NC State Shibboleth Attribute Release Policy (ARP)

Version 2.0
17 November 2018

Introduction

This document identifies the specific data elements that are provided by North Carolina State University's Shibboleth Identity Provider service in order to authorize individuals to services (via their associated Service Providers) delivered by their web site/application. For more information about NC State's implementation of Shibboleth, please see:

- [Overview](#)
- [Technical Documentation](#)
- [General documentation about the Shibboleth Project](#)

Glossary

Attributes - Data elements that are used to provide identity information to requesting SP's. Attributes are based on standard LDAP definitions or the eduPerson, eduOrg or eduCouse object classes.

Federation - A federation, through its trust agreements and federating software, allows identity providers to manage user privacy and information exchange. Service providers no longer need to provision identity accounts, instead leveraging the identity provider's identity system.[1]

Identity Provider (IdP) - Provides single-sign on capabilities for web services, authenticating users and supplying data to services. In addition to a simple yes/no response to an authentication request, OIT's Identity Provider infrastructure can provide a rich set of user-related data to services. This data can help the service provide a more personalized user experience, save the user from having to manually enter data the service requires, and refresh the data each time the user logs into the service.

Service Provider (SP) - enables web SSO and federation for web applications.

---

[1] https://www.incommon.org/federation/basics.html

Attribute Release Policy (ARP)

NC State University belongs to a number of different trust federations which include different member populations. Each federation has a distinct ARP based on the trust relationship among the federation members, the specific attributes to be released by default, and the risk associated with sharing those attributes with the federation members.

It is the expectation of the University that only attributes needed will be requested. Exceptions to a default attribute release policy can occur in any federation. All such requests will be vetted by the Office of Information Technology's Security & Compliance division. Release of additional attributes at a later time may be requested.

Any release of attributes to corporate or other external entities, whether a member of a Federation or not, requires a contract or legal agreement which explicitly states how the attributes will be used. This is generally provided as part of the Service Provider On-boarding Process[2] (which is required regardless of the status or location of the requesting customer).

Federations

InCommon

The InCommon Federation is an international federation whose participants include higher education, research, governmental agencies as well as sponsored partners that include corporate and governmental agencies. For more information, please see
https://www.incommon.org/federation/

Institutions who are qualified by InCommon as members of the "Research and Scholarship" community[3] also receive EPPN, givenName, sn, and mail attributes in addition to the attributes below.

Attribute	Attribute Description
EPTID	eduPersonTargetedId - Unique identifier (per service provider)

[2] https://oit.ncsu.edu/campus-it/identity-management/shibboleth/shibboleth-access-request/
[3] https://www.incommon.org/federation/categories/index.html

EPPA	eduPersonPrimaryAffiliation - Primary Affiliation status (staff, student, etc) w/o scoping suffix
EPSA	eduPersonScopedAffiliation - Affiliation status (staff, student, etc) with scoping suffix (@ncsu.edu, @uncg.edu)

NC State University

The NC State Federation is commonly used by University services (on- and off-premises) to provide access solely to member of the university community.

Attribute	Attribute Description
NAME Attributes	- sn - surname (last name) - givenName - first name - displayName - eduPersonNickname
mail	Email address
EPPN	eduPersonPrincipalName - scoped username (unityid@ncsu.edu)
EPTID	eduPersonTargetedId - Unique identifier (per service provider)
EPSA	eduPersonScopedAffiliation - Affiliation status (staff, student, etc) with scoping suffix (@ncsu.edu, @uncg.edu)
EPPA	eduPersonPrimaryAffiliation - Primary Affiliation status (staff, student, etc) w/o scoping suffix
uid	Un-scoped username, eg unityid
campusPermanentId	9-digit Campus ID number with scoping suffix (123456789@ncsu.edu)
ncsuCampusId	9-digit Campus ID number (123456789), only released upon request
ncsuPrivate	Flag indicating FERPA privacy block
ncsuPasswordExpired	Flag indicating password has expired. This is now implemented by the IdP and prevents any userid with an expired password to proceed with the authentication process.
ncsuPasswordExpDate	No longer required, but still available for reminder purposes

ncsuEnrolledTwoFactor	Y or N indicating if the user has enrolled in Duo
ncsuAuthedTwoFactor	Y or N indicating if the user successfully used Duo 2FA during the current session

Additional Attributes Available

These attributes may be requested but do require justification and a description of their use to be provided on the [Service Provider onboarding form](#).

General Attributes

Attribute	Attribute Description
isMemberOF	a multi-valued attribute listing individual group identifiers of WolfTech AD groups that have the user as a member. Examples: ● CN=NCSU-B-Unity Users,OU=Managed Groups,OU=NCSU,DC=wolftech,DC=ad,DC=ncsu,DC=edu ● CN=WT-OIT-Shared Services,OU=Managed Groups,OU=NCSU,DC=wolftech,DC=ad,DC=ncsu,DC=edu Important Note: This attribute will not deliver inherited groups.

Employee Attributes

Attribute	Attribute Description
departmentName	Unit name of employee's department (eg, Shared Services)
departmentNumber	Numeric identifier of employee's department (eg, 57101)
employeeTitle	Position Title of Employee (eg, IT Manager)
employeeType	Position Type of Employee (eg, SHRA Employee)
ncsuAffiliation	Department that the employee is affiliated with (eg, Office of Information Technology)

Student Attributes

Attribute	Attribute Description
ncsuClassCode	Short code representing the academic class of a student (eg, FR, SO)
ncsuClassName	Full academic class name (eg, Freshman, Sophomore)
ncsuCurriculumCode	Short code representing curriculum of student (eg, HB)
ncsuCurriculumName	Full academic name of student (eg, Biological Science - Human Biology)