

Libraries walk-in-user pilot

Super Walk-In Users Portal - Library Pilot Scenarios 2 & 3

- [Super Walk-In Users Portal - Library Pilot Scenarios 2 & 3](#)
 - [Introduction](#)
 - [Kiosks for Walk-In Users](#)
 - [Problems With A Purely IP-Address Kiosk](#)
 - [Possible Solution: Managing accounts for Walk-In Users](#)
 - [Possible Solution: IP Address Authentication at the library IdP](#)
 - [Implemented Pilot Solution: A shared, easily configured IdP service for Walk-In users](#)
 - [Authentication and User Attributes](#)
 - [How the Pilot Service Was Configured](#)
 - [Practical Implications](#)
 - [Demonstration: An Example User Journey](#)
 - [Summary/references/repositories/status](#)

Introduction

Reliance on using IP addresses to authenticate users prevents some university libraries from moving to fully federated access to online resources. Despite the many disadvantages of controlling access using IP addresses, they are relatively simple to set up at a small scale, and can be useful in two contexts: accessing out-dated eresources that do not support modern authentication (which has been explored by AARC [in another pilot](#)) and providing access to "walk-in" users.

Kiosks for Walk-In Users

Many libraries use IP-address authentication for providing access to "walk-in" library users. Walk-in users are people who do not have institutional IT accounts (and so cannot use normal IdPs). Walk-in users may be alumni, local residents, employees of companies working with the library or children at local schools. It may be too slow or costly to manage IT accounts for these users.

Walk-in users visiting a library can be given access to eresources by using "kiosk" terminals - PCs that have been locked-down to be secure enough for anonymous use. Kiosks will limit the software and websites that can be accessed, and provide a friendly menu of available resources.

Eresources will normally grant access to these terminals by relying on IP address authentication: each kiosk will have a static public IP address or be in a range of network addresses known to be used by walk-in users.

Problems With A Purely IP-Address Kiosk

Dependency on legacy technology: In order to support walk-in users all accessible eresources must continue to provide IP-address authentication. This discourages them from properly modernising and federating access to their service.

Scalability: All eresources (potentially a large number) must be configured with the IP addresses of all kiosks. Adding a new kiosk will be awkward and time-consuming and require changes at many different websites. In some cases changes must be requested by email.

Security and licensing risks: De-provisioning or updating the IP addresses of networks or individual kiosks can be easily overlooked, creating potential access problems

Possible Solution: Managing accounts for Walk-In Users

If a library provides accounts for walk-in users they can log in normally, using the same IdP as staff and students, and access federated resources and IP-authenticated resources via EZProxy.

Unfortunately this is often impractical for the potentially large number of casual, occasional walk-in users that could potentially visit a library.

Possible Solution: IP Address Authentication at the library IdP

A SAML IdP (such as the Shibboleth IdP) can be configured to automatically authenticate users logging in from defined IP addresses or ranges of IP addresses. This can be used to provide modern, federated access to eresources for walk-in users at library kiosks.

However, this approach has a few disadvantages:

Not all libraries have available SAML IdPs. The configuration is via XML files, and the IdP needs to be restarted to load them. Library staff cannot easily make changes or see the current status, and the IdP may be managed by a different department. This can lead to delays and deprovisioning risks, and leave library staff feeling frustrated.

Implemented Pilot Solution: A shared, easily configured IdP service for Walk-In users

This pilot demonstrated the use of a dedicated, IP-address based IdP. The pilot service has some distinctive features:

- It is for use only by walk-in users
- It is authenticated only by IP addresses
- It is managed by library staff via a web-based admin interface
- Library staff access the administration interface using their own institutional credentials
- Changes to the configuration for access control are available immediately.
- The IdP can be run for one organisation or for many, as a shared service. It can be shared by a group of institutions in the same region, or even at a national federation level.

Authentication and User Attributes

The pilot service will not allow authentication from IP addresses that are not listed in its admin UI.

All authenticated users are given a walk-in-user affiliation.

Every IP address or network address range can be configured to share arbitrary entitlement information.

IP addresses can be assigned different domain scopes, determined by the scope of the administrator who configured the ip address range. This allows SPs access using the service to differentiate between users at different libraries.

