

SSO Security Context

SSO Security Context plug-in for IBM Content Analytics with Enterprise Search



Highlights

Automatically generated security context profiles

No need to supply credentials in the „My Profile“ dialog

Include in the search application

To extend the functionality of *IBM Content Analytics with Enterprise Search* IBM offers the *SSO Security Context* plug-in.

SSO Security Context

With this plug-in it is possible to automatically generate security context profiles. The *SSO Security Context* plug-in can be used to automatically update the *IBM Content Analytics / IBM OmniFind* security profiles of a user with his group membership in a directory service.

After implementation of *SSO Security Context* the users of the search application do not need to enter their user credentials on the “My Profiles” dialog any more to search the secured documents coming from the supported data source.

This plug-in can be easily integrated into the standard search application by customization. There is no need to modify source code of the search application.

Supported Directory Services

- Microsoft Active Directory 2003 and 2008
- Novell eDirectory
- Domino LDAP

Support for other directory services is possible and can be supplied on a per-effort base. Alternatively the groups for a given user can also be retrieved from:

- IBM WebSphere Application Server user repository (when running inside IBM WebSphere Application Server context)
- A database accessible using JDBC
- IBM WebSphere Portal user repository



Supported Secured Sources

The current version of the service offering supports automatic generation of IMC profiles for these secured sources:

- Windows File System Crawler
- Windows Agent Crawler
- Microsoft SharePoint (requires OF 9.1 FP 4)
- IBM FileNet P8 3.5 using IBM Content Integrator
- IBM Lotus Notes using Domino LDAP
- IBM WebSphere Portal using Seedlist Crawler
- IBM Quickr for Portal using Seedlist Crawler

Support for other secured sources is possible and can be supplied on a per-effort base.

Technical Information

The directory services must be accessible via LDAP. The module needs a bind user with the appropriate access rights to issue LDAP queries. The Plug-in supports *IBM OmniFind 9.1*, *IBM Content Analytics 2.2* and *IBM Content Analytics with Enterprise Search 3.0*.

SSO Security Context is fully available only for the search application; installation for the text miner application must be evaluated separately. The module is designed to work as a part of the search application, it requires the *OminFind/ICA* SI-API to access the backend server.

The automatically generated IMC profiles can not be used for post-filtering of the search results. Only pre-filtering (based on the security information in the index) is possible. Configuration of secured search itself for the respective data source is not part of this service offering – secured search must be configured already.

Not part of this Plug-in is a single sign on the web application. This must be configured using the underlying application server. This is not a prerequisite to use the *SSO Security context* module.



IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Homepage is reachable below:
ibm.com

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Other company, product or service names may be trademarks or servicemarks of others.

© Copyright IBM Corporation 2014
