Temporary Passcode Authentication

https://campus.barracuda.com/doc/98227966/

As of **Friday, March 31, 2023**, auto-authentication has been disabled for end users from quarantine email digests. End users will now be required to authenticate before they can view their account and make updates to their quarantined emails. With this update, many users of shared mailboxes and distribution lists were unable to manage their quarantine messages.

During the **week of April 24, 2023**, Email Gateway Defense will release a temporary passcode authentication method to allow users access to their shared mailbox and distribution list accounts.

For more information, see https://esstimeline.barracudanetworks.com/publications/temporary-passcode-authentication.

To watch a video about what the temporary passcode authentication is and how to use it, see Temporary Passcode Authentication Video.

You can allow users to sign in with a temporary passcode. This is useful for users signing into a shared mailbox or distribution list, if users forgot their password, or if SSO is unavailable.

Users can request a temporary passcode when they click on a link in the quarantine notification email or when logging into Email Gateway Defense. A passcode is then sent to the user's email address that they can use to log in. If the user is using a shared mailbox or part of a distribution list, the passcode will be sent to the Shared Mailbox email address. To designate an individual to managed the shared mailbox or distribution list, see How to Designate an Individual to Manage a Shared Mailbox or Distribution List.

This feature will create the below sign-in scenarios:

- If both SSO and temporary passcodes are enabled, users can choose to continue with normal SSO login or request a temporary passcode.
- If SSO is enabled but temporary passcodes are disabled, users will sign in through SSO as usual and will not be given the option to request a temporary passcode.
- If SSO is disabled but temporary passcodes are enabled, users will have the option to log in with their EGD credentials or request a temporary passcode.
- If both SSO and temporary passcodes are disabled, users will have to sign in with their EGD email and password credentials.

Enable Temporary Passcode Feature

Notes:

- This option is available to account admins only. To enable the feature for a specific domain, sign in as a domain administrator.
- Passcodes are valid for 15 minutes.
- User sessions expire after 24 hours.
- Only 5 passcodes are active on each account during any given 15-minute time window.

By default, the temporary passcode authentication feature is **disabled** and set to **No**. To enable temporary passcode authentication for your users, the administrator of the account must follow the below steps:

1. Log into Email Gateway Defense as the administrator, and go to the **Users > Quarantine Notification** page.
2. For the **Allow users to sign in with temporary passcode**, click **Yes**.
3. Click **Save Changes**.

Sign In with Temporary Passcodes for Users

Once the temporary passcode setting is enabled, the users of a shared mailbox or distribution list will see a new option when they attempt to sign into the shared email address.

Users will use the following instructions to authenticate with a temporary passcode:

1. Click on a link or button in their quarantine digest email (Manage Quarantine, View Message Log, Deliver, Allow List, Block List) or manually log into Email Gateway Defense https://ess.barracudanetworks.com/.
   You are prompted to sign into Email Gateway Defense.
2. Enter a shared inbox or distribution list email address in the **Email Address** field and click **Next**.
3. If the account is SSO enabled, you will see an intermediary page to log in with SSO or request a temporary passcode. Note that the SSO login is not for shared email addresses.
4. If the account does not have SSO enabled, you will enter your password or shown the option to request a temporary passcode.
5. Click **Email a temporary passcode** to send a passcode to the shared mailbox.
   Note that passcodes are valid for 15 minutes.
6. You will receive an email to the shared inbox with the temporary passcode. Copy and paste the passcode into the **Temporary passcode** field. Note that passcodes are case sensitive.

7. Click **Log in**.
   You are now logged into your **Message Log** and can manage your quarantine emails. You can also use the **Deliver**, **Allow List**, **Block List** buttons in the quarantine digest email as normal.

For help logging into Email Gateway Defense, contact Barracuda Networks Technical Support.

Frequently Asked Questions (FAQs)

What if someone else in the shared mailbox also requests a temporary passcode?

If you received multiple passcode emails, you can click **Already have a passcode?** on the Email Gateway Defense login page, and enter one of the passcodes you received in your emails. Note that passcodes are only valid for 15 minutes.

If two users request a temporary passcode around the same time, two separate emails with different passcodes will be sent to the shared inbox. Both passcodes will be active for 15 minutes after they are requested, and either user can use either passcode within these 15 minutes. One passcode does not invalidate another. A passcode only becomes invalid after its 15-minute lifespan expires.

Note that only 5 passcodes are active at a given time for each account. If users request 5 passcodes within the same 15 minutes, users are unable to request more passcodes. Any of the five active passcodes can be used to authenticate. Once 1 of the 5 passcodes expires, users can request another temporary passcode.

How frequently do I need to sign in with a temporary passcode?

After you are signed into Email Gateway Defense with a temporary passcode, you are authenticated for the length of your browser session which is 24 hours. After your browser session has ended, you will need to request another temporary passcode to start another 24-hour session.

What if my account uses SSO (Microsoft Entra ID or LDAP) to login?

If your administrator has set up your account to use Microsoft Entra ID or LDAP authentication with Single Sign-On, they will need to enable the temporary passcode feature in the *Enable Temporary Passcode Feature* section above. This will allow users to sign in with a temporary passcode for a shared mailbox. For non-shared email addresses, users will still be able to sign in with their AD or LDAP credentials.

How do I request a new temporary passcode?

Click the **resend temporary passcode** link on the **Enter temporary passcode** page. If you are requesting a temporary passcode for a shared mailbox or distribution group, wait a couple of minutes

before requesting a new passcode as multiple emails may be sent to everyone in your shared mailbox or distribution group.

What if I am still having trouble signing in?

Contact Barracuda Networks Technical Support to help you log in or escalate your issue to the correct team.