MUSE KNOWLEDGE | PROXY

SEAMLESS AND SECURE REMOTE ACCESS TO RESOURCES

VERSION 1.4 · 19 MARCH 2018 · EDULIB, S.R.L.

MUSE KNOWLEDGE HEADQUARTERS

Calea Bucuresti, Bl. 27B,
Sc. 1, Ap. 10,
Craiova 200675, România
phone +40 251 413 496

MUSE KNOWLEDGE EMEA

Khalifa21 El El Mamounst.
Roxy Tower, Heliopolis,
11341, Cairo, Egypt
phone +202 241 87 349

MUSE KNOWLEDGE NORTH AMERICA

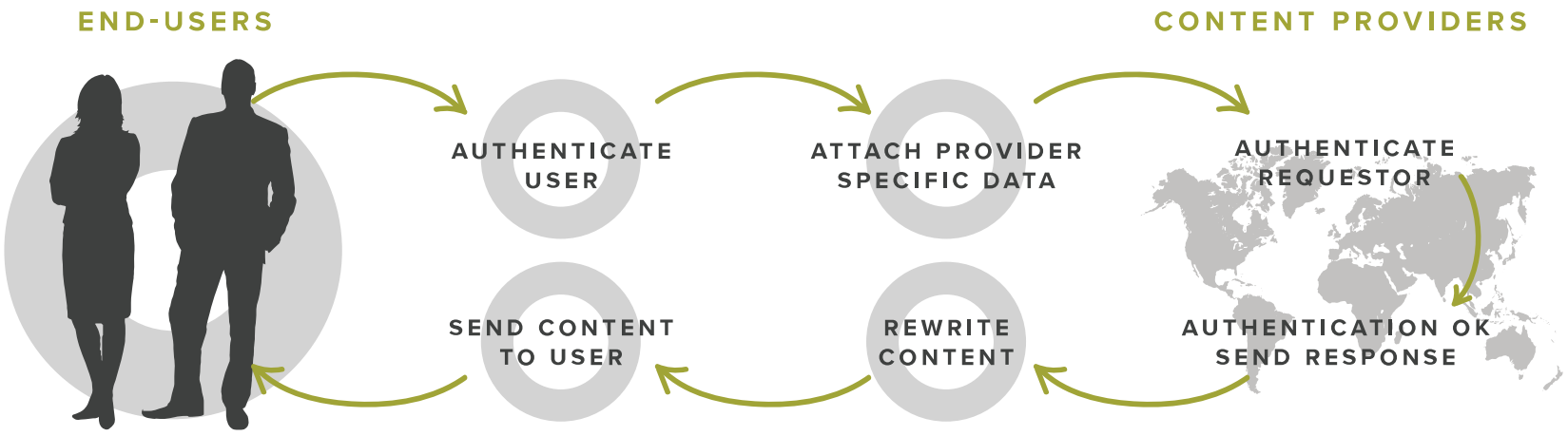
340 Madison Avenue
19th Floor
New York NY 10173 USA
phone +1 212 220 9250

MUSEKNOWLEDGE™ PROXY

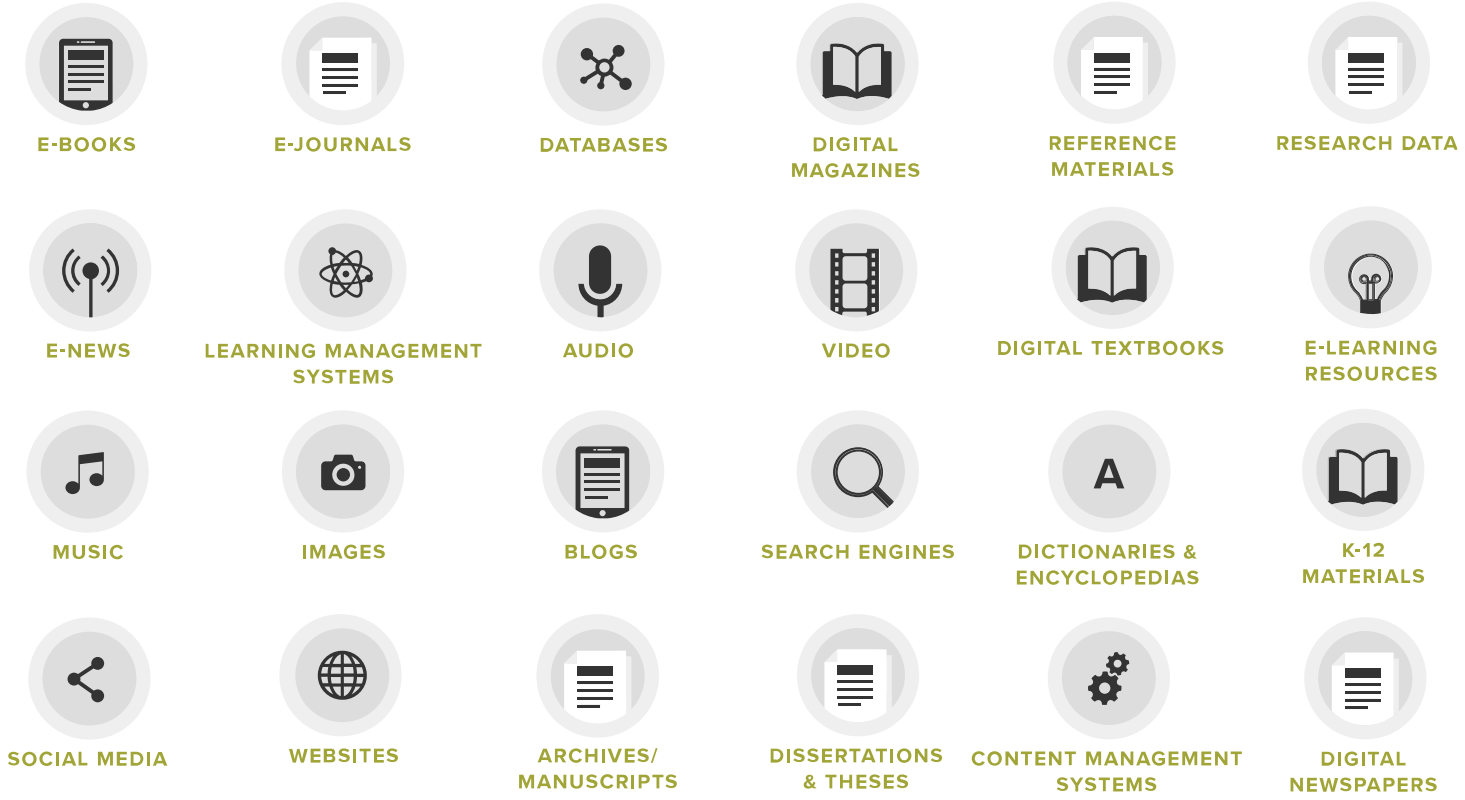
Highly customizable multi-platform proxy server

- Easy to use and configure via the MuseKnowledge™ Proxy Administrator Console
- Gateway to authenticated restricted content
- Rewriting web server
- Web Access Management (WAM)
- Proxy server and reverse proxy

More than 15 years within the Muse Federated Search Platform to manage the authentication to resources and the navigation to full text.



MUSEKNOWLEDGE™ PROXY



Overview

- SAML 2.0 Single Sign-on
- Learning Tools Interoperability® integration
- Quickly delivers rewritten pages
- Search widgets and form integration
- Corporate infrastructure: load balancer ready, API ready
- Compatible with all browsers deliver results conveniently and reliably
- Hands-off approach to system maintenance via Muse Navigation component update distribution service
- Online privacy, protection, and data transparency
- Proxyfied URL (shortcuts to entry point URLs)
- Rewrite by path and rewrite by host

GENERAL FEATURES

- **Multi-tenant** architecture.
- **Regular HTTP proxy with** HTTP and HTTPS (CONNECT tunnel) support.
- **Cache** support.
- **Separate cache** directory per each Server IP, based on the configuration.
- **Configurable authentication** using pluggable authentication login modules.
- **Patterns for** defining the list of server IP(s) on which to listen.
- **Individual authentication** per each Web Module (running inside a Web Context) in part.
- **Supports public,** authenticated and private resources in each Web Context.
- **The static resources** are served using the Last-Modified HTTP response header in order to be cached by the browsers.
- **Default log** for messages regarding the activity and errors encountered in a human readable format.
- **Access log** in which there are written the requests served by Muse Proxy. The Access log can be analyzed using tools like AWStats (http://awstats.sourceforge.net/).
- **Statistics log** with detailed messages regarding Muse Knowledge™ Proxy activity in a machine readable format.
- **Global proxy chaining** with a next proxy using Proxy Host and Proxy Port or using Proxy PAC.
- **IPv6 and IPv4** addresses.

