USC Federated Guest Registration Service

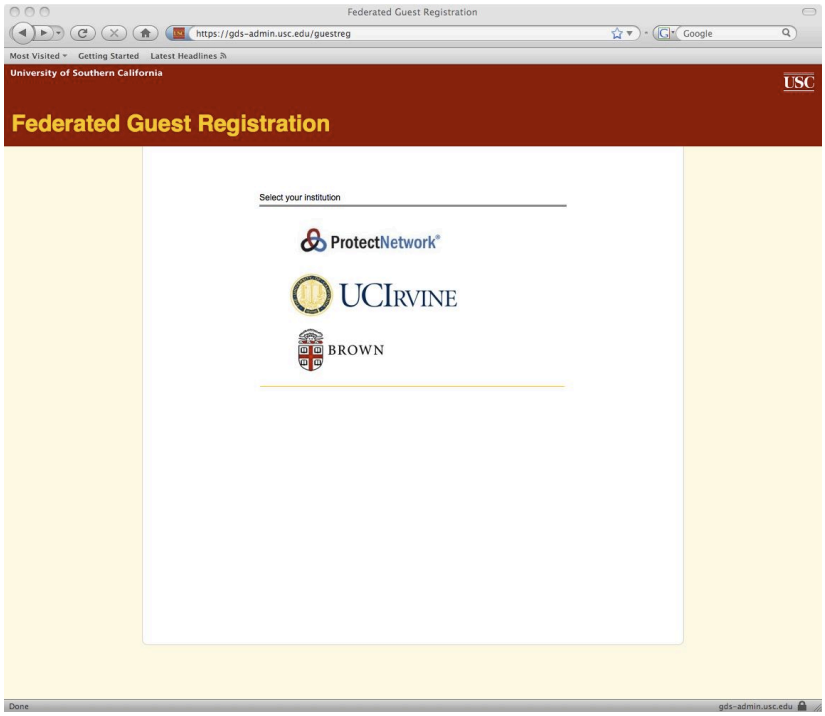
(7/14/2011, B Bellina, USC ITS Enterprise Information Services IdM)

The Federated Guest Registration Service is a self-service application that allows an external party with credentials at approved non-USC institutions to register their home institution account with USC and then use it to access USC federated applications.

Because the user information provided is self-asserted the class of applications best suited for such identities are low-security applications, such as those used for inter-institutional collaboration. For access to higher-security applications the individual should be sponsored for a USC identity through the iVIP system.

Location of the Registration page: <http://gds-admin.usc.edu/guestreg>

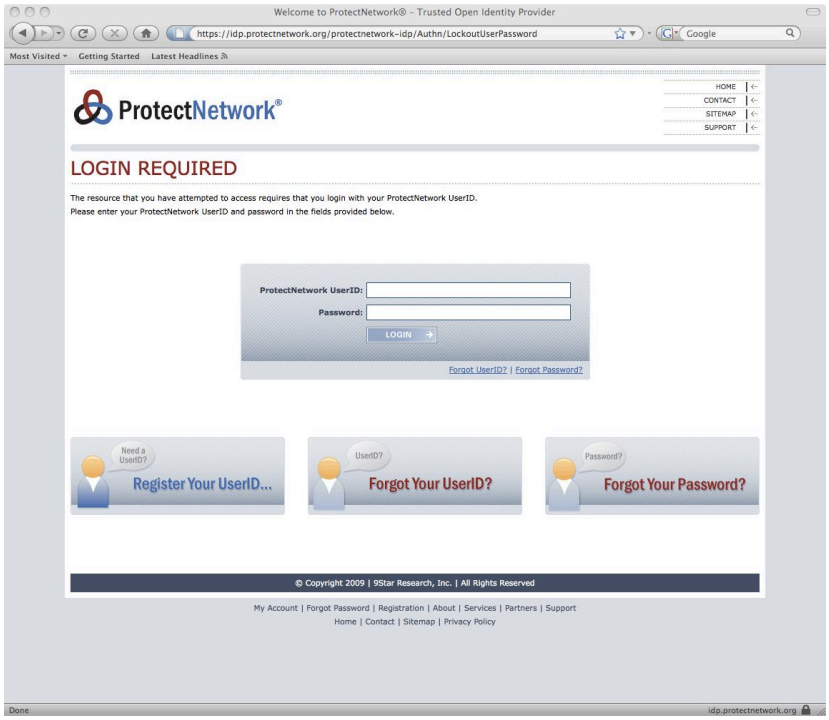
Federated Guest Registration Site



Selecting the home institution

The Registration page is configured to allow the external party to select their home institution and login to that institution. The institution MUST release the eduPersonPrincipalName attribute (eppn) upon successful login. The eppn MUST be scoped to the institution and MUST NOT be reassignable. The released eppn is then used as a key in the USC Global Directory Service. Changes to an eppn will require re-registration. The system provides no automatic resolution of such events.

