Migration from Proxy.cgi to Web SSO

Revision 1.0
November 17, 2006

Table of Contents

Introduction ................................................................................................2
Proxy.cgi background and migration plan ..............................................2
What problems do Web proxy services solve and how do they work? .............. 2
Why retire the SNAP proxy.cgi? .............................................................. 3
Web single sign-on basics...................................................................... 3
The migration plan and timeline ......................................................... 4
Getting assistance .................................................................................. 4
Modification of target sites ................................................................. 4
Is the target site still in production? Is authentication still needed? ................. 5
For sites resident on the nuinfo server .................................................. 5
For sites not resident on nuinfo ............................................................. 5
Special considerations for target site CGIs ............................................ 6
Modification of referring sites ............................................................... 6
References within the target site .......................................................... 7
References within other Northwestern sites ............................................. 7
References from outside Northwestern ................................................... 7
Links in e-mail messages ....................................................................... 7
Advisory and technical resources for administrators .............................. 7
The Web SSO software system ............................................................. 7
Advice on Web server and SSO agent issues ........................................ 7
Coordinating nuinfo-based site migration to SSO ................................... 7
Notifying referring sites ..................................................................... 8
References ............................................................................................ 8
Introduction

Northwestern University Information Technology (NUIT) will retire the current SNAP proxy.cgi service as a portion of the current project to replace the SNAP system. The SNAP proxy service will be replaced by use of the Online Passport Web Single Sign-On facility (Web SSO). For Web site administrators, this document describes the migration process and the advisory resources available.

This migration process was designed jointly between NUIT Technology Support Services (TSS), NUIT Information Systems Architecture (ISA) and University Relations Web Communications (UR Web Communications). Web site administrators facing the need to migrate their sites to the Web SSO system can get advice and guidance from NUIT ISA and UR Web Communications.

The migration described will take place between November 2006 and June 2007. Site administrators will have responsibility to work with ISA to implement the Web SSO service before June 2007.

Proxy.cgi background and migration plan

What problems do Web proxy services solve and how do they work?

A Web proxy service restricts access to a particular Web site (the “target site”) to those users who are vetted under rules kept within the Web proxy itself. The rules could include criteria such as authentication with NetID and password, network address, time-of-day, or user standing as faculty, staff, or student. At Northwestern, the initial use of SNAP proxy.cgi was to authenticate access to external information resources purchased by the Library. The authentication served as a gateway to limit access to only those within the University. Over time, University Web site administrators have expanded use of the SNAP proxy services to authenticate internal Web sites that contain sensitive information.

Setting up Web proxy access to a target site is not simple. The “referring page”, which has a link to the target site, must be coded to direct the user’s browser to the Web proxy service instead. Encoded into this proxy service URL is an argument which the Web proxy server translates into the true target site URL. The Web proxy server, itself simulating a Web browser, then invokes the target site URL. For its part, the target site Web server must restrict access to the
target URL to only the Web proxy server itself (otherwise the direct target URL could be entered by the user and bypass the authentication and vetting process). Therefore, the target site administrator must cooperate with the Web proxy administrator to correctly set up the linkage.

The connection between the user’s browser and the target site Web server is a “captive” session maintained through the Web proxy. All rendered pages from the target site which reference other parts of the target site must be recoded on-the-fly by the proxy service before being presented to the user’s browser to maintain this “captive” state.

**Why retire the SNAP proxy.cgi?**

NUIT ISA is currently in a project that will replace the SNAP system with a new identity management and access control system. The SNAP proxy.cgi facility is tightly-coupled to the overall SNAP system and should be replaced with more modern techniques. These newer techniques are more efficient and can be used to address additional authentication problems.

Authenticating access to off-campus service providers can be solved by either a newer proxy service or through use of “federated authentication.” The University Library has purchased its own proxy server and has moved all of its linkages to off-campus providers to that facility. This was necessary due to the increasing complexity of Web site programming techniques that could not be supported within the SNAP proxy.cgi code. As for federated authentication, a full discussion is outside the scope of this document; however, this technique addresses the same problem of off-campus providers through a standards-based exchange of identity assertion messages and does not require maintaining a captive Web session. NUIT ISA will be deploying federated authentication before June 2007.

Using the SNAP proxy.cgi facility to authenticate and limit access to on-campus Web sites will be replaced by the Online Passport Web SSO facility. This service performs exactly the needed authentication and attributed-based access controls used through the proxy.cgi service, again without requiring a captive Web session. The remainder of this document describes the migration process for this case.