GENERAL FEATURES

- **Support for** configuring different SSL certificate for each server IP.
- **Compression (GZIP) support** both for pages that are served after being rewritten (remote rewritten content from vendors) and for content originating to Muse Proxy itself.
- **For rewritten pages there is support** for SSL termination to ensure Load Balancing HTTPS traffic in a manner that avoids unnecessary encryption cycles. This is achieved by MuseKnowledge™ Proxy understanding *X-Forwarded-Proto* header field or the RFC 7239's Forwarded header field containing "proto=https" or "proto=http".
- **Support for** configuring the redirect of HTTP requests against Applications and Administrator Console to HTTPS.
- **Rewrite by Host** is selectable on a source by source basis.

MUSEKNOWLEDGE™ NAVIGATION MANAGER (REWRITING COMPONENT) FEATURES

- **Flexible URL patterns**, using include and exclude rules, matching all URL components (domain, port, path, CGI parameters), to specify which URLs will be rewritten.
- **Automatic rewriting** of links from HTML attributes.
- **Automatic rewriting** of links constructed with JavaScript.
- **Server side management** of Cookies from the Set-Cookie HTTP Headers received from the target rewritten sites.
- **Automatic rewriting** of Cookies from *document.cookie* JavaScript object.
- **Automatic rewriting** of links from CSS files.
- **Automatic rewriting** of links written in page in plain text, using *document.write* sequences.
- **Rewriting links** from XML and JSON using Muse Navigation Manager filters.
- **Automatic rewriting** of HTML OBJECT and EMBED tags.
- **Rewriting** Flash Objects Parameters, using Muse Navigation Manager filters.
- **Rewriting** HTTP and HTTPS sites.
- **Automatic authentication** for rewritten links using authentication token.
- **Supporting custom charset** in the Content-Type HTTP header returned by the rewritten pages.
- **Chaining support for the rewritten links**, at server side level with a next proxy via Proxy Host and Proxy Port or Proxy PAC.

MUSEKNOWLEDGE™ NAVIGATION MANAGER (REWRITING COMPONENT) FEATURES

- **Proxy-Authorization** using Basic and Digest authorization schemes, at server side level, with a next proxy, for the rewritten links. Support for separate proxy authorization for different rewritten links.
- **HTTP Authorization** for the rewritten links using Basic and Digest authorization schemes, at server side level, with the target site. Support for separate HTTP authorization for different rewritten links.
- **The Muse Navigation Manager** component (*mnm.jar* file) can be updated at run-time, without restarting Muse Proxy.
- **Tiny URL(s)** support.
- **Support for** setting an initial set of Cookie HTTP headers, at server side level, when navigating on a rewritten link. Support for separate sets of cookies for separate rewritten links navigated for the same target site.
- **Support for** setting an initial Referer, at server side level, when navigating on a rewritten link. Support for separate Referer authorization for different rewritten links.
- **Configurable Find and Replace filters** acting on the HTTP body can be crafted in the XML source profiles and will be interpreted at run-time, without the need to write Java code. Two types of filters: regular Proxy Java filters. Simple (just find/replace) and complex filter expression based and MuseKnowledge™ Proxy token rule based, similar to the token rules written in Muse configurations involving conditions (such as *APPLY_IF_FIRST*) and variables are supported.

MUSEKNOWLEDGE™ PROXY APPLICATIONS FEATURES

- **A MuseKnowledge™ Proxy Application can be** configured to respond only on certain server IP(s) (domains) on which Muse Proxy listens.
- **A MuseKnowledge™ Proxy Application supports** expiry after a certain date.
- **MuseKnowledge™ Proxy Applications users can** be authenticated using configurable Authentication Groups.
- **An Authentication Group used** in a MuseKnowledge™ Proxy Application performs the authentication using a list of configurable Login Modules. The current list of Login Modules that can be used by MuseKnowledge™ Proxy Applications is: IP, User/Password, LDAP, IMAP, SQL, FTP, Referer, HMAC, HTTP External Authentication, LTI, SAML, OAuth, OAuth2, OpenID Connect and CAS based SSO authentications.
- **An Authentication Group has** a dedicated login page, corresponding with the list of logon parameters required by the Login Modules configured in that Authentication Group.
- **An Authentication Group used** in a MuseKnowledge™ Proxy Application allows access to the Sources from a Sources Group.
- **The MuseKnowledge™ Proxy Application web interface is** completely configurable using FreeMarker template files (see http://freemarker.sourceforge.net/)
- **A MuseKnowledge™ Proxy Application supports** a configurable HTML index page to be displayed when accessing the Muse Proxy Application's home URL.
- **Automatic logon** in a MuseKnowledge™ Proxy Application with IP authentication.
- **MuseKnowledge™ Proxy Applications** are ready for Load Balancing.

MUSEKNOWLEDGE™ PROXY APPLICATIONS FEATURES

- **MuseKnowledge ™ Proxy supports** Single Sign on Authentication as a Client. A wide range of OAuth, OAuth2, OpenID Connect SSO based authentication are supported.
- **MuseKnowledge ™ Proxy supports** HTTP authentication to an external source.
- **A MuseKnowledge™ Proxy Source can be** profiled via *EXTRACTOR*s, *URL*s, and *POST_PARAMETER*s to conduct an extract and navigation scenario in order to obtain tokens or navigate to the desired link before handing over control to the browser with the first rewritten link.
- **MuseProxyFoundation based application supports** source icon configuration. If configured, the image will be displayed under the Source name, next to the source description.
- **Sources can be** hidden from the source listing but still usable via Entry Points either shortcuts, extended or normal.
- **A MuseKnowledge™ Proxy Application supports** a configurable logout page that is displayed when the user was logged out.
- **Links to MuseKnowledge™ Proxy Sources** from MuseKnowledge™ Proxy Applications can be embedded dynamically in external portals. In this way, a customer may use the external portal authentication, but still provide access to MuseKnowledge™ Proxy Sources links.
- **Support for** creating categories of MuseKnowledge™ Proxy Sources (grouping); E.g. group sources by subject, type, vendor, alphabetically - A to Z.

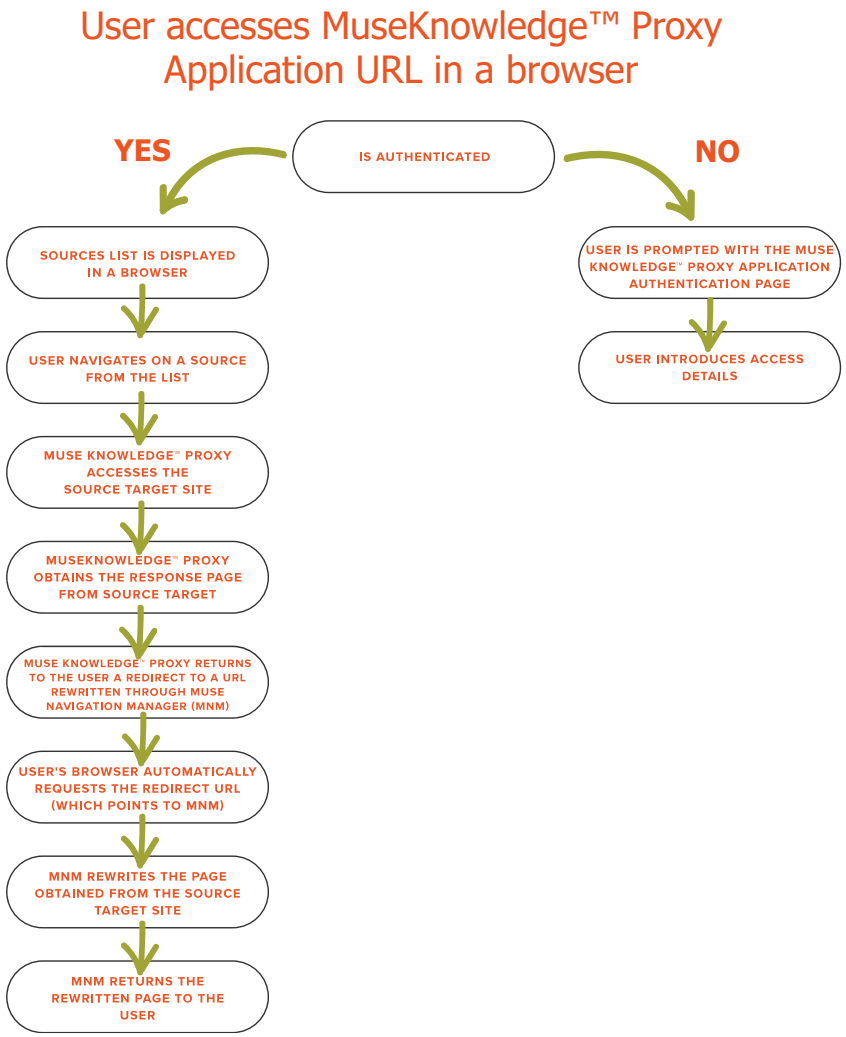
MUSEKNOWLEDGE™ PROXY APPLICATIONS FEATURES