If the external party's home institution is not listed then the individual can register a UserID with ProtectNetwork. The ProtectNetwork registration process is self-asserted, real-time, free, and requires only a valid email account. Once the ProtectNetwork account is registered, verified, and activated it can be used to register with USC.

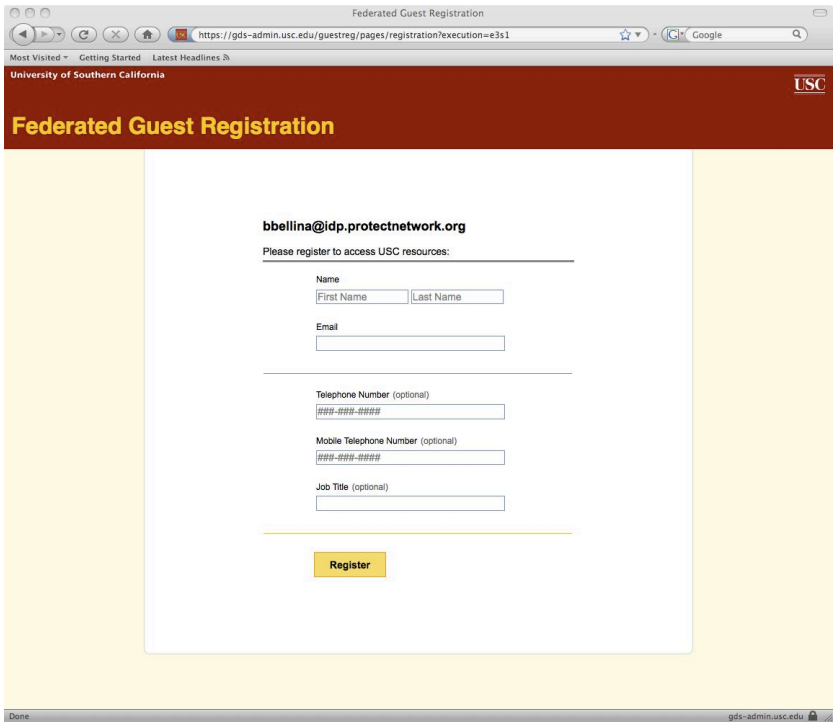


ProtectNetwork Login Page

Self-Asserted Information Provided by External Party

The following information is self-asserted by the external party during registration with USC:

- email address
- Given name
- Surname
- telephone number (optional)
- mobile telephone number (optional)
- job title (optional)



New User Registration Page

Only a single email address can be specified and it must be in valid syntax. A post-registration email will be sent to this address so it is important that it be a valid address accessible by the external party.

Names can contain only valid ASCII letters, spaces (not leading or trailing), hyphen (not leading or trailing), and apostrophe and be between 1 and 50 characters. Both given name and surname are required.

Telephone numbers must be entered in standard ITU format. (#-###-###-####)

Title must contain only ASCII letters and be restricted to 255 characters.

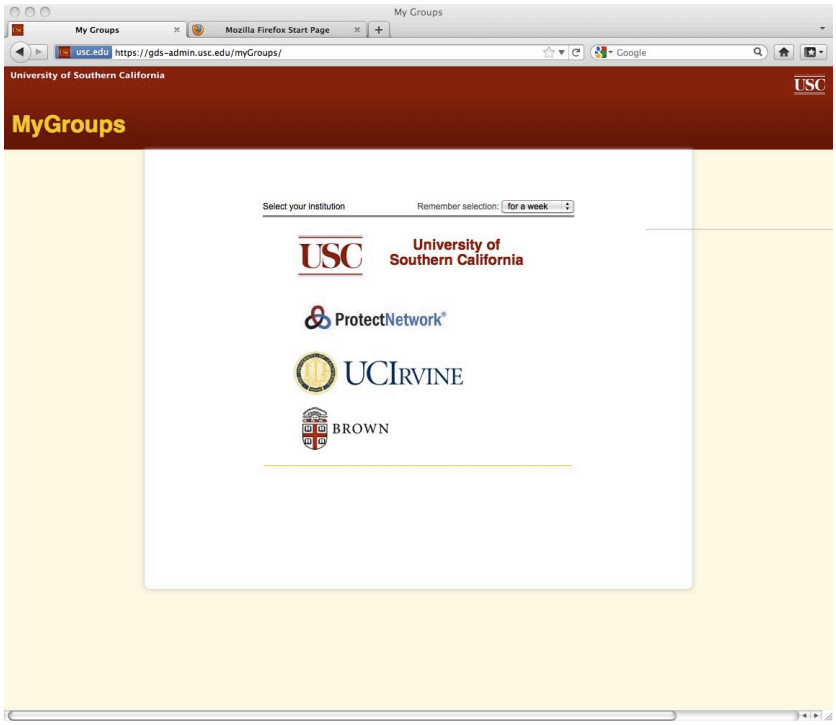
If following successful registration the registered guest wishes to change the information submitted then he/she can do so by logging in to the registration application again and the application will display the current information and allow it to be updated.

