Abstract

This document contains the step-by-step instructions for configuring single sign-on (SSO) for IBM Content Navigator using IBM Security Access Manager (ISAM) on a WebSphere Application Server.

Notes:

- The steps described in this document are for guidance only. The steps required in your environment might be different. Refer to the ISAM and WebSphere Application Server documentation for additional details.
- IBM Security Access Manager used to be named Tivoli Access Manager.

Content

To configure single sign-on integration between IBM Security Access Manager and IBM Content Navigator, perform the following high-level steps:

1. Install and configure the IBM Security Access Manager (ISAM) environment.
2. Configure and deploy IBM Content Navigator with ISAM.
3. Verify your deployment of IBM Content Navigator with ISAM.
4. Complete additional configuration tasks for IBM Content Manager repositories.

Each of these steps is described in more detail in the remainder of this document.

Before you begin

Ensure that you have the appropriate ISAM and ICN software available.

For the latest support information, see the IBM Content Navigator Software Product Compatibility Report. Use the following web site to generate the appropriate report:

http://www.ibm.com/software/reports/compatibility/clarity/index.html

Important: The following applications that might be part of your environment do not support ISAM single sign-on but can work with a Content Navigator installation that is configured with ISAM SSO:

- IBM Content Navigator Task Manager services

  Task Manager supports Basic Authentication only.

  When IBM Content Navigator is configured with ISAM SSO, the SSO configuration must exclude Task Manager from the SSO authentication configuration; that is, do not create an IBM Security Access Manager junction for Task Manager.

The Task Manager URL should contain either the web server or the load balancer host name in highly available environments, or the URL should contain the Content Navigator host name on single server environments, as illustrated in the following examples:

Highly available environments

https://webserverhostname_or_loadbalancername:port/taskManagerWeb/api/v1

Single server environments

https://navigatorhostname:port/taskManagerWeb/api/v1

- IBM Content Navigator Sync Client and Sync Services

  When IBM Content Navigator is configured with ISAM SSO, the SSO configuration must exclude the Sync Services from the SSO authentication configuration; that is, do not create an IBM Security Access Manager junction for Sync.

  The Sync Services public URL and ping page should contain either the web server or load balancer host name in highly available environments, or the URL should contain the navigator host name in single server environments, as illustrated in the following examples:

  Highly available environments:

  https://webserverhostname_or_loadbalancer:port/sync/notify

  https://webserverhostname_or_loadbalancer:port/sync/api/configurations/ping

  Single server environments:

  https://navigatorhostname:port/sync/notify

  https://navigatorhostname:port/sync/api/configurations/ping

Step 1 – Install and configure the IBM Security Access Manager (ISAM) environment

This step consists of the following tasks.

- Task 1: Install and configure the ISAM software
- Task 2: Install and configure Security Access Manager Runtime for Java

Task 1:

Install and configure IBM Security Access Manager following the instructions in the IBM Security Access Manager Installation Guide. For more information, see the IBM Security Access Manager Knowledge Center:
https://www.ibm.com/support/knowledgecenter/SSPREK/welcome.html

You must install the following ISAM components:

- Base system components
- WebSEAL

Task 2:

Install and configure the Security Access Manager Runtime for Java component on the application server where you are planning to install and deploy Content Navigator. Refer to the Security Access Manager Knowledge Center for information on installing the Security Manager Runtime for Java component.

After you install the Security Access Manager Runtime for Java component, configure the component for use within the current Java Runtime Environment (JRE) by running the **pdjrtecfg** command on each application server in the cluster.

Refer to the information on the Security Access Manager Utilities in the IBM Security Access Manager Knowledge Center and the WebSphere Application server Knowledge Center for further details.

Highly Available Environments:

If the nodes in the application server cluster are on different servers, install the Security Access Manager Runtime for Java component on each node in the cluster.

For the Java application server to communicate with the Policy Server and for the Trust Association Interceptor (TAI) to establish trust for a request, run the WebSphere **SvrSslCfg** utility on each Application Server in the cluster with the config action and the cfg_action create option. Running the **SvrSslCfg** utility, creates a **PDPerm.properties** file on each application server.

For more information and details on how to run **SvrSslCfg** utility, see the WebSphere Application server Knowledge Center.

Step 2 - Configure and deploy IBM Content Navigator with ISAM

This step consists of the following tasks:

- Task 1: Configure the ISAM server for IBM Content Navigator.
- Task 2: Configure IBM Content Navigator.

Prerequisites

Install and configure the repositories that will be accessed using IBM Content Navigator; such as, IBM FileNet P8 Content Platform Engine and IBM Content Manager. For more information, see the relevant repository product documentation.

Task 1:

Use the server task **pdadmin** on the WebSEAL server to create two junctions, one for IBM Content Navigator and one for the integrated help system. You can create junctions from the IBM Security Access Manager Console or using the **pdadmin** command line.

Procedures for creating the junctions are provided in this section, but for more information about the syntax and the options that you use to create a junction, see the server task create entry in the WebSEAL Administration section of the Security Access Manager Knowledge Center.

Important: IBM Content Navigator and the integrated help system only support transparent junctions.

Option 1: Create transparent junctions using the IBM Security Access Manager Console:

From the IBM Security Access Manager Console, go to Secure Web Settings > Reverse Proxy > ***Select your Reverse Proxy Instance*** > Manage > Junction Management > New > Standard Junction

1. On the Junction Tab
    - For the Junction Point Name, enter: /navigator
    - Check the Create Transparent Path Junction box
    - For the Junction Type, select TCP
2. On the Servers Tab
    - Click New.
    - In the Hostname field, enter the host name of your IBM Content Navigator server.

