IBM ®

Redbooks

How to Successfully Integrate IBM Content Navigator with Box

This document contains the procedures for configuring a Box repository in IBM® Content Navigator and some other related Box product usage information when integrating with IBM Content Navigator. This document incorporates information from the IBM Support website (https://ibm.biz/Bdi3Lc) and additional important information to successfully configure Box integration with IBM Content Navigator.

What is Box

Box is a cloud platform that helps you securely store, share, and manage all your files. Whether you need to secure confidential business information, develop a custom mobile application, or simplify paper-based office processes, Box can help you do more with your content. Box provides easy internal and external file sharing so that you can stop sending insecure, large attachments through email. Use customized Box shared links with passwords, expiration dates, and controlled download access. You can collaborate externally and share with vendors, clients, or partners, no matter what computer phone or tablet they use.

IBM Content Navigator Version 2.0.3.5 includes the ability to search, browse, and view files in Box. In addition, versions 2.0.3.6 and above include share, copy, and cross-repository search with Box. Version 3.0 IBM Content Navigator introduces OAuth2 with JWT security.

Before adding a Box repository to IBM Content Navigator , ensure that you can connect to IBM Content Navigator by using HTTPS .

Integration with Box requires an HTTPS connection URL to IBM Content Navigator. To validate your SSL configuration and HTTPS connectivity, use the web server administrative console to check that the server hosting IBM Content Navigator has a valid SSL server certificate, which is self-signed or signed by a recognized authority. Ensure that the desktop browser (Internet Explorer, Chrome, or Firefox) can establish a trusted HTTPS connection to the web server **without any certificate errors or security risk warnings**.

Note: It is important that you are not presented with a certificate error.

If you need to configure your browser for secure trusted connections, see *Configuring your Browser for Trusted HTTPS connections to IBM Content Navigator and Box*, TIPS1351, found at:

http://www.redbooks.ibm.com/abstracts/tips1351.html

Creating a Box application to integrate Box with IBM Content Navigator server

To integrate IBM Content Navigator with Box, you must create a Box application. This application is used as the bridge between IBM Content Navigator and Box, and to a large degree is invisible to users. The only time the users are aware of this bridge is the first time that they access the Box repository from IBM Content Navigator. They are prompted for their Box credentials to authorize this application to access their Box environment.

To create a Box application to integrate Box with the IBM Content Navigation server, complete the following steps:

1. Go to https://developers.box.com/, select **Apps**, and log in.

2. Click **My Apps**, and then click **Create a Box Application**.

3. In the Application Name field, enter a meaningful name that represents this application usage. (If prompted for an application type, select **Box Content**.)

4. Click **Create Application**.

5. In the General Information window, under OAuth2 Parameters, set the `redirect_uri` parameter to match the URL of your IBM Content Navigator server, https://hostname:port/navigator/jaxrs/oauth2/client_id, where `client_id` is the OAuth2 `client_id` that is shown in the OAuth2 Parameters area of this Box application. The URI must be HTTPS (it can be only http for either `localhost` or `127.0.0.1` and for development purposes only). This URI is used by IBM Content Navigator to perform authentication actions when accessing the Box repository. If you use a high availability/load-balanced environment, this URI should be the primary common URI that is used to access the IBM Content Navigator environment.

   The host name format in this URL must match the host name format that is used in the browser address URL and the host name in the server's SSL certificate (either all occurrences use the short name or all use the fully qualified DNS name).

6. Select **Standard 3-legged authentication** and allow **Read write all files** (where required).

7. Scroll to the bottom of the window and click **Save Application** to save your changes.

Figure 1 shows an example of a Box application for use with IBM Content Navigator.

Figure 1. Make sure that redirect_uri has the correct name format

Important: The `redirect_uri` parameter here must use the same host name format that you enter in your desktop browser to access IBM Content Navigator (either the short name or FQDN).

