

Identity Management Office
Division of Information Technology



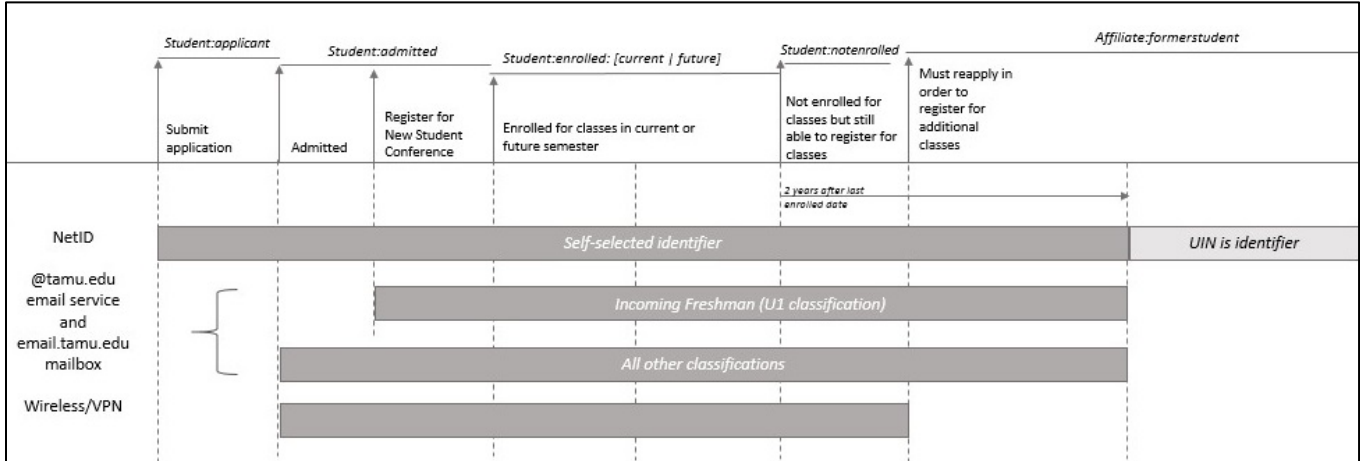
NetID Account Management

For Texas A&M University Students

Table of Contents

| | |
|---|----|
| Student Lifecycle Stages | 3 |
| NetID Account | 7 |
| NetID Account Management | 8 |
| Appendix A: Student Data sent to the Texas A&M NetID IdMS | 13 |
| Appendix B: Student Directory Entries | 14 |

The NetID account is a Texas A&M University student’s primary login account and is used to access all Texas A&M on-line resources. This document summarizes the management of a student’s NetID account through the various stages of the student lifecycle to assist departments and students better understand the processes at work.



Student Lifecycle Stages

The Texas A&M NetID Identity Management System (IdMS) utilizes data from the Texas A&M Banner (Compass) system to manage student accounts, so an understanding of how students are tracked in this system is helpful for understanding a student’s NetID account management.

It is possible for an individual to have multiple student roles at the same time. For example, a currently enrolled senior undergraduate who has applied to graduate school will be both an enrolled student and an applicant. It is also possible for a student to have a relationship with more than one campus or site. Students commonly apply to more than one Texas A&M campus (e.g. College Station and Galveston), are admitted to more than one campus, and may even enroll for courses at more than one campus in the same semester.

Applicant

An applicant is a prospective student who has submitted an application for a specific Texas A&M campus, semester, and major.

- Office of Admissions manages the admission process for all undergraduate applicants.
- Each department manages the admission process for their graduate students so methods governing graduate student admissions vary.

The student’s information enters the Texas A&M student information system, Compass, in one of three ways:

- Student submits an application for admission to Texas A&M University at www.applytexas.org. Submitted applications are downloaded by Admissions nightly.

- Student delivers paper application to the Office of Admissions. Data is manually entered by personnel in that office.
- The Mays Business School maintains an independent system to process applicants to their graduate programs. Once admission is approved, they load the student's information into Compass.

Type of applicants:

Students apply under a variety of circumstances. The application acceptance timeframe varies according to the applicant type, with international applicants having a much longer period of time to submit an application.

