

Sharing Box Content in IBM Content Navigator

Overview

IBM offers two different ways of integrating the Box environment with IBM Content Navigator for Enterprise Content Management (ECM):

- Option 1: The Box environment can be presented to IBM Content Navigator as an additional ECM repository, which users can browse and search in a similar way to an existing IBM FileNet® P8 or Content Manager repository.

This first form of integration uses standard 3 legged OAuth 2.0 authentication, and requires the user to provide Box login credentials (typically an email address) to authorize the Box developer application to access the Box environment using the user's Box profile. With this method, the Box folder structure is visible to the IBM Content Navigator user and can be browsed and searched.

Detailed configuration information is available at this website for this integration option. Read this information first before configuring Box Share:

<http://www.redbooks.ibm.com/abstracts/tips1350.html?Open>

- Option 2: The Box environment can be used to share ECM documents with users who do not have logon access to either IBM Content Navigator or Box. This configuration is done by using the IBM Content Navigator Box Share facility. IBM Content Navigator Box Share provides a way to email a link that is connected to a document object to allow collaboration with an external user.

In this scenario, the ECM object is copied to an otherwise invisible share location on Box, and a link is generated that can be emailed to the external user. The IBM Content Navigator object is flagged with a **Shared** icon. The location of the shared copy and the actual copy process is managed by IBM Content Navigator using server to server authentication, and the Box application service account. This second form of integration uses the OAuth 2.0 with JSON Web Token (JWT) authentication in the Box developer application, and uses the Box application service account.

With the method described in Option 2, the Box folder structure is NOT added to the IBM Content Navigator desktop as a searchable ECM repository. It is added to the Box Share configuration only.

If you want to provide users with the ability to browse and search a Box repository, and share ECM objects externally by using Box Share, configure two Box developer applications: One using standard 3 legged OAuth 2.0 authentication, and another using server to server JWT authentication. Also, configure two repository definitions in IBM Content Navigator:

- One for Desktop repository browsing and searching (using the standard 3 legged OAuth 2.0 authentication)
- One for Box Share (using JWT authentication)

Configuration guidance for enabling Box Share in IBM Content Navigator v 3.x

If you already have a Box developer application for an existing Box repository in an upgraded IBM Content Navigator deployment that is used for folder browsing, searching, and sharing, create a new Box application for Box Share.

The Box Share application has the same prerequisites as a Box repository. Read the existing documentation before configuring Box Share:

<http://www.redbooks.ibm.com/abstracts/tips1350.html?Open>

The new Box developer application must use OAuth 2.0 with JWT authentication.

Figure 1 shows OAuth 2.0 as the selected authentication method.

Authentication Method
Choose how your app will authenticate to the Box APIs. [Learn more.](#)

Standard OAuth 2.0 (User Authentication)
Requires Box users to log in with a username and password to authorize your app to access content in their account.

OAuth 2.0 with JWT (Server Authentication)
Allows your app to authenticate directly to Box using a digitally signed JSON Web Token instead of user credentials. For use with Service Accounts and App Users.

Figure 1: Choose OAuth 2.0 with JWT

On the same configuration page, set the application access required. Figure 2 shows the application access.

Application Access
Select the access level requested when an admin authorizes your app. This will determine which users and content your app may access.

Application
Default access. Provides access only to the service account and any app users and content created by your app.

Enterprise
Allows your app to request access to its own service account, app users and content, as well as existing users and scopes below.

Figure 2: Choose the Application access option

Note: A service account is always automatically created when you create the Box developer application. You do not need to manually create the service account. The service account is not visible in the application configuration.

The access scope requires that you select **Read and write all files and folders stored in Box** (Figure 3).

Application Scopes

Select the scopes shown on the OAuth consent screen when users or admins authorize your app. [Learn more.](#)

- Read and write all files and folders stored in Box
- Manage users
- Manage groups
- Manage webhooks
- Manage enterprise properties
- Manage retention policies

Figure 3: Minimum required access scope

From the My Apps level, open the Developer Admin Console to authorize the application (Figure 4).

