



Globus Auth: expanding the  
services ecosystem for  
protected data

**Rachana Ananthakrishnan**  
[ranantha@uchicago.edu](mailto:ranantha@uchicago.edu)





Globus is ...

a non-profit service  
developed and  
operated by



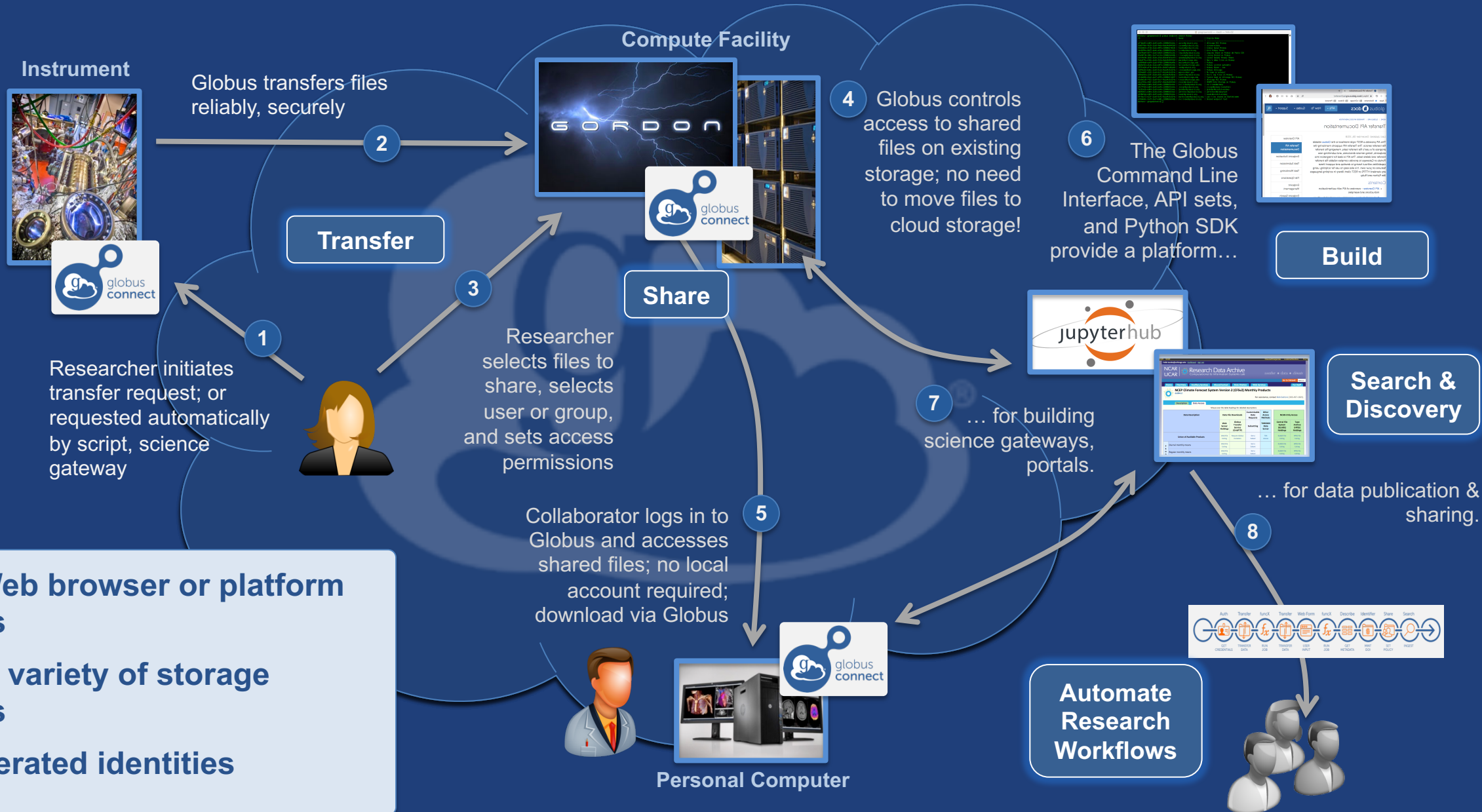
THE UNIVERSITY OF  
CHICAGO



# Delivered as data management platform



# Globus SaaS / PaaS: Research data lifecycle





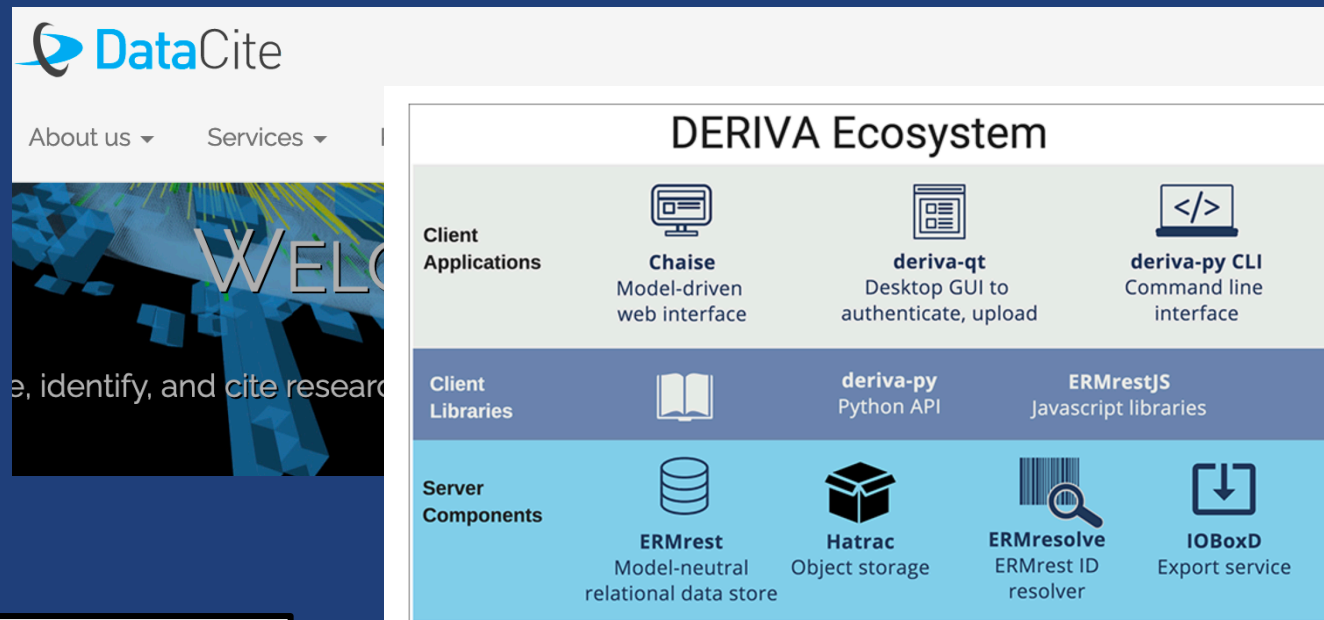


# Globus Auth

# Globus Auth: Foundational IAM service

## **Brokers authentication and authorization among...**

- End-users
- Identity providers: enterprise, external (federated identities)
- Services: resource servers with REST APIs
- Apps: web, mobile, desktop, command line clients
- Services acting as clients to other services
- **OAuth 2.0 Authorization Framework (a.k.a. OAuth2)**
- **OpenID Connect Core 1.0 (a.k.a. OIDC)**

