Administrator's Reference Guide to Two-Factor Authentication using Duo

What are the responsibilities of an administrator of two factor authentication at Georgia Tech?

The Institute is adopting two-factor authentication in order to protect student, faculty, and staff data. When assuming the responsibilities of an administrator for two-factor implementation for your department, please adhere to the following responsibilities.

1. Administrators are expected to verify the identities of users they are enrolling.

2. Administrators are expected to limit their role as an Administrator to the staff they support, particularly when accessing the Duo console for Administrators.

3. Administrators are responsible for abiding by the two-factor authentication policies and recommended practices. Included, but not limited are the following:
    a. Do not create long-term, reusable bypass codes
    b. When placing users in Bypass Mode, document reason in notes and do not leave in Bypass mode for more than 48 hours.

Pre-Planning: Know before you enroll

1. Communications Tools
    a. Materials for communicating about two factor authentication are available to you to disseminate to your users prior to enrolling them in two-factor authentication. They include presentations, sample letters, quick reference guides, FAQs, etc. For more information, go to the two-factor authentication website at www.twofactor.oit.gatech.ed

2. Technical Support

    The Two-factor Authentication Project Team has knowledgeable resources ready to support you in the planning and implementation of two-factor authentication enrollment for your department.

How do I request to enroll my team or department in two-factor authentication using Duo?

1. Send an email to**:** 2FA@oit.gatech.edu

2. Include the following in the subject line: "*Two-factor authentication enrollment request for < Name, Team, Department>"*

Note: *This process will create a Service Desk ticket and you will receive a confirmation email in response. All requests to enroll Georgia Tech faculty and staff in two-factor authentication will be reviewed by the Two-Factor Authentication Support Team.*

Administrator's Reference Guide to Two-Factor Authentication using Duo

How do I become an administrator for two-factor authentication for my department?

1. Send an email to 2FA@oit.gatech.edu

2. Include the following in the subject line: *"Two-factor authentication enrollment request for <Name, Team, Department>"*

Note: *This process will create a Service Desk ticket and you will receive a confirmation email in response. All requests to enroll Georgia Tech faculty and staff in two-factor authentication will be reviewed by the Two-Factor Authentication Support Team.*

Once I'm an Administrator, what next? Accessing the Duo® Admin Console

1. In order to become a two-factor authentication administrator, you'll need access to the Duo Administrator's Panel via a username and password. The Office of Information Technology (OIT) will provide you with these once you've requested access.

2. Once your account has been created, you may access the Duo Administrator's Panel at the following link: https://admin.duosecurity.com (*link to Duo.com site*)

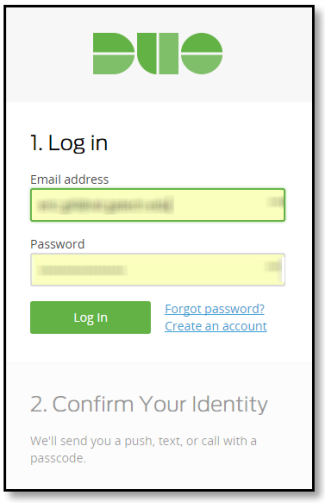
3. You will need to enter your username and password and then confirm your identity using a second factor.

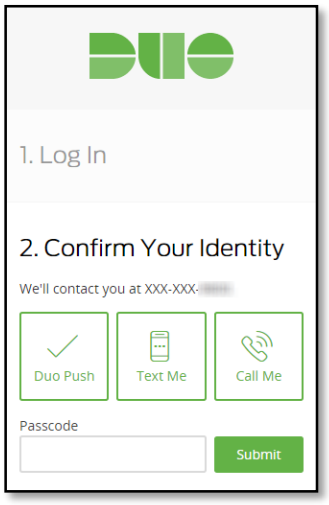
Recommended Approach to Onboarding Users

As a general rule, the one-on-one approach is currently the recommended and approved method of onboarding users for two-factor authentication.

This approach consists of visiting or having users meet with their departmental CSR to be individually set up for two-factor authentication on an as-needed basis.

Initial login screen to access the Duo Administrator Console





For more information, refer to the following link: https://duo.com/docs/administration#accessing-the-admin-panel

Administrator's Reference Guide to Two-Factor Authentication using Duo

What functionality will be available to you as a two-factor authentication administrator?

Using Duo, the administrator will be able to access the following functions:

1. **Dashboard:** *(Read Only Privileges)* *https://admin-4b6bfd4c.duosecurity.com/*
   - View the Duo Administrator's Dashboard
   - See Authentication Log of the latest 10 attempts

2. **Applications:** *(Read Only Privileges)* *https://admin-4b6bfd4c.duosecurity.com/applications*

   See information about the applications at Georgia Tech which are using the Duo service for two-factor authentication

3. **Users:** ***(Active Administration)*** *https://admin-4b6bfd4c.duosecurity.com/users*

   a. **New User** - recommended method of enrolling users
      - This is where a new two-factor authenticated user is added for the first time.

   b. **Manage Users** - recommended method of managing users
      - This is where a user is managed including updating their profile, changing their status (active, bypass, disabled), adding to a group; adding notes, adding a phone, adding a hardware token, adding a Bypass Mode, etc. (see information below on using Bypass Mode)

   c. **Bulk Enroll Users** – ***NOTE:*** *Do not "Bypass" users for more than 48 hours*
      - Warning: if users are added using this method they will be required to use their tokens immediately to access web applications

   d. **Import Users** - ***NOTE:*** *Do not "Bypass" users for more than 48 hours*
      - Warning: if users are added using this method, they will be required to use their tokens immediately to access web applications

4. **Activation Links - choose to send to users who have not activated their Duo Mobile**
   - **CAUTION: Do Not Use this option**. This is not recommended to use since this will send Activation Links to users outside of your administrative responsibilities.

5. **Groups -** Not integrated with Georgia Tech systems
   i. Groups may be helpful for organizing users in Duo, however these groups are not supported or integrated into any Georgia Tech systems. Therefore, it is solely the administrator's responsibility to maintain the groups they create.

6. **Reports -** There are numerous of reports available (see *Additional Duo Application Resource Links*)

7. **Directory Sync - DO NOT USE**

Administrator's Reference Guide to Two-Factor Authentication using Duo

Two-factor authentication Policy and Recommended Practices ***Caution***

1. **Using Bypass Mode in any scenario:
    a. This allows the bypassed User to not be required to use two-factor authentication in ALL two-factor authentication required situations such as OIT employees required to use two-factor authentication for VPN use or two-factor authentication for Mage Admins.
    b. The requested approach is:
        i. The two-factor authentication administrator should enroll each individual user on a 1 on 1 basis by either visiting them or having the users visit their two-factor authentication administrator.
2. How to respond to requests to be "Opted-Out" or removed from Two-Factor Authentication:
    a. Please submit a ticket to the 2fa@oit.gatech.edu with your request to opt-out users.

How do I remove myself as an administrator for two-factor authentication?

1. Send an email to 2FA@oit.gatech.edu

2. Include the following in the subject line: *"Two-factor authentication REMOVE administrator <Name> for <Department>"*

Note: *This process will create a Service Desk ticket and you will receive a confirmation email in response. All requests to enroll Georgia Tech faculty and staff in two-factor authentication will be reviewed by the Two-Factor Authentication Support Team.*

Additional Duo Application Resource Links

Duo Documentation - https://duo.com/docs

Duo Knowledgebase - https://kb.duo.com