Creating the Box repository on IBM Content Navigator

Before you attempt to configure a Box repository in IBM Content Navigator, the web server must be configured to use the Box SSL certificates that are used to secure connections between the web server and the Box application. **You must import two Box SSL signer certificates** .

To configure SSL certificates for Box repository access, complete the following steps:

1. Log in to the IBM WebSphere® Application Server administrative console where IBM Content Navigator is deployed. Go to the appropriate signer certificates console option:

   - For cluster configurations, select **Security** > **SSL certificate and Key management** > **Key stores and certificates** > **CellDefaultTrustStore** > **Signer certificates** .

   - For stand-alone configurations, select **Security** > **SSL certificate and Key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates** .

2. Click **Retrieve from port**.

3. Specify the Box host name URL in the format `<<subdomain>>.app.box.com`. For example, in the Host field, enter `ecmsup.app.box.com`, and in the Port field, enter `443`. If your Box environment does not use a subdomain, just enter `app.box.com`.

4. Provide an alias name, for example, `ecmsup.app.box.com`.

5. Click **Retrieve signer information**. This action must succeed. The web server must be able to connect to `app.box.com` and `api.box.com`.

6. Save the certificate and save your changes.

7. Repeat the steps by using the additional host name `api.box.com` with an alias of `api.box.com`.

8. Click **Retrieve signer information**.

9. Save the certificate and save your changes.

You must import the signer certificate from each of the two external Box resources (app.box.com and api.box.com). When this task is successful, it also establishes that the IBM Content Navigator server can access the external Box resources. The web server must be able to make SSL connections to these Box external resources (app.box.com, api.box.com, and dl.boxcloud.com).

Figure 2 shows the WebSphere console page for Signer Certificates.

 Figure 2. Example of imported Box SSL signer certificate

If you cannot configure access to external Box resources through HTTPS directly from WebSphere Application Server due to firewall restrictions, consider configuring WebSphere Application Server to use an existing internal internet proxy server, where available. To do so, complete the following steps:

1. Log on to the WebSphere Integrated Solutions Console.

2. Select **Servers** > **Server Types** > **WebSphere Application Server**.

3. Click the appropriate server, for example, server1.

4. Under Server Infrastructure, click **Java** and select **Process Management** > **Process Definition**.

5. Under Additional Properties, click **Java Virtual Machine**.

6. Click the **Configuration** tab.

7. Under Additional Properties, click **Custom properties**.

8. Click **New**.

9. Specify the appropriate Name and Value based on the required configuration. To provide internet access to Box, use Properties for HTTPS connections. For more information, see Table 1.

10. Click **OK**.

11. Repeat steps 8 - 10 for each required property pair.

12. Click **Save** directly to the master configuration.

13. Restart WebSphere Application Server.

Table 1. JVM property name and value pairs for an outbound HTTPS proxy server configuration.

Name	Sample values	Description
`https.proxyUser`	`admin`	The user name that is used to authenticate to the proxy for HTTPS connections.
`https.proxyPassword`	`password`	The password that is used to authenticate to the proxy for HTTPS connections.
`https.proxyHost`	`https.proxy.ibm.com`	The host name or IP address of the HTTPS proxy.
`https.proxyPort`	`3128`	The port of the HTTPS proxy.
`http.nonProxyHosts`	`host1.ibm.com|internal.ibm.com`	A list of hosts, which are separated by |, for which a proxy must not be used.

Note: The `http.nonProxyHosts` property applies for both HTTP and HTTPS connections. The minimum requirement is `https.proxyHost` and `https.proxyPort`.

It is also necessary to import the root SSL certificate for the Box environment into the WebSphere Trust Store. Complete the following steps:

1. On Windows, you can use the Certificate Management tool (certmgr.msc) or Internet Explorer to export the CA Trust Certificate that is named 'GeoTrust Global CA'.

2. Export this certificate to a DER or Base64 format file with the .cer extension.

3. Then, import into the WebSphere Trust Store. Use the WebSphere Application Server administrative console and select **Security** > **SSL certificate and key management** > **Key stores and certificates** > **Default Trust Store** > **Signer certificates** > **Add**.

