

IBM Content Manager OnDemand Single Sign-On for IBM Content Navigator



6/10/2020

**Rob Russell
Software Engineer - Content Manager OnDemand**

Introduction

This article provides a high level overview of the single sign-on (SSO) implementation for IBM Content Navigator (ICN) and Content Manager OnDemand and what is necessary to implement it. This document is meant to serve as an accompaniment to the standard IBM Content Navigator documentation. Installing and configuring IBM Content Navigator is beyond the intended scope of this document. For detailed installation instructions, you should refer to the online documentation provided by IBM Content Navigator.

What is Single Sign-On?

Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (such as user name and password) to access multiple applications. With IBM Content Navigator, an application server (such as WebSphere or WebLogic) can be configured to use one of many different SSO technologies. For example:

- SAML with Tivoli® Federated Identity Manager
- SPNEGO/Kerberos on Oracle WebLogic Server
- SPNEGO/Kerberos on WebSphere Application Server

Leveraging one of these technologies means a user can log into one of the above services and automatically be granted access to IBM Content Navigator.

For example, with SPNEGO/Kerberos, a user logs into their domain-based PC, establishing their identity on the network. The user then navigates to the IBM Content Navigator Desktop. In this example, the application server first verifies the user's identity based on the information the user provided to logon to their PC. If verified, IBM Content Navigator logs that user in to all repositories defined to the desktop without prompting the user for credentials.

The following link provides information that outlines the supported SSO technologies available to IBM Content Navigator users as of the time of this writing:

[IBM Content Navigator Support for Single Sign-on \(SSO\)](#)

Note: You should always refer to the latest version of IBM Content Navigator documentation for the most current information regarding supported SSO technologies.

Overview

Prior to version 10.1.0.3 of Content Manager OnDemand and version 3.0.4 of IBM Content Navigator, there was no native support for single sign-on. It was, however, still possible to implement SSO. Using a custom Content Manager OnDemand security exit (ARSUSEC) and optionally an IBM Content Navigator

plugin that extended the IBM Content Navigator Class PluginODAuthenticationService, you could still implement single sign-on. While this solution worked very well, it did require custom code.

By leveraging new functionality in V10.1.0.3 and V3.0.4, you can now implement SSO without the need for custom code. The functionality used to implement SSO in FileNet P8 is now officially supported for Content Manager OnDemand. For customers that run both FileNet P8 and Content Manager OnDemand, you can now have seamless single sign-on across multiple disparate repositories in a single IBM Content Navigator Desktop without the need for customization.

Note: To take advantage of this feature, **both** the Content Manager OnDemand server and any server running IBM Content Navigator must have Content Manager OnDemand V10.1.0.3 or later installed.

Preparing your system

The first step in configuring your Content Navigator server for Content Manager OnDemand single sign-on is to ensure all prerequisites are met. This means a minimum of Content Manager OnDemand V10.1.0.3 and a minimum of IBM Content Navigator V3.0.4.

The next step is to configure your application server for one of the supported IBM Content Navigator SSO technologies listed in the IBM Content Navigator SSO configuration roadmap at the link previously provided in this document. Refer to your application server’s website for further configuration instructions.

Once your version prerequisites are met and your application server is properly configured for SSO, you can now either install or redeploy IBM Content Navigator.

The reason it may be necessary to redeploy IBM Content Navigator is due to the fact that, in order for SSO to function properly, you must have selected “Application server authentication” as the IBM Content Navigator authentication type.

