OpenInsight 10

OpenInsight Single Sign-On (SSO)

Version 2.0

REVELATION
SOFTWARE
A Division of Revelation Technologies, Inc.

COPYRIGHT NOTICE

SOFTWARE COPYRIGHT NOTICE

TRADEMARK NOTICE

Part No. 217-965

Printed in the United States of America.

Table of Contents

Section I: OpenInsight Single Sign-On (SSO)

OpenInsight Single Sign-On (SSO) allows OpenInsight users and system administrators to simplify their OI security and administrative tasks. By configuring SSO, OpenInsight users can be authenticated via traditional OpenInsight methods, via Windows security, or via a combination of both.

To enable SSO, administrators must create or modify a record in the SYSENV table named CFG_LOGIN, or an application-specific record named CFG_LOGIN*<appname> (ie, CFG_LOGIN*EXAMPLES) to configure SSO for the specific application. The layout of the CFG_LOGIN and CFG_LOGIN*<appname> records is:

ID: CFG_LOGIN (global) or CFG_LOGIN*<appname> (for a specific application)
1. SSO flag
2. Normal groups] (for SSO flag = 2 only)
3. Admin groups] (for SSO flag = 2 only)
4. System Admin groups] (for SSO flag = 2 only)
5. Validation Mode (for SSO flag = 2 only)

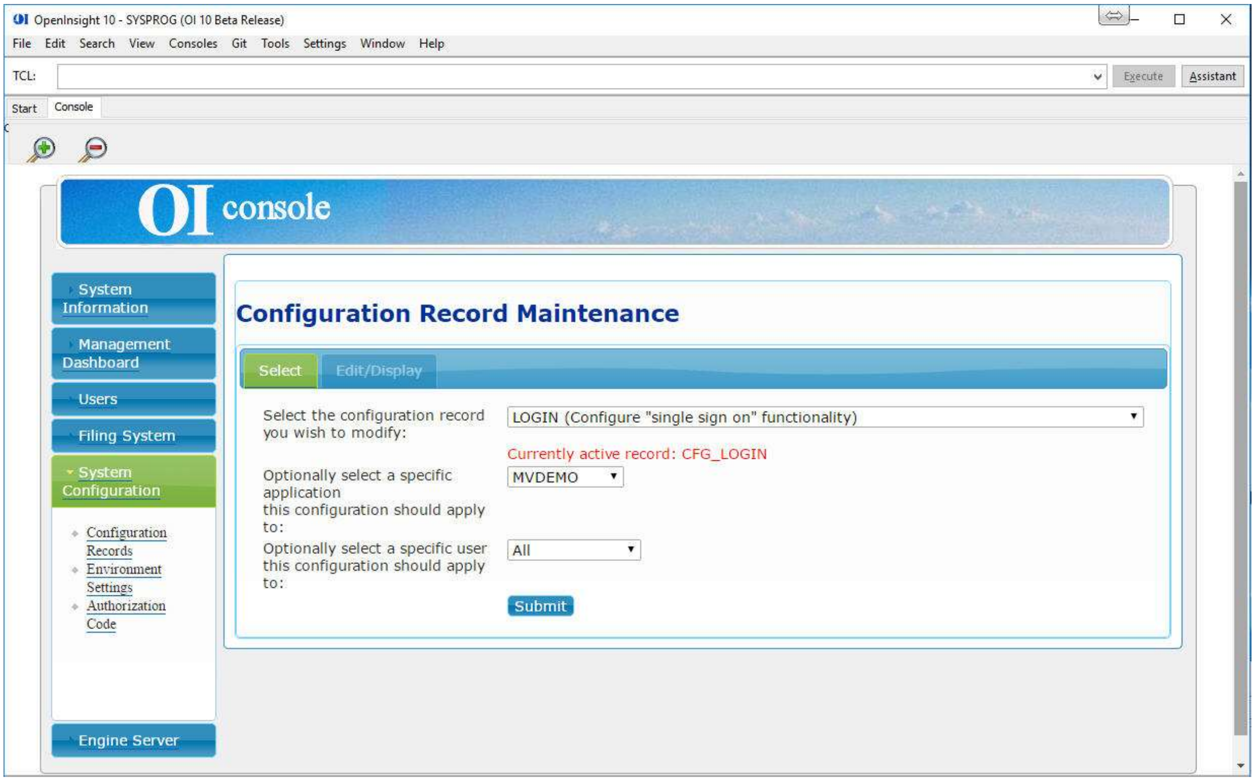
If the SSO flag is set to 0 in the CFG_LOGIN*<appname> record, or in the CFG_LOGIN record if no CFG_LOGIN*<appname> record is found (or if neither CFG_LOGIN*<appname> nor CFG_LOGIN record is found), OpenInsight operates in "legacy" mode, continuing to use its existing (legacy) methods for authentication and validation. Usernames and passwords, either entered in response to OpenInsight prompts or passed via command-line parameters, will be checked against OI system records, and the user will either be admitted or denied admittance depending on the entered information.