4. Enter an alias name (box.com) and the path to the exported .cer certificate file, select the type, and import by clicking **Apply**.

Restart the IBM Content Navigator - WebSphere instance. WebSphere Application Server now uses the configured proxy server to make outbound HTTPS requests from WebSphere Application Server to Box.

If your version of WebSphere Application Server does not have the POODLE vulnerability fix, complete the following steps:

1. Select **Servers** > **Server Types** > **WebSphere Application Server**.

2. For each IBM Content Navigator server, click the server name and select **Java and Process Management** > **Process definition** > **Java Virtual Machine**.

3. For generic JVM arguments, add the argument
   `-Dhttps.protocols="TLSv1,TLSv1.1,TLSv1.2".`

4. Save your changes.

5. Restart all instances of the IBM Content Navigator server.

For more information about the POODLE vulnerability, see Security Bulletin: Vulnerability in SSLv3 affects IBM WebSphere Application Server (CVE-2014-3566), found at:

http://www.ibm.com/support/docview.wss?uid=swg21687173

Creating a Box repository on IBM Content Navigator to connect to a Box application from one or more IBM Content Navigator desktops

Note: In IBM Content Navigator FP7 and FP8, there are some minor issues with using IE 11, as described in step 7.

To create a Box repository on IBM Content Navigator, complete the following steps:

1. Open the IBM Content Navigator administration tool in the web client.

2. Click **Repositories** > **New Repository**, and select **Box** as the repository type.

3. Enter the repository name (any meaningful name).

4. Enable **Authenticate with OAuth 2** and specify authentication parameters for OAuth2 `client_id` and OAuth2 `client_secret`, which you can get from the Box application General Information configuration page. When you enable this option, the OAuth2 `client_id` and OAuth2 `client_secret` are used to connect to Box from IBM Content Navigator.

   A single OAuth2 client_id **cannot** be shared among multiple IBM Content Navigator configurations. However, you may have multiple instances of IBM Content Navigator that share a common configuration database for HA or load balanced clustering by using the same client_id.

   If you disable this option, developer tokens that expire in 60 minutes can be used to log on to Box with **any** Box user ID by using the developer token as the **password**. Developer tokens are temporary tokens that you can generate on the Box application configuration page.

5. Save the settings. The Connect button is enabled when you save the settings.

6. To test the new repository, click **Connect** and log on and authorize Box by using a valid Box user ID and password.

7. After a successful authorization, the authorization window and redirection message is removed, the Connect button is removed, and the IBM Content Navigator information bar at the bottom of the window displays the date, time, and Box logged on user ID. (With IBM Content Navigator FP7 and FP8, when using IE 11 the window is not removed after successful authorization. Simply close the blank window and click the redirection link.)

Figure 3 shows an example of a typical Box repository configuration in the IBM Content Navigator administration desktop.

Figure 3. Example Box repository configuration in IBM Content Navigator

Note: Your Box account may be in an enterprise subdomain. In this example, the Box domain is `ecmsup.app.box.com` and `ecmsup` is the Box subdomain.

Save the configuration and click **Connect**. Authorize the Box application to use the Box environment.

Figure 4 shows an example of authorizing the application to access the Box environment.

Figure 4. Authorizing the application to access to the Box environment

Adding the Box repository to an IBM Content Navigator desktop

For IBM Content Navigator Version 2.0.3.6 or later, you can select a Box repository as the primary authentication repository for the desktop.

For IBM Content Navigator Version 2.0.3.5, you cannot select a Box repository as the primary authentication repository. Select an IBM FileNet® Content Manager, IBM Content Manager, IBM Content Manager OnDemand, or CMIS repository as the authenticating repository.

For your desktop authentication settings, if you specify a Box repository that uses OAuth2 authentication, when a user opens the desktop, the browser is redirected to Box:

- If the user is already logged in to Box, the user must grant access to connect IBM Content Navigator to Box.