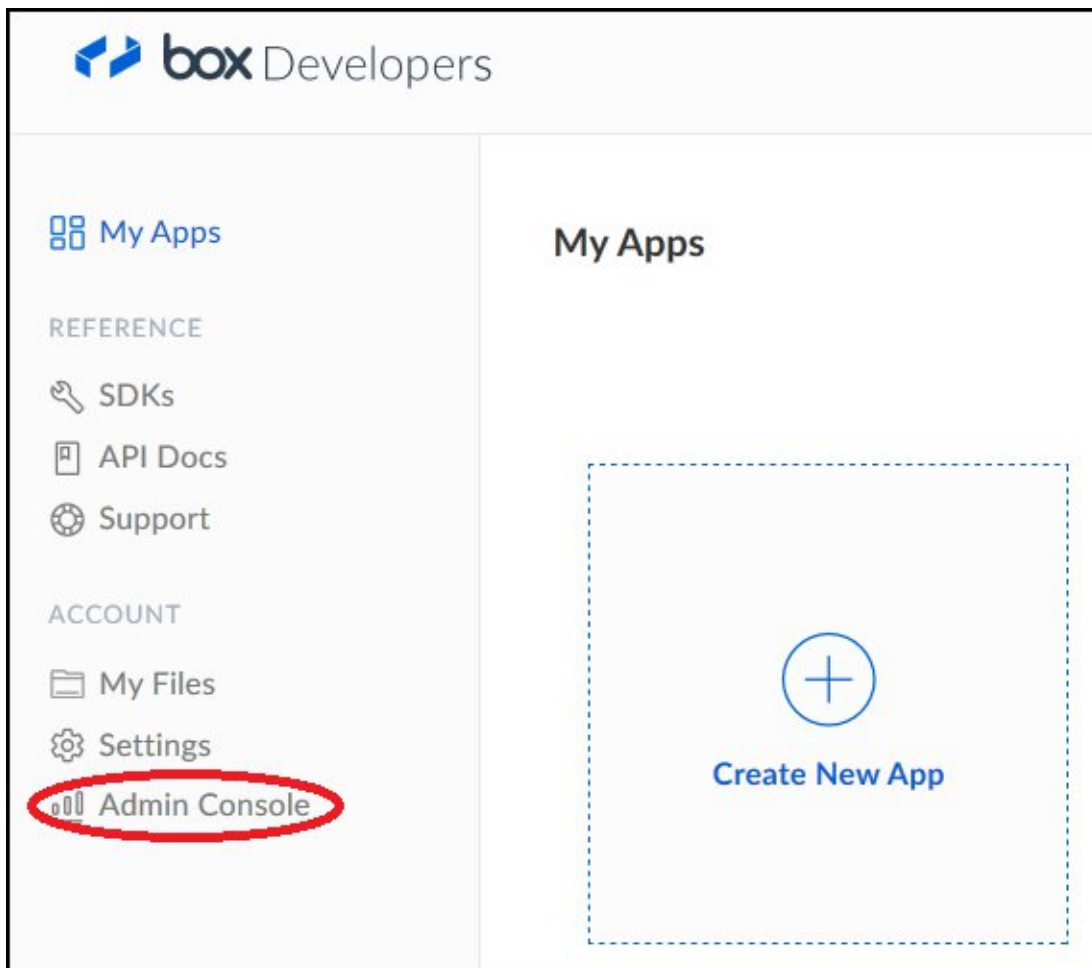


Figure 4: Open the Admin console using the link

Select **Enterprise Settings** or **Elite Settings** (depending on your Box license) in the **Gear** menu (Figure 5).

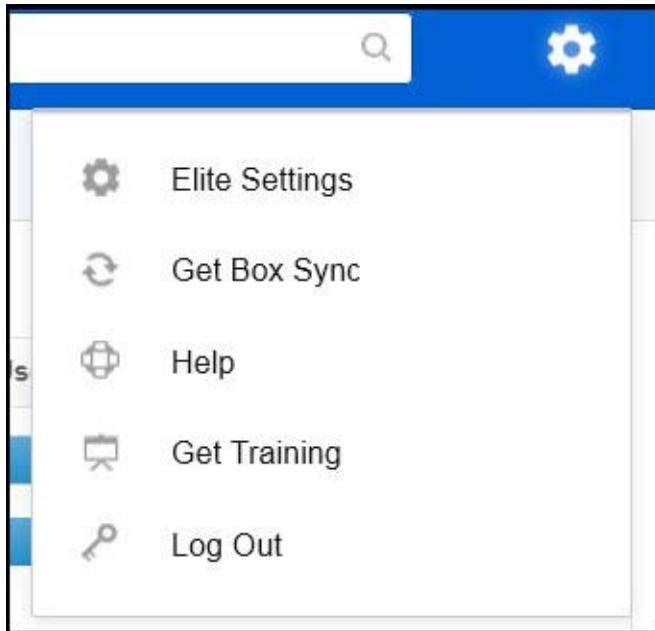


Figure 5: Select the settings menu option

Select the **Apps** menu as shown in Figure 6.