How the Pilot Service Was Configured

A standard Shibboleth IdP v3 was used.

Authentication was configured to only use IP addresses using the default network address authentication module that is included in the Shibboleth IdP. All IP addresses were permitted by default.

An IdP extension was used to collect the user's IP address. This can also be done using Javascript within the IdP, if Shibboleth IdP v3 is used.

Attributes for the user were searched for (using a numeric version of their IP address) in an LDAP directory. Records in the LDAP directory contain normal user attributes but records are for network address ranges, not users.

If a matching LDAP record with suitable attributes is found, the user authenticates as normal and attribute data is shared with the destination resource.

By default all IP address ranges can authenticate, so the LDAP attribute information (or lack of it) is used to provide a second authentication step. An intercept filter was added to the IdP to halt authentication if no record for that IP address was found in the LDAP directory.

LDAP records were configured using a stand-alone administration interface supplied by DAASI. Any utility capable of updating LDAP could be used, but the DAASI application used in the pilot allows administrators from many different institutions to log in and edit records for their own organisation, so that one service can provide IP-address-based authentication for many


Practical Implications

The IdP can be used by many different organisations as a shared service, and can use a variety of scopes, but it cannot be used to access existing resource SPs without additional configuration at the SP, and additional licensing agreements.

Scopes must be configured in the SP's metadata to be accepted: basic security checks in most SPs prevent IdPs from using arbitrary scopes.

Most academic resources are configured to permit access according to licence agreements by matching the licensee's entity ID to supplied attribute data. As the shared IdP in the pilot has a new entity ID that is potentially shared by many organisations, each SP must configure access for each user of the shared IdP by checking against both scope and entity ID.

Demonstration: An Example User Journey

<div>1.</div> <div><p>This is a user story featuring two users at a university called Typical University One.</p><p>Andy Walker is a journalist and external guest at University One. He does not have an IT account but he does have walk-in access to the University library.</p><p>Barbara Jensen is a librarian at University One.</p></div>	
<div>2.</div> <div><p>Andy is writing a newspaper article about dogs living on boats, and he visits University One's library to do some research.</p><p>He attempts to access a suitable photo archive using a university terminal for walk-in users.</p><p>https://saml-eresource.libs3.aarc.demo.university/</p></div>	<div><div><div>The Canine Navigation Archive</div><div>Browse DatabaseProfile[?]Login</div></div><div><div>The Canine Navigation Archive</div><div></div><div><div>The leading academic archive of photographs of dogs on canal boats</div><div><p>I orem insum dolor sit amet. consectetur adipiscing. Suscipiendisse enestas quam sit amet erat nharetra. Interer clauibus temnor temnor. Nam aliquet. turpis.</p></div></div></div></div>

3. However, he's blocked - the site requires Shibboleth authentication and he does not have an account.

Select an identity provider

The Service you are trying to reach requires that you authenticate with your home organization, enter the name below.

Recently used organizations:

[Typical University One](#)

[Walk-In Library Users](#)


Enter institution name:

Or choose from a list:

Typical University One

Remember for session

Need assistance? Send mail to [administrator's name](#) with description.



Web Login Service - Access Denied

You are not eligible for the service requested.

4. He reports this to Barbara at the library support desk and asks for help.

Barbara knows that University One has access to a special IP address-based IdP and that it has access to the archive, so she decides to add the terminal Andy that is using.

Barbara visits the administration page for the IdP, and logs in with her University One credentials.

<https://adminportal.lib.pilots.aarc-project.eu/loi/daportal.pl>

AARC Library IP Ranges Management



[Home](#)

[AARC Scenario 23 Portal](#) / [Login](#)

[Toggle help texts](#)

Login to system

© DAASI International

Select an identity provider

The Service you are trying to reach requires that you authenticate with your home organization, enter the name below.

Recently used organizations:

[Typical University One](#)

[Walk-In Library Users](#)

Enter institution name:

Or choose from a list:

Need assistance? Send mail to [administrator's name](#) with description.



Typical University One: Login

Login to Canine Navigation
Archive

Username

[> Forgot your password?](#)

[> Need Help?](#)

Password

☐ Don't Remember Login

☐ Clear prior granting of permission
for release of your information to this
service.