**Web single sign-on basics**

The Web SSO facility relies upon cooperation between the application Web server and a policy server which enforces security based upon rules defined by the application administrator. This cooperation is implemented through a software module installed on the application Web server (the “agent”) which intercepts all Web page requests and determines how to treat each one. If the agent determines that the request should be allowed, then it passes it to the Web server which handles the requests as it normally would. If the requests must be denied, or if a credential challenge is necessary, then the agent and policy server take appropriate actions.

If a credential challenge (e.g. NetID and password) is successfully passed, then the policy server and agent install a session-limited “cookie” into the user’s browser. This cookie holds the information that a past credential challenge was successful. When the user returns to the same Web server, or to another Web server within the same Web SSO security realm, the policy server will recognize that the challenge has already been passed and will not issue a new challenge. As a result, the user only needs to enter his or her credentials one time in a browser session which may span many applications – hence the term “single sign-on”.

Revision 1.0

Last printed November 17, 2006
The software agent is a plug-in to the Web server, and hence it is dependent upon the particular Web server software and version. By using caching and other techniques, the software agent operates efficiently and does not measurably delay messaging between the user’s browser and the application.

The migration plan and timeline

The migration plan requires that all Northwestern target sites be Web SSO compliant by June 2007. In June 2007, NUIT will disable the SNAP proxy.cgi service and replace it with an error message Web page.

The plan allows for target sites to accommodate both proxy.cgi and Web SSO access for an overlap period. The target site administrator must decide when that overlap period will begin. The period will end when SNAP proxy.cgi is disabled.

Getting assistance

The target site administrator should contact NUIT and UR Web Communications for assistance by the sending e-mail to “webmaster@northwestern.edu”. This e-mail is monitored both by UR Web Communications and NUIT ISA staff. NUIT ISA will advise on technical aspects of the migration process and will set up the Web SSO configurations as arranged. UR Web Communications can advise administrators on communication issues. When sending e-mail to “webmaster”, please include the target site URL.

Modification of target sites

The first step in the migration from proxy.cgi to Web SSO is modifying the target site so that it will work correctly under both access methods. This modification is straightforward for those target sites on the “nuinfo” server because NUIT has already prepared the software. For other target site servers, prerequisite steps are required to install the Web SSO agent software.
Is the target site still in production? Is authentication still needed?

First, the site administrator should decide if the target site should be migrated. Many sites in the proxy.cgi database are no longer in production and some may no longer exist. The site administrator should also confirm that the target site continues to require NetID authentication. The migration process should only be undertaken for target sites which are in active use and must be authenticated. Obsolete target sites should be examined and cleaned (see box) and then reported to webmaster@northwestern.edu as no longer requiring proxy.cgi services. Please report these sites by URL or proxy name and NUIT will remove them from the monitoring list.

The contents of directories at obsolete URLs will remain hidden from any Web access so long as the .htaccess file remains in place. NUIT strongly recommends that site administrators remove unneeded files to avoid potential compromise from future changes in web site configuration.

Having determined that the target site must be migrated, the site administrator then follows one of the following procedures, dependent upon where the target site is located.

For sites resident on the nuinfo server

For target sites on the nuinfo server, the following steps must be taken for each URL currently identified within the proxy.cgi service:

1. Determine the new public-facing target URL. The proxy.cgi service maps a "proxy name" into a target URL. The target URL is not visible with proxy.cgi, but would be visible under Web SSO. Under Web SSO, an authenticated site located on the nuinfo server, within the main document directory "htdocs", would appear to be a subdirectory of the normal departmental URL. However, an authenticated site located outside "htdocs" is probably at a target URL not chosen for public consumption. For Web SSO, it may be desirable to configure a new URL under an associated departmental site. This applies to sites on nuinfo under the directories "proxy-cgi" or "more-docs".

2. Identify special access policies. The proxy.cgi service may have been configured to examine certain user attributes and limit access based upon the values for each user. For example, a site might only be accessible by students, or by students in a single school. This must be re-confirmed between the site administrator and NUIT ISA in order to mirror those limitations within the Web SSO system.

3. Enable the site under Web SSO. The last step is to “turn on” the Web SSO access to the target site. NUIT ISA will coordinate this with the site administrator for a given weekday morning. This will not affect proxy.cgi access to the site.

For sites not resident on nuinfo

For target sites that are not located on the nuinfo server, the site administrator and the local server administrator must coordinate installation of the Web SSO agent software before proceeding further. Once this is installed, the process parallels the nuinfo steps above.