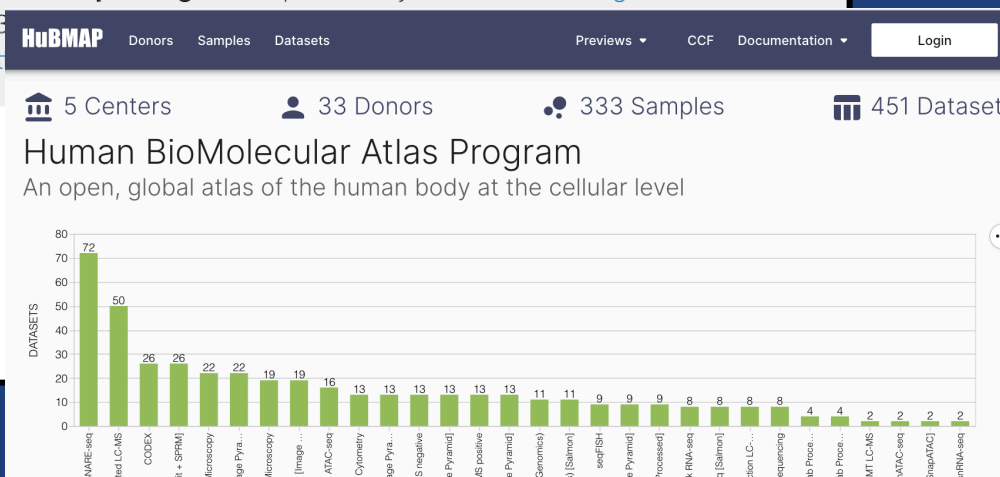


# Sanger Imputation Service

## Before you start

Be sure to **read through the instructions.**

You will need to set up a free account with **Globus** and have **Globus Connect** running at your institute or on your computer to transfer files to and from the service.



## Support a range of assurance levels, authentication policy and access control



# Motivating use cases



# Some of the use cases driving new features

- **High Assurance data access**
- **High assurance access to applications**
- **Administrator managed service credentials for Globus Connect**
- **HTTPS data access**
- **(Web) Applications with optional functionality/capability access**
- **Identity for task flow instances in Automation platform**
- **...**





# Overview of select features



# Sessions

- **Authentication context per application instance, per browser**
- **Session context provided to applications and resource servers to use in policy enforcement**
  - All derived tokens belong to same session
- **Support user flows to add authentication to session**
  - Error returned from service with message to user and required identity/identities
- **Logout/browser session close closes session**



# Session information

- **Introspect returns session context**

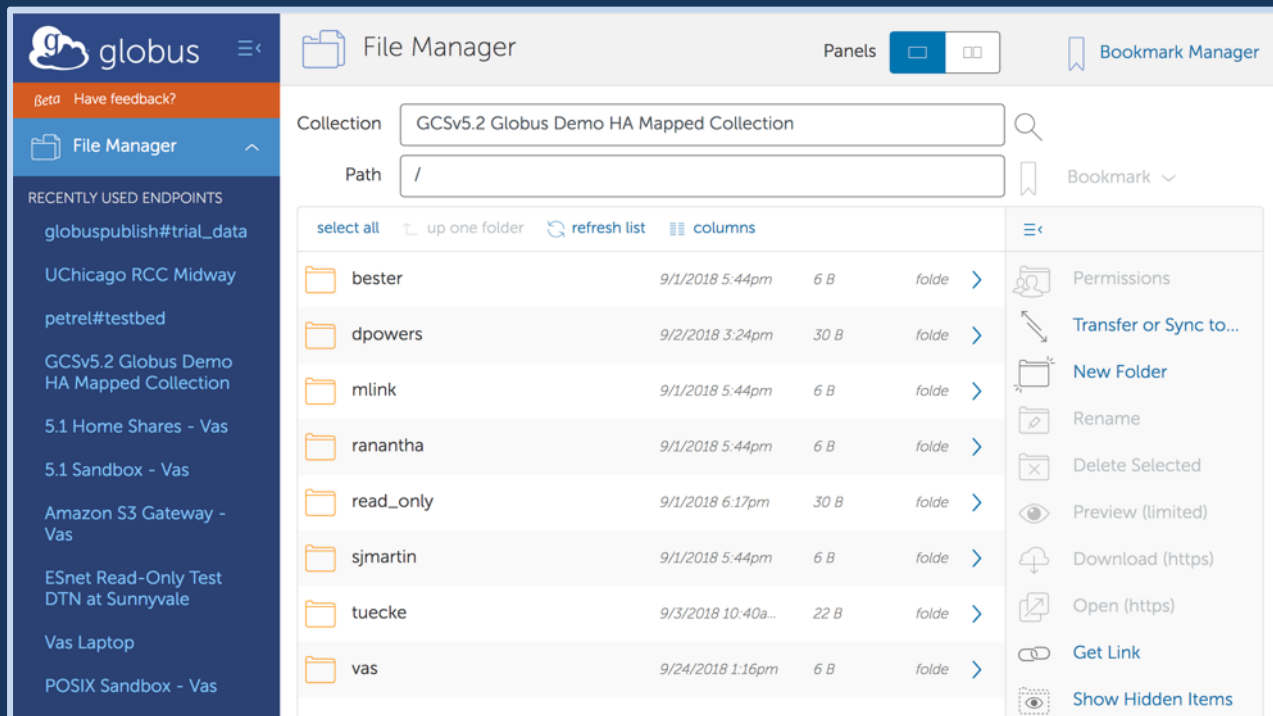
```
"session_info" : {  
  "session_id" : <uuid>,  
  "authentications" : {  
    <identity_id1> : {  
      "auth_time" : <seconds-since-epoch>,  
      "idp": <idp-id>,  
    }, <identity_id2> : {  
      ..  
    }  
  }  
}
```

