Service Description

CIT's authentication service provides a means for verifying that the user of a restricted service is the correct individual. The end customer is the holder of a Cornell NetID (students, faculty, staff, alumni, affiliates, Cornell Medical personnel, and exceptions with sponsor), a Cornell GuestID, or a Cornell ApplicantID. The user is prompted for this ID and a password before gaining access to the application.

Service Hours

This service is designed and managed to be available on a 24x7 basis, including weekends and holidays. Redundant servers ensure most scheduled maintenance on the servers will not impact availability.

Service Availability

Target availability is 99.9999%.

Reliability

Two service breaks per year of less than one hour each can be tolerated.

Any time period during which an individual is unable to authenticate to a service due to a problem with the authentication service (not the target application or service itself), and unrelated to scheduled maintenance, would constitute a break.

Customer Support

Priority 1 incidents:

Network Operations Center (24x7)
607-255-9900
noc@cornell.edu

See NOC OLA for call answer target. Staff supporting the authentication service are available to the NOC 24x7

Support for end user incidents:

Contact Center
607-255-8990
helpdesk@cornell.edu

Backline support for application and service specific incidents

idmgmt@cornell.edu

Incident response time target – one business day to respond to customer with solution, status, request for clarification (debug logs, for example) or information regarding action being taken.

Developer resources:

http://identity.cit.cornell.edu/

Target for Incident resolution (Fix) times.

Priority 1: Authentication service itself is not working – 1 hour
Priority 2: Critical University service is unable to use the authentication service, or there is a high-risk security vulnerability with the service – 1 day unless negotiated with customer due to time of year, day of the week
Priority 3: A service owner has a specific problem interoperating with the authentication service – negotiated with the customer based on impact to the business unit

Service Performance

The main authentication server handles over 38 million transactions a month, with server capacity far below alarm thresholds.

The server handling authentication for web-based applications (CUWebLogin) handles about three million real-time authentications per month, with server capacity far below alarm thresholds.

Functionality (if appropriate)

Not applicable

Change Management Procedures

Procedures established by the Process Improvement Office are followed:

https://confluence.cornell.edu/display/change/ccab/

Maintenance

Routine maintenance is performed during the standard maintenance window Monday – Friday between 5:00 and 7:00. If a longer window is required, an early Sunday morning window will be negotiated with campus stakeholders. Maintenance is planned so that at least one server is up at all times to handle customers.

There is an average of two releases a year, usually associated with new authentication services or enhanced capabilities for current services.

At least one month in advance of the release, customers are first notified via the net-admin-l discussion list and the Identity Management campus developers monthly

meeting. Within three days of the release the announcement is made to the net-announce-l discussion list as part of the change management process.

There will be little advance notice of such a release to fix a security vulnerability. As soon as a fix is available, service owners will be notified and provided with instructions for implementing.

Customer Responsibilities

Customer or subcontractor responsibilities for:

1) maintaining current software or hardware
2) testing software or hardware updates
3) responding to security alerts involving the covered product/system
4) responding to security incidents involving the covered product/system

The customer or subcontractor is responsible for maintaining the current version of CUWebAuth and testing with the application. Participation in beta testing of new releases is strongly recommended. If a security vulnerability is discovered in CUWebAuth or any other service component CIT provides, the customer or subcontractor is responsible for applying the fix as soon as it becomes available.

The customer or subcontractor must subscribe to cuwa-l@cornell.edu

IT Service Continuity

Ez Backup is used to back up data that would have to be restored should a catastrophic hardware failure occur. In such an event, staff who support the authentication service would be on site to assist in restoring the service. Target availability and incident response times do not apply to this category of failure.

Security

If there is a system compromise to the application or service which results in a security vulnerability for the authentication service, the customer or subcontractor is responsible for reporting the incident in accordance with University policy 5.4.2, Reporting Electronic Security Incidents, and for remediation.

Printing

Not applicable.

Charging (if applicable)

Not applicable

Glossary

ApplicantID—Type of Cornell electronic identifier issued to prospective students who have submitted an application for admission.

Authentication – Process of verifying a user's identity when accessing information technology (IT) resources. Typically, identification is based on a user's Cornell electronic identifier and an associated password, personal identification number (PIN) or a card encoded with unique identification information.

Cornell Electronic Identifier—String of alphanumeric characters issued to users by Cornell Information Technologies ofr the purpose of authentication to IT resources. Generally, there are four types of identifiers used at Cornell: ApplicantIDS, NetIDs, GuestIDs, and Sponsored NetIDs.

CUWebAuth – Software that allows a web application using Unix/Apache or Windows/IIS to use CIT's authentication service

CUWebLogin (CUWL) – Centralized login servers that process user logins via CUWebAuth by proxying credentials securely to Kerberos from a dynamic login page tied to a one-time session key. Currently CUWL has single sign-on capabilities leveraged via a secure session cookie issued by the CUWL web service.

GuestID – Type of Cornell electronic identifier issued to guests of the university, who are not eligible for a NetID, but who may require access to restricted IT services. Guests may include conference attendees, visiting speakers, or vendor representatives, for example.

NetID – Type of Cornell electronic identifier issued to all new faculty, staff, students, alumni and affiliate staff.

Service owner – A service owner is the individual having the established position, decision-making authority, and responsibility to shape all aspects of a product or service subject to policy, funding and competitive constraints.

Sponsored NetID—Type of Cornell electronic identifier issued upon the request of a unit head or designee to individuals, such as independent contractors, who are not eligible for a NetID as a member of the community, but who provide services to the university.

Amendment Sheet

To include a record of any agreed amendments, with details of amendments, dates and signatories.