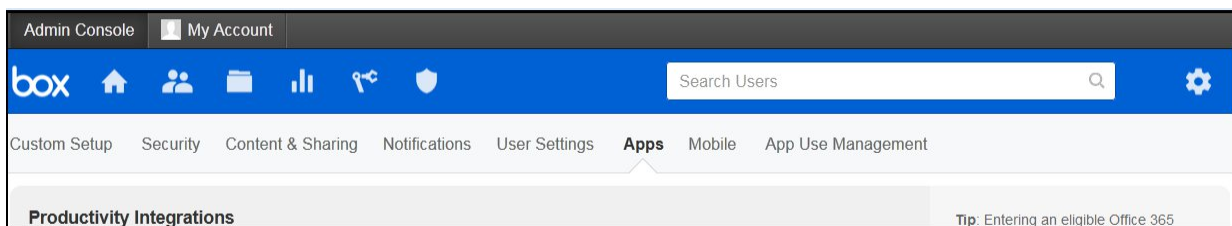


Figure 6: Open the Apps page

Scroll down the page to Custom Applications and click **Authorize New App** as shown in Figure 7.

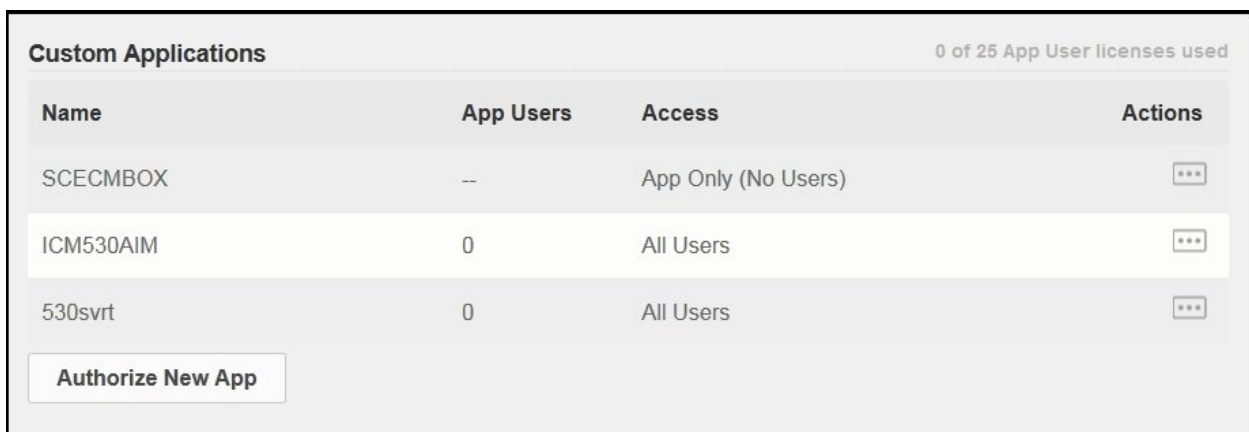


Figure 7: Click the Authorize New App button

You are prompted to enter the API key. This is the application Client ID, and can be copied from the Application configuration page in the Box developer application, as shown in Figure 8.



Figure 8: Copy the API key (Client ID)

Note: When using JWT authentication, communication with the Box application requires an RSA public and private key pair. The Box application configuration page does provide a mechanism for generating these pairs for you. However, the format of the private key is not easy to work with. It still requires access to an SSL toolkit to decrypt the key and generate an alternative version of the private key in a different format for use with IBM Content Navigator.

Download and install OpenSSL from this website:
<https://www.openssl.org/>

To create the key pairs, complete the steps in the following sections.

Create your own private key pair

To create a private key pair, complete these steps:

1. Issue the following OpenSSL commands:

```
openssl genrsa -aes-256-cbc -out <<path>>\my_private_key.pem 2048
```

You are prompted for a passphrase that encrypts and secures your private key. Securely record the passphrase for future use. When the Box configuration is completed, securely store this private key.