Freshman Domestic

A Domestic Freshman applicant is:

- a citizen or permanent resident of the United States; someone who has applied for permanent residency; or who qualifies for Texas residency based on Senate Bill 1528;
- a degree-seeking applicant without college credit or whose only college credit was received prior to high school graduation.

Freshman International

An International Freshman applicant:

- is **not** a citizen or permanent resident of the United States,
- has never enrolled at Texas A&M as an undergraduate degree-seeking student, and
- is a degree-seeking applicant without college credit or whose only college credit was received prior to high school graduation.

Transfer Domestic

A Domestic Transfer applicant:

- is a citizen or permanent resident of the United States; someone who has applied for permanent residency; or who qualifies for Texas residency based on Senate Bill 1528;
- is a degree-seeking applicant,
- has graduated from high-school or equivalent,
- has enrolled in a post-secondary institution,
- does not have a bachelor's degree, and
- does not qualify for readmission.

Transfer International

An International Transfer applicant:

- is **not** a citizen or permanent resident of the United States, and
- is a degree-seeking applicant,
- has graduated from high-school or equivalent,
- has enrolled in a post-secondary institution,
- does not have a bachelor's degree, and
- does not qualify for readmission.

Readmission Undergraduate

An applicant for Readmissions at the Undergraduate level:

- is a former degree-seeking Texas A&M undergraduate student (including an international student),
- does not have a bachelor's degree, and
- did not officially register for the previous semester (excluding summer sessions) at Texas A&M.

Type of applicants, continued:

Readmission Graduate

An applicant for Readmissions at the Graduate level:

- previously attended Texas A&M University and did not complete the degree they were seeking at time of last enrollment, and
- did not officially register for the previous semester (excluding summer sessions) at Texas A&M.

Note: Applicants whose only previous enrollment at Texas A&M has been at a non-degree status do not qualify for readmission.

Post-baccalaureate Undergraduate

A Post-baccalaureate Undergraduate applicant:

- has a bachelor's degree, and
- wishes to pursue a second undergraduate degree.

Non-Degree (Undergraduate)

A Non-Degree (Undergraduate) applicant:

- wishes to take specific undergraduate course work, and
- does not wish to pursue a degree at Texas A&M.

Graduate Domestic

A Domestic Graduate applicant:

- is a citizen or permanent resident of the United States, or someone who has applied for permanent residency,
- is a student who holds a bachelor's or professional degree (or equivalent), and
- is a degree-seeking applicant.

Graduate International

A International Graduate applicant:

- is **not** a citizen or permanent resident of the United States, and
- is a student who holds a bachelor's or professional degree, or equivalent, is seeking a degree at the graduate level, and
- has not previously attended Texas A&M University. (International students with a bachelor's degree from Texas A&M University who wish to pursue a graduate degree here will need to submit a "domestic graduate" application.)

Graduate Non-Degree Seeking

A Graduate Non-Degree Seeking applicant:

- has completed an undergraduate degree, and
- wishes to take graduate level courses without applying for admission into a graduate degree program.

Possible transitions:

1. Application approved and person admitted to plan of study. Record switches to **admitted** status.
2. Application is not approved.

Admitted Student

An admitted student:

- is eligible to enroll for courses, and
- either the enrollment period for the admitted semester has not begun or, once the enrollment period is open, the admitted student has not yet enrolled for courses.

Possible transitions:

1. Student enrolls for courses in the admitted semester. Record switches to **continuing enrolled** status.
2. Student does not enroll for courses in the admitted semester.

Note: *If a student does not enroll for the applied semester, they must request a deferral to change their admitted semester to a later semester. Otherwise, they must submit a new application to the University.*

What is the Enrollment Period?

The enrollment period for a semester lasts from the first day of early enrollment to the 5th day of classes for that semester. A student can initiate enrollment for a semester as late as the 12th class day. The official reporting date of a semester is when Texas A&M knows a student is not planning to attend that semester. This is the 20th class day of long semesters, 15th class day of the summer sessions (1st and 10 week summer sessions have the same reporting date, 2nd summer session has a separate date).

Continuing Enrolled Student

A continuing enrolled student is enrolled in courses for the current or a future semester.

