Identity and Access Management Policy

Document Name: NCSA Identity & Access Management Policy
Version: 1.3
Accountable: Alex Withers
Authors: Adam Slagell, Alex Withers

Reviewed: 2023 Aug 22
Approved: IIB approved 2024 March 7

- 1 Mission & Purpose
- 2 Scope
- 3 Policy
  - 3.1 User Enrollment
    - 3.1.1 Terms of Service and Confidentiality Agreement
    - 3.1.2 User ID Assignment
    - 3.1.3 Service Accounts
    - 3.1.4 Identity Vetting
  - 3.2 Authentication
    - 3.2.1 Passwords
    - 3.2.2 Multi-factor
    - 3.2.3 Account Lockouts
  - 3.3 Authorization & Groups
    - 3.3.1 Additionally, new NCSA workforce Deprovisioning
    - 3.3.2 Auditing & Logging
  - 3.4 Privacy
    - 3.4.1 Information Collected
    - 3.4.2 Sharing of Information
  - 3.5 Accessing External Services
    - 3.5.1 Amazon Web Services
      - 3.5.1.1 AWS Instances
      - 3.5.1.2 AWS Console
  - 3.6 Policy for Accepting Federated IdPs
    - 3.6.1 Exporting NCSA Identities
  - 3.7 Password Management and Secret Sharing
- 4 Exceptions Process
- 5 Updates
- 6 References

Mission & Purpose

NCSA maintains its own user database, authentication systems, and authorization framework distinct from the University. This policy sets the requirements for these systems and their associated processes, such as, provisioning, deprovisioning, account lockouts, etc.

Scope

This policy applies only to NCSA-specific services and accounts, and not those of other University systems or our partners.

Policy

User Enrollment

Terms of Service and Confidentiality Agreement

Users will be presented an NCSA Acceptable Use Policy when their accounts are created and whenever there are significant changes. The AUP includes a confidentiality agreement that applies to users accessing sensitive data, such as ePHI and CUI, on NCSA systems. New NCSA workforce members acknowledge the AUP as part of the onboarding process.

Group owners may add additional terms for their projects as part of the group enrollment process, however, these must not conflict with University or NCSA policy elsewhere.

User ID Assignment

When an NCSA user account is created, it is automatically assigned a unique identifier, which is a primary key in the NCSA user database. All NCSA logon IDs map to a single such identifier. This allows the database implementation to enforce uniqueness of user account login IDs.

This login ID can usually be selected by the user at the time of account creation, assuming it is available. Certain character restrictions apply, and names cannot ever be reassigned even if associated accounts are inactive. NCSA also reserves the right to reject any logon ID deemed inappropriate.

This login ID is consistent across all NCSA authentication systems. Therefore, NCSA staff can use system access logs to consistently identify actions across any NCSA system to a unique person.

Usernames are between 3 and 20 characters such that they

1. contain only lowercase letters and numbers for regular users
2. start with a letter
3. do not contain restricted names as any substring

Service Accounts

Service accounts may contain the special characters "-" or "_". These accounts are required for use by multiple persons as user account passwords cannot be shared. Service account requests must be approved by the Security Office and audited annually.

Identity Vetting

The processes to issue new credentials and reset passphrases are designed to be secure in the sense that the original party who started the process is the same person that receives the credential and can later reset it. However, the common process does not by itself validate more than an email address.

NCSA and other University staff are additionally vetted as part of the human resource processes of the UIUC campus when they fill out tax forms, set up direct deposits, and receive their iCard with a photo ID and unique identifier. This same University identifier is tied to their NCSA identity and linked to their campus network ID when their NCSA staff account is created. Therefore, NCSA relies upon the University to vet workforce members to their real names.

NCSA supports many user communities both inside and outside the University with additional vetting requirements. Such verification processes must be determined by group managers and can be tied to group enrollment and approval processes. HIPAA Business Associates are responsible for vetting their own workforce and managing which of them has access to the associate's data at NCSA.

Authentication

Passwords

NCSA passwords have a minimum length of 12 characters.

Passwords less than 16 characters in length require:

1. contains at least one uppercase and one lowercase letter
2. contains at least one number or special character
3. does NOT contain 4 sequential characters of your logon ID
4. does NOT contain dictionary words longer than 3 characters
5. is NOT the same as the previous password

Passwords greater than 15 characters need only:

1. contain at least one uppercase and one lowercase letter
2. NOT contain 4 sequential characters of your logon ID
3. be different than the previous password

Multi-factor

NCSA requires multi-factor authentication for system administration, accessing resources with high-risk data, and on shared-user systems providing command line access.

No portion of an approved MFA system can be used or recovered using telephony based methods (eg SMS and phone call)

Because these systems have extra per user costs, they are not made available to all projects. An NCSA project or partner must pay for NCSA multi-factor tokens~~/licenses~~ for non-staff.

NCSA currently uses Duo to provide multi-factor authentication services. Duo uses offsite, cloud-based servers to provide the multi-factor capabilities and as such would not function if NCSA was cut off from the internet or if Duo was down. In these situations, Duo can be configured to fail "open" or "closed". In the first case, Duo cannot be contacted and would not be required and thus users can authenticate with a single factor (i.e. their passphrase). In the second case, Duo cannot be contacted and users would not be able to authenticate until Duo could be contacted again thereby locking users out of authenticating where multi-factor is required.

The default policy is to configure Duo to fail ***"closed"***. Systems can be configured to fail "open" with the prior approval of NCSA's Cybersecurity Division: help+sec@ncsa.illinois.edu.

Account Lockouts

Multiple failed login attempts may lockout access based on the IP address of the client system. Accounts may also be suspended globally by the Security Office.

Authorization & Groups

Newly created accounts have no authorizations to access resources until they are specifically added to a group.

