Service Description

CIT’s authorization service provides a means for controlling who can access which applications or services not intended for public use. The end customer is the holder of a Cornell NetID (students, faculty, staff, alumni, affiliates, Cornell Medical personnel, and exceptions with sponsor), a Cornell ApplicantID or Cornell GuestID. The user is prompted for this ID and a password before gaining access to the application. The user must first authenticate before gaining access to the services for which he is authorized. Authentication and authorization are different services which complement each other.

Service Hours

This service is designed and managed to be available on a 24x7 basis, including weekends and holidays. During maintenance windows or complete failure of the primary server, the secondary server will take over without manual intervention or an interruption in service.

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. Network Operations Center change management procedures will be followed to ensure that proper campus notification of service interruption is provided. If the Customer requires consultation before scheduling such maintenance this requirement should be stated.

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 access a service due to a problem with the authorization service, 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 SLA for call answer target. Staff supporting the authorization 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, or information regarding action being taken.

Web resources for developers:

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

Target for Incident resolution (Fix) times.

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

Service Performance

The service currently handles 104 million real-time user authorization queries 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

See Service Availability section.

Customer Responsibilities

Not applicable

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 authorization 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

Not applicable

Printing

Not applicable.

Charging (if applicable)

Not applicable

Service Reviews:

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.

Authorization – Process of granting a user access to IT resources and IT information based on predetermined access rights.

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.

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.

Permit – An authorization record or group with a unique name, a list of permissions for ownership, update, administration, and lookup privileges, and security attributes. NetIDs are said to "have a permit" if they are members of a permit or group.

Amendment Sheet

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