2. Create your own public key from your private key:

```
openssl rsa -pubout -in <<path>>\my_private_key.pem -out  
<<path>>\my_public_key.pem
```

3. Create a DER format pkcs8 key for IBM Content Navigator from your private key:

```
openssl pkcs8 -topk8 -inform PEM -outform DER -nocrypt -in  
<<path>>\my_private_key.pem -out <<path>>\my_private_key_pkcs.der
```

4. Put the DER format private key in an accessible shared path on the IBM Content Navigator server, such as:

```
\\<<serverName>>\key\my_private_key_pkcs.der
```

You will use this path when configuring the box repository in IBM Content Navigator. If you have a cluster or farm of IBM Content Navigator instances, this key file must be accessible by all the instances that will use Box Share.

5. Upload the public key to the Box application.

Note: This process requires that 2-step verification be enabled on your account.

6. At the upper right of the Box developer web page, select the pull-down menu from your **Profile** icon shown in Figure 9.

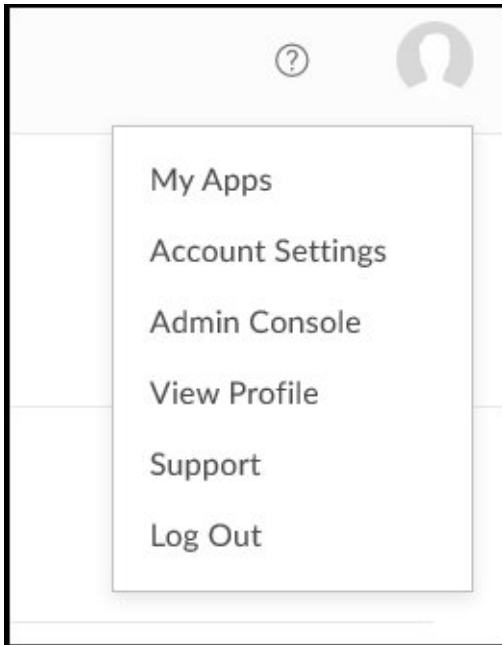


Figure 9: Select Account Settings

7. Select the box for 2-step verification, highlighted in Figure 10.

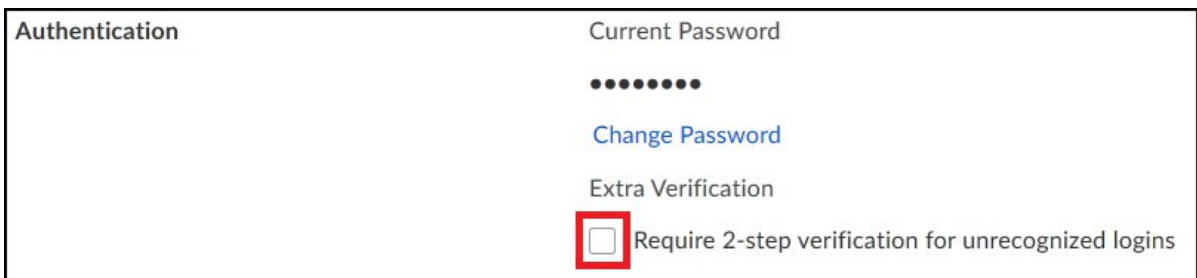


Figure 10: Select 2-step verification and provide a mobile phone number for SMS text messages

8. Now you can add your public key by clicking **Add a Public Key** on the Box application configuration page shown in Figure 11.

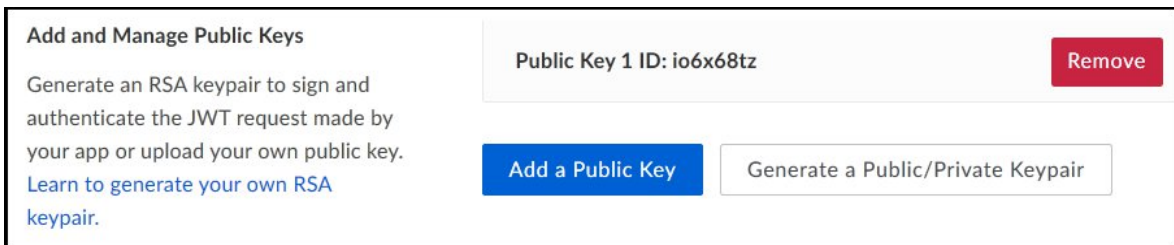


Figure 11: Add your generated public key

Important: After you have added your Public Key, remove the 2-step verification from your account settings.

