Follow these instructions to ensure Clinics and Organizations can receive emails from VAMS.

To ensure communications do not get delayed or blocked by organizations' exchange servers, we are asking clinic POCs and employer POCs to whitelist these email addresses:

- vams@cdc.gov
- no-reply@mail.vams.cdc.gov
- VAMSHelp@cdc.gov
- no-reply@enevlope.mail.vams.cdc.gov

and in some cases *@salesforce.com. Additionally, allowing mail from specific IPs will greatly improve email deliverability in a timely fashion: **VAMS users will need to coordinate with their IT departments to whitelist the addresses above and allow mail from the following IPs:**

- Salesforce
  - 96.43.152.64 - 96.43.152.80 (subnet mask = 255.255.255.0)
  - 96.43.153.64 - 96.43.153.80 (subnet mask = 255.255.255.0)
- Amazon Web Services
  - 23.251.255.1 - 23.251.255.150
  - 23.251.253.228 - 23.251.254.250
  - 54.240.40.1 - 54.240.40.54

For reference, users can expect the following kinds of emails from VAMS email addresses:

- **vams@cdc.gov –** auto-generated emails related to Clinic, Jurisdiction, Organization/Employer Portal messages as well as re-occurring two-factor authentication for logins
- **no-reply@mail.vams.cdc.gov** – auto-generated emails for Recipient Portal and two-factor authentication for VAMS
- **NEW: no-reply@enevlope.mail.vams.cdc.gov** - auto-generated emails for Recipient Portal and two-factor authentication for VAMS
- **VAMSHelp@cdc.gov** – communicating back and forth with the VAMS Help Desk
- ***@salesforce.com** - depending on some email server configurations, we have heard of rare cases where emails are delivered directly from Salesforce. Potential cases include password resets and interacting with VAMS Help Desk agents.

Updated solution for the password reset loop

The VAMS team is providing you with the following suggestions to assist with anyone experiencing the password reset loop. Please note that these suggestions should be shared with your IT Department to approve the VAMS password reset URL in Office365.

> Based on the issue you are experiencing; it is likely that your IT department is using **Microsoft Office365 with Safe Links protection.** A good way to verify this for certain is that links in your emails show up with a "safe links" preface similar to the example below:
>
> https://ind01.safelinks.protection.outlook.com/?url=https%3A%2F%2Flogin.salesforce.com%<xxxx...>
>
> The suggested resolution available for this issue is to whitelist the VAMS and Salesforce domains within Safe Links policy. This would be done by your organization's IT department. **This will resolve the issue for all users with your email domain.**

The below instructions should be given to your IT department and needs to be performed by your Microsoft Office365 Admin at their own discretion. If your admin completes the steps below, the links you receive should no longer have the “safe links” preface.

Suggested steps for your IT Organization to approve VAMS in the Office360 Safe Links Policy (from Microsoft documentation):

1. Launch https://protection.office.com/safelinksconverged with Office365 admin credentials
2. Edit appropriate Safe links policy defined under "Policies that apply to specific recipients" section
3. Click on 'settings' and add the following under “Do not rewrite the following URLs:” section:
    a. “[https://*.cdc.gov]https://*.cdc.gov”
    b. “https://vams.cdc.gov/*”
    c. "https://login.salesforce.com/*"
    d. "[https://*.salesforce.com]https://*.salesforce.com"
4. Save changes

Additional documentation from Microsoft can be found at the links below:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide

Accessing Multiple Portals

Please communicate to all existing clinics and any new clinics that **individuals who will have a clinic role in VAMS and will also be a vaccine recipient should be added as a clinic user first.** This means, the clinic administrator should add them to the clinic in the appropriate clinic role before the employer/organization adds them as a vaccine recipient. This will help prevent the user from experiencing any errors accessing multiple portals in VAMS.

People who will have multiple roles in VAMS **can disregard the registration link for their second role**. They can simply log in to VAMS with their current username and password and should be able to see their portals. If the user does click the email registration link for their additional roles, t**hey should not attempt to create a new password**. Instead, the user should select the VAMS logo located at the top left of the screen and they will be transitioned to the VAMS login page where they can proceed with the VAMS login they previously created.

Two Factor Authentication Emails

All VAMS users will have to enter a One Time Password (OTP) when they initially create their VAMS account. This OTP password email comes from:

- **no-reply@mail.vams.cdc.gov**,
- **no-reply@enevlope.mail.vams.cdc.gov**
- VAMS@cdc.gov

and is sent after they click the link to register. This password is good for 60 minutes. If a user is unsuccessful with registering for whatever reason and tries to register again within 60 min, they will not receive a new OTP code each time. They should use the original OTP code. After five invalid attempts, VAMS will generate a new code.

VAMS or CDC will **never** ask you for your password. Do not give anyone the password to your VAMS account.

Thank you,

VAMS Operations Team