Possible transitions:

1. Student drops all classes prior to the drop date. Record switches to previous status.
 - a. If student was admitted, the record switches to **admitted** status.
 - b. If student completed coursework at Texas A&M previously, they will switch to **not enrolled** or **former student** status depending on whether or not they remain eligible to register for classes.
2. Student withdraws from the university during the semester. Since a withdrawn student's eligibility for enrollment in future semesters is the same as for a student that completes the current semester's courses, their status will not change until the semester ends. At that time, the status will change based on whether they enroll for courses in the upcoming semester.
3. Student dismissed from the university due to poor grades, etc.
4. Student completes current semester courses and enrolls for courses in the next semester. The record remains in the **continuing enrolled** status.
5. Student completes courses and does not enroll for courses in the next semester. Record switches to **not enrolled** status.
6. Student graduates and receives degree. Record switches to **former student** status.

Not Enrolled Student

A not enrolled student:

- is eligible to enroll for courses, and
- is not enrolled for courses in the current or a future semester, and
- has accrued hours at the university.
Note: *A newly admitted student that registers for courses and then drops them will not transition to the not enrolled state. They will revert back to an admitted status.*

Possible transitions:

1. Student enrolls for courses before their enrollment eligibility expires. Record returns to **continuing enrolled** status.
2. Student does not enroll for courses before the enrollment eligibility expires. Record switches to **former student** status.

Enrollment Eligibility Duration

The length of time a student is eligible to enroll for courses varies based on classification:

Undergraduate Students:

- must have been enrolled in the previous long semester (Fall or Spring)
- did not graduate in previous semester
or
- have been approved for continuous enrollment (exception indicator)

Graduate students

- may skip one long semester for enrollment
- did not graduate in the previous semester
or
- have been approved for continuous enrollment (exception indicator)

Active Student

Students that are eligible to register for classes are often collectively referred to as active students. This group encompasses admitted students, continuing enrolled students and not enrolled students.

Former Student

A former student:

- has accrued hours at the university,
- has or has not completed a degree program, and
- is not eligible to enroll for courses (they must reapply and be readmitted in order to take more courses).

Deceased Student

A deceased student is a student that has died. This can happen at any point during the academic program.

NetID Account

What is a NetID account?

A NetID account is the Texas A&M University login account. It consists of the following:

| | Example |
|---|---|
| Identity Data | |
| Biographical information | name, birth date |
| Contact information | work address, office phone number, email address |
| Identifiers | UIN, NetID |
| Affiliations with organization | faculty, staff, employee, student, affiliate For employees: position type, title, department For students: classification, major department |
| Login Credential | |
| Login Identifier | NetID |
| Material used to verify person logging in is the account holder | Password Password + Duo two-factor authentication |

How is the NetID account used?

Campus personnel use the NetID account to access a variety of university, commercial and federal services.

When a person logs in to an application, two things happen:

- They enter the login credential to verify they are the account holder (authenticate).
- The application evaluates what features should be displayed to the person (authorization).

To make the authorization decision, the application can use either internally or externally maintained information. The Canvas Learning Management System is an example of an application using internally maintained information, which are preloaded class rosters. When the student or instructor logs into Canvas, they will only see the sections on which they are listed, and the functionality they have is determined by their role. Instructors can assign homework and see grades for all students in the section, while students can edit and submit their own homework and view their own grades. An example of an application using externally maintained information is Linked In Learning. It uses information in the NetID IdMS to determine whether or not someone is eligible to access material under the Texas A&M contract.

Because applications increasingly rely on data in the NetID record to determine what features an account holder is allowed to use, the identity data associated with a NetID account is just as important as whether or not the login credential is functioning.

NetID Account Management

The NetID account lifecycle consists of an initialization phase, an operational phase, and a termination phase.

Initialization Phase

The initialization phase results in the successful enrollment of the student in the Texas A&M NetID Identity Management System (IdMS) and the establishment of the NetID Credential.

Enrollment

Creation of a record for the student in the Texas A&M NetID IdMS

In order for a student to claim a NetID account, the following basic identity data is required by the Texas A&M NetID IdMS: UIN, Full Name, and Date of Birth. Systems of Record that sponsor NetID accounts typically provide information about a person's role or relationship with the university in addition to this basic data.