Add the Box application for Box Share in IBM Content Navigator

Box Share requires the Task Manager component to be configured and deployed with IBM Content Navigator.

Open the IBM Content Navigator Admin desktop and navigate to **Settings -> General -> Task Manager Configuration**. Enable the Task Manager service, and set the Task Manager URL to use an https connection, for example:

```
https://myicnhost.domain:9443//taskManagerWeb/api/v1
```

Copy the URL and paste it into a new browser tab address. You should see the Task Manager Status page.

If Task Manager is not available, you must reconfigure the Content Navigator application and add the Task Manager Service. For more information, see the documentation:

<https://ibm.co/2hgLHde>

Then, redeploy the Content Navigator application using the IBM Content Navigator Configuration and Deployment Tool.

When Task Manager is configured and available, add and configure the new Box Share repository. Open the Content Navigator Admin desktop, and navigate to Repositories. Click the **New Repository** button and select **Box**. Complete the fields as required, making sure to select the Server JWT authentication type, as shown in Figure 12.

Box repository: **JWTBOX**

General

You must enable Standard or Server authentication before you connect to the repository.

* Display name: ?

* ID: ?

* Authentication Type: ?

- Standard Authentication (3-legged OAuth2.0)
- Server Authentication (OAuth 2.0 with JWT)
- Developer Authentication

Figure 12: Select the authentication type

Complete the rest of the repository fields using the configuration data from the Box developer application pages. The repository Display name that is shown here is just an example. Use your own repository name as required. The Enterprise ID is on the Box developer application General information page. The Client ID, Client Secret, and Public Key ID are on the Configuration page. The Private key file path is the path to the DER format pkcs8 private key file that was created previously.

When all the fields are completed, click **Connect**. IBM Content Navigator then retrieves the Box application service user email account, and shows a connection status on the status bar similar to that shown in Figure 13.

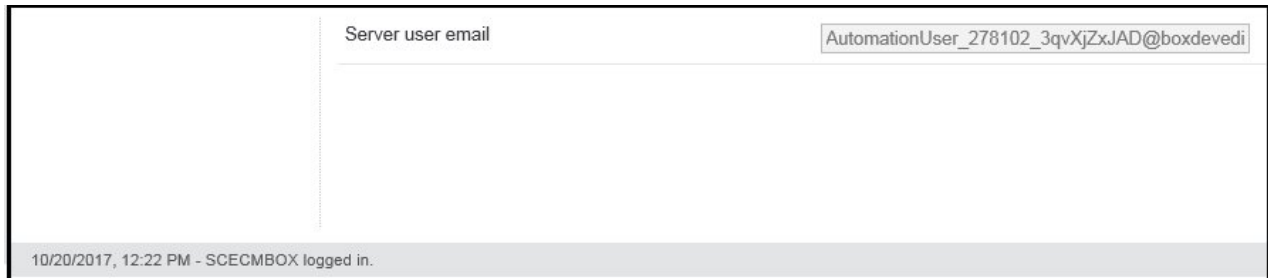


Figure 13: Service account email retrieved and login status displayed

Enable Box Share in the Content Navigator Desktop and Content Engine Repository

In the Content Navigator Admin Desktop, open the user desktop configuration for editing. On the General tab, scroll down to the Box share services section, as shown in Figure 14.



Figure 14: Enable Box Share and select the JWT Box repository

Note: You can either allow users to manually enter and edit email addresses that are associated with Box Share links, or you can install the email mapping plug-in. For more information, see the Appendix.

You also need to enable Box Share for the ECM repository that contains the document objects you want to share. Edit the repository configuration in the Content Navigator Admin desktop. For example, if you want to share document objects for collaboration from a FileNet P8 Object Store, edit the Content Navigator repository associated with the FileNet P8 Object Store. Connect to the Content Engine, and then select the Configuration tab. Scroll down to Optional Features and enable Box Share as shown in Figure 15.