The Internet's leading collection of photos of
dogs on boats

5. She adds the IP address of the terminal. (82.69.55.233)
- Barbara then asks Andy to try again, and to use the IPA IdP.

AARC Library IP Ranges Management



[Home](#)[AARC Scenario 23 Portal / Trusted IP ranges](#)[Toggle help texts](#)

[Trusted IP Ranges](#)[Logout](#)

Manage trusted IP ranges

The following trusted IP ranges could be found

<input type="checkbox"/>	Begin ▲	End ▼	Affiliation ▼	Entitlement ▼	Description ▼	
<input type="checkbox"/>	203.0.113.115	203.0.113.115	library-walk-in@uni-one.demo.university		Front Desk Kiosk	<input type="button" value="edit"/>
<input type="checkbox"/>	203.0.113.233	203.0.113.233	library-walk-in@uni-one.demo.university		Kiosk One	<input type="button" value="edit"/>
<input type="checkbox"/>	203.0.113.245	203.0.113.245	library-walk-in@uni-one.demo.university		Kiosk Two	<input type="button" value="edit"/>

Showing 1 to 3 of 3 rows

© DAASI International

AARC Library IP Ranges Management



[Home](#)[AARC Scenario 23 Portal / Trusted IP ranges](#)[Toggle help texts](#)

[Trusted IP Ranges](#)[Logout](#)

Manage trusted IP ranges

The following trusted IP ranges could be found

<input type="checkbox"/>	Begin ▲	End ▼	Affiliation ▼	Entitlement ▼	Description ▼	
<input type="checkbox"/>	203.0.113.115	203.0.113.115	library-walk-in@uni-one.demo.university		Front Desk Kiosk	<input type="button" value="edit"/>
<input type="checkbox"/>	203.0.113.233	203.0.113.233	library-walk-in@uni-one.demo.university		Kiosk One	<input type="button" value="edit"/>
<input type="checkbox"/>	203.0.113.245	203.0.113.245	library-walk-in@uni-one.demo.university		Kiosk Two	<input type="button" value="edit"/>
<input type="checkbox"/>	203.0.113.247	203.0.113.247	library-walk-in@uni-one.demo.university		Kiosk Three	<input type="button" value="edit"/>

Showing 1 to 4 of 4 rows

© DAASI International

6. Andy returns to the terminal and tries again - and this time he can log in to the eResource. He is now able to do research for his article.

The Canine Navigation Archive

Browse Database




Profile

[?]

Login

Browse Database

Found 2048 images

Image	Location	Details	
	Ashton Canal, UK	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque arcu justo, suscipit at erat sed, sollicitudin cursus erat	Download
	Ashton Canal, UK	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque arcu justo, suscipit at erat sed, sollicitudin cursus erat	Download
	Peak Forest Canal, UK	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque arcu justo, suscipit at erat sed, sollicitudin cursus erat	Download

[<<](#)

[<](#)

Page 1 of 808

[>](#)

[>>](#)

Summary/references/repositories/status

Task1, Pilot 2	Walk by users
Focus	Support authorized access for citizen scientists to library resources (SAML+IP to SAML with authZ)
Approach/AARC identified solution	Establish a guest SAML IdP which adds attributes to authorize non-institutional users. In addition, explore exploitation models: per library or per national library consortium deployment.
Components piloted	Shibboleth v3 for IdP with IP-based AuthZ attribute
Gain for end-users /administrators	<ul style="list-style-type: none"> More consistent interface no matter which resource is being approached Ability to use this access method and at the same time maintain full privacy Admin interface for librarians to scope/configure valid IP ranges
Demo	Flow Demo admin portal Demo user portal
Detailed technical description	AARC wiki
Documentation of components	Documentation for walk by user access component, access control wiki Documentation of the IdP-extension to release the user's IP address Documentation of the portal that allows library administrators to manage their campus IP address ranges
Software source(s)	Shibboleth v3 for walk by user access
Lead	GARR/DAASI
Community partners	IT: GARR, Library NL: UKB library consortium
Status	Close to finalization. Awaiting final phase of feedback from communities