Questions: Auburn IAM RFP

1. In order to accurately price the IAM service, please provide the number of identities you plan to manage and the estimated % of that population that will likely authenticate at least once each month for the following groups: Students, Employees, Affiliates and Service Accounts.

The Office of Information Technology currently maintains the identities of approximately 70,000 active user accounts consisting of Students, employees, affiliates and service accounts, as well as approximately 46,000 alumni accounts. Annual turnover is approximately 15,000 users. User ID's originate from both our ERP system (Banner) as well as some external processes for departmental and service accounts. During semester changeover there may be updates or additions of 30,000 identities in a single night.

80% active users will authenticate at least once/mo

25% Alum ( though currently only to o365 – not enterprise )

2. Appendix A, under Lifecycle, lists 'Unique NetID generation' as a requirement. Does Auburn have a specific, single algorithm that is used for that today? Are the current algorithm(s) for such required to be used by the solution? If not, what range of options (rule sets) for how to generate such does Auburn consider to be 'good enough'? Does Auburn currently allow any population to choose their NetID, and if so, is it a requirement to continue that support? When in the user lifecycle is a NetID assigned? For example, do all students who are applying to Auburn get one assigned, or do they only get one assigned at the point they accept an offer for admission?

NetID format is FMLnnnn for all person entities. We are not looking to change at this time. User names are assigned upon hire for employees, upon institutional acceptance for students.

2. Banner is the only "system of record" that is explicitly mentioned in the RFP as a source of identities. Can the solution assume that is the only source of identities that needs to be accounted for by the proposed solution today? There is no other source of identities that needs to be accounted for?

Currently true for person entities, but ideally solution would not make that assumption going forward to allow for changes in HR/SIS systems in the future.

4. Appendix A, under Lifecycle, lists a requirement of 'auto expire unclaimed accounts'. Is there one fixed "after X days" remove such an account? Or does the policy need to vary by role (e.g. faculty versus staff versus student)? What, exactly, does Auburn consider "expire" to mean? Simply make the account as needing manual handling to activate, delete the account altogether (but then there is a discrepancy between Banner and the identity registry), or what? And is there some sort of notification requirement if this is done, and to whom?

Should be variable – employee, student, graduate student, affiliate, etc. Expire would be a state where the account could no longer be claimed and marked for future deletion.

5. Appendix A, lifecycle, Auburn does not explicitly mention anything about identities/accounts that are established from the start with a specified end date (e.g guess. sponsored account), and any needed requirements around associating a sponsor with such an account, notification of when such an account is due to expire, etc. Are there current requirements for such?

Our current vault maintains attribute for recording that information, and a custom workflow for expiration if not renewed.

6. Appendix A, under Data Governance, there is a requirement of 'Real-time access reports'. What does that mean, exactly? Real-time access to what? Is that talking about logins through SSO, is it talking about admins currently logged into and managing stuff within the solution, or is that meant to cover users logging in and using any provisioned service? Or does that simply mean "tell us who the identity system currently considers has access to X"? Noting that the only visibility an identity solution would usually have to "who is logged into what" would be based on current SSO sessions to the extent such could be identified.

In this context one view of all resources granted to the individual, whether requested or birthright.

7. Appendix A, under Data Governance, there is a requirement of 'Real time access revocation'. What is that intended to mean? Does that simply mean being able to push through in "real time" a

de-provisioning access update to impacted downstream services? If not, what all functionality is supposed to be covered by this requirement?

Yes – ability to remove access to resources in real-time or near real time upon termination or revocation of affiliation with AU.

8. Appendix A, under Password Management, there is requirement of "Multiple password policies". Can you elaborate on this requirement? What would be the criteria for one password policy being applied to a given person/account versus a different policy? And, if that is supposed to be based on roles, but a person has multiple roles, then what policy is supposed to apply?

Ability to enforce different password complexity and or expiration based on role. Mainly considering different type of accounts (normal, privileged, service account, etc ) but if base don roles most stringent policy should be applied.

Auburn University IAM RFP Questions.

1. In order to accurately price the IAM service, please provide the number of identities you plan to manage and the estimated % of that population that will likely authenticate at least once each month for the following groups: Students, Employees, Affiliates and Service Accounts.

The Office of Information Technology currently maintains the identities of approximately 70,000 active user accounts consisting of Students, employees, affiliates and service accounts, as well as approximately 46,000 alumni accounts. Annual turnover is approximately 15,000 users. User ID's originate from both our ERP system (Banner) as well as some external processes for departmental and service accounts. During semester changeover there may be updates or additions of 30,000 identities in a single night.