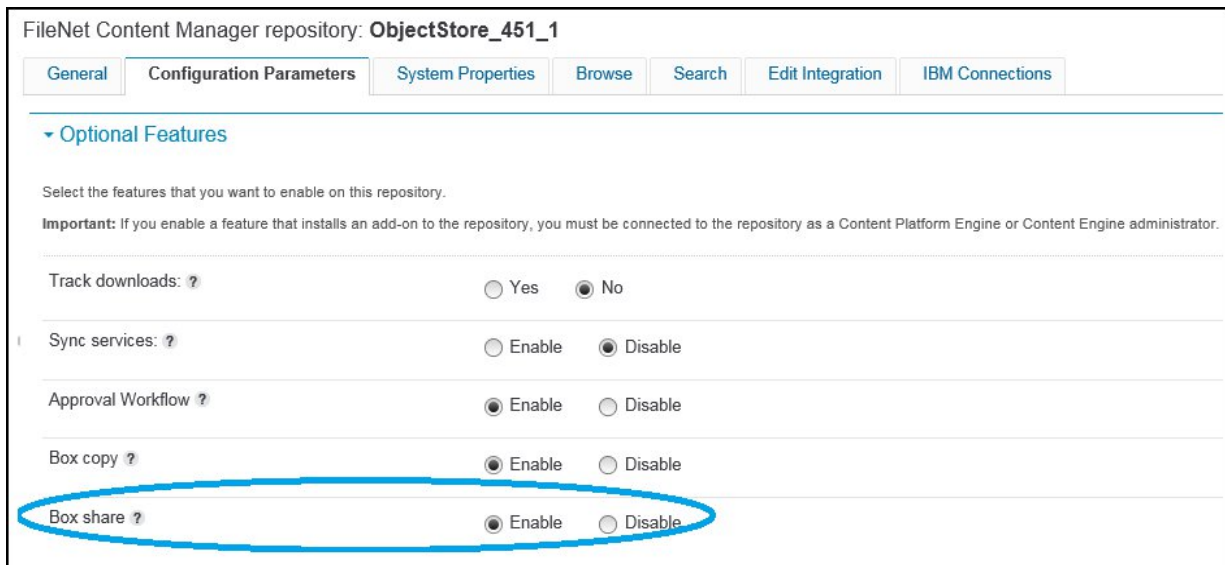


Figure 15: Enable Box Share on the source repository

Note: Enabling Box Share in Content Navigator automatically adds the new menu options for Box Share.

Make sure all your changes are saved, and log off from the Admin Desktop. Log on to the Content Navigator Desktop where you have enabled Box Share services and select the ECM repository where you have enabled Box Share. Browse to or search for a document object.

Users can share a document if they have permission to edit or view the document. Users who have edit access can share a document and can update the share options regardless of who shared the document. Users who have view access can share a document and can update the share options for documents that they share, but cannot update the share options for documents that someone else shared.

For more information, see the existing documentation for enabling Box Share, which can be found at this URL:

<https://ibm.co/2h8uHlv>

When you open the menu for a document where you have the appropriate access, you see a **Box** menu option with submenus of **Share** and **Delete Share**. When you share a document, you are prompted to provide the email address of the collaborator who will receive the email containing the link. After the share link has been created and emailed, the document is marked with an icon indicating that it has been shared, as shown in Figure 16.

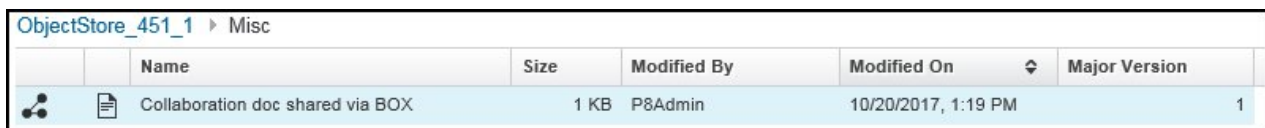


Figure 16: Example of an object shared by using Box Share

To enable IBM Content Navigator to send email links, the IBM WebSphere® mail service must be configured with an outbound SMTP server. IBM Content Navigator uses the Mail Session named `CNMailSession`. This service can be configured using the WebSphere administrative console.

Note: If you were using Box Share before IBM Content Navigator Version 3.0, the `boxShareAdminRefresh` task must also be manually deleted from the Asynchronous Tasks view. Log on to IBM Content Navigator as a Tasks Admin, locate and select `boxShareAdminRefresh` from the Asynchronous Tasks view, and then delete the task.