NCSA operates a centralized authorization service for systems in the High Performance Data Center zone (See NCSA Network Security Policy). Local password files and other authentication/authorization services can only be used if a formal exception is approved by the NCSA Internal Infrastructure Board (IIB).

Additionally, new NCSA workforce Deprovisioning

Staff are removed from the NCSA staff group during the NCSA exit process as stated in the NCSA Information Security Policy. An automated process to remove staff access is initiated by HR and completed on the date of departure. Automated processes are followed up by NCSA staff to ensure that access is removed.

Group owners are responsible for promptly removing users from other groups as roles and access needs change.

Auditing & Logging

Group owners must audit their membership in their groups at least annually. This does not apply to system generated groups driven by processes like HR transactions.

The security team must have a method to perform real-time queries against authorization and authentication logs, for both failed and successful attempts. These logs must contain information on authentication or authorization events to determine time, target system, account used, and source host. Other information may be required to support the non-security, business needs of the Center.

Privacy

Information Collected

NCSA minimally collects the following information when creating an account:

- Full name
- Primary email address
- Affiliation or Home Institution

NCSA may collect the following information and some projects/activities may require:

- phone/fax number(s)
- mailing address(es)
- recovery/secondary email address(es)
- position (e.g., faculty, researcher, student, vendor, etc.)
- country of residence
- academic degree(s)

Projects may not collect information disallowed by NCSA or University policy elsewhere.

Sharing of Information

As an identity provider, NCSA may share full names, account names, email addresses, and provided user type attributes of authenticated users as part of the InCommon Research and Scholarship program. No additional information are shared publicly.

NCSA does not sell any user information to third parties.

Accessing External Services

Amazon Web Services

Access to Amazon Web Services (AWS) is available through the University of Illinois (see: https://aws.illinois.edu).

AWS Instances

Whether an NCSA managed asset is hosted in the cloud or on site, all NCSA security policies still apply to the individual hosts including this IAM policy. NCSA IAM services, such as, Kerberos, LDAP, shibboleth, and Duo are available and should be used the same as they would for a local host.

AWS Console

Amazon also provides the ability to use other IAM systems for the management console besides local Amazon accounts. The following methods are acceptable for authenticating to the AWS Management Console:

1. Campus authentication via https://shibboleth.illinois.edu/ (enabled by default for University of Illinois AWS accounts). Duo MFA must be enabled for the campus account.
2. NCSA authentication via https://idp.ncsa.illinois.edu/ (requires custom setup: contact help+idp@ncsa.illinois.edu for assistance). Duo MFA must be enabled for the NCSA account. This method supports NCSA external collaborators creating NCSA accounts at https://identity.ncsa.illinois.edu/.
3. An AWS User account, for emergency access in case illinois.edu is offline, to meet specific service level agreement obligations. The password for this account must: 1) meet NCSA password requirements, and 2) be stored in LastPass Enterprise in a shared folder owned by an NCSA employee. The owner of the shared folder is responsible for keeping the LastPass Enterprise shared folder membership up-to-date and changing the shared password whenever someone is removed from the shared folder.

The following methods are acceptable for managing authorization to the AWS Management Console:

1. For campus identities, map Active Directory group memberships to AWS Roles. An Admin group/role is set up as part of University of Illinois AWS account setup.
2. For NCSA identities, map LDAP group memberships to AWS Roles (requires custom setup: contact help+idp@ncsa.illinois.edu for assistance).
3. Access to the AWS User account, for emergencies during illinois.edu outages, is managed via a LastPass Enterprise shared folder, shared only with specific personnel who are responsible for emergency operations.

Policy for Accepting Federated IdPs

Identities from external providers may be used for access to applications with baseline authentication needs, i.e., without requirements for higher level of assurance such as multi-factor authentication or face-to-face identity vetting. Only one account per IdP can be bound to a user's NCSA identity. NCSA resources may choose from the following valid supported identity providers; the default for a resource is to only access NCSA identities and approval is needed from the CISO to allow the use of linked identities:

- identity providers in the InCommon (incommon.org) federation, including research and education providers in the United States and international providers from eduGAIN (edugain.org) member federations.
- open access identity providers: Google (accounts.google.com), GitHub (github.com), and ORCID (orcid.org)
- identity providers operated by NCSA industry partners

Using a Federated IdP does not exempt a system from the NCSA MFA requirements above.

Support for higher level of assurance from external identity providers requires custom configuration. Contact help+idp@ncsa.illinois.edu for assistance with higher level of assurance use cases. Changes in the list of acceptable federated IdPs is approved by the CISO.

Exporting NCSA Identities

NCSA supports Shibboleth and OpenID Connect/OAuth services to allow other organizations to securely use NCSA identities. New interfaces to NCSA IdM services must be approved by the IIB before being added.

Password Management and Secret Sharing

NCSA requires the use of its official password and secret sharing solution (i.e. Lastpass Enterprise) for storing and sharing passwords and secrets inline with NCSA's cybersecurity and acceptable use policies.

Old accounts from the password and secret sharing solution will be disabled after HR exit or 1 year of inactivity and removed after 2 years of inactivity.

The service may not use NCSA's or the U of I's authentication and authorization infrastructure to provide access to shared passwords or secrets.

The service managers of Password Management and Secret Sharing will have the ability to recover user secrets when necessary.

Exceptions Process

There are exceptions and special cases to any policy. Requests for exceptions should be made to the NCSA Security Office and may be approved by either that office or the NCSA Director's Office.

Updates

This policy is reviewed annually by the Security Office. Feedback is solicited from the Internal Infrastructure Board for any recommended changes. New versions are approved by the NCSA Director's Office.

References

- NCSA Acceptable Use Policy
- NCSA Information Security Policy
- NCSA Network Security Policy