# Application instance isolation in action

Re-authentication required in different app, same browser(app instance 2)



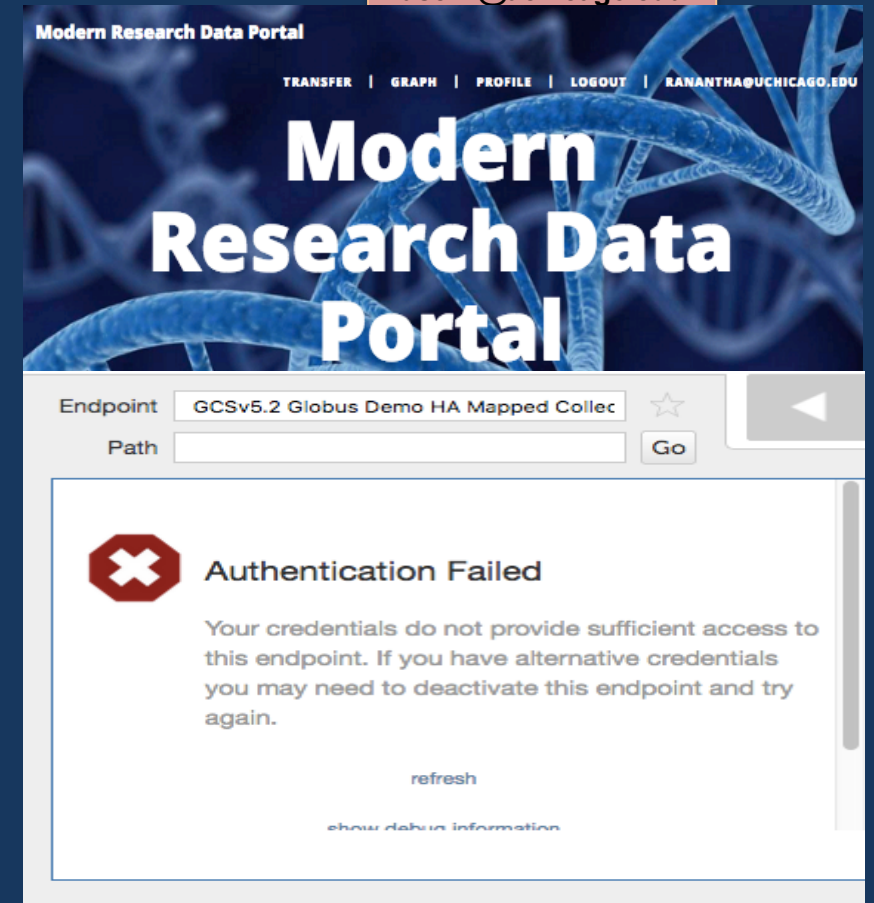
Authenticated in browser session (app instance 1)



The screenshot shows the Globus File Manager interface. The left sidebar lists "RECENTLY USED ENDPOINTS" including "globuspublish#trial\_data", "UChicago RCC Midway", "petrel#testbed", "GCSv5.2 Globus Demo HA Mapped Collection", "5.1 Home Shares - Vas", "5.1 Sandbox - Vas", "Amazon S3 Gateway - Vas", "ESnet Read-Only Test DTN at Sunnyvale", "Vas Laptop", and "POSIX Sandbox - Vas". The main area displays a "File Manager" view for the "GCSv5.2 Globus Demo HA Mapped Collection". It shows a list of folders: "bester", "dpowers", "mlink", "ranantha", "read\_only", "sjmartin", "tuecke", and "vas". Each folder entry includes a date, time, size, and type. A right-hand menu contains options like "Permissions", "Transfer or Sync to...", "New Folder", "Rename", "Delete Selected", "Preview (limited)", "Download (https)", "Open (https)", "Get Link", and "Show Hidden Items".