The Texas A&M Banner (Compass) system serves as the System of Record and sponsor for applicant, admitted student, continuing enrolled student, not enrolled student and former student NetID accounts and sends data about students, along with details about their role and degree program, to the NetID IdMS. This data is used to automate management of the student NetID accounts. The NetID IdMS receives updates from Texas A&M Banner once per day. Enrollment of a new student in the Texas A&M NetID IdMS is triggered when a record for the student is received by Texas A&M Identity Services via the Banner update.

Credential Issuance

Establishment of student's Texas A&M NetID Credentials

Initially, a student will establish a NetID Credential that consists of a NetID/password pair. Texas A&M NetID Credential establishment or activation is a self-service on-line process, accessed by going to <http://gateway.tamu.edu> and clicking the **Claim Your NetID** link. The student will then be stepped through the process of selecting a NetID and setting a password.

Two-factor NetID Credential

Students that are concerned about their account security have the option of setting up two-factor authentication on their NetID account. The Texas A&M University System uses Duo Two-Factor Authentication to support the second factor. A student enables Duo on his or her NetID account by completing the enrollment process using the self-service NetID Duo Enrollment application (<https://gateway.tamu.edu/duo-enroll>).

Continuing Enrolled students are required to have Two-Factor Authentication set up on their account.

Operational Phase

During the operational phase, the student manages his or her NetID Credential and keeps it secure. The Texas A&M NetID IdMS manages the NetID Credential data and status and securely maintains the identity information supplied by the Texas A&M Banner system. The student uses his or her NetID Credential to access on-line resources.

Student Use of Credential

Campus applications have the option of utilizing the NetID account for their users instead of maintaining their own accounts. When a student authenticates to an application that relies on the NetID account for authentication, the application passes the authentication request to the NetID IdMS to verify the supplied Credential is valid.

NetID IdMS Credential Management

Temporary Lockouts

If a student mistypes their password multiple times in a row, the student will be temporarily locked out. CAS will not accept an authentication attempt from a user for 15 minutes after they type their password incorrectly seven times in seven minutes. For students with Two-Factor authentication set up on their account, Duo will not accept an authentication attempt for 15 minutes after seven consecutive failed Duo authentication events.

Monitoring Suspicious Credential Activity

Monitoring of NetID Credential activity is a program operated by Texas A&M NetID IdMS Operations in conjunction with the Division of IT Security.

CAS login activity is audited for suspicious Credential activity. Reports are delivered to the Texas A&M NetID IdMS Operations administrators for review and further action if necessary. If a Credential is determined to be compromised, the Credential is revoked and the student's NetID account locked.

The student's NetID account can be unlocked only by designated Division of IT Security or NetID IdMS Operations staff.

Credential Expiration/Re-issuance

For security reasons, students are required to change their passwords periodically. The life of a password depends on the length. Passwords that are eight to sixteen characters must be changed after one year of use. Passwords over sixteen characters can be used for four years before the student has to set a different password.

Three weeks prior to password expiration, the student is notified via e-mail of the pending expiration. If the student does not establish a new password, a second notice is sent via e-mail two weeks prior to the expiration date. One week prior to the expiration date, a final notice is sent.

The student can set a new password in one of three ways:

- The student logs into the Password Change application (<https://gateway.tamu.edu/change-password>) with his or her existing NetID Credential prior to the expiration date and set a new password.
- If the student has previously set up Self-Service Password Reset, the student may use the Self-Service Password Reset application (<https://gateway.tamu.edu/password-reset/>) to set a new password. The Self-Service Password Reset application sends a short-lived single use Secret to the e-mail or phone number on record that the student must submit in order to establish a new Credential.
- The student may call or stop by Help Desk Central to have their NetID account flagged for a password reset via the Forgotten Password Reset application.

If the student does not change his or her password prior to the expiration date, the NetID Credential will be destroyed and the student will not be able to authenticate to any application until a new password is set. At this point, the student will only be able to reset their password by using Self-Service Password Reset or by contacting Help Desk Central for assistance.

Termination Phase

In the termination phase, the student's NetID account is deleted. The only students whose accounts are fully deleted are applicants and admitted students that have never accrued course credit at Texas A&M University.