About 1,000 MuseKnowledge™ Proxy Sources Profiles to download at this time.

SAML 2.0 Authentication as a Service Provider is supported for a MuseKnowledge™ Proxy Application. Being based on Spring Security SAML Extension, theoretically all products supporting SAML 2.0 in Identity Provider mode (e.g. ADFS, Okta, Shibboleth, OpenAM, Efecte EIM or Ping Federate) should be compatible; some of the SAML 2.0 related features are:

- **Includes** a local Discovery service.
- **Supports** external Discovery.
- **Metadata management** supporting adding IDP metadata and generating of SP metadata, pre-validation of IDP metadata to detect the need of certificates, tests for authentication, seeing SAML attributes, guidelines and more.
- **Supports specifying** the IDP metadata either by uploading the IDP metadata file or by specifying the IDP metadata URL with a local file backup with periodically refreshes.
- **Supports specifying** IDP metadata as a file/URL containing one EntityDescriptor or as multiple EntityDescriptor wrapped in *EntitiesDescriptor* (e.g. a federation) with filters eliminating conflicts if the SP metadata is also present in the same file.
- **Post-SAML authentication** decisions via server side JavaScript on letting the user in the application, choosing a source group, choosing an attribute to be logged into the statistics. These, as well as other settings are grouped in the *ProxyLoginModuleSAML.xml* configuration file of the SAML login module.

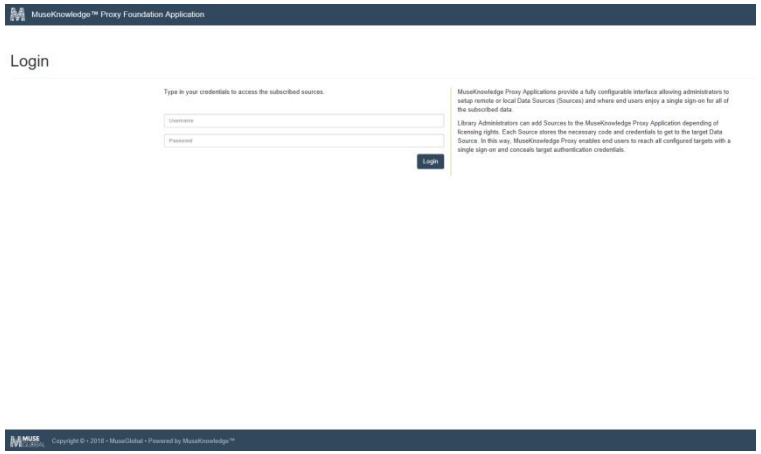
MUSEKNOWLEDGE™ PROXY APPLICATIONS

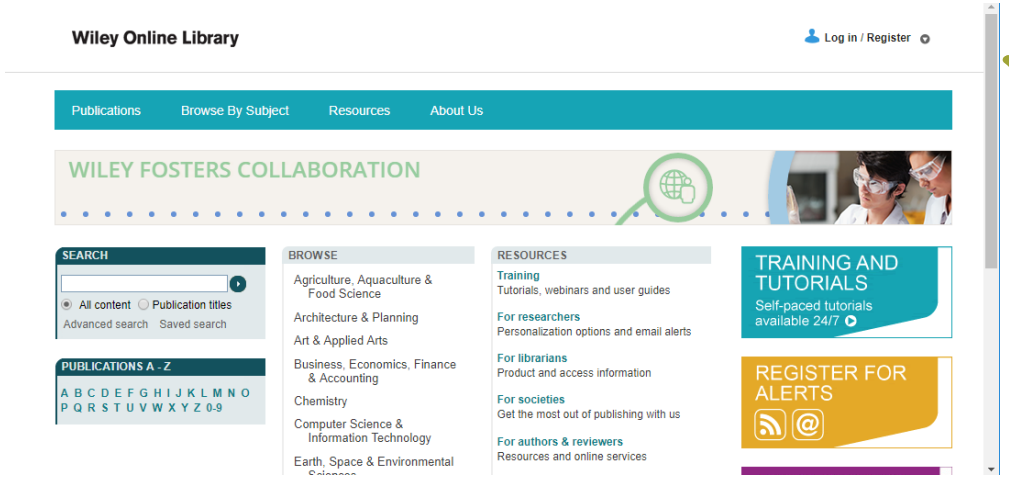


MuseKnowledge™ Proxy Applications are web interfaces providing end-users grouped access to various resources from Internet or Intranet.

- The authentication is made via configurable authentication login modules, allowing various authentication types:
  - User/ Password, IP, LDAP, FTP, IMAP, SQL, Referer, HMAC, SAML, SSO or any combination
- Multiple Authentication Groups can be defined in order to allow end-users to authenticate differently based on their location
- 2 default templates are available:
  - MuseProxyFoundation
  - Anonymous

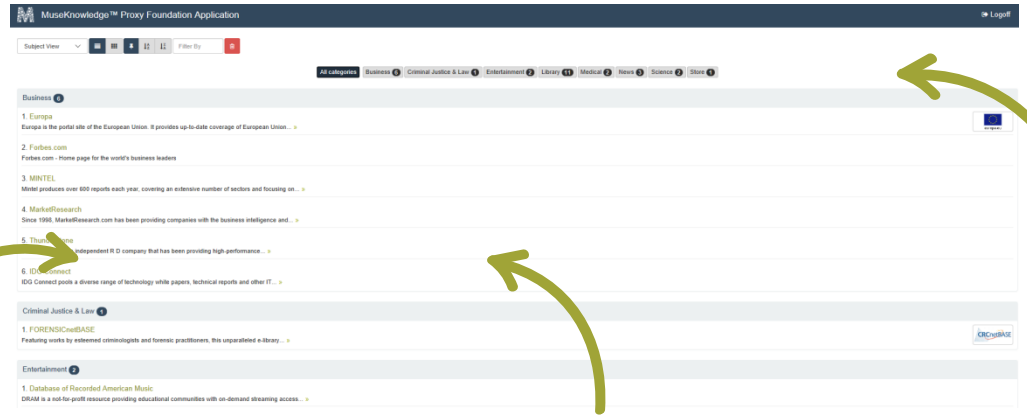
MUSEKNOWLEDGE™ PROXY APPLICATION - FOUNDATION