userX@uchicago.edu



The screenshot shows the "Modern Research Data Portal" interface. The header includes links for "TRANSFER", "GRAPH", "PROFILE", "LOGOUT", and "RANANTHA@UCHICAGO.EDU". The main heading is "Modern Research Data Portal". Below this, there's a section for "Endpoint" and "Path". The "Endpoint" is set to "GCSv5.2 Globus Demo HA Mapped Collec". The "Path" is empty. A "Go" button is present. Below this, a red octagon with a white 'X' icon is displayed next to the text "Authentication Failed". The message states: "Your credentials do not provide sufficient access to this endpoint. If you have alternative credentials you may need to deactivate this endpoint and try again." At the bottom, there are links for "refresh" and "show debug information".



# Dynamic dependent scopes

- **Dependent scope defined at time request is made for dependent tokens**
  - Use of *[scope name]* to indicate dynamic dependency
  - User will be prompted for consent prior to issuing token
- **For example:**
  - urn:globus:auth:scope:printservice.org:print[urn:globus:auth:scope:document1.documentservice.org/read]



# Optional scopes & incremental consent

- **Specification of scopes that the user may optionally consent to**
  - Use of *\*scope\_name* to indicate that the scope is optional
  - Also supported for dependent scopes
- **Incremental consent to new scopes**
  - Usability improvement to allow users to see only the scopes that need consent
- **Supports building applications**
  - With core functionality, and optional functionality with perhaps degraded capability
  - Request least privilege and add as needed



# FQDN based scopes

- **Resource server can request a FQDN based scope string**
  - Register FQDN with Auth
  - DNS TXT record must have registered client id
  - Once validated, scope has FQDN in the string  
*“https://auth.globus.org/scopes/<FQDN>/<scope name>”*
- **Supports construction of scope string**
  - Dynamic dependency use case
  - E.g. HTTPS server



# Walkthrough of features in use



# Globus Connect as Resource Server

globus  developers

> Register your app with Globus

> Register a new Globus Connect Server v5

> Developer documentation

Example Univ RCC Storage

[Globus Connect Server]

Client ID

2d29f661-b74d-4698-8d35-ddb8dae53e80

Client Secrets

Generate New Client Secret

Service Scopes

no service scopes for this client

Requested Scopes

urn:globus:auth:scope:auth.globus.org:view\_identities (View the identities in your Globus account)

urn:globus:auth:scope:transfer.api.globus.org:all (Manage data using Globus Transfer)

openid (View your identity)

email (View your email address)

profile (View identity details)

Privacy Policy URL

none provided

Terms and Conditions URL

none provided

Test project

contact email: rachana@globus.org

Add



NCSA demo app

Add new app

Add new Globus Connect Server

Add/remove admins



Edit Admins in *Test project*

Add admin to project

vas@uchicago.edu

Add

USERNAME

NAME


ranantha@uchicago.edu

Rachana Ananthakrishnan



# Application with optional scope/incremental consent

Start with required scopes

 globus Account ▾

Globus Web App would like to:

- ✓ Manage your Globus Groups ⓘ
- ✓ Manage data using Globus Transfer ⓘ
- ✓ View the identities in your Globus account ⓘ

To work, the above will need to:

- ✓ View the identities in your Globus account ⓘ
- ✓ Manage your Globus Groups ⓘ

By clicking "Allow", you allow **Globus Web App**, in accordance with its [terms of service](#) ⓘ and [privacy policy](#) ⓘ, to use the above listed information and services. You can rescind this and other [consents](#) ⓘ at any time.