80% active users will authenticate at least once/mo

25% Alum (though currently only to o365 – not enterprise )

2. What is the total number of student workers?

   ~ 8500

3. In your current solution, what is the system of record for Affiliate, Departmental and Service accounts?

   Affiliates via Banner
   Non-person accounts direct entry to identity vault after request approved.

4. Are there any other authoritative sources of information besides Banner in your existing NetIQ system and if so, please describe the source system and what data is being pulled in.

   ID badge info – Lennel/LSI via JDBC

5. Are Affiliate, Departmental and Service accounts managed in your existing IAM system?
   Yes

6. How do users request access today?

   In-house account request forms, submitted via computing coordinators.

7. What kind of approval processes do you envision for access requests in the new system?

   On-line, manager/Director or Data owner where appropriate.
8. Please provide a list of all current integrations with your NetIQ environment. Are there any logical or physical diagrams of the existing IAM solution that can be shared?

   See document provided.

9. Please describe your Active Directory environment. How many forests/domains and what does the hierarchy look like. i.e; all users in a single OU, or distributed across multiple OU's. If multiple OU's what is the business logic used to determine where to place a user.

   Single forest. Multiple OU's based on home org ( dept. )

10. How are you currently managing users in Microsoft Azure/Office 365?
    AAD Connect

11. How do you currently assign Office 365 licenses to users?
    Azure Dynamic groups

12. Please describe the type of integration you would like to see with Service Now. Is this for managing Service Now accounts, or integration with ticketing, or using Service Now as a front end for access requests.

    Would like to integrate access requests into service catalog.

13. In your existing NetIQ environment, can you please describe the Identity schema? What attributes are being stored for each identity?

See Schema document

14. In your existing environment today, what are the biggest challenges that you would like to see solved with a new platform?

Reduce or eliminate premise dependency for could services, better access reporting and auditing.

15. Please describe your requirements for password synchronization.

Password sync is only used for a couple of targets, would like to see better SSPR and account claiming process than we have with in-house application.

16. Can the University please clarify what they are requesting within Tab 11: Vendor Disclosure Statement? What format should this vendor disclosure statement be in?

Defer to Purchasing

Q1: How many affiliate/contractor accounts are in the current system and, of those, how many are able to authenticate?

A1: Roughly 3000 total affiliate accounts and about half are authenticable.

Q2: How many student alumni require authentication privileges?

A2: Currently we have about 40,000 alumni who have retained AU branded Office 365 e-mail accounts; however, they fall out of our primary authentication source, Active Directory, 1 year after graduation. We hope to shift into a model where all alumni are able to authenticate to something other than Active Directory in order to request transcripts, update their mail forwarding preference, etc.

Q3: Is there a desire to be able to automatically lock down physical access should AU come under a physical attack from an outside threat?

A3: That is not in the scope of this RFP.

Q4: To what downstream systems/platforms do the various identities that come into the IAM system through Banner or are created ad hoc by the IAM group (departmental accounts) flow?
A4: See attached reference document AU-IAM-NetIQ-Data-Provisioning.docx.

Q5: What is the breakdown of the various types of employees?
A5: Roughly 15,000 total employees composed of full time, part time and student workers. Full time number is around 5300.

Q6: Is there an account claiming process?
A6: Yes, through our home grown *MyAccount* site that we would like to replace. We currently provision accounts with a *just in case* method and we would like to move to a *just in time* method so that we have less security and account compromise risk.

Q7: Is Auburn looking for any continued managed services?
A7: No.

Q8: How flexible is Auburn on the timing with regard to the pre-bid conference and any follow-up questions vendors may have? Current deadline for submitted questions is Feb 12, 2020 – can that be pushed?
A8: PPS will update the vendor site with a new date; likely Feb 19, 2020.

Q9: When is the projected go-live date?
A9: As an academic institution, we prefer a summer time frame when there are less people and things going on around campus. We are not expecting full implementation by then but hope to get the bulk completed in the 2020 calendar year.

Q10: What is the most important component to this project for it to be considered successful?
A10: High level of availability and business continuity should AU lose power.
Modernization of our IAM system as we are beginning to fall behind with our current technologies.
Real time provisioning and de-provisioning of users.
Auditability – knowing what access a user has to which system, last logon, etc.