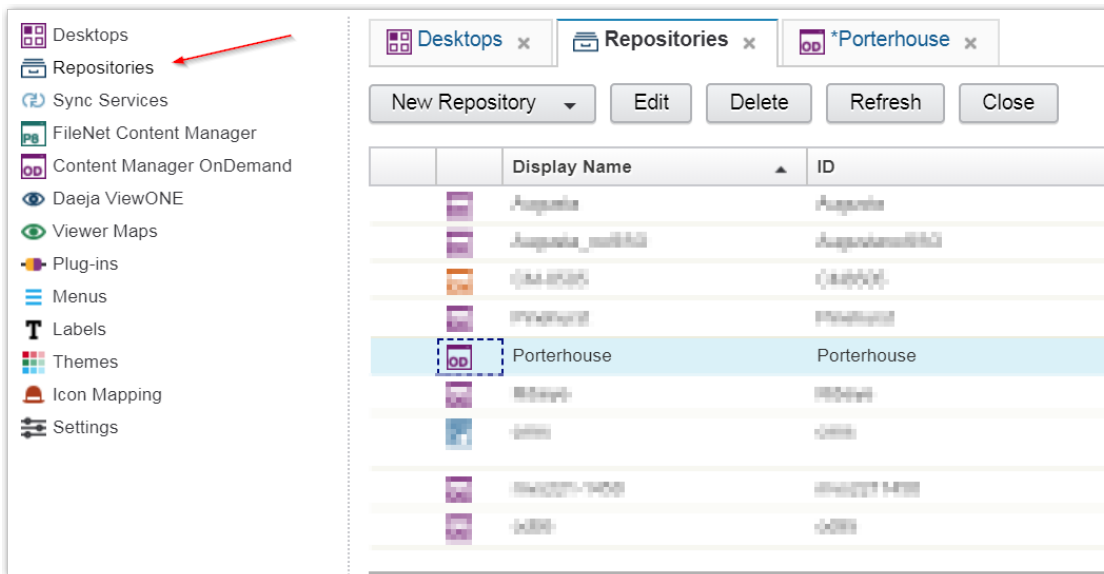
The screenshot shows a configuration window titled "Configure the IBM Content Navigator Web Application". It includes a "Save" button and a "Run Task" button. Below the title, there is a text box with the instruction: "Enter the information that the configuration and deployment tool uses when it creates the IBM Content Navigator web application, such as the name for the application." The configuration fields are as follows:

IBM Content Navigator authentication:?	Application server authentication
IBM Content Navigator configuration directory:?	C:\IBM\ECMClient\config Browse...
IBM Content Navigator schema name:?	
JDBC data source name:?	ECMClientDS
Temporary directory:?	C:\IBM\ECMClient\configure\tmp Browse...

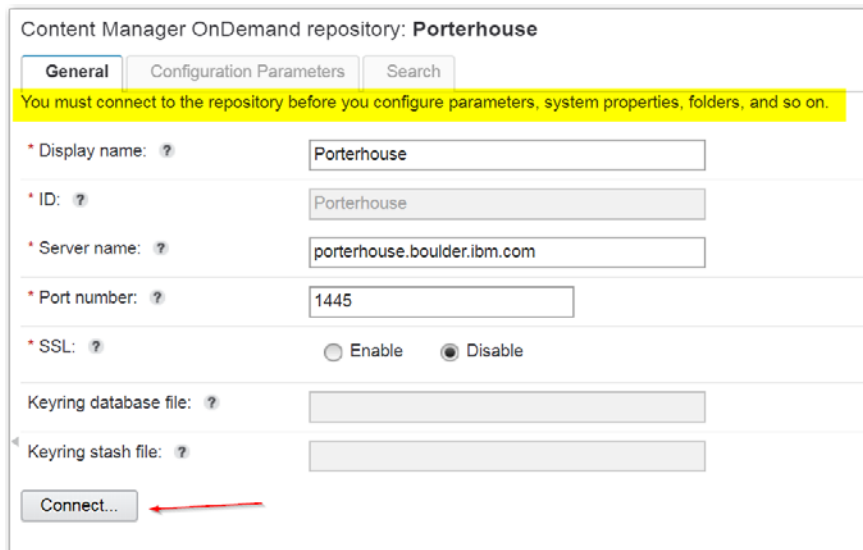
If, during the “Configure the IBM Content Navigator Web Application” phase, you selected any other method of authentication, redeploying is the only option. There is no method to change this in an existing deployment.