AllowDeny







# Application with optional scope/incremental consent


User selects  
resources/capabilities  
to access


 Collection Search


Collection





Cancel


 **Globus Staff GCSv5.4 Demo POSIX No Guests HA**  
Owner: fccc470f-268b-4f36-a84e-1e1c09301aba@clients.auth.globus.org  
no description provided








 **Globus Staff GCSv5.4 Demo POSIX No Guests**  
Owner: fccc470f-268b-4f36-a84e-1e1c09301aba@clients.auth.globus.org  
no description provided




 **Globus Staff GCSv5.4 Demo POSIX HA**  
Owner: fccc470f-268b-4f36-a84e-1e1c09301aba@clients.auth.globus.org  
no description provided





 **Globus Staff GCSv5.4 Demo POSIX**  
Owner: fccc470f-268b-4f36-a84e-1e1c09301aba@clients.auth.globus.org  
no description provided





# Application with optional scope/incremental consent

## Identity Required

An identity from one of the following identity providers is required

Please select the identity or identity provider to continue:

- [rachana@globus.org](mailto:rachana@globus.org)
- Link an identity from [Globus Staff \(globus.org\)](https://globus.org)

Consents and  
authentication policy  
for the scope

Globus Web App would like to:

- ✓ Manage collections on Globus Staff GCSv5.4 Demo Endpoint ⓘ
- ✓ Access your data on Globus Staff GCSv5.4 Demo POSIX via HTTPS ⓘ
- ✓ Manage data using Globus Transfer ⓘ
- ✓ Manage your data on Globus Staff GCSv5.4 Demo POSIX ⓘ

To work, the above will need to:

- ✓ View the identities in your Globus account ⓘ
- ✓ Manage data using Globus Transfer ⓘ
- ✓ Manage your Globus Groups ⓘ



# Application with optional scope/incremental consent

Tokens with required scope returned, and resource can be accessed

Collection

Globus Staff GCSv5.4 Demo POSIX

Path

/home/globus-shared-user/

☐ select all

up one folder

refresh list

view

NAME	LAST MODIFIED	SIZE
Alt	08/21/2020 03:30pm	—
attach.svg	07/28/2020 08:24pm	1.22 KB
Binary Data	09/14/2020 11:46am	—
Brigitte	11/08/2020 09:10pm	—
foo.html	09/14/2020 11:52am	156 B
Gigi	11/03/2020 03:09pm	—
globus_metadata.json	08/10/2020 04:44pm	1.94 KB
Greg	10/06/2020 10:18am	—
http-test	08/10/2020 05:04pm	—
josh	11/10/2020 10:21am	—
one down	10/29/2020 04:50pm	—



# Application with optional scope/incremental consent

Access HTTPS  
server, which is a  
separate resource  
server

File Manager

Panels

Collection

Path

view

	NAME	LAST MODIFIED	SIZE
<input checked="" type="checkbox"/>	1951.csv	10/16/2020 10:57am	34.29 KB
<input type="checkbox"/>	1952.csv	10/16/2020 10:57am	34.34 KB
<input type="checkbox"/>	1953.csv	10/16/2020 10:57am	34.28 KB
<input type="checkbox"/>	1954.csv	10/16/2020 10:57am	34.27 KB
<input type="checkbox"/>	1955.csv	10/16/2020 10:57am	34.3 KB
<input type="checkbox"/>	1956.csv	10/16/2020 10:57am	34.34 KB
<input type="checkbox"/>	1957.csv	10/16/2020 10:57am	34.27 KB
<input type="checkbox"/>	1958.csv	10/16/2020 10:57am	34.29 KB
<input type="checkbox"/>	1959.csv	10/16/2020 10:57am	34.28 KB
<input type="checkbox"/>	1960.csv	10/16/2020 10:57am	34.38 KB
<input type="checkbox"/>	1961.csv	10/16/2020 10:57am	31.72 KB



# Application with optional scope/incremental consent

## Identity Required

An identity from one of the following identity providers is required to continue.

Reason: To gain access you must authenticate with an identity from one of following domains: globus.org

Please select the identity or identity provider to continue:

- [rachana@globus.org](#)
- Link an identity from [Globus Staff \(globus.org\)](#)

Collection "Globus Staff GCSv5.4 Demo POSIX" would like to:

- ✓ Manage your data on Globus Staff GCSv5.4 Demo POSIX ⓘ
- ✓ View identity details ⓘ

By clicking "Allow", you allow **Collection "Globus Staff GCSv5.4 Demo POSIX"** (this client has not provided terms of service or a privacy policy to Globus) to use the above listed information and services. You can rescind this and other [consents](#) ⓘ at any time.