Rewritten content

Enter access details to login into the MuseKnowledge™ Proxy Application

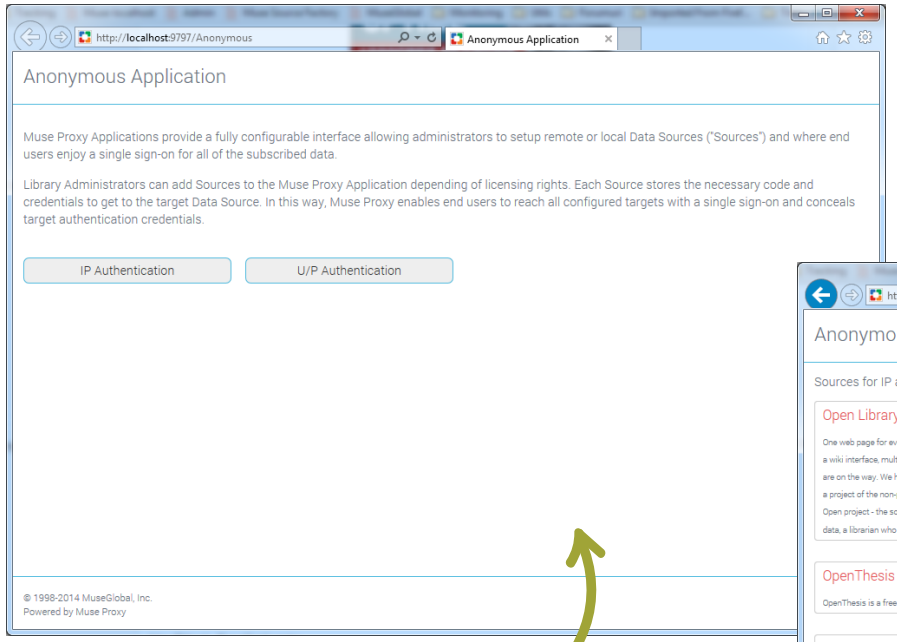


Filter, Sort, Groups, A to Z, Page display options

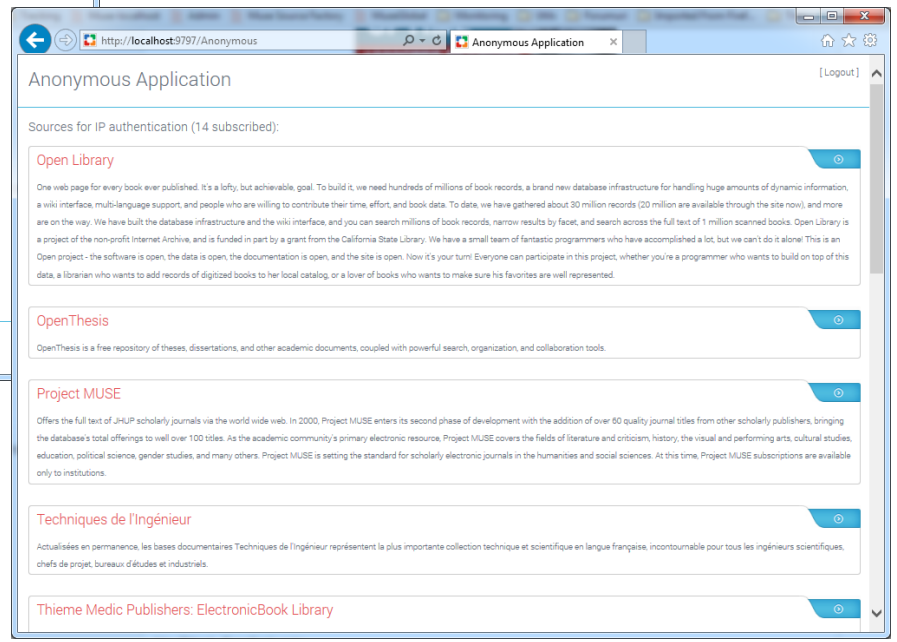
Click on the link and navigate to the rewritten content

List of subscribed Sources

MUSEKNOWLEDGE™ PROXY APPLICATION - ANONYMOUS



List of Sources in a light Application interface



Two Authentication Groups available, each having different Sources

MUSEKNOWLEDGE™ PROXY ADMINISTRATOR CONSOLE FEATURES

Run-time configuration of:

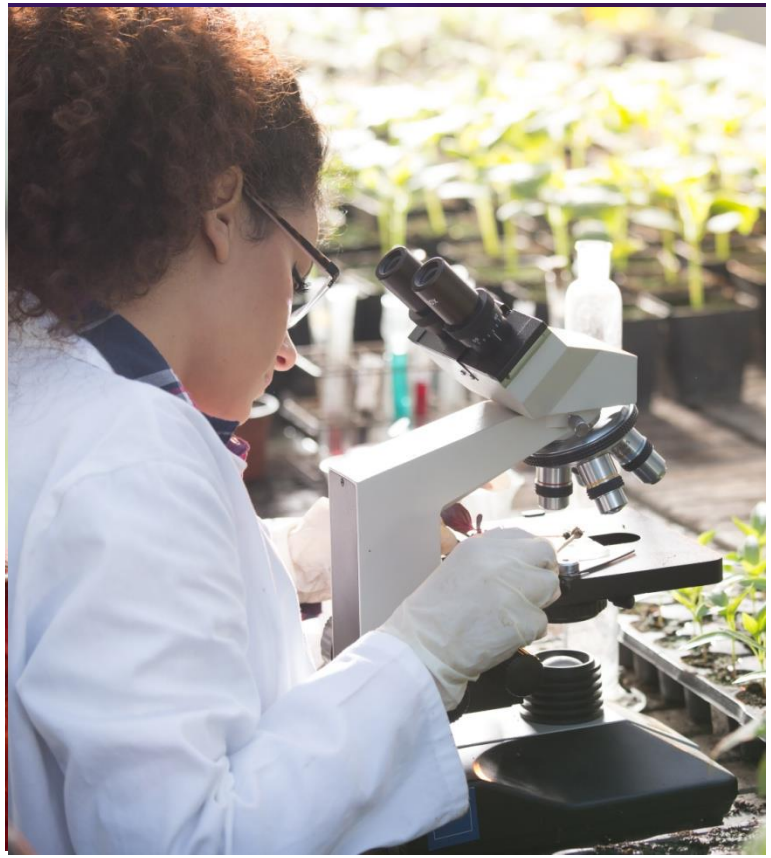
- Patterns for the server IP(s) on which MuseKnowledge™ Proxy must listen
- Administrative Access Rules
- Administrative Passwords
- The list of Administrative Login Modules executed to authenticate each Administrative Web Context and the regular Proxy requests
- Java Policy Rules
- Access details to Global InfoBase, used for downloading the Muse Navigation Manager (*mnm.jar*) component
- SAML Authentication
- SSO Authentication

Monitoring

- Connections, Client sessions, TinyURL(s)
- View the Cache Status global statistics
- View the Cache Files for each cache directory

Download log files

MUSEKNOWLEDGE™ PROXY ADMINISTRATOR CONSOLE FEATURES



Utilities:

- Generate Type 1 rewritten links and Tiny URL(s)
- Un-Rewrite a MuseKnowledge™ Proxy Rewritten URL in Type 1 or Type 2 format
- Evaluate Shortcut URL
- Encrypt a password using SHA1, SHA512, SHA256, DES or MD5 algorithms
- Decrypt password
- HMAC URL generator
- Evaluate Regex

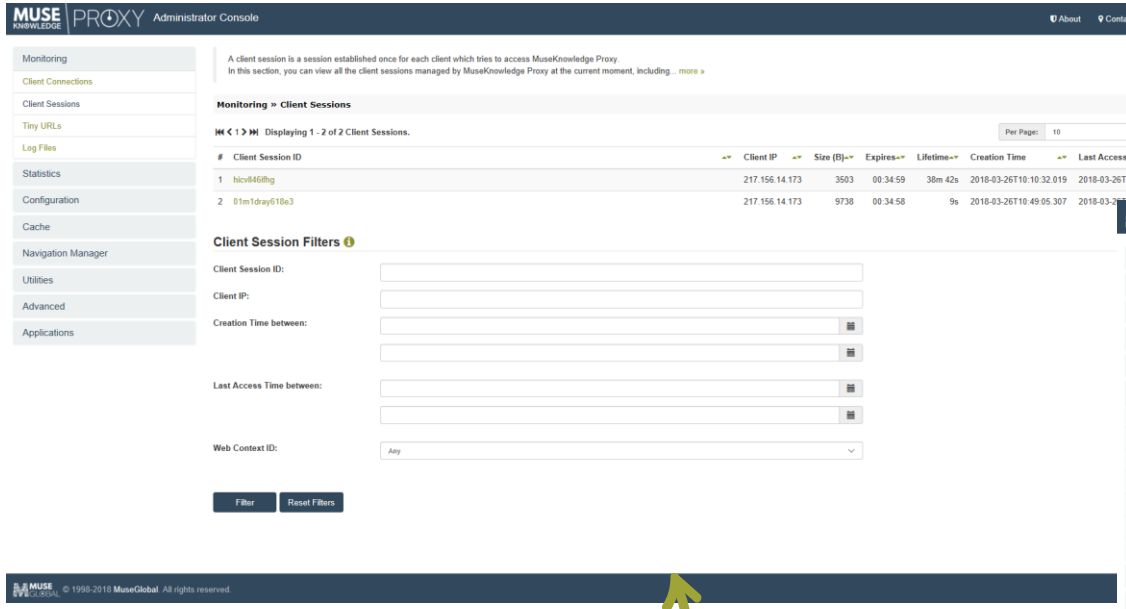
Operations:

- Clean Proxy PAC Cache, Refresh Applications, Refresh Configuration

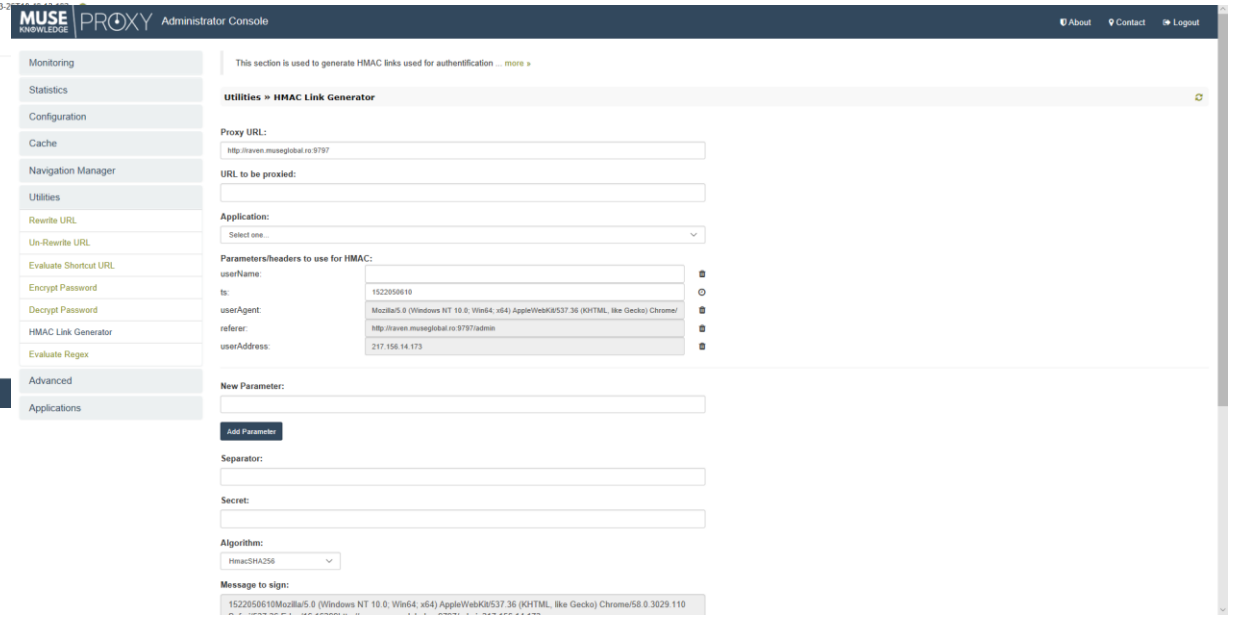
Applications:

- Manage MuseKnowledge™ Proxy Applications and their resources.

MUSEKNOWLEDGE™ PROXY ADMINISTRATOR CONSOLE

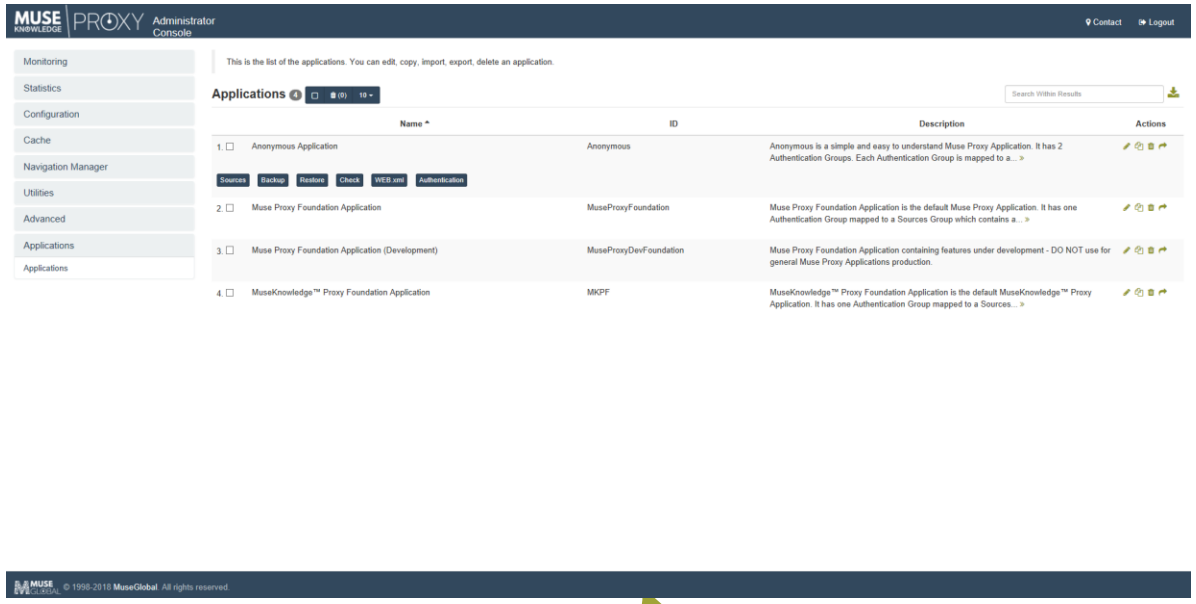


Utilities, HMAC Link Generator



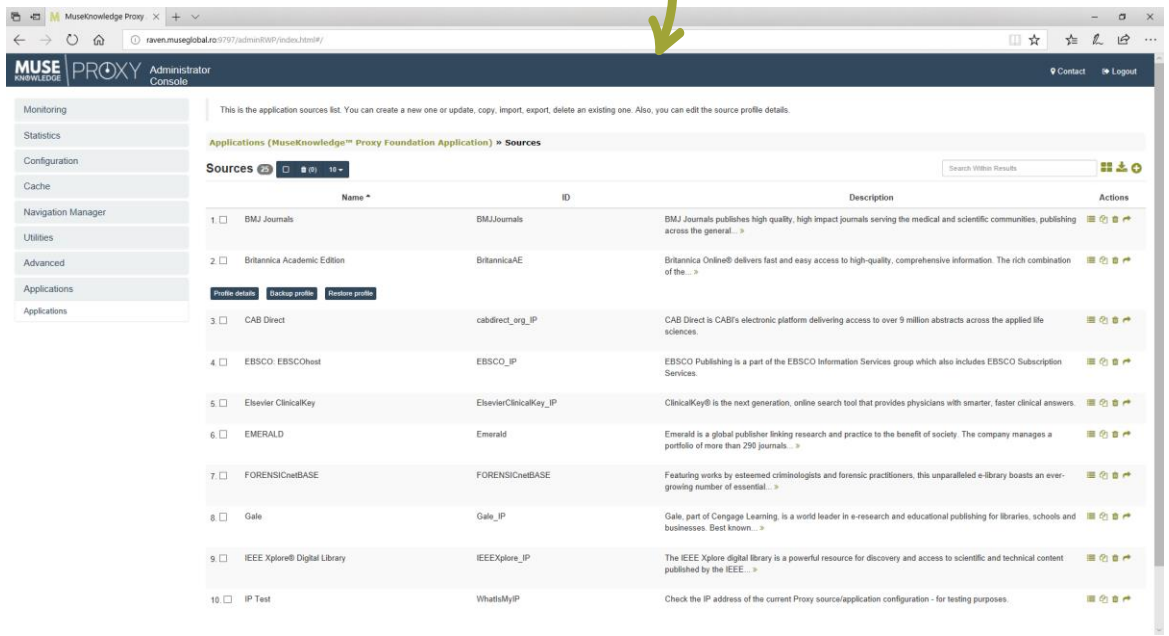
Monitoring, Statistics, Configuration, Cache, Muse Navigation Manager, Utilities, Advanced and Applications sections

MUSEKNOWLEDGE™ PROXY ADMINISTRATOR CONSOLE



MuseKnowledge™ Proxy Applications Management

MuseKnowledge™ Proxy Source Profiles Management



MUSEKNOWLEDGE™ PROXY ADMINISTRATOR CONSOLE

MUSE KNOWLEDGE PROXY Administrator Console

Contact Logout

- Monitoring
- Statistics
- Configuration
- Server IP(s)
- Proxy Configuration
- Administrative Access Rules
- Administrative Passwords
- Jaas Config
- Jaas Policy
- SAML Authentication
- SSO Authentication
- Cache
- Navigation Manager
- Utilities
- Advanced
- Applications

Generates new metadata for a service provider located on raven.museglobal.ro . Output can be used to configure your securityContext-metadata.xml descriptor.