Enabling SSO for a Content Manager OnDemand Repository

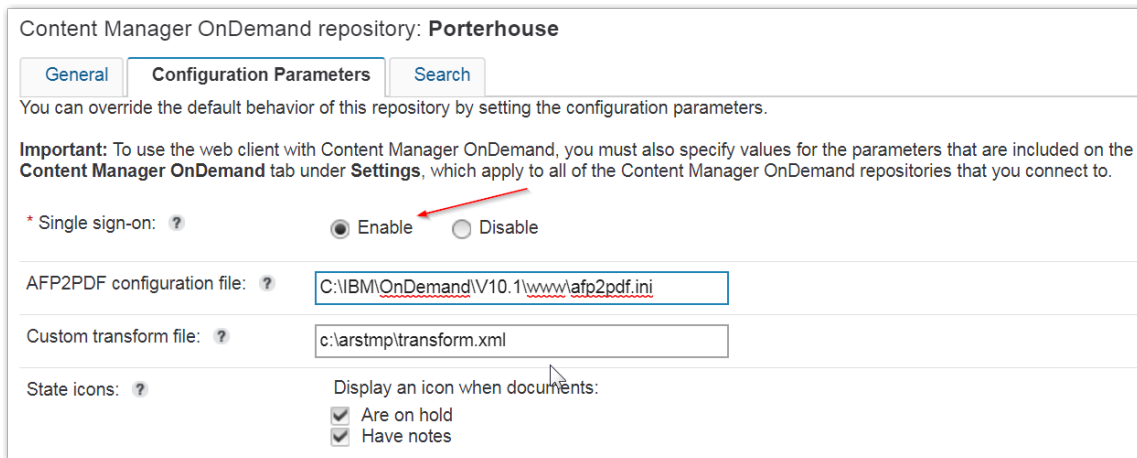
Once IBM Content Navigator is deployed, you can enable SSO for a Content Manager OnDemand repository. Using the IBM Content Navigator admin desktop, navigate to the repositories feature. From here you can either add a new Content Manager OnDemand repository or edit an existing one. In this example, we will edit an existing repository with an ID of Porterhouse:



In order to edit the configuration parameters (where SSO is enabled/disabled), you must first “Connect...” to the repository:



Once connected, navigate to the “Configuration Parameters” tab where you can now enable Single sign-on:



With Single sign-on now enabled, you can select “Save and Close” to exit. It is not necessary to restart the application server for these changes to take effect.

The final step in configuring your IBM Content Navigator system for single sign-on is to add the following new parameter to your ARS.CFG configuration file located on your Content Manager OnDemand server:

```
ARS_TRUSTED_SSO_HOSTS=<IP address of IBM Content Navigator Server>
```

The ARS_TRUSTED_SSO_HOSTS parameter can be a single IP address or a comma-separated list in the case of multiple IBM Content Navigator servers. Only requests from trusted IPs will be allowed to access Content Manager OnDemand by using single sign-on.

If you are unsure of the IP address to add here, the simplest way to get this information is to attempt a login from IBM Content Navigator. This will produce a failed login message in the Content Manager OnDemand System Log. The message will have the following format:

```
2018-06-20 08:42:41.255442 CNADMIN 27003 Warning No 31  
Failed login: porterhouse.steaks.com 168.1.0.4 non-SSL (Windows 64) (ODWEK  
JAVA API) (10.1.0.3)
```

Using the above message as an example, the following would be the correct setting for ARS_TRUSTED_SSO_HOSTS:

```
ARS_TRUSTED_SSO_HOSTS=168.1.0.4
```

With the parameter now added, recycle the ARSSOCKD process and test the access from IBM Content Navigator. Your system should now be configured for single sign-on.