Once a student has completed a semester of coursework at Texas A&M, they will always be eligible to have a NetID account¹. The resources the student is able to access with the account and the management of the account will change, but the student will always have access to an account.

Credential Revocation

To render the student's NetID Credentials invalid and unusable.

Applicants and Admitted Students

For applicants and admitted students,

- Admissions stops sponsoring the student's NetID account on the 20th class day of the application semester and the student's record ceases to be included in the update sent to the NetID Identity Management System.
- Seven days later, the student's NetID account is deleted.

¹ Electronic management of student records started when the Student Information Management System (SIMS) was implemented in the mid-1980s. Records for students that graduated prior to Fall 1985 were not loaded into the student information system unless the student requested electronic access to their student records.

While a student that graduated prior to Fall 1985 will need to have their data loaded into the student and NetID system before they can claim a NetID account, they are eligible for the account.

If the applicant or admitted student is associated with the university in multiple ways², the presence of the other affiliations on the NetID account will prevent the account from being locked or disabled in any way. Otherwise, to extend access to the account the applicant or admitted student will need to have the semester associated with their application changed to a future semester or submit a new application to the university for a future semester.

Former Students

Students that have accrued semester hours will slowly lose access to resources as part of transitioning from a continuously enrolled to former student:

- Most services (for example, wireless, VPN, and remote library access) become unavailable once the student transitions to a former student status.
- Two years after the last enrollment date³:
 - the student's @email.tamu.edu mailbox, Google Drive contents and @tamu.edu email service are deleted

Former Student email service options

While a former student will only retain their @email.tamu.edu mailbox for two years after their last enrollment date, they have the option of setting up an Association of Former Students' Aggie Network email account. These accounts are also hosted by Google and a former student can transfer ownership of any email and Google Drive contents they wish to retain to the Aggie Network account, ensuring that they will continue to be able to access these messages and files.

For more information, visit <https://www.aggienetwork.com/email/>.

- the student transitions from a Full-Service NetID account with a self-selected identifier to a Former Student NetID account that uses their UIN as the identifier⁴

Handling of Deceased Student Accounts

As soon as a student's status switches to deceased in the NetID system, the student's NetID account is locked, the White Pages directory entry is suppressed (no longer publicly available) and @tamu.edu email delivery is disabled.

The GoogleApps account locking and deletion will vary depending on whether or not the student was also an employee.

- If the student was also employed, the supervisor will be notified of pending account deletion over a 3 week period. Once all notifications have been sent, the GoogleApps account is locked and one week later it is deleted.
- If the student was not also employed, the GoogleApps account is locked as soon as the student's status is switched to deceased. The GoogleApps account is deleted 3 weeks later.

² For example, the individual is an employee as well as an applicant.

³ Where the last enrollment date is defined as the date the student was last enrolled in classes.

⁴ If the student is not a US citizen, they will retain access to the Full-Service NetID for 3 years instead of 2 years to facilitate their interactions with Immigration Services for Students for that additional year.

Extended Account Access

In some situations, a former student may have a legitimate need to continue accessing resources typically limited to active students. Most often this is due to an ongoing relationship with their former department where the student is actively engaged in research or some other program.

To preserve the former student's access to campus resources, the department will fill out and submit a NetID Request Form⁵ documenting the nature of the new relationship. The Identity Management Office will then update the NetID account with a role that reflects the person's new affiliation.

⁵ The NetID Request Form can be downloaded from <http://url.tamu.edu/netidrequest>.

Appendix A: Student data sent to the Texas A&M NetID IdMS

Texas A&M student data is received from the student information system, Compass (TAMU Banner). This appendix documents the record inclusion criteria for the main and supplementary student feeds.