      High Availability Environments: Use the web server host name.
    - For the TCP port, enter the port number that IBM Content Navigator will be running on. For example, the default values are 9080 for a single server deployment, and 80 for a cluster deployment.
    - Click Save.
3. On the Identity Tab
    - For the HTTP Basic Authentication Header, select Supply.
    - For the HTTP Header Identity Information, check IV-USER, IV-USER-L, and IV-CREDS

- For the HTTP Header Encoding, select UTF-8 URI Encoded

When you are finished configuring the junction, click **Save**.

To create the second junction for the integrated help system junction, repeat the steps, but use **/wcdocs** as the junction name.

The new junction names should appear in the table under **Junction Point Name**. To verify that the junctions are correctly configured, complete the following steps for each junction:

1. Select the new junction
2. Click **Edit**.
3. Click on the **Servers** tab
4. Verify that the Server state value is **running** and the Server Operational State is **Online**.

Option 2: Creation junctions using the pdadmin command line

To create the IBM Content Navigator junction for a single server, run the following command:

```
pdadmin>server task default-webseald-ISAM_Server create -t tcp -h
IBM_Content_Navigator_host_name -p port_number -c iv_creds,iv_user,iv_user_l
-b supply -x /navigator
```

Example command for a single server

```
pdadmin>server task default-webseald-abc.net.com create -t tcp -h xyz.net.com
-p 9080 -c iv_creds,iv_user,iv_user_l -b supply -x /navigator
```

To create the IBM Content Navigator junction for a high availability environment, run the following command:

```
pdadmin>server task default-webseald-ISAM_Server create -t tcp -h
HTTP_host_name -p port_number -c iv_creds,iv_user,iv_user_l -b supply -x
/navigator
```

Example command for a high availability environment:

```
pdadmin>server task default-webseald-abc.net.com create -t tcp -h xyz.net.com
-p 80 -c iv_creds,iv_user,iv_user_l -b supply -x /navigator
```

To create the integrated help system junction for a single server, run the following command:

```
pdadmin>server task default-sebseald-ISAM_Server create -t tcp -h
IBM_Content_Navigator_host_name -p port_number -x /wcdocs
```

Example command for a single server

```
pdadmin>server task default-webseald-abc.net.com create -t tcp -h xyz.net.com
-p 9080 -x /wcdocs
```

To create the integrated help system junction for a high availability environment, run the following command:

```
pdadmin>server task default-webseald-ISAM_Server create -t tcp -h
HTTP_host_name -p port_number -x /wcdocs
```

Example command for a high availability environment:

```
pdadmin>server task default-webseald-abc.net.com create -t tcp -h xyz.net.com
-p 80 -x /wcdocs
```

Task 2:

Configure IBM Content Navigator using the following steps:

1. Run the IBM Content Navigator Configuration and Deployment Tool to create a new deployment on WebSphere Application Server.
2. Run all the configuration and deployment tasks that apply to your system. For more information, see Configuring and deploying IBM Content Navigator in the IBM Content Navigator Knowledge Center.

   NOTE: When you run the *Configure the IBM Content Navigator Web Application* task, ensure that you select **Application server authentication** for the **IBM Content Navigator authentication** option. This option configures IBM Content Navigator for IBM Security Access Manager.

3. Restart the application server where IBM Content Navigator is deployed.
4. Restart the WebSEAL server instance.

   High availability environments: Restart the IBM Content Navigator cluster, the web server, and the node agent for each node in the cluster.

5. **Optional**: WebSEAL has the option to prevent cross-site scripting, which is a common security problem for web servers.

   To enable this option, add the **HTTPOnly** attribute **Failover Set-Cookie** headers and change the value of the **use-http-onlycookies** in the server stanza of the WebSEAL configuration file to **yes**.

   The WebSEAL default value is **use-http-only-cookies=no**.

Note: IBM Content Navigator configured with Security Access Manager and WebSEAL SSO also supports ISAM form-based authentication. You can login to a Content Navigator desktop using the ISAM login form.

Step 3 - Verify your deployment of IBM Content Navigator with ISAM

To verify the deployment, in a web browser, enter a URL with the following format:

http://ISAM_Server/<context_root>

The default context root is **navigator**.

For example, http://ISAM_server_name/navigator.

Login to IBM Content Navigator repositories from the Content Navigator Admin desktop is manual, and repositories will not be logged into automatically even if SSO is configured.

Important: You must provide the Security Access Manager credentials to access the Content Navigator desktop.

Step 4 – Complete additional configuration tasks for IBM Content Manager repositories

If you are planning to connect to IBM Content Manager repositories from a Content Navigator desktop that is configured with ISAM SSO and want to avoid an additional login to that repository, you must configure Content Manager for trusted logins. Refer to the following Tech Note for more information:

https://www.ibm.com/support/docview.wss?uid=swg27028309

Troubleshooting your deployment and known issues

If you receive an error in relation to "connecting to the repository" and "administrator credentials" in Asynchronous Tasks for deleting teamspaces, use the instructions in the following Content Navigator knowledge center topic to resolve the issue:

https://www.ibm.com/support/knowledgecenter/en/SSEUEX_3.0.6/com.ibm.installingeuc.doc/eucin019.htm