Configuration » SAML Authentication » Metadata administration » Metadata generation

Metadata generation

Entity ID: http://raven.museglobal.ro:9797/

Entity ID is a unique identifier for an identity or service provider. Value is included in the generated metadata. If there are more Muse Proxy Applications intended to be accessed differentiate between the Entity IDs.

Entity base URL: http://raven.museglobal.ro:9797/ssoRWP

Base to generate URLs for this server. For example: https://proxy.example.com/ssoRWP. **The public address** used to access your server **must be used here**. Make sure you and the correct ports if Muse Proxy or the load balancer is configured on ports other than the standard 80 or 443.

Entity alias: MKPF

Alias is an internal mechanism allowing collocating multiple service providers on one server. For Muse Proxy the alias must be the Muse Proxy Application ID.

Enable IDP discovery profile: Yes

Discovery profile enables service provider to determine which identity provider should be used for a particular user. Spring Security SAML contains it's own discovery service wh from.

Custom URL for IDP discovery: Yes

When not set local IDP discovery URL is automatically generated when IDP discovery is enabled.

Custom URL for IDP discovery: No

Custom URL for IDP discovery: apollo (apollo)

Key used for digital signatures of SAML messages. Public key will be included in the metadata.

Encryption key: apollo (apollo)

Key used for digital encryption of SAML messages. Public key will be included in the metadata.

Show Advanced Settings >>

Generate metadata

SAML Authentication, Generate New Service Provider Metadata

SAML Authentication, Add New IDP Metadata Files

MUSE KNOWLEDGE PROXY Administrator Console

Contact Logout

- Monitoring
- Statistics
- Configuration
- Server IP(s)
- Proxy Configuration
- Administrative Access Rules
- Administrative Passwords
- Jaas Config
- Jaas Policy
- SAML Authentication
- SSO Authentication
- Cache
- Navigation Manager
- Utilities
- Advanced
- Applications

This page helps on configuration of new IDP metadata either by providing an URL to the resource where the metadata is extracted from or a local file. Note that the metadata resource can represent an `EntitiesDescriptor` containing more `EntityDescriptor` entries, as in case of a federation.

The SAML component behind requires a Servlet Engine restart and due to the SAML complexity it is hard to have things work from the first try, requiring analysing the log file, `D:/muse/proxy/logs/ext.log`, too. To minimize downtime we provide some first level testing (simulation) so that possible needs of defining a certificate, or wrong URL, or wrong XML file are spotted before real configuration and restart.

Configuration » SAML Authentication » Metadata administration » Add New IDP Metadata files

Add New IDP Metadata files

By URL | By Upload

Provide the URL pointing to the IDP metadata (it can be a federation URL, too). After final configuration, the system will refresh it periodically from that URL, caching it to a disk file, so that, in the event that the metadata may not be pulled from the URL it may be pulled from disk using the last fetched data.

Take metadata from URL:

Timeout in ms to wait for metadata: 20000

Metadata Trust Check: No

Test IDP metadata

JMX FEATURES

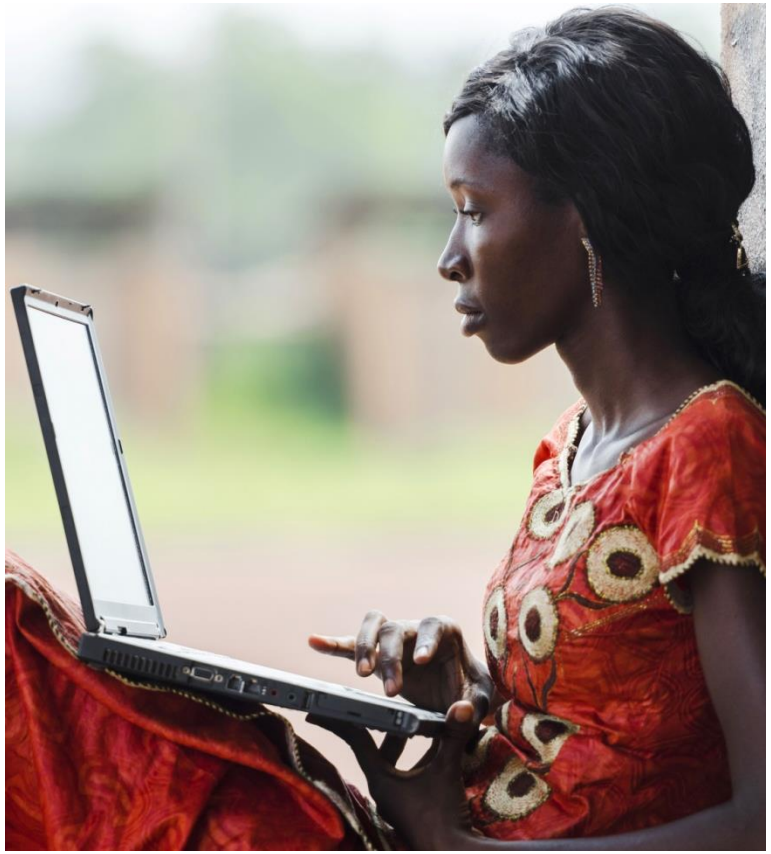
View at run-time:

- **Information regarding the memory** and CPU used by MuseKnowledge™ Proxy
- **Information** regarding the MuseKnowledge™ Proxy threads
- **File Sets mappings** (public, authenticated and private) for each Web Context
- **MIME Mappings** for each Web Context
- **Global proxy configuration** fields and update the editable fields
- **MuseKnowledge™ Proxy Statistics** (traffic statistics and other server statistics) globally and per server IP

Set at run-time:

- **Authentication Timeout** for Proxy Requests and save the configuration to disk
- **Default Authentication Timeout** and Client Session Timeout for the Web Contexts and save the configuration to disk
- **Authentication Timeout** for a specific Web Context and save the configuration to disk
- **Configurable parame**ters for each Web Module and see the value for the read-only parameters
- **Patterns for the server IP(s)** on which MuseKnowledge™ Proxy must listen and save the configuration to disk

MUSEKNOWLEDGE™ PROXY VERSION



MuseKnowledge™ Proxy 4.5 released on October 6th 2017

- **Learning Tools Interoperability® (LTI ®)** – a MuseKnowledge™ Proxy Application or a proxified source can be used as an External Tool within a Learning Management System (LMS) using the LTI® launch requests standard.
- **HTTP headers** from requests and responses can now be processed using new configuration elements within a new or existent filter. Optionally, dynamic processing via scripting is possible.
- **Static resources** within MuseKnowledge™ Proxy Application interfaces can now be served.
- **Special variables** (such as the user ID that is also logged, the Application URL) can be referred by using a new configuration element.
- **Links** generated by MuseKnowledge™ Search Connectors can now point to a MuseKnowledge™ Proxy Application root to cover cases where a higher level of rewriting configuration is necessary.
- A new configuration option is available for specifying the Server header field for the content served directly by MuseKnowledge™ Proxy.

Available for download on the EduLib website here
http://www.edulib.com/products/muse-proxy/download/.

Free 30 Day Trial period for evaluation is offered. Request a Trial License Key by simply filling in the trial form here
http://www.edulib.com/products/muse-proxy/try/.