Primary student data feed

Enterprise Information Systems (EIS) supplies identity and degree plan information nightly for:

- Current⁶ and future semester applicants
- Current⁵ and future semester admitted students
- Current⁷ and future semester continuing enrolled students
- Current⁸ and future semester not enrolled students

Table 1: Rules governing inclusion of Texas A&M student records in data feed

| Student Status | Texas A&M NetID IdMS feed inclusion rules | Status Code in feed |
|---------------------|--|---------------------|
| Applicant | application submitted for a current ⁵ or future semester | set to 'P' |
| Admitted | admitted for a current ⁵ or future semester | set to 'A' |
| Continuing Enrolled | enrolled in current ⁶ or future semester courses OR registered to graduate in the current ⁴ or future semester | set to 'E' |
| Not Enrolled | eligible to register for current ⁵ or future semester classes | active status code |

The primary control for the inclusion of student records in the data feed is the semester. Reliance on the semester has some consequences that should be kept in mind:

- A student whose application is denied will still show as an applicant for that semester in the feed. This is done to ensure that the student is notified of the denial by Admissions, not as a consequence of loss of access to the application web site.
- A student that dies will still show as an applicant, admitted or enrolled student for that semester in the feed. The feed contains a deceased flag which is set to indicate that the student has died.

⁶ Applicants and admitted students are included in the nightly data feed up to the 21st class day of the semester to which they applied. The record is excluded from the data feed prior to the 21st class day only if the decision status field in Compass is set to 'Offer Declined/Cancelled'.

⁷ A semester is defined as current on the first class day of the earliest scheduled section offering in that semester. The semester loses current semester status on the day after the last class day of the latest scheduled section offering in that semester.

⁸ Not enrolled students eligible to register for current semester classes are included in the nightly data feed up to the 21st class day of the semester. The feed then switches to including the not enrolled students eligible to register for the upcoming semester.

- An enrolled student that withdraws or is dismissed will still be included in the feed as enrolled for that semester.

Supplementary student data feed

It is fairly common for students to switch majors or make other degree program changes during their time at the university. Just as with the student’s application to the university, all degree program changes are associated with a particular semester. Degree program changes made after the 20th class day of the current enrollment semester are associated with the upcoming, rather than the current, enrollment semester.

To ensure students changing majors immediately receive access to resources tied to their new major, EIS sends a supplementary feed that includes future semester degree plan information nightly for all active⁹ students.

Once a semester, EIS sends a file containing the list of all students that have accrued credit for the semester. This data is appended to a table that contains all semester credit data and is used to manage former student status and accounts.

Appendix B: Student Enterprise Directory Entries

TAMU Banner-supplied data stored in Enterprise Directory People branch entries

Table 2: TAMU Banner data in Enterprise Directory People branch entries

| Attribute | Comments |
|--|--|
| Personal data | |
| Universal Identification Number (tamuEduPersonUIN) | |
| TAMU BannerID (tamuEduPersonBannerID) | |
| Name: | |
| Official Name (tamuEduPersonOfficialName) | |
| Common Name (cn) | cn attribute will always have tamuEduPersonOfficialName as one of the values |
| Last Name (sn) | |
| First Name (givenName) | |
| Date of Birth (birthDate) | |
| Student Local Phone (tamuEduPersonLocalPhone) | |

⁹ This encompasses admitted, enrolled and not enrolled students.

| Attribute | Comments | | | | | | |
|--|---|---------------|---------------|---------------|--------------|--------------|--|
| Personal data, continued | | | | | | | |
| Privacy Flags (tamuDeduSuppress) | <p>FERPA suppression flags used in directory:</p> <ul style="list-style-type: none"> - name: all directory information suppressed - email: email address suppressed - homephone: local telephone number suppressed - major: plan of study information suppressed - classification: classification information suppressed - studentID: student's UIN suppressed | | | | | | |
| Student data | | | | | | | |
| TAMU Role-based Affiliations tamuDeduPersonAffiliation | <p>Recognized roles:</p> <p>affiliate:appliedstudent – applicant for current or future semester</p> <p>affiliate:admittedstudent – admitted for current or future semester</p> <p>student:enrolled:[current future] – continuing enrolled student</p> <p>student:degreeonly – student registered in current semester only to graduate (taking no classes)</p> <p>student:notenrolled – former student eligible to register in current/future semester without reapplying</p> <p>affiliate:formerstudent – former student, i.e. a person that completed courses at Texas A&M in the past</p> <p>affiliate:alumni – student that has received a degree from Texas A&M University</p> <p>student:deceased – deceased student</p> | | | | | | |
| Higher Ed Role-based Affiliations eduPersonAffiliation eduPersonPrimaryAffiliation | Broader role categories (student/member/affiliate) | | | | | | |
| TAMU Location-based Affiliations | | | | | | | |
| <i>Campus:</i> | | | | | | | |
| tamuDeduPersonScopedAffiliation scoping for all TAMU students | <table border="0"> <tr> <td>@cs.tamu.edu</td> <td>@hsc.tamu.edu</td> <td>@law.tamu.edu</td> </tr> <tr> <td>@gv.tamu.edu</td> <td>@qt.tamu.edu</td> <td></td> </tr> </table> | @cs.tamu.edu | @hsc.tamu.edu | @law.tamu.edu | @gv.tamu.edu | @qt.tamu.edu | |
| @cs.tamu.edu | @hsc.tamu.edu | @law.tamu.edu | | | | | |
| @gv.tamu.edu | @qt.tamu.edu | | | | | | |
| Role@Location Affiliations | | | | | | | |
| TAMU Scoped Affiliations (tamuDeduPersonScopedAffiliation) | Student's tamuDeduPersonAffiliation flag scoped to TAMU campus, e.g. student:enrolled:current@cs.tamu.edu | | | | | | |
| Higher Ed Scoped Affiliations (eduPersonScopedAffiliation) | eduPersonAffiliation flags scoped to identity provider domain (@tamU.edu) | | | | | | |