- If the user is not logged in to Box, the user must enter a valid Box user account and password to grant access to connect IBM Content Navigator to Box.

Adding a Box repository to a desktop

To add a Box repository to a desktop, complete the following steps:

1. Open the administration desktop in the IBM Content Navigator web client.
2. Click **Desktops**, and either create a desktop or select a desktop to edit.
3. In the Repositories window, select the Box repository from the available repositories list and add it to the selected repositories list.
4. Save your changes.
5. If you want to use this Box repository as the authenticating repository for the desktop, go to the General window, and for the desktop authentication settings, select the Box repository. In most cases, the authenticating repository is an ECM repository, which is either P8 Content Engine or Content Manager on Demand.)

Figure 5 shows an example of adding a repository to a desktop configuration.
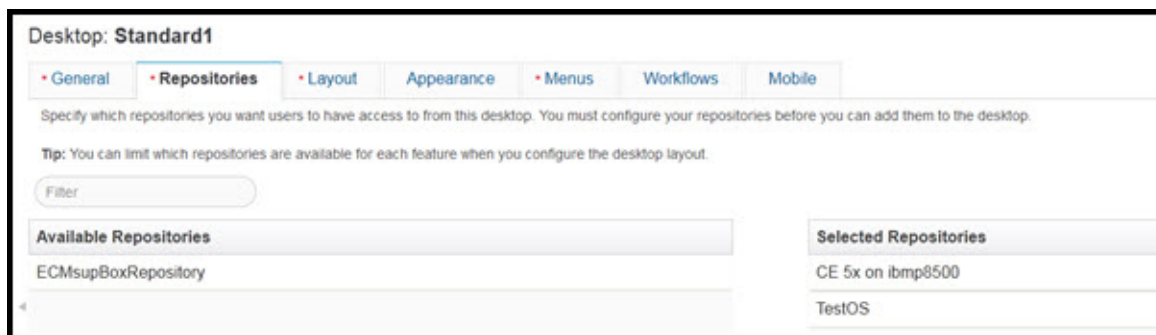

Figure 5. Adding the repository to a desktop and saving the changes

Refresh the browser view and select the Box repository from the list of available repositories, as shown in Figure 6.
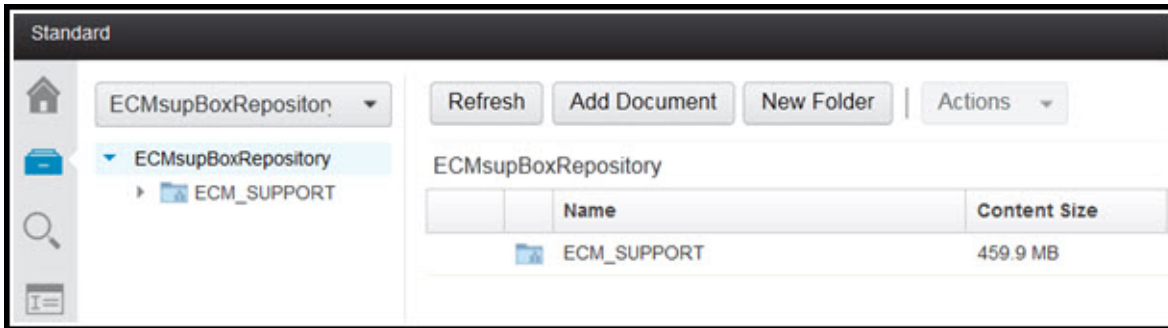

Figure 6. Choosing the Box repository from the list of available repositories

Review and, if required, modify the viewer map to set the viewer type that is used to open or display Box objects, as shown in Figure 7.

Figure 7. Modifying the viewer map as required

The current Box repository logon details are shown in the User menu, as shown in Figure 8.

