

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



9/26/2023

**Rob Russell and Kevin Van Winkle
Content Manager OnDemand Development**

Introduction

This white paper provides an overview of single sign-on (SSO) and delineates the various steps necessary to configure SSO for IBM Content Navigator (ICN) and Content Manager OnDemand. It is intended to be a supplement to the “Planning, installing, and configuring IBM Content Navigator” documentation.

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

By leveraging one of these technologies, a user can log into one of these services and automatically be granted access to IBM Content Navigator.

For example, with SPNEGO/Kerberos, a user logs into their domain-based workstation, 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 workstation. 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 \(SSO\)](#)

Overview

SSO can now be configured by leveraging new functionality in Content Manager OnDemand V10.1.0.3 and IBM Content Navigator V3.0.4. The functionality used to implement SSO in FileNet P8 is now officially supported for Content Manager OnDemand. If you 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.

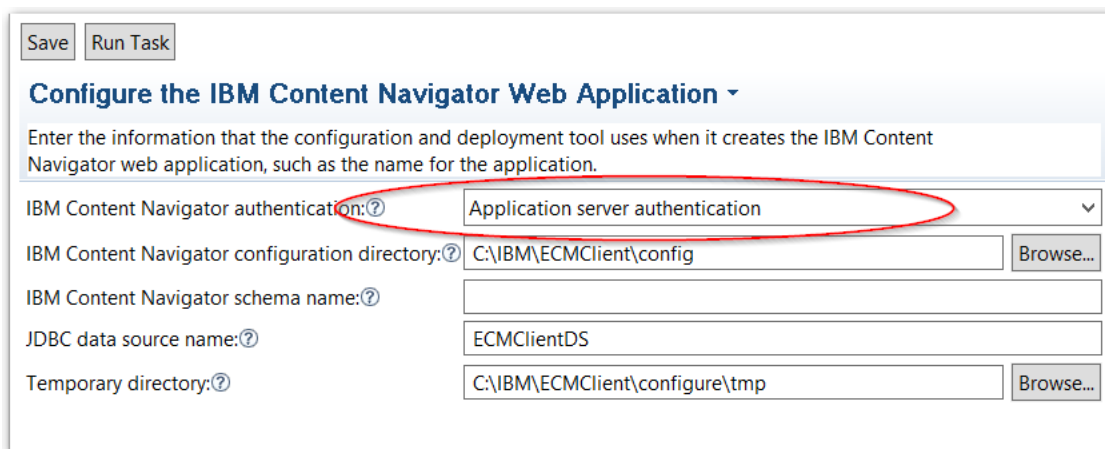
Preparing your system

The first step in configuring your IBM 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 the version prerequisites are met and the application server is properly configured for SSO, installation and deployment of IBM Content Navigator can proceed.

If IBM Content Navigator is already deployed, you will likely need to modify the configuration and redeploy. Using the ICN configuration and deployment tool, navigate to the "Configure the IBM Content Navigator Web Application" step. Verify that the "IBM Content Navigator authentication" was set to "Application server authentication" (see below). If it was not set to this option during initial deployment, set it now and proceed with redeploying ICN with the new setting. Refer to the "Configuring and deploying IBM Content Navigator components" section of the ICN documentation for guidance on deploying the ICN application.

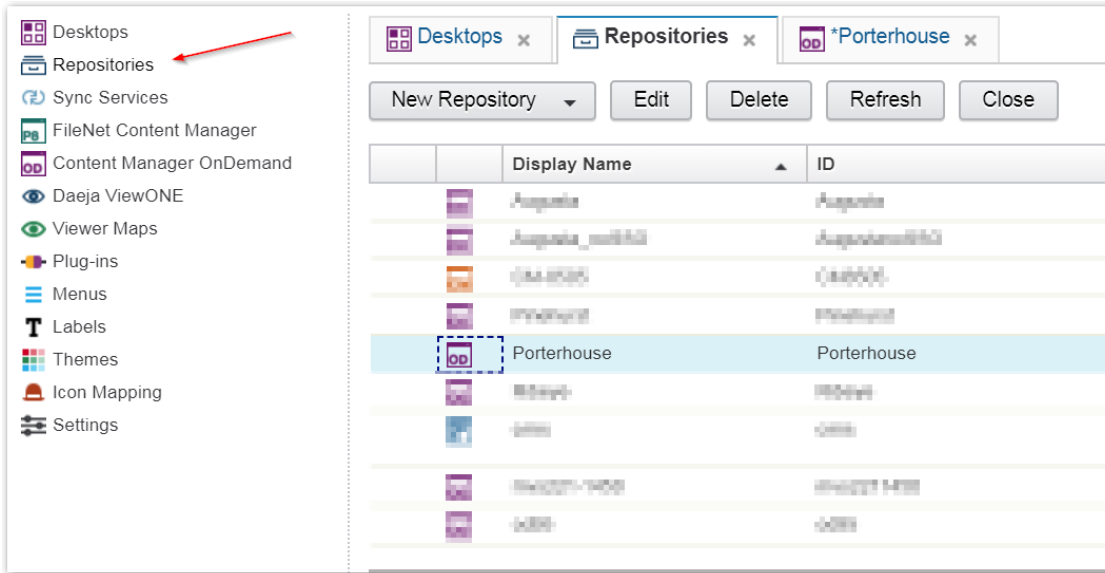


The screenshot shows a configuration window titled "Configure the IBM Content Navigator Web Application". At the top left are "Save" and "Run Task" buttons. Below the title is a text box with the instruction: "Enter the information that the configuration and deployment tool uses when it creates the IBM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