| Attribute | Comments |
|---|---|
| Student data, continued | |
| Course Affiliations | |
| Course Affiliation URNs (eduCourseOffering) | Current semester courses in which a student is enrolled. |
| Scoped Course Affiliations (eduCourseMember) | Role@course for all current semester courses in which a student is enrolled. |
| Plan of Study: | |
| Major Codes (tamuEduPersonMajor) | populated for current or future enrolled students only |
| Primary Major Code (tamuEduPersonPrimaryMajor) | populated for current or future enrolled students only |
| Primary Major (tamuEduPersonPrimaryMajorName) | populated for current or future enrolled students only |
| Classification Code (tamuEduPersonClassification) | populated for current or future enrolled students only |
| Classification (tamuEduPersonClassificationName) | populated for current or future enrolled students only |
| Data Source (tamuEduDataFeed) | EIS is listed as one of the account owner's data source affiliations TAMUROSTER is listed if course affiliation attributes populated using EIS roster data |

Student-supplied data stored in Enterprise Directory People branch entries

In addition to data provided by TAMU Banner, students can add the information itemized in Table 3 to their directory entries.

Table 3: Account holder-supplied data in Enterprise Directory People branch entries

| Attribute | Comments |
|---|----------|
| NetID (tamuEduPersonNetID) | |
| Display Name (displayName) | |
| Published Email Address (mail) | |
| Primary and Alternate Aliases (mailLocalAddress) | |
| Email Destination Address (mailRoutingAddress) | |
| @email.tamu.edu Alias (tamuEduNeoLocalAddress) | |
| All Texas A&M Email Aliases (tamuEduLocalMailAddresses) | |
| Published Home Page URL (personalURI) | |

Management of TAMU Banner-supplied data in Enterprise/White Pages People Branch Entries

Presence/absence of data

Storage of student information in LDAP is affected by the student's status:

- When a student record drops out of the TAMU Banner data feeds, all attributes listed under the **Student Data** category except the affiliation attributes are cleared of TAMU Banner data.

Accessibility of data

Data in the Enterprise Directory is accessible only via web services or Shibboleth.

The default data returned about a person from the web services is that classified as publicly or anonymously readable. In order to access restricted data, a request for data access must be submitted and approved.

Applicants, admitted students, not enrolled students and former students are defaulted to full data ('name') suppression if the account owner has no other role at the university. Continuing enrolled student data will vary in accessibility based on the student's specified FERPA suppression. Continuing enrolled students may request the following types of data withheld:

- Name (full record)
- Universal Identification Number (UIN)
- email address
- local address
- permanent address
- local telephone number
- permanent telephone number
- program of study
- classification
- dates of attendance
- previous educational institutions attended
- degrees, honors and awards received
- participation in officially recognized activities and sports

Only a subset of the above information is loaded into the Enterprise Directory, so only six suppression flags are needed to enable/disable access to a student's data. These flags are stored in the tamuEduSuppress attribute. Table 4 summarizes the impact of each flag on the accessibility of a student's data.