Figure 8. How to find the current Box logon details

How to Successfully Integrate IBM Content Navigator with Box

Users accessing the repository for the first time are prompted for their Box credentials to authorize the application to access their Box environment, as shown in Figure 9.
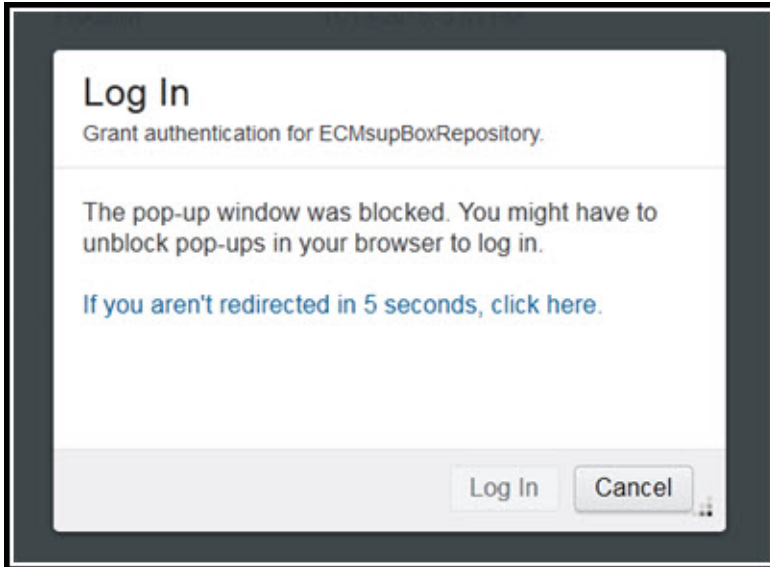

Figure 9. Authorization redirection prompt

The user is prompted to grant access to the Box environment, as shown in Figure 10.
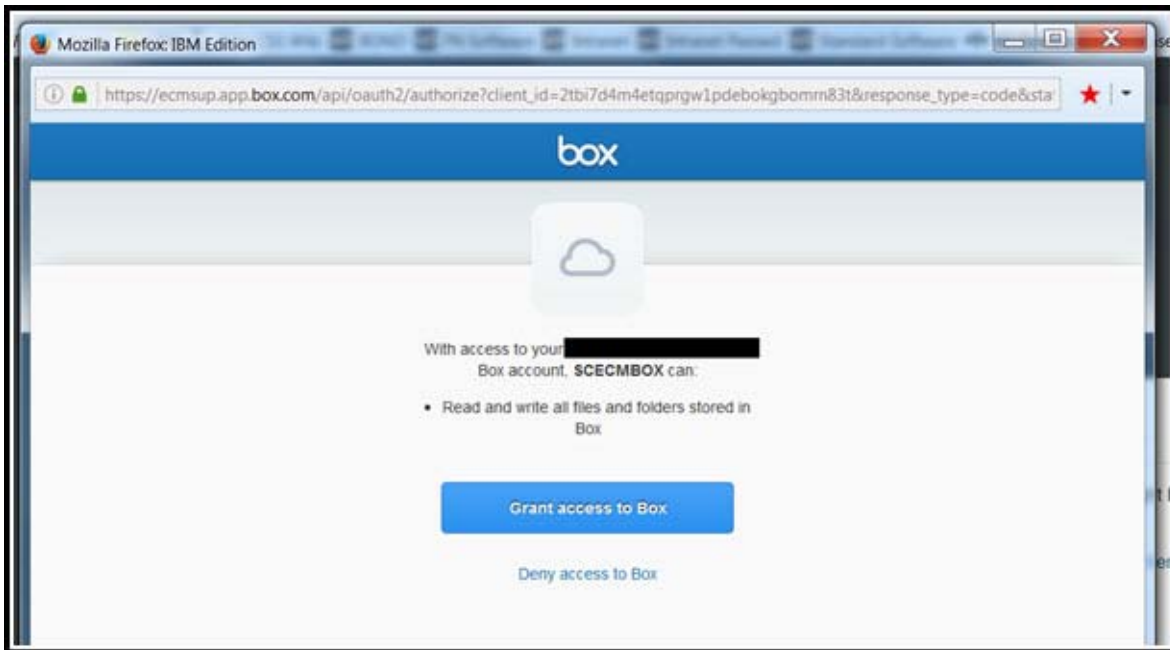

