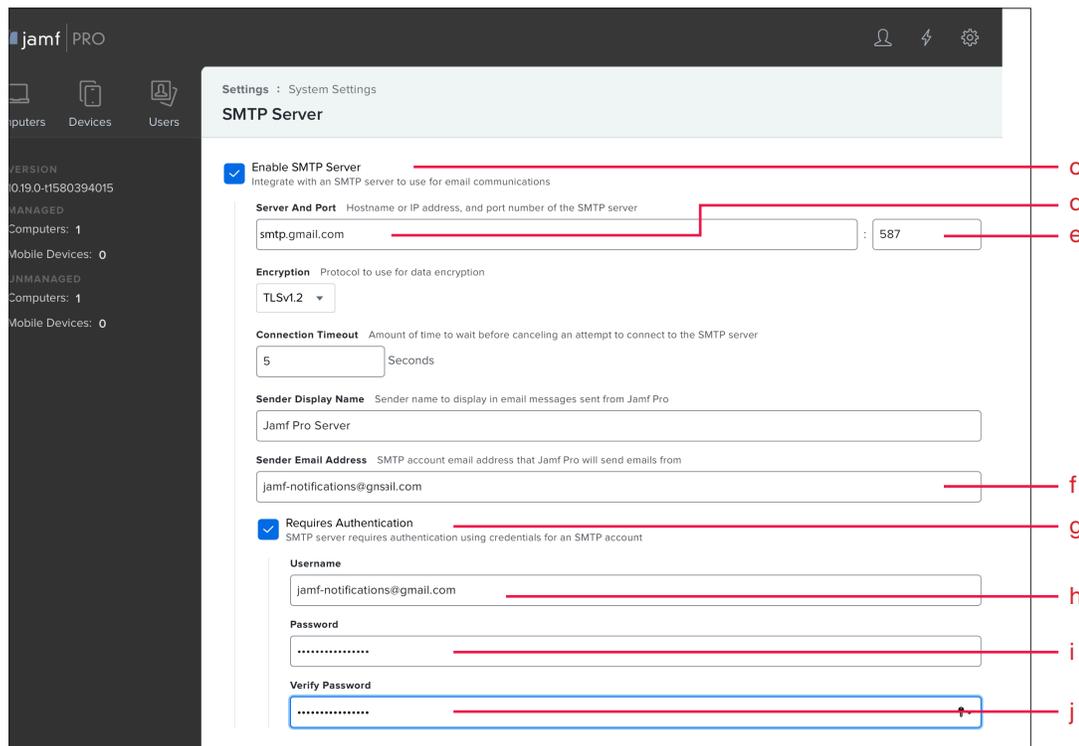


Configure Jamf Pro to use your newly-configured Google account

1. Use the following steps to configure the SMTP Server in Jamf Pro.
 - a. In Jamf Pro, select Settings > System Settings > SMTP Server.



- b. Click Edit.
- c. Ensure that the checkbox for Enable SMTP Server is selected.
- d. In the Server field, enter **smtp.gmail.com**.
- e. In the Port field, enter **587**.
- f. In the Sender Email Address field, enter your G Suite E-mail address.
- g. Ensure that the checkbox for Requires Authentication is selected.
- h. In the Username field enter your G Suite Email address.
- i. In the Password field enter the app password that you copied in the previous section.
- j. In the Verify Password field enter the app password again



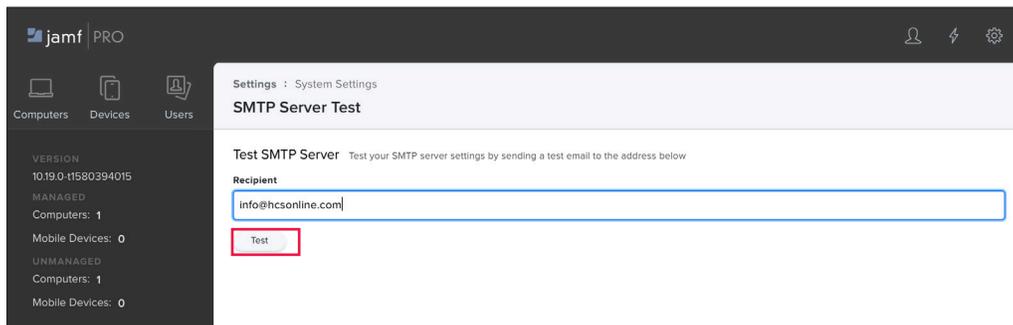


13. Click Save.

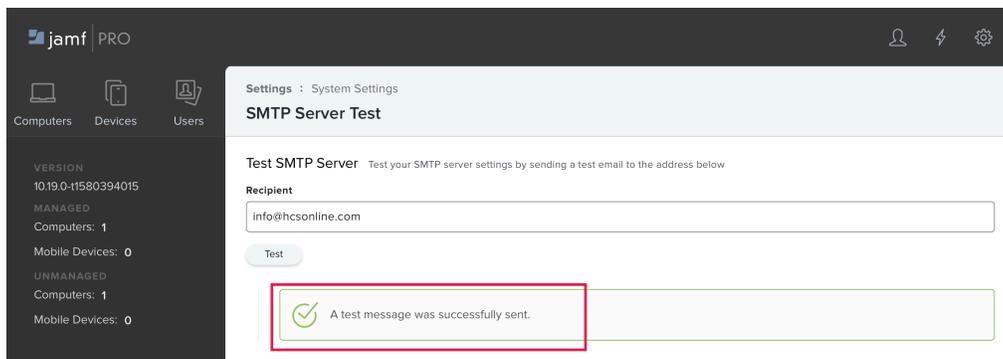


14. Click Test.

15. Enter a test e-mail address, then click Test.



16. Confirm that Jamf Pro displays "A test message was successfully sent."



17. Check the email for the test recipient and confirm that it received the test message.