Q11: Is there currently a formal attestation process for access requests?
A11: Yes; however, we are limited in scope to only key aspects of our ERP system with our home-grown application and process. We would like a more elegant system to better address attestation across multiple systems, especially as more applications are brought on to the AU network.

Q12: How is privileged account management handled?
A12: We currently do this in house with secondary accounts when elevated privileges are necessary, and a better implementation is on our radar but not formally part of this RFP. Possibly to be addressed in a second phase.

Q13: Are there standard reports for attestation?

A13: Yes, through a home grown application; however it is too narrow in scope and we need a more broad reporting system.

Q14: Are there any typical attributes of identity stored in the IAM system that AU considers PII?
A14: We carry the last 4 of SSN, mag stripe info for access control badges and any FERPA related constraints with regard to student privacy.

Q15: Are there any person types coming from a source other than Banner?
A15: No. Banner generates our unique NetID so all person types come through banner for that purpose; however, we would like to be flexible with regard to NetID generation as Banner may not always be our ERP system.

Q16: Is there a need to support social identities?
A16: Yes. Active Directory is our primary authentication source and we are very interested in the idea of having lighter weight affiliations (parents, lifelong learners, contractors, etc) not having to be in our Active Directory system in order to access applications.

Q17: Will the solution provider be required to help migrate from the current IAM solution?
A17: Yes. Our current solution is MicroFocus / NetIQ's Identity Manager 4.0.2 and is supplemented by several in house add-ons. A couple of examples of said add-ons include our *MyAccount* website for account claiming and password management and a nightly Active Directory processing routine which handles placement of users in the tree along with building hundreds of departmental groups.

Q18: Will all respondents be invited to an onsite visit?
A18: No, just the finalists.

Q19: Would the solution be part of AU's own cloud instance or a vendor provided cloud instance? For example, would the solution use AU's current Azure environment as part of the solution?
A19: We prefer a vendor provided solution.

Q20: Are there any restrictions with regard to offshore providers?
A20: AU data must reside in a US based facility.
Engineers assisting with the implementation do not have that same restriction.

Q21: AU mentioned DR recovery and high availability as a primary focus. Does this include all facets of the solution or would some pieces have a heavier weight than others?
A21: Some aspects would weigh heavier than others. For example, SSO will require a very high level of availability while some reporting features may be of a lesser concern.

Q22: What systems will AU be concerned with auditing?
A22: Initially our ERP system (Banner) will be our primary concern. We want to understand what options are available as we have other systems, like our CRM system (Salesforce), which may be of concern.

Q23: How should vendors price a "helping with transition" versus a "standard install" since they may not know all the components of the existing NetIQ system?

A23: See attached reference document for a more detailed listing of the NetIQ system components. We welcome a more modern approach to replace our older technologies where applicable, but a standard install is not an option as we will require implementation assistance.

Q24: Would the current system and the new system run in parallel?
A24: Yes. We anticipate this to be a phased approach where one component is moved to the new system while the other components continue to function on the NetIQ system until they are eventually all implemented on the new system.

Q25: AU mentioned modernization and a few other key components as driving factors. Are there any other things that solution providers should focus on?
A25: We would like to adhere as closely as possible to an off the shelf product with minimal customized modifications and as close to a real time, event driven solution.

Q26: AU's current NetID's are all in Active Directory. Is the desire to maintain this method?
A26: No. We would like an ID store beyond Active Directory. It is desired to be able to authenticate light weight users, such as alumni, at a different level of authentication than those accessing our more high profile systems, like the ERP system.

Q27: How many applications will SSO serve? Are they standards based or custom? Will the vendor be expected to transition all endpoints?
A27: Please reference the SSO Services document for details on current number of endpoints and protocols used. Roughly, about 80 endpoints.
We would like to move heavily towards a standards base.
The vendor will be expected to assist in AU's effort to transition endpoints and provide documentation for AU to use going forward; however, it is not expected that the vendor will fully service the entire transition of all endpoints in the SSO Services document.

Q28: From an end user perspective, do you have a common login ID?
A28: Yes. The NetID is currently generated by Banner. We are open to change as we may not always use Banner for our ERP system.

Q29: What is AU's current 2-Factor method(s)/vendor?
A29: We are a Duo campus and uninterested in changing.

Q30: Where is AU in the budgetary process for an IAM system?
A30: We have budgeted funds available for purchase.