Figure 10. Granting Box access

With Internet Explorer 11, the authorization window is not removed and the redirection back to IBM Content Navigator does not happen automatically. Simply close the blank window and click the redirection link after completing the authorization, as shown in Figure 11.
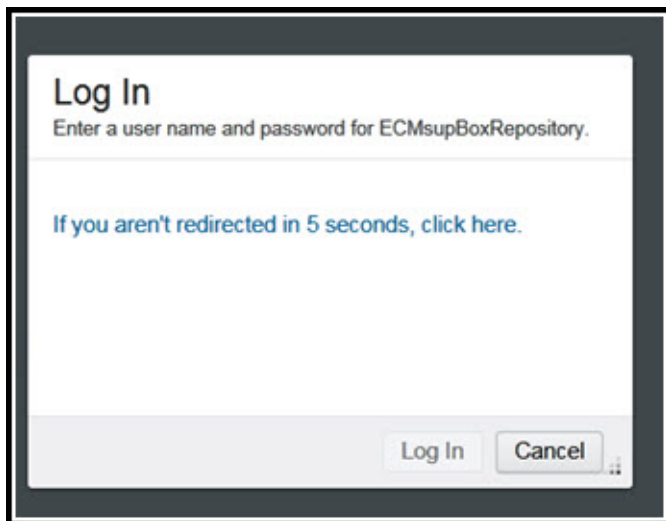

Figure 11. Completing the redirection after authorization with IE 11 by clicking the "click here" link

Connecting to a Box repository on a WebLogic server

If you want to add a Box repository to IBM Content Navigator that is running on the WebLogic server environment that uses SSL, you must add the following JVM parameter to the WebLogic server start configuration settings:

```
–DUseSunHttpHandler=true
```

You must update the class path of the application server to include `jsse.jar` in the JDK `lib` folder.

These settings ensure that the WebLogic server makes outbound SSL requests by using the HTTP handler that is preconfigured by IBM Content Navigator instead of using the default WebLogic server HTTP handler. If you do not set this parameter, you cannot connect to the Box repository.

For more information about the errors that can occur if WebLogic with SSL is not configured correctly, see Troubleshooting: Cannot connect to a Box repository on a WebLogic Server, found at:

http://www.ibm.com/support/docview.wss?uid=swg27046674

End-to-end SSL with IBM Daeja™ ViewONE Virtual viewer requires that the IBM Content Navigator server signed certificate is imported into the Java default `cacerts` keystore for the local JVM by running the following command:

```
%JAVA_HOME%/jre/bin/keytool -import -v -trustcacerts -alias selfsigned -file
"C:\Oracle\Middleware\Keystore\ibmp8500c-rootCA.der" -keystore cacerts
-storepass changeit
```

Links and references

This document uses information from many IBM sources, including the following IBM Content Navigator notes:
http://www.ibm.com/support/docview.wss?uid=swg27046488
http://www.ibm.com/support/docview.wss?uid=swg27047330

IBM Content Navigator and Box general information:
https://www.ibm.com/blogs/ecm/2015/09/30/ibm-content-navigator-now-supports-box/
https://www.ibm.com/blogs/ecm/2015/12/18/ibm-and-box-the-latest-integrations-and-offerings/

IBM Content Navigator installation and configuration documentation:
http://www.ibm.com/support/knowledgecenter/SSEUEX_2.0.3/contentnavigator_2.0.3.htm

WebSphere OutBound Proxy configuration:
https://ibm.biz/Bdi3LH

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

This document was created or updated on June 29, 2017.

Send us your comments in one of the following ways:
- Use the online **Contact us** review form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at http://www.ibm.com/redbooks/abstracts/tips1350.html .

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Daeja™
FileNet®
IBM®
Redbooks (logo)®
WebSphere®

The following terms are trademarks of other companies:

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.