Table 4: Data access for Enterprise Directory attributes storing student data as a function of account owner’s FERPA suppression category.

| Attribute | Accessibility of data | | | | | | |
|---|-----------------------|------------|------------|------------|------------|----------------|------------|
| Account owner’s FERPA suppression category: | none specified | name | email | homephone | major | classification | studentID |
| Personal data | | | | | | | |
| Universal Identification Number (tamuEduPersonUIN) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| TAMU BannerID (tamuEduPersonBannerID) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Name: | | | | | | | |
| Official Name (tamuEduPersonOfficialName) | public | restricted | public | public | public | public | public |
| Common Name (cn) | public | restricted | public | public | public | public | public |
| Last Name (sn) | public | restricted | public | public | public | public | public |
| First Name (givenName) | public | restricted | public | public | public | public | public |
| Display Name (displayName) | public | restricted | public | public | public | public | public |
| Date of Birth (birthDate) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Student Local Phone (tamuEduPersonLocalPhone) | public | restricted | public | restricted | public | public | public |
| Home Page URL (personalURI) | public | restricted | public | public | public | public | public |
| Privacy Flags (tamuEduSuppress) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Student data | | | | | | | |
| Role-based Affiliations | | | | | | | |
| TAMU Role-based Affiliations (tamuEduPersonAffiliation) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Higher Ed Affiliations (eduPersonAffiliation) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Higher Ed Primary Affiliation (eduPersonPrimaryAffiliation) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Role@Location Affiliations | | | | | | | |
| TAMU Scoped Affiliations (tamuEduPersonScopedAffiliation) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Higher Ed Scoped Affiliations (eduPersonScopedAffiliation) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Course-based Affiliations | | | | | | | |
| Course Affiliation URNs (eduCourseOffering) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Scoped Course Affiliations (eduCourseMember) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Plan of Study: | | | | | | | |
| Major Codes (tamuEduPersonMajor) | public | restricted | public | public | restricted | public | public |
| Primary Major Code (tamuEduPersonPrimaryMajor) | public | restricted | public | public | restricted | public | public |
| Primary Major (tamuEduPersonPrimaryMajorName) | public | restricted | public | public | restricted | public | public |
| Classification Code (tamuEduPersonClassification) | public | restricted | public | public | public | restricted | public |
| Classification (tamuEduPersonClassificationName) | public | restricted | public | public | public | restricted | public |

| Attribute | Accessibility of data | | | | | | |
|---|-----------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| Account owner's FERPA suppression category: | none specified | name | email | homephone | major | classification | studentID |
| Account-related data | | | | | | | |
| NetID (tamuEduPersonNetID) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| Email: | | | | | | | |
| Primary/Published Email Address (mail) | public | restricted | restricted | public | public | public | public |
| Primary and Alternate Aliases (mailLocalAddress) | public | restricted | restricted | public | public | public | public |
| Email Destination Address (mailRoutingAddress) | restricted | restricted | restricted | restricted | restricted | restricted | restricted |
| @email.tamu.edu Alias (tamuEduNeoLocalAddress) | public | restricted | restricted | public | public | public | public |
| All Texas A&M Email Aliases (tamuEduLocalMailAddresses) | public | restricted | restricted | restricted | restricted | restricted | restricted |

Managing data access for account holders with multiple roles

In addition to pursuing a course of study, Texas A&M applicants, admitted students, continuing enrolled students, not enrolled students or former students may work for the Texas A&M University System. Accessibility of the student's data may be affected by the employee relationship.

Texas A&M University System employees in faculty and staff positions are not allowed to restrict access to information about their position—their name, title, department, office phone, email address, etc.—unless requested by a law enforcement agency. For an applicant, admitted student, not enrolled student or former student who is also Texas A&M University System faculty or staff, the full data suppression requested in the TAMU Banner feed is ignored and the data accessibility rules for employees are used to manage access to data in the record. However, for university faculty or staff personnel who are also continuing enrolled students, the suppression settings in the TAMU Banner feed will be honored.

If the employee holds a student worker position, access to position data is always restricted in the directory to comply with FERPA. For these employees, the suppression settings in the TAMU Banner feed are always honored.