If the SSO flag is set to 1 in the CFG_LOGIN*<appname> record, or in CFG_LOGIN if no CFG_LOGIN*<appname> record is found, OpenInsight operates in "hybrid SSO" mode. No username or password is required for entry (either systemwide if CFG_LOGIN record is used, or in the particular application if CFG_LOGIN*<appname> is used), so long as the username (as logged into Windows) is found in the OpenInsight system records. Administrators must, therefore, continue to create OpenInsight user entries for all valid OpenInsight users, defining which permissions level (normal, admin, or system admin) they should be granted. Hybrid SSO operation is provided mostly as a convenience to users, who need not specify their username and password to enter OpenInsight. If the OpenInsight user is not set as an administrator then an Application Entry Point must be set for the application.

If the SSO flag is set to 2 in the CFG_LOGIN*<appname> record, or in CFG_LOGIN if no CFG_LOGIN*<appname> record is found, OpenInsight operates in "strict SSO" mode. No username or password is required for entry (either systemwide if CFG_LOGIN record is used, or in the particular application if CFG_LOGIN*<appname> is used), so long as the user (as logged into Windows) belongs to one of the Windows groups defined in fields 2, 3, or 4. In strict SSO mode, the administrator is not required to enter the user into OpenInsight's system records; they need only ensure that the Windows user is a member of the appropriate group. If the Windows user is a member of any of the groups listed in field 4 (@VM delimited), they are admitted into OpenInsight with System Administrator privileges; if the user is a member of any of the groups listed in field 3 (@VM delimited), they are admitted with Administrator privileges; if the user is a member of any of the groups listed in field 2 (@VM delimited), they are admitted with normal privileges. Note that a user will be admitted with the highest privilege that can be found in any of the groups he or she is a member of. Also note that if the user _does_ have an entry in the OI legacy system records, they will be admitted with the privileges found in the OI system (similar to "hybrid SSO" mode).

If the SSO flag is set to 2, field 5 controls how the group information is obtained. If set to 0 (the default), then OpenInsight will communicate with the local LDAP server on the network (such as the Active Directory server) to get group information. If set to 1, then OpenInsight will first communicate with the LDAP server if possible, and then query the local Windows system for the local group information as well. If set to -1, then OpenInsight will only query the local Windows system for the local groups. Note that operating in mode “0” requires an LDAP server on the network.

When operating in strict SSO mode, OpenInsight provides a "legacy override" function; when logging in to the SYSPROG application, if the user is NOT a member of any of the specified groups, they will be prompted for their username and password (as though CFG_LOGIN was set to legacy mode). This provides for the possibility that the user groups have been incorrectly specified, for example, preventing the system from becoming inoperable.



Configuration Record Maintenance

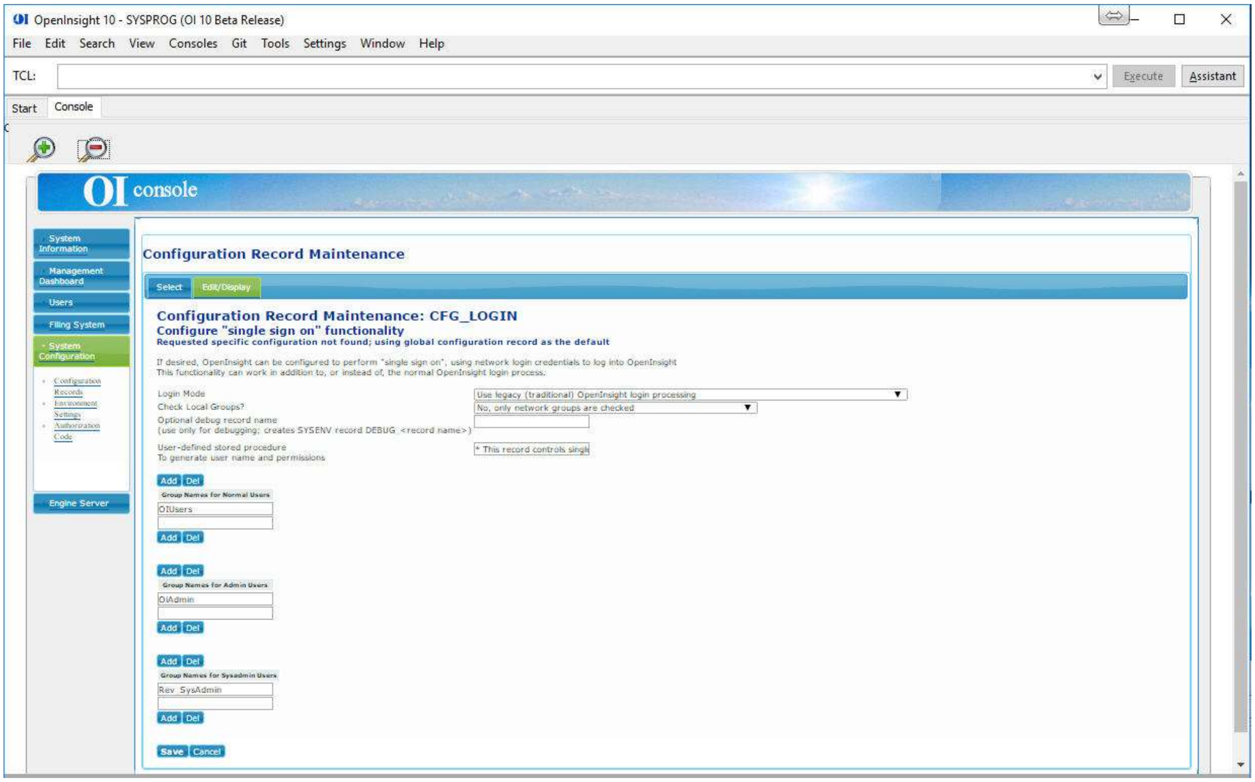
Select the configuration record you wish to modify: LOGIN (Configure "single sign on" functionality)