USAGE SCENARIOS EDUCATION AND LIBRARIES

- **MuseKnowledge™ Proxy offers** convenient access to students and professors.
- **MuseKnowledge™ Proxy isolates** and protects organizational sensitive credentials. MuseKnowledge™ Proxy ensures the decoupling of such sensitive credentials from the normal usage scenarios, keeping the credentials and resource URLs transparent with regard to end-users.
- **MuseKnowledge™ Proxy offers** library patrons access to bibliographic databases. Library patrons at home or elsewhere can log in through their library's MuseKnowledge™ Proxy server and gain access to bibliographic databases to which their library subscribes either based on IP, user/password or other credentials.
- **MuseKnowledge™ Proxy reduces hardware.** MuseKnowledge™ Proxy Server can run on a machine that has multiple IP(s). Thus, instead of having many physical or virtual machines running with many MuseKnowledge™ Proxy instances, it is enough to have just one, no matter it is physical or virtual. This means saving money for both hardware acquisition and for power consumption.
- **MuseKnowledge™ Proxy offers better network** and subscription change control. The access from the in campus computers to the Content Providers is done many times by authenticating all the IPs used by these computers to the target sites. There are situations when the campuses are changing the Internet provider, thus the entire class(es) of IPs. If all the on-campus access to the Content Providers is put through MuseKnowledge™ Proxy then this offers a fluent control of these changes.

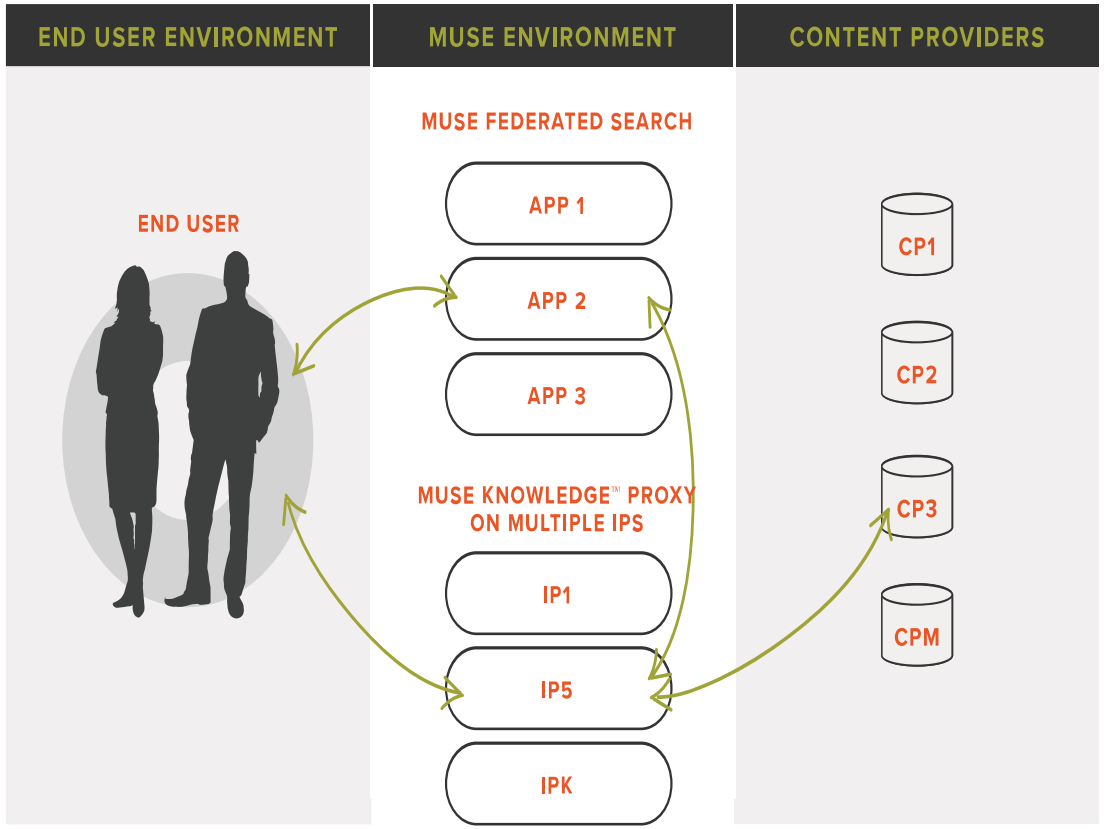
USAGE SCENARIOS BUSINESS AND ENTERPRISE

- **MuseKnowledge™ Proxy simplifies external access** to internal web resources. Instead of using a VPN which requires additional software or hardware, by using Muse Knowledge™ Proxy the external access becomes straight forward even for mobile devices. Issue Tracking Systems, Help Desk Systems, CMS Systems, CRM Systems, ERP Systems, Internal Demonstration Systems, could selectively be grouped under one or more MuseKnowledge™ Proxy Application(s).
- **MuseKnowledge™ Proxy offers company accounts protection.** Simplified administration of the user groups authorized to access online company subscribed accounts, without the need to hand on company credentials for accessing important protected resources constitutes sensitive data and at the same time are a burden to maintain by each employee.
- **MuseKnowledge™ Proxy adds extra SSL protection.** Muse Knowledge™ Proxy can be used to encrypt the communication between the client and the proxy server using HTTPS even when loading non-SSL sites. MuseKnowledge™ Proxy only requires a single SSL certificate, because you will always access its host/domain, all the resource URLs being translated to point back to that.
- **MuseKnowledge™ Proxy offers strict access to Internet.** Enforce strict rules or access to web sites outside your Intranet. MuseKnowledge™ Proxy will then be the only gateway to the permitted resources via a configurable MuseKnowledge™ Proxy Application serving as index to those resources.

USAGE SCENARIOS SOFTWARE INTEGRATION

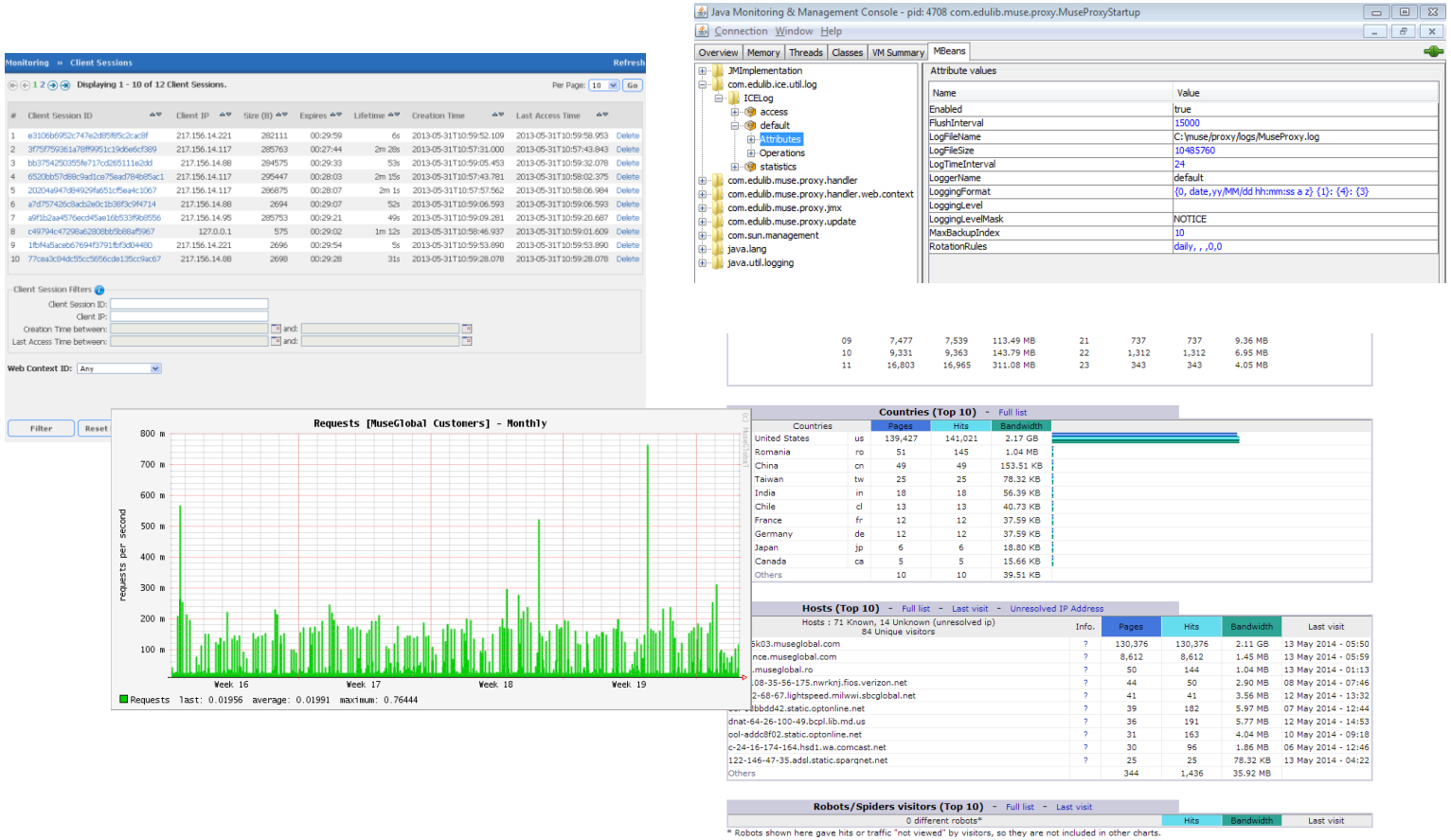
- **MuseKnowledge™ Proxy replicates web session and context.** If you need to transfer and use a web session from a server-side application to a distant front-end browser or a different application, then your Software can interact with MuseKnowledge™ Proxy by using session authorization elements such as cookies, referrer, HTTP authorization, to migrate web sessions and contexts from servers to clients or other servers. Examples: Federated Search Engines, Discovery Services, Crawling, Harvesting or ETL processes.
- **MuseKnowledge™ Proxy can translate** even POST or long GET requests. If the server-side handles long URLs which have more than 2047 characters then these cannot be navigated by some browsers as they are truncated. Using the Tiny URL feature, such long URL can be transformed dynamically to shorter ones.
- **MuseKnowledge™ Proxy offers distinct domains integration.** In case you need two or more distant web sites with complex JavaScript processing to be placed under the same domain use MuseKnowledge™ Proxy as a reverse URL rewriting proxy by accessing the distant site through a MuseKnowledge™ Proxy located in the first domain.