Following registration an email will be sent to the provided email address communicating that the account has been registered and activated. The email can be expected within 5-10 minutes, although delays of an hour or more are possible depending on other processing.

Managing Privileges of Federated Users within an Application

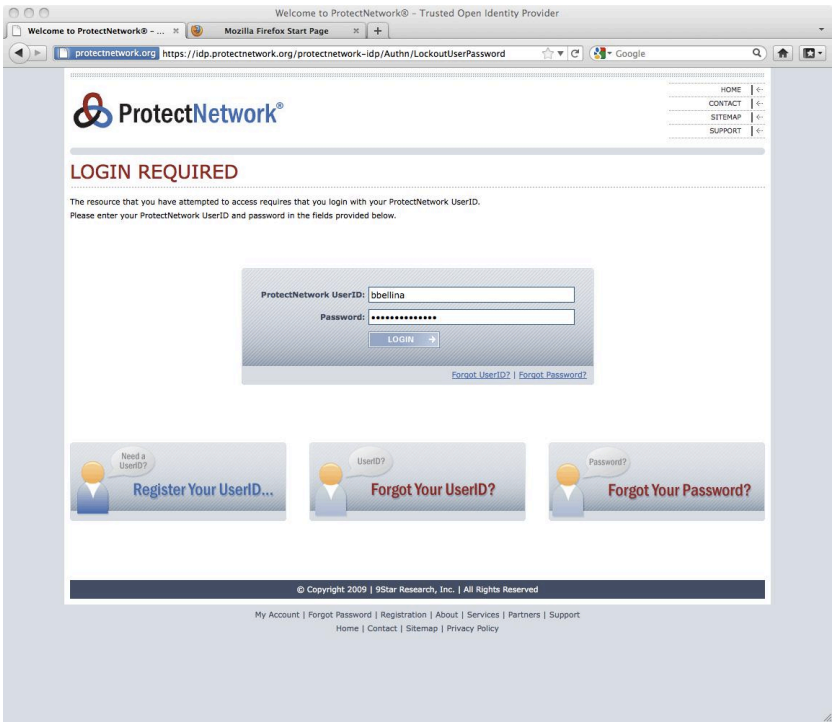
Privileges within an application can be managed by memberships in GDS groups managed via the MyGroups utility <http://gds-admin.usc.edu/mygroups> or by local information stored within the application database and managed by an application administrator. The basic guest information asserted at registration can be provided to the application at login or via a separate provisioning process.

Logging into a Federated Application



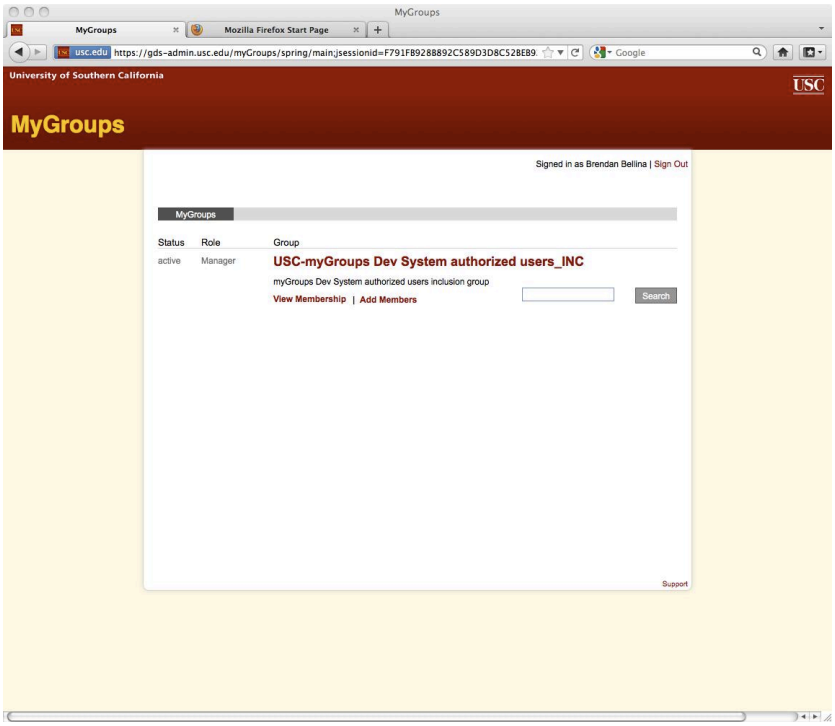
Accessing a Federated USC Application – Discovery Service

Guests will be able to use their federated login to access any federated application for which they have been authorized. Authorization is generally assigned by an administrator of the application adding the guest's identifier (communicated to the guest in the post-registration email) to the group of authorized users of the application using MyGroups. Once the guest is in the authorized user group of the application they can login to the application by going directly to its URL, clicking on their home institution, and logging in at their home institution. If they are already logged in to one federated application and then transition to another then the single sign-on feature of Shibboleth will prevent a second login.