Currently active record: CFG_LOGIN

Optionally select a specific application this configuration should apply to: MVDEMO

Optionally select a specific user this configuration should apply to: All

From the OpenInsight 10 IDE, go to Consoles, Management Console. Log into the Management Console and go to System Configuration, Configuration Records. Choose the LOGIN configuration record and select the application you want to apply Single Sign On to.



Configuration Record Maintenance

Configuration Record Maintenance: CFG_LOGIN

Configure "single sign on" functionality

Requested specific configuration not found; using global configuration record as the default

If desired, OpenInsight can be configured to perform "single sign on", using network login credentials to log into OpenInsight
This functionality can work in addition to, or instead of, the normal OpenInsight login process.

Login Mode	Use legacy (traditional) OpenInsight login processing ▼
Check Local Groups?	No, only network groups are checked ▼
Optional debug record name (use only for debugging; creates SYSENV record DEBUG_<record name>)	
User-defined stored procedure To generate user name and permissions	* This record controls single

Group Names for Normal Users: OIUsers

Group Names for Admin Users: OiAdmin

Group Names for Sysadmin Users: Rev_SysAdmin

From this form you can manage the SYSEN CFG_LOGIN*APPLICATION record for Single Sign On options.

Section II: Examples

ID: CFG_LOGIN
1. 0

The system operates in full legacy mode, similar to all prior versions of OpenInsight

ID: CFG_LOGIN
1. 0

ID: CFG_LOGIN*EXAMPLES
1. 1

The system operates in legacy mode for all applications other than EXAMPLES. When logging into the EXAMPLES applications, users need not specify their username and password; however, the username (as logged in to Windows) must exist in the OI system tables for the Examples application.

ID: CFG_LOGIN
1. 2
2. win_users]win_remote
3. localadmin]power_users
4. admin

The system operates in strict SSO mode (with the exception of the legacy override). Users who wish to access the system must belong to the "admin" group (in which case they are granted system administrator privileges), "localadmin" or "power_users" group (in which case they are granted administrator privileges), or "win_users" or "win_remote" group (in which case they are granted normal user privileges). The information as to which groups are defined will be obtained from the LDAP server on the network.

ID: CFG_LOGIN
1. 2
2. win_users]win_remote
3. localadmin]power_users
4. admin
5. 1

The system operates in strict SSO mode (with the exception of the legacy override). Users who wish to access the system must belong to the "admin" group (in which case they are granted system administrator privileges), "localadmin" or "power_users" group (in which case they are granted administrator privileges), or "win_users" or "win_remote" group (in which case they are granted normal user privileges). The information as to which groups are defined will be obtained from both the LDAP server on the network and the local Windows system.

REVELATION
SOFTWARE

Revelation Software, Inc.
99 Kinderkamack Road Ste 109
Westwood, NJ 07675
U.S.A
Toll Free: 800-262-4747
Phone: 201-594-1422
Fax: 201-722-9815
www.revelation.com

Revelation Software Ltd.
Boundary House
Boston Road
London, W7 2QE
U.K.
Phone: +44 0 208 912 1000
Fax: +44 0 208 912 1001
info@revsoft.co.uk

BrightIdeas New Zealand
44 Cockle Bay Rd, Howick
Auckland, 2014
New Zealand
Phone: +64 9 534 9134
info@revelationsoftware.asia

Revelation Software is a division of Revelation Technologies, Inc.

Part No. 217-965