

SSO for Opmantek Applications

- [Overview](#)
- [Requirements](#)
- [Configuration](#)
- [Using Patch Config for SSO Configuration](#)
 - [Check the Current Configuration](#)
 - [Configure SSO/Auth options](#)

Overview

All Opmantek applications releases since late 2015 have included a simple form of cross-server [Single-Sign-On](#) (which is not enabled by default). This page describes the configuration and operational characteristics of this SSO setup.

Requirements

1. On every server that should be subject to SSO, at least one of your (commercial) Opmantek Application releases must be newer than 12 Nov 2015.
As our applications share a common core, the SSO capabilities become available as soon as you upgrade or install *one* sufficiently new product release.
A simple test without checking application version numbers is to look for the property "auth_sso_domain" in `/usr/local/omk/install/opCommon.nmis`;
if it's present (but blank or undef) then your installation is SSO-capable.
2. If any Opmantek Application releases newer than 22 May 2018 are installed on any involved server, then all involved servers require one or more new application releases to be installed.
Our SSO setup cannot interoperate across old and new applications.
3. All servers in question must share a common DNS domain, and all servers must be accessed via their fully qualified DNS names within that domain.
This is because our current SSO setup relies on an HTTP cookie that is shared between nodes in the same domain.
4. SSO is NOT supported when using the IP address to access the server.
5. All servers in question must have at least one shared application secret in their `omkd_secrets` config properties.
Please note that all Opmantek software released after 27 October 2016 set the application secret to a unique new value on installation or upgrade; to enable SSO you have to change the first entry under `omkd_secrets` to the same value on all your nodes. For maximum security we recommend that you configure a single application secret only.
6. If you want the Opmantek [SSO setup to also cover NMIS](#), then you need NMIS version 8.6.3G or 8.6.4G for older Opmantek Applications, or 8.6.5 G and newer for releases newer than 22 May 2018.
 - a. To configure NMIS to share authentication cookies with Opmantek Applications, it is necessary that you change the `nmis conf/Config` configuration item `auth_cookie_flavour` from the default "nmis" to "omk" and set the configuration item `auth_web_key` to the same value as the OMK application's first `omkd_secrets` configuration.

Configuration

To enable SSO you need to edit the configuration file `/usr/local/omk/conf/opCommon.nmis`, set the 'omkd_secrets' to your shared secret, and set the 'auth_sso_domain' property to your desired DNS domain **with an extra leading "."**, like in the example below:

```
%hash = (  
  'authentication' => {  
    # ...other stuff  
    'auth_sso_domain' => '.opmantek.com',  
    # ...lots of other stuff  
  }  
  'omkd' => {  
    'omkd_secrets' => [  
      'theseareNOTtheseecretsyourelookingfor',  
    ],  
  },  
)
```

The configuration in this example instructs the authentication code component to generate an authentication/session cookie that is sharable among all nodes in or under `opmantek.com`: the SSO domain property instructs the browser to submit this cookie when accessing a node within the domain, and the application secret ensures that all nodes can decode the cookie.

After setting this up you need to restart the Opmantek Daemon with `sudo service omkd restart`. Under certain circumstances It may also be required to delete all your browser cookies when switching from per-node sign-on to SSO.

Please note:

- Setting up SSO has to be done at least one of your involved servers, not necessarily all of them.
The first system with SSO on that you log in to will create a session cookie for subsequent server accesses, and as long as all your nodes share the same application secret, the SSO session cookie will be accepted by them.

- Our SSO setup with a shared domain strictly requires that your shared domain has at least two DNS name components. Hence, using `test.mydomain.id.au` would work for nodes `a.test.mydomain.id.au`, `an.other.test.mydomain.id.au` and so on. However, attempting to set the SSO domain to `.com` or `.au` will *not* work.
- SSO across Opmantek Applications and servers is not supported by legacy application series (like `opMaps`, `opFlow 2`) or NMIS before 8.6.3G.
- The authentication code component logs SSO-related issues to `log/auth.log`.

Using Patch Config for SSO Configuration

Check the Current Configuration

Check how SSO is currently configured.

```
/usr/local/nmis9/admin/patch_config.pl -r /usr/local/nmis9/conf/Config.nmis auth_cookie_flavour
/usr/local/nmis9/admin/patch_config.pl -r /usr/local/nmis9/conf/Config.nmis auth_sso_domain
/usr/local/nmis9/admin/patch_config.pl -r /usr/local/nmis9/conf/Config.nmis auth_web_key
/usr/local/nmis9/admin/patch_config.pl -r /usr/local/omk/conf/opCommon.json auth_sso_domain
/usr/local/nmis9/admin/patch_config.pl -r /usr/local/omk/conf/opCommon.json omkd_secrets
```

The NMIS `auth_cookie_flavour` should be "omk", the `auth_sso_domain` should match, and so should the `auth_web_key` and `omkd_secrets` (which can have a few secrets, one should match).

Configure SSO/Auth options

A quick way to configure SSO on a server, run this on all the servers in your cluster and you will get SSO working quickly.

```
# Some handy environment variables.
SHARED_KEY=MySecretKeyIMustCreate
# the domain must include a leading "." (period), so if domain is opmantek.net, then .opmantek.net
SSO_DOMAIN=.opmantek.net

cp /usr/local/nmis9/conf/Config.nmis /usr/local/nmis9/conf/Config.nmis.backup1
cp /usr/local/omk/conf/opCommon.json /usr/local/omk/conf/opCommon.json.backup1
/usr/local/nmis9/admin/patch_config.pl /usr/local/nmis9/conf/Config.nmis /authentication/auth_cookie_flavour=omk
/usr/local/nmis9/admin/patch_config.pl /usr/local/nmis9/conf/Config.nmis /authentication
/auth_sso_domain=$SSO_DOMAIN
/usr/local/nmis9/admin/patch_config.pl /usr/local/nmis9/conf/Config.nmis /authentication
/auth_web_key=$SHARED_KEY
/usr/local/nmis9/admin/patch_config.pl /usr/local/omk/conf/opCommon.json /authentication
/auth_sso_domain=$SSO_DOMAIN
/usr/local/nmis9/admin/patch_config.pl /usr/local/omk/conf/opCommon.json /omkd/omkd_secrets[0]=$SHARED_KEY
```