MUSEKNOWLEDGE™ PROXY WITH MUSEKNOLEDGE™ FEDERATED SEARCH



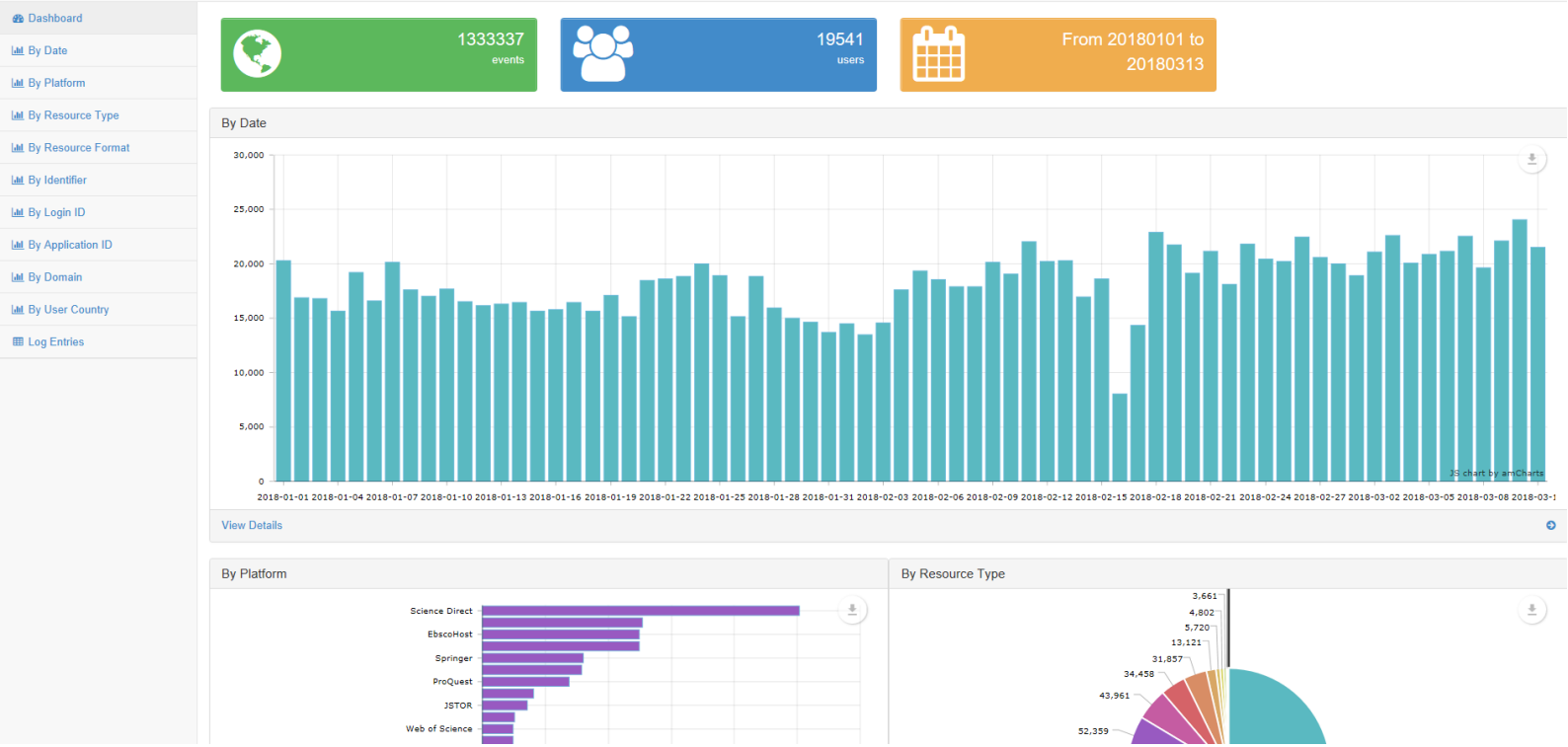
- **End user logins** into Muse Search Application 2 and begins a search
- **The search passes through** the authenticated and configured IP – IP5
- **Information is extracted** and the processing starts
- **MuseKnowledge™ Records** are created and stored in temporarily workroom including cookies and session IDs
- **MuseKnowledge™ Proxy is queried** for services and URLs are matched against configured patterns and rewritten
- **Tiny URLs are created** and stored in the Muse Knowledge™ Proxy session
- **MuseKnowledge™ Application** displays the records to the End user
- **End user clicks** on a rewritten record link or Tiny URL to access full content
- **The MuseKnowledge™ Proxy connects** to Content Provider 3 via IP5 to get the full content page; the initial search connection is recreated due to the cookies and session IDs
- **The MuseKnowledge™ Proxy connects** to Content Provider 3 via IP5

MUSEKNOWLEDGE™ PROXY MONITORING



- Real time monitoring with JMX
- RRD graphs
- AWStats like statistics for Muse Knowledge™ Proxy Access log files
- MuseKnowledge™ Proxy Administration Console

MUSEKNOWLEDGE™ PROXY STATISTICS USE CASE



Needs:

- **Provide usage statistics** per publisher, downloads (full text PDF/HTML/EPUB, etc.), journals, books;
- **Provide visual charts, reports;**
- **COUNTER** Compliant Statistics https://www.projectcounter.org/

Use case ezPAARSE and ezVIS

- **Analyze** MuseKnowledge™ Proxy access log files with ezPAARSE to generate the COUNTER statistics;
- **Visualize** the COUNTER statistics with ezVIS.

REFERENCES

- Muse Proxy.pdf
- Muse Proxy Advanced Configuration.pdf
- Muse Proxy Administrator Console.pdf
- "Muse Knowledge Proxy Administration Console" presentation
- "Muse Knowledge Proxy and OAuth Authentication" presentation
- "Muse Knowledge Proxy and SAML Authentication" presentation
- "Muse Knowledge Proxy Applications" presentation
- "Muse Knowledge Proxy Integration" presentation
- "Muse Knowledge Proxy Source Profiling" presentation

MUSE KNOWLEDGE | PROXY

SEAMLESS AND SECURE REMOTE ACCESS TO RESOURCES