Q31: If the solution requires an on-campus hardware component, who will fund the hardware?
A31: Assume that whatever is needed would drop into AU's VMWare infrastructure and be hosted by AU.

Q32: Will the finalists have an opportunity to adjust pricing once a more in-depth analysis is performed with AU?
A32: Yes.

Q33: How will scope changes be addressed?

A33: If there is a change in scope after a best and final, the RFP will be re-bid to accommodate the change.

Q34: Are there any AU apps with customized session management?
A34: We do not currently have any that fall outside of the default session handling, but we do see potential for that in the future. While we are not currently doing anything in this area, we would like the option to be flexible in this area.

Q35: Is AU happy with CAS?
A35: We do have some campus applications that are dependent on CAS as they do not support SAML.

Q36: Are there situations where AU is the Identity Provider (IDP) as opposed to the Service Provider (SP)?
A36: AU is typically the IDP and we participate in InCommon Federation.

Q37: Does AU have a Project Management Office that will be available to work with the selected vendor?
A37: Yes. A dedicated PM has been assigned to this project already and has been involved during all phases thus far.

Q38: Do you use Grouper?
A38: No. We've looked at it and like it but have not had the bandwidth to move forward or test. We have a home grown process that sort of emulates Grouper and it works but have no issue with re-evaluating this process.

Q39: As an educational institution where users may have multiple concurrent roles, are there well defined policies regarding the various roles a user may have?
A39: AU has opportunity for improvement. Some roles are straightforward, and others have a bit of wiggle room. For instance, an employee may be effectively terminated on the 15th of the month but remain active in the ERP system in order for payroll to run on the 30th of the month to pay the final paycheck.

Q40: How does AU handle multiple roles today?
A40: As best as possible. We recognize that we can do better in identifying rights and privileges as employee or student based access. In most instances we do not currently have that delineation.

Q41: What are the terms for pricing?
A41: Three years with an option to renew for two additional years.

Q42: Are there any implementations AU has seen that we like?
A42: AU has done IAM the AU way for so long that we are a bit out of touch with other implementations. We would like to do IAM more efficiently and our aging infrastructure and focus to the cloud lends itself to a new solution as we are falling being in our ability to support security and auditing requirements.

1. Is this proposal for the integration project, or is it for the entire integration plus managed services?
   Integration and costs of any hosted / IDaaS components
2. Do the three years terms apply to the software licenses plus Integration & Managed Services or just license?
   License and services a needed.

1. What's the current SAML platform? Is it ADFS, Shibboleth, etc.
   Currently maintain 2 SAML providers – SimpleSAML.php, Shib. Both delegate Authn to CAS.
2. Is the current CAS system Banner Elucian?
   Aprereo
3. Is the current MFA solution using Duo and Azure?
   Yes – we are a DUO campus for students and staff, 98% deployed. Azure may be implemented for Alum email and a few Azure integrated cloud services.
4. Is the current Service Now integration via REST API's, via import/export, or ticketing via another agent like email?
   Import/export via LDAP
5. What is Auburn currently using for data protection? Office 365
   CloudLock.
6. What is Auburn currently using data classification? Is O365 the platform to be used for future?
   Nothing at this time.
7. What is your current app development and code review platform?
   Primarily .net, c#
8. What is the scope of the training and target audience? IT only or the entirety of the end user population?
   IT
9. 24/7 support: does that apply to end user or is this for IT support only Tier 1-3?
   IT

| | |
|---|---|
| **Person vault or Directory** | encrypted at rest |

1. What is meant by "encrypted at rest", is this referring to REST apis or "rest" when the data is not in use. If referring to when data is "rest" (ing) what are the specific requirements or questions? If related to REST api, are you just asking what is encrypted (header, body, both)?

At rest ie when not in use. Stored in encrypted format.

| | |
|---|---|
| **Provisioning /integration** | SCIM |

2. What SCIM operations and schema is required OR what applications are you looking to integrate using SCIM?

Only a couple of apps at this time, Box, Snowflake, but desire support for future integration and JiT provisioning.

| **Single Sign On (SSO)** | Native InCommon/Edugain federation support |
|---|---|

3. What is the realm of support needed for EduGain is it service provider related or protocol related for things like RADIUS authentication?

Native IDP participation – should be able to auto-ingest federation metadata.

4. **Tab 4**: A listing of the company projects/customers similar in size and scope to the services described in the RFP. This list must include the name, address, telephone, and email address of the client contract administrator. If applicable, please list examples of services rendered in the state of Alabama, particularly within institutions of higher learning.

