Texas A&M Duo Two Factor Authentication Service Request

For help with completing this form, contact IT Infrastructure & Operations at idm-support@tamu.edu.
To begin the approval process, email the completed form to idm-support@tamu.edu; fax to **979.845.6090** or mail to the Identity Management Office, MS 3374.

Requesting Office/Department: _____

Account used for Primary (username/password) Authentication:

- ☐ **NetID**
- ☐ **Other (administrator) account:** _____

Service Details:

1 Name and description of application or service that will use Duo Two Factor Authentication

2 Service type:

- ☐ **Local and remote (ssh) logins on Unix systems (UNIX integration)**
- ☐ **SSL or IPSec VPN Logins. Enter specific brand:** _____
- ☐ **Other VPNs, including RADIUS-based devices and applications (RADIUS)**
- ☐ **Microsoft services. Enter specific Microsoft service:** _____
- ☐ **Any device or system that supports authentication via LDAP (LDAP Proxy)**
- ☐ **Web applications. Enter specific application:** _____

3 Contacts for service:

	Administrative sponsor	Technical contact(s)	Service Security Contact(s)
Name			
UIN			
Email			
Title			
Department			
Telephone			

Service Security:

4 Who will have access to the service integration secret key? Attach sheet with additional personnel information if needed.

Name	UIN	Role/Responsibilities

Two Factor AuthN Settings:

5 New user policy

☐ **Require Enrollment** Unenrolled users will be prompted to enroll in Duo whenever possible.
☐ **Allow Access** Unenrolled users will pass through without two-factor authentication.
☐ **Deny Access** Unenrolled users will be denied access.

6 Trusted Networks

Allow bypass of two-factor authentication for logins from trusted networks? ☐ **Yes** ☐ **No**

If yes, specify IP networks:

Note: We only recommend this feature for UNIX integrations if you are integrating with OpenSSH. Other systems and tools may not reliably provide a valid client IP address.

☐ **Enroll new users logging in from trusted networks.** If checked, unenrolled users will be subject to the new user policy, even if the login is from one of the IP addresses specified above.

7 Group policy

☐ **Only allow authentication from users in certain groups**

8 Voice greeting This is read to users who authenticate with a phone callback, followed by authentication instructions.

TEXAS A&M IDENTITY SERVICES USER AGREEMENT TO ACCEPT RESPONSIBILITY

- Use of University computing resources is restricted to authorized Texas A&M University business.
- Your application configuration must use encrypted connections for any connecting clients or services.
- **You agree to NOT collect and store NetID passwords.**
- You will be held responsible for any security breach traceable to you or your specific authorization. You will be held liable for any willful misuse or deliberate system damage traceable to you or your specific authorization.
- **You agree to all of the following conditions related to logs and TAMU Directory Services personnel:**
  1. **To deliver, on request, security logs from the application servers.**
  2. **To provide, on request, access to application logs of any service connecting to the application servers.**
  3. **To participate in any event correlation/event monitoring solution in use by TAMU Directory Services personnel.**
- Violation of this agreement may result in disciplinary action or legal action or both.
- **If approved, access will need to be renewed annually.**

The agreement is bound by the Texas A&M Identity Services Acceptable Use Policy, the University FERPA Policy and University Acceptable Use Guidelines.

I HAVE READ, UNDERSTOOD AND AGREED TO THE ABOVE TERMS

Requestor Name (Printed)	Supervisor Name (Printed)
Requestor Title	Supervisor Title
Requestor Department	Supervisor Department
Requestor Signature Date	Supervisor Signature Date

For IT Infrastructure & Operations Use Only

Notes:

Signatures:

ITIO Director Signature Date	CISO Signature Date

Date Received	Request Number
Assigned Contact:	