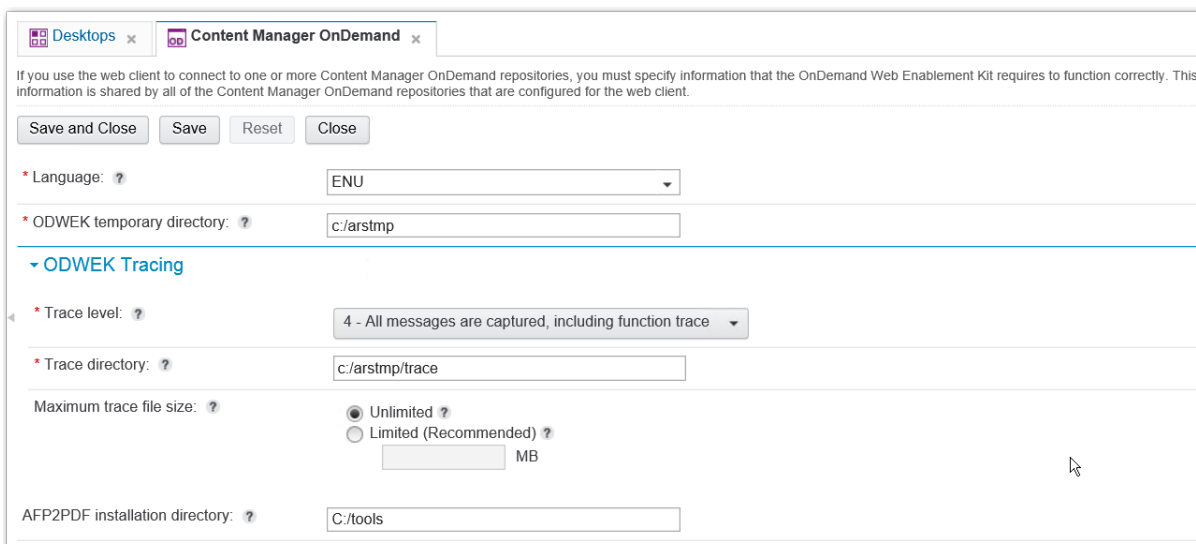
Hints and Tips

The user name that authenticates to your application server must be exactly the same as it is defined to your Content Manager OnDemand server with exception of case. This is true unless you have enabled case sensitive user IDs in Content Manager OnDemand. This, however, is not very common. If a user has authenticated to the application server but is not defined to Content Manager OnDemand, a failed login will occur and the user will be presented with the standard IBM Content Navigator login prompt.

Single sign-on is only available for IBM Content Navigator. For users of the OnDemand Administrator client or the OnDemand Windows desktop client, the standard Content Manager OnDemand login process handles authentication.

Customers who have implemented a custom single sign-on solution using a Content Manager OnDemand security exit program and an IBM Content Navigator plugin will continue to function as before. Native single sign-on will only be invoked if IBM Content Navigator is not using the PluginODAuthenticationService plugin. It may be possible to simply remove your IBM Content Navigator plugin and security exit and leverage the new native single sign-on functionality. You should analyze your custom code to determine if there is functionality that is still required before making this change.

The ODWEK trace file and your application server's log failures will provide a good source of information when troubleshooting single sign-on issues. By default, ODWEK tracing is not enabled. To enable it, navigate to the IBM Content Navigator admin desktop and select the Content Manager OnDemand tab. The following is a typical configuration for a Windows-based application server:



The screenshot shows a configuration window titled "Content Manager OnDemand" with several settings:

- Buttons: Save and Close, Save, Reset, Close
- Language: ENU
- ODWEK temporary directory: c:/arstmp
- Section: ODWEK Tracing
- Trace level: 4 - All messages are captured, including function trace
- Trace directory: c:/arstmp/trace
- Maximum trace file size: Unlimited, Limited (Recommended) MB
- AFP2PDF installation directory: C:/tools

After you have your system functioning properly, you can and should disable tracing. Refer to your application server's documentation for instructions on how to set the various levels of trace it may offer.