Is this asking for the contract administrator? The person that administers the license agreement?

I'd think this is the lead of the IAM operations

5. **Tab 7**: A list of at least five (5) references where the Offeror has provided the services described in the RFP. Include the organization, contact name, title, location, telephone number, and email address. Provide the information on past and current contracts. References should be higher-education schools preferably in the Southeast. Reference current customers/installations of similar size, scope and complexity to Auburn University.

This is very similar to the item above. Please review the differences.

4 is within state of Alabama – 5 is more for peer-level intuitions within the southeast.

6. Q4: To what downstream systems/platforms do the various identities that come into the IAM system through Banner or are created ad hoc by the IAM group (departmental accounts) flow?

A4: See attached IAM Provisioning reference document.

There is no attachment.

Attached to email or should appear in vendor portal area soon.

Q: The current IAM system consists of approximately 30 inbound/outbound connectors and numerous external provisioning flows via file feed or database view. SSO is primarily accomplished via CAS and SAML and Auburn is a DUO campus for MFA.

- What is the number of service accounts?
- What do the Alum really do or need access to?

A: Roughly 15k employees, 55k students, approx. 12k affiliate, retiree, dept.

Numbers don't add due to over-lapping roles.

Alumni currently authenticate only to email/o365 but would be desirable for them to be able to authenticate for transcript requests, managing alumni email forwarding, etc

Q: I have a user question from the RFP. How many Internal users(employees) and How many external users (Students/ alumni) out of the 70,000 users?

A: Roughly 15k employees, 55k students, approx. 12k affiliate, retiree, dept.

Numbers don't add due to over-lapping roles. Ie student employees, employees taking classes, etc

Hosted: Are there plans to implement new software or services in the near future?

Yes – we are constantly evolving. A couple of notable examples of known services that are coming in the very near future are integrations with Snowflake and Salesforce.

Hosted: Has AU previously undertaken to replace the IAM/SSO in-house systems? if so, what challenges did you encounter?

No, not in recent years.

Hosted: Is there any current health and performance monitoring in place and any regular reporting period?

Nagios monitors basic functionality of the hosted servers but nothing beyond an “is up” status.

Hosted: Is there any software End-of-Life/Expiration upcoming?

No.

Hosted: Please provide the deployment architecture for your current systems. Are these configured for High-Availability?

SS0 – yes

Person vault – yes

Connectors - no

Hosted: Please specify the locations from which these users will be requesting support - USA only ?, Other countries?

Predominantly US based users; however, students and alumni could, at any given point, be located anywhere in the world.

Hosted: What is AU's current Disaster Recovery plan for business continuity?

DC’s in the cloud, snapshot backups of IAM virtual machines

Hosted: What is the current "standard" infrastructure configuration for applications: Dev, Test, Stage, Prod? how many instances of each and is this a requirement going forward?

Currently, we essentially have only a production environment; however, as mentioned in the RFP: if the solution is a hosted or IAAS solution provide at least 2 instances for Dev/Test.

Hosted: What programming language or technologies have been used to develop the current IAM and SSO systems?

C#, vb.net, powershell, mssqsql, proprietary NetIQIDM

Hosted: why does AU want 2 instances of Dev/Test as noted in the RFP?

One environment for development and another for QA testing.

IGA: Are there specific compliance/regulations the University must meet?

Yes, FERPA, HiPAA  for example.

IGA: Have there been any audit findings recently?

No material findings.

IGA: How is Access Reviews currently performed?

Home grown web application that we would like to replace.

IGA: How many applications need access certification reviews?

Currently, we are limited by the scope of our home grown application that focuses primarily on Banner Admin access.

IGA: What does AU understand by "Identity and Access Governance" -does it mean Access Reviews/Certifications?

Partially – ensuring access granted is approved, appropriate and verifiable.

LCM: Ability to accommodate multiple concurrent user roles or affiliations - Can you give example of "affiliations"?

Student, Alumni, Employee and Retiree are all pretty standard for a university.  Our other affiliations vary and include users such as visiting scholars/professors,  employee/student spouse, general contractors, medical clinic staff, etc.

LCM: Are there any existing Provisioning Roles, Rules, Policies in place for Joiner, Movers, Leavers? if so, any approximate numbers

Joiners and Leavers have well defined provisioning roles.  Movers are less rigidly defined.