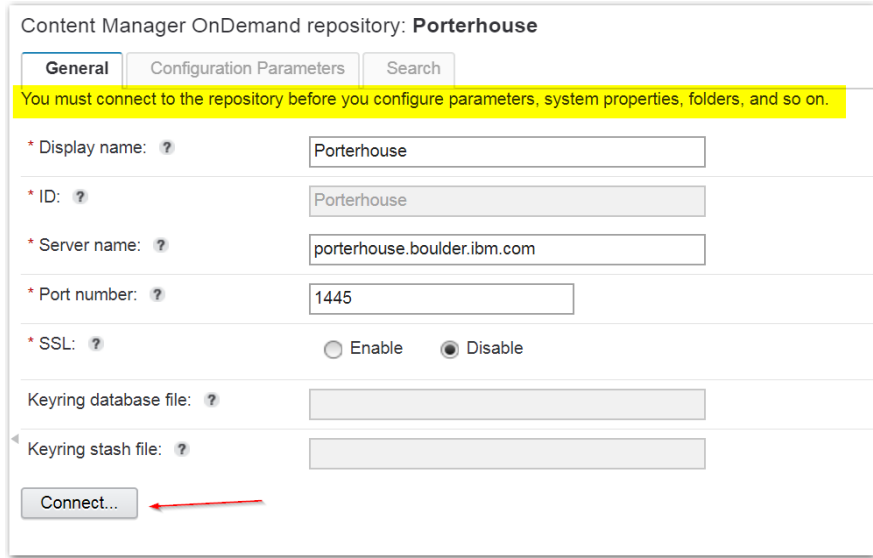
IBM Content Navigator authentication:?	Application server authentication
IBM Content Navigator configuration directory:?	C:\IBM\ECMClient\config <input data-bbox="1149 1276 1230 1304" type="button" value="Browse..."/>
IBM Content Navigator schema name:?	<input type="text"/>
JDBC data source name:?	ECMClientDS
Temporary directory:?	C:\IBM\ECMClient\configure\tmp <input data-bbox="1149 1402 1230 1430" type="button" value="Browse..."/>

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 administration desktop, navigate to the "Repositories" section. From there, 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 click “Connect...” to connect to the repository:



Once connected, navigate to the “Configuration Parameters” tab where you can now click “Enable” for the “Single sign-on” setting as shown in the following example.

Content Manager OnDemand repository: **Porterhouse**

General Configuration Parameters Search

You can override the default behavior of this repository by setting the configuration parameters.

Important: To use the web client with Content Manager OnDemand, you must also specify values for the parameters that are included on the **Content Manager OnDemand** tab under **Settings**, which apply to all of the Content Manager OnDemand repositories that you connect to.

* Single sign-on: ? Enable Disable

AFP2PDF configuration file: ?

Custom transform file: ?

State icons: ? Display an icon when documents:

- Are on hold
- Have notes

Once SSO is enabled, click “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 value 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 specify, 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 to the ARS.CFG file, you need to stop and restart the Content Manager OnDemand server by using the ARSSOCKD process on Content Manager OnDemand for Multiplatforms or z/OS or the End TCP Server (ENDTCPSVR *ONDMMD) and Start TCP Server (STRTCPSVR *ONDMMD) commands on IBM i. Then test the access from IBM Content Navigator. Your system should now be configured for single sign-on.

Hints and Tips

- The user ID that authenticates to your application server must be exactly the same as it is defined to your Content Manager OnDemand server.
- If a user has authenticated to the application server but the user ID is not defined in Content Manager OnDemand, a failed login will occur and the user will be presented with the standard IBM Content Navigator login prompt.
- The case of the user ID is ignored unless you have enabled case-sensitive user IDs in Content Manager OnDemand.
- Single sign-on is only available for IBM Content Navigator. For users of the OnDemand Administrator client or the OnDemand Client on Windows, the standard Content Manager OnDemand login process handles authentication.
- For more information when you are troubleshooting single sign-on issues, refer to the application server logs. It can also be beneficial to refer to the ODWEK trace file. However, ODWEK Tracing is, by default, disabled in ICN. To enable it, navigate to the IBM Content Navigator administration desktop and select the Content Manager OnDemand tab. The following example shows a typical configuration for a Windows-based application server. Note: Make sure to disable ODWEK Tracing once troubleshooting is complete.

The screenshot shows the 'Content Manager OnDemand' administration console. At the top, there are two tabs: 'Desktops' and 'Content Manager OnDemand'. Below the tabs, a message states: 'If you use the web client to connect to one or more Content Manager OnDemand repositories, you must specify information that the OnDemand Web Enablement Kit requires to function correctly. This information is shared by all of the Content Manager OnDemand repositories that are configured for the web client.' Below this message are four buttons: 'Save and Close', 'Save', 'Reset', and 'Close'. The configuration fields are as follows:

- * Language: ?
- * ODWEK temporary directory: ?
- ▼ ODWEK Tracing
 - * Trace level: ?
 - * Trace directory: ?
 - Maximum trace file size: ?
 - Unlimited ?
 - Limited (Recommended) ? MB
- AFP2PDF installation directory: ?