1. Get the documentation for the Web SSO implementation process here at Northwestern. See “References” for the Web site address.

2. Implement or upgrade to a supported Web server.
3. Obtain the Web SSO agent software from either NUIT or the SUN software repository.
4. Install and configure the Web SSO agent software to permit all access except to a test URL.
5. Contact NUIT ISA to define, confirm, and configure the test URL for NetID & password policy and then open that URL for testing.
6. After testing is completed, contact NUIT ISA to coordinate a date to implement Web SSO production policies for the target URL and remainder of the server.
7. On the agreed-upon date, remove any access restriction rules from the target site directories, configure the Web SSO agent for production status, and after NUIT has confirmed policies are in place, test the target URL.

**Special considerations for target site CGIs**

For target sites that execute local application code, the site administrator may have to make changes to accommodate the following differences between proxy.cgi and Web SSO:

1. The user identifier (NetID) is presented to the Web site in different environment variables.
   - Proxy.cgi presents the NetID in variable: `HTTP_REMOTEUSER`
   - Web SSO presents the NetID in variable: `REMOTE_USER`

2. The client IP address is presented to the Web site in different environment variables.
   - Proxy.cgi presents the client IP address in variable: `HTTP_REMOTEADDR`
   - Web SSO presents the client IP address in variable: `REMOTE_ADDR`

3. Other attributes may be presented to the Web site under proxy.cgi, which are not presented under Web SSO. This should be handled by working with NUIT ISA to craft access policies which enforce restrictions prior to connecting with the Web server at all. If that is not practical, NUIT ISA can provide advice on alternative means. This applies to CGIs that use the environment variables `HTTP_SEMPLID`, `HTTP_USERTYPE`, `HTTP_USERSCHOOL`, `HTTP_USERORG`, `HTTP_HEMPLID`, or `HTTP_UNAME`.

4. CGI scripts that construct links to authenticated content will probably need to be modified to use the new URLs.

**Modification of referring sites**

Over the period from November 2006 to June 2007, target site administrators will receive listings of all URLs that reference their site via the proxy.cgi method. Any such references must be changed to the new target URL (operating under Web SSO) before the June 2007 date or they will fail when proxy.cgi is retired. The target site administrator must notify all referring sites that they should change their proxy-based references to direct target URL references. There are four possible sources for these proxy-based invocations.
References within the target site

The target site itself may have embedded HTML documents which reference pages within the site through proxy.cgi. This must be fixed by the target site administrator by searching the HTML of the target site for the strings "p/p.cgi" and "proxy/proxy.cgi" to identify absolute URLs that must be fixed. These are often found in templates for page headers or footers. For complex cases, it may make sense to create a copy of the entire site at a new URL.

References within other Northwestern sites

By far the most common proxy-based invocations will come from other sites within Northwestern. The target site administrator should make an effort to contact the administrator of the referring page to advise him or her of the new target URL. The referring page administrator is responsible for changing the HTML documents within his or her site to correctly invoke the new SSO-based URL for the target site.

References from outside Northwestern

External site references to proxy-based target pages are rare and usually come from cached referring pages within Internet search engines. Unless the target site administrator knows of special arrangements with specific external sites, these references may be ignored.

Links in e-mail messages

E-mail messages with embedded URLs will appear to be invocations from email servers (through Webmail) or will not appear at all. Because most messages of this sort are created by target site application scripts themselves, the target site administrator should carefully check for these references internally. Unfortunately, other sites sending e-mail with proxy links cannot be detected and will break when proxy.cgi is retired.

Advisory and technical resources for administrators

The Web SSO software system

Visit the Web SSO documentation page (see “References”) and additional SUN documentation referenced there. Additional questions can be sent to nuit-isa@northwestern.edu.

Advice on Web server and SSO agent issues

Particular technical problems encountered during installation of the Web SSO agent should be sent to NUIT ISA at nuit-isa@northwestern.edu. A software engineer will work with you to diagnose the problem.

Coordinating nuinfo-based site migration to SSO

Target sites on the nuinfo server may not have technical support to address all of the concerns raised by this document. If that is the case, please notify webmaster@northwestern.edu for assistance.
Notifying referring sites

Those target site administrators who have problems finding the administrator of a referencing site should contact UR Web Communications at webmaster@northwestern.edu.

References

Web SSO at Northwestern, with links to the SUN agent software repository: http://www.it.northwestern.edu/about/departments/isa/services/wam/index.html