LCM: Are there any Roles defined or memberships rules ? Are there any birthright access configured?

Broad roles currently – Faculty, Staff, Students, Alumni, others

Yes, currently roles have associated birthright provisions ( AD, wifi, email, office, Box, Canvas, etc )

LCM: Are there any specific IAM reporting requirements?

We need to be able to easily see what systems a user has access to and a what level of provisioning within said systems.

LCM: Can AU provide some examples of what current "connectors" are in use? Standard SQL , Standard LDAP, custom-coded connectors? and are these used as

provisioning "targets"?

See attached AU-IAM-NetIQ-Data-Provisioning.docx if there is not one currently in the vendor portal.

LCM: Could you please specify the number of access requests you receive in a month

Requests for ERP access varies by the time of the year.  At the beginning of each term we tend to have an uptick in requests due to employee/student turnover.  In the last 12 months, we have received 1900 total requests for ERP system related access changes.

LCM: How are 30,000 ids updated in one night - self-service, manually administrator or feed files

Feeds from Banner Student and HR extracts.

LCM: How many applications can be requested for Provisioning/deprovisioning? That is, how many Access Request forms are needed?

Most provisioning is ‘just in case’ currently.

LCM: How many applications part of the Access Request Process? Connected and disconnected.

Base provisioning only is currently in IAM request forms ( AD, email, web space/shell account, back up, email alias, shared/dept accounts. )

LCM: How many Approval and Escalation Workflows does the current IAM system have and how are the Approvers defined?

Most workflows requiring escalation are currently in our ERP

LCM: How many staff support the current IAM system?

Currently 5 FTE's; however, 2 more will be brought on in Feb 2020.

LCM: How many support tickets does the team receive today ?

In 2019, the IAM team resolved just over 900 incidents.

LCM: Is provisioning done to "disconnected systems", that is , where no connector exists to automate the provisioning?

Yes.

LCM: Is there anything unusual or specific to AU for New account claiming use case?

It depends on your definition of unusual or specific. Nothing specific as compared to other higher ed institutions. Employees generally claim accounts soon after being hired where-as students may be admitted several months prior to actually attending AU. Both currently are provisioned just in case at the time of employment or acceptance. We prefer a just in time approach going forward.

LCM: Number of password resets

From 1/1/2019 to 12/31/2019 there were just over 43K password resets on Active Directory through our home grown MyAccount password sync application.

LCM: What statistics does AU have for : Access Requests, Password Resets, new user creation, user modifications, user deletions?

Nothing readily available.

SSO: Are there any unusual SSO use cases, for example, different user populations accessing a common target?

We do have a small auxiliary authentication database connected to CAS for some special use applications. (community largely )

SSO: Can AU provide authentication flow diagrams for the different categories of apps (non-SAML, SAML)?

Generally, all SSO requests have authentication delegated to CAS, may perform Authn at SAML level. CAS uses AD for authentication source.

SSO: How is the authentication information collected and used in reporting during an audit?

Generally, only needed for incident investigation – logs are collected on Splunk.

SSO: How many authentications: average and peak?

All SAML signons run through CAS. CAS averages about 37,000 successful authentications per weekday (17,500 or so on Saturdays and Sundays). Peak events (such as first day of class) can push this number over 90,000.

SSO: How many Rules and Authentication flows exist in the current system?

Authentication flows are generally streamlined. All SAML auth is pushed through CAS. MFA described below. Every SAML and CAS service can be customized (attributes, etc).

SSO: How many staff support the SSO platform?

One currently with a backup to be hired in Feb 2020.

SSO: Is mobile authentication is use? what protocols are used?

CAS front-end is mobile friendly. No separate mobile apps are needed. MFA (DUO) generally uses moblie app as second factor.

SSO: Provide MFA process flow

DUO is used for MFA. All services in CAS (and thus all services coming through CAS from SAML) can be configured individually to require MFA. At the time a service ticket is issued (when a user initiates any login), MFA requirements are checked and MFA is prompted if necessary. MFA authentication is maintained for the duration of user's session.

SSO: Provide use cases wherein the MFA is used

Any off-campus access of authenticated resources, on-campus access of sensitive resources.

SSO: What methods/protocols are used to protect non-SAML apps? -OAUTH, OATH, agent-based

CAS accounts for a little over half of our applications. We have a very small number of applications that are using a token-based auth but those are being actively converted whenever possible to CAS or SAML.