Allow























Deny

Consents and  
authentication policy  
for the scope





# Optional scopes and consent management

CONSENT GRANTED TO	TIME GRANTED	
Globus Web App	a month ago	
 Access your data on Globus Staff GCSv5.4 Demo S3 via HTTPS	 	
 Manage your data on Globus Staff GCSv5.4 Demo S3	 	
 Access your data on Globus Staff GCSv5.4 Demo POSIX via HTTPS	 	
 Manage collections on Globus Staff GCSv5.4 Demo Endpoint	 	
 Manage your data on Globus Staff GCSv5.4 Demo POSIX	 	
 Manage your Globus Groups		
 View the identities in your Globus account		
 Manage data using Globus Transfer		



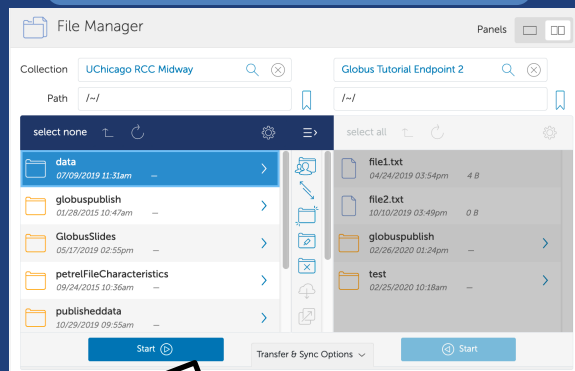
# Usability considerations



# Granularity of scopes

Transfer  
files

Web application



Transfer

Transfer data

Auth

Get  
authentication  
context

Groups

Get Groups

STATEU



STATEU

What set of scopes  
should the web  
application get,  
and remember?



# Consents

Login to  
application



Log in to use Globus Web App

Use your existing organizational login  
e.g., university, national lab, facility, project

Look-up your organization...

Didn't find your organization? Then use [Globus ID to sign in](#). ([What's this?](#))

Continue

Or

Sign in with Google Sign in with ORCID ID

Profiles Stage would like to:

- ✓ Know who you are in Globus. ⓘ
- ✓ Know some details about you. ⓘ
- ✓ Know your email address. ⓘ

By clicking "Allow", you allow **Profiles Stage**, in accordance with its [terms of service](#) and [privacy policy](#), to use the above listed information and services. You can rescind this and other [consents](#) at any time.

Allow

Deny

- ✓ Know who you are in Globus. ⓘ

Allows this client to identify you in Globus (returns an id\_token)

As 0000-0002-2187-9988@orcid.org, with access to information (e.g. name, email, organization) for all of your account's identities.

Subject to its [terms of service](#) and [privacy policy](#).

- ✓ Know some details about you. ⓘ

Allows this client to know details like your name (e.g. Jane Doe) and organization.

As 0000-0002-2187-9988@orcid.org, with access to information (e.g. name, email, organization) for all of your account's identities.

Subject to its [terms of service](#) and [privacy policy](#).

- ✓ Know your email address. ⓘ



# Consents with dependent services



This is a dependency tree – how best do we explain this to the user?

Globus Web App would like to:

- ✓ Transfer files using Globus Transfer ⓘ
- ✓ Manage your Globus Groups ⓘ
- ✓ View your identities on Globus Auth ⓘ

To work, the above will need to:

- ✓ View your identities on Globus Auth ⓘ
- ✓ Manage your Globus Groups ⓘ

By clicking "Allow", you allow **Globus Web App**, in accordance with its [terms of service](#) and [privacy policy](#), to use the above listed information and services. You can rescind this and other [consents](#) at any time.

Allow

Deny



# Upcoming work

- **MFA attribute and policy for data access**
- **UI enhancements for consent management**
- **API for app registration and management**
- **NIH Researcher Auth Service collaboration & integration**
- **...**



# Summary

**Applied token based authentication to broader range of services, and new features in Globus Auth to support**

**dynamic resource access**

**multiple levels of assurance**

**application built with least privilege model**

**usability concerns**

# Resources

- Globus : [globus.org](https://globus.org)
- Globus documentation: [docs.globus.org](https://docs.globus.org)
- Globus Helpdesk : [support@globus.org](mailto:support@globus.org)
- Globus Auth API : [docs.globus.org/api/auth](https://docs.globus.org/api/auth)