Logging in at the Home Institution

The eppn from the home institution identity provider is combined with the self-asserted information in the GDS and the group permissions and released as a whole to the application. If the user is authorized then their information will be available for use by the application, otherwise an error page will be displayed.



Federated Guest logged into MyGroups

Appendix: Technical Representation of a Federated User in the GDS

When a Federated user registers a person entry and an account entry are created in the GDS. The attributes of the account entry will be set such that the entry is added to a Registered Guests GDS group and when that occurs an email communicating their account (eppn) will be sent to the user at the email address they specified during registration.

The created person entry is populated as follows:

dn: (a standard person entry dn generated based on uscPvid)
objectclass: top
objectclass: uscDirectoryEntry
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: eduPerson
objectclass: uscEduPerson
objectclass: uscMailRecipient
uscGuid: (a standard GUID generated based on uscPvid)
uscRDN: (a standard uscRDN generated based on uscPvid)
uscPvid: (a standard uscPvid randomly generated)
uscOwnedAccount: (the dn of the account entry)
uscEntryStatus: active
uscEntrySource: external
uscEntryCategory: person
uscEntryCreateDate: (date in YYYYMMDDHHMMSSZ)
uscEntryNote: (optional notation)
uscAffiliation: guest
uscPrimaryAffiliation: guest
mail: (email address provided by the user)
telephoneNumber: (optional telephone number provided by the user)
mobile: (optional mobile telephone number provided by the user)
title: (optional job title provided by the user)
sn: (surname provided by the user)
givenName: (given name provided by the user)
displayName: (derived: givenname + " " + surname)
cn: (derived: givenname + " " + surname)
uscSortedDisplayName: (derived: surname + "," + givenname)
uscDisplayGivenname: (given name provided by the user)
uscDisplaySn: (surname provided by the user)
eduPersonAffiliation: affiliate
eduPersonScopedAffiliation: affiliate@usc.edu
eduPersonPrimaryAffiliation: affiliate
eduPersonPrincipalName: (eppn provided through Shibboleth)

uscNetID: (eppn provided through Shibboleth)
uscRegistryID: -

The created account entry is populated as follows:

dn: (standard account entry dn generated based on account uscPvid)
objectclass: top
objectclass: uscDirectoryEntry
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: eduPerson
objectclass: uscEduPerson
objectclass: uscMailRecipient
objectclass: posixAccount
objectclass: uscAccount
uscGuid: (a standard GUID generated based on account uscPvid)
uscRDN: (a standard uscRDN generated based on account uscPvid)
uscPvid: (a standard uscPvid randomly generated)
uscOwnerPvid: (person entry uscPvid)
uscEntryStatus: active
uscEntrySource: external
uscEntryCategory: account
uscEntryCreateDate: (date in YYYYMMDDHHMMSSZ)
uscEntryUsage: external
uscEntryNote: (optional notation)
owner: (the dn of the person entry)
seeAlso: (the dn of the person entry)
uscAffiliation: guest
uscPrimaryAffiliation: guest
mail: (email address provided by the user)
telephoneNumber: (optional telephone number provided by the user)
mobile: (optional mobile telephone number provided by the user)
title: (optional job title provided by the user)
sn: (surname provided by the user)
givenName: (given name provided by the user)
displayName: (derived: givenname + " " + surname)
cn: (derived: givenname + " " + surname)
uscSortedDisplayName: (derived: surname + "," + givenname)
uscDisplayGivenname: (given name provided by the user)
uscDisplaySn: (surname provided by the user)
uid: (eppn provided through Shibboleth)
uidNumber: -
gidNumber: -
homeDirectory: -
uscAccountType: individual

uscAccount: (eppn provided through Shibboleth)
uscAccountLogin: (eppn provided through Shibboleth)
uscAccountScope: -
uscAccountAffiliation: guest
eduPersonAffiliation: affiliate
eduPersonScopedAffiliation: affiliate@usc.edu
eduPersonPrimaryAffiliation: affiliate
eduPersonPrincipalName: (eppn provided through Shibboleth)
uscNetID: (eppn provided through Shibboleth)
uscRegistryID: -

In order to force the ds_sync_groups process to update the Registered Guest group the attribute uscGroupLevel should be replaced with “updated” in group uscrdn=usc.edu.scfg7bb9,ou=groups,dc=usc,dc=edu.