Appendix

The Email mapping plug-in provides a service that returns an email address that is associated with an IBM Content Navigator user. The email address that the service is returning is the address for the user who is sending the share link.

If you enable a desktop and repository for Box Share, a mapping of user IDs and email addresses might be required so that a user's email address can be displayed and used to send the link for the document. The email address can be provided in one of the following ways:

- For a FileNet P8 Content Manager repository, IBM Content Navigator attempts to use the email address from FileNet Content Manager. If the LDAP Directory Service is configured with a populated mail attribute, this value is used. If the LDAP Directory Service is MS Active Directory, the Principal Name is used when the mail attribute is empty.
- For a FileNet P8 Content Manager repository that does not use Active Directory and does not provide email addresses, or when using an IBM Content Manager repository, you can create a custom list of user IDs and email addresses, and configure the email mapping plug-in.
- If you do not use the email addresses from FileNet Content Manager or from the email mapping plug-in, you can set a configuration option for the IBM Content Navigator Desktop to allow users to modify or enter the sender's email address when sharing a document.

If you decide to use the plug-in, create a custom list of user accounts and email addresses, update the JSON file for the email mapping plug-in, rebuild the JAR file, and then configure the email mapping plug-in in IBM Content Navigator.

Important: If you are using the Email mapping plug-in from IBM Content Navigator, Version 2.0.3 Fix Pack 6 or Fix Pack 7, you must reconfigure and use the updated plug-in from IBM Content Navigator, Version 2.0.3 Fix Pack 8 or later. This change is needed because the way the plug-in service is called from IBM Content Navigator has changed.

If you made any customizations to the JSON file or Java code that was provided in Version 2.0.3 Fix Pack 6 or Fix Pack 7, you must apply the same customizations to the updated plug-in.

For a new deployment where you are using IBM Content Navigator 3.x, use the plug-in from the installed version.

Before you begin

If you are using the mapping file list, determine the user IDs and email addresses that you want to set up for the Box Share action. Create a custom list of user IDs and email addresses as a comma-separated list enclosed in braces:

```
{"User1":user1@emaildomain.com,  
 "User2":user2@emaildomain.com}
```

Procedure

Extract the contents of the JAR file and edit the `emailMapping.json` file that is contained in the JAR file. The default JAR file path for the installation directory on Windows is as follows:

```
C:\Program Files (x86)\IBM\ECMClient\plugins\emailMappingPlugin.jar
```

In the Data folder, find the sample list of user IDs and email addresses in the file `emailMapping.json`, and replace it with your custom list of user IDs and email addresses. Save the file. Then, complete these steps:

1. Optional: If you want to customize the email mapping service, you can modify the code in the `emailMappingPlugin.java` file.
2. Rebuild the `emailMappingPlugin.jar` file with the original MANIFEST.MF file, and save it in the original JAR file path.
3. Open the administration tool in the IBM Content Navigator web application, and click **Plug-ins -> New Plug-in**.
4. Enter the JAR file path for the Email mapping plug-in. You might need to create a shared path. The default JAR file path for the IBM Docs Integration plug-in class on Windows is as follows:
`C:\Program Files (x86)\IBM\ECMClient\plugins\emailMappingPlugin.jar`
5. Click **Load**.
6. Save your changes.

What to do next

Ensure that Box Share is enabled for your desktop and any source repositories. In the desktop configuration settings, select a Box repository for the shared files, and select whether to allow users to update the “send from” email address when they share a document. Refer to Table 1 to see how the **Allow users to modify the Send from email address** configuration option changes what is possible in the Box share email action.

Table 1. Configuration options

| Allow or do not allow modify option | Is the User ID included in .json file? | Result in the Box Share action |
|--|--|---|
| Yes. Allow users to modify the email address when they share a document. | Yes. The user ID is included in the file <code>emailMapping.json</code> , or email is available from the Directory Service. | The mapped email address is displayed, and the user can change it to a different email address. |
| Yes. Allow users to modify the email address when they share a document. | No. The user ID is not included in the file <code>emailMapping.json</code> , and email is not available from the Directory Service. | The email address is blank, and the user can enter an email address. |
| No. Do not allow users to modify the email address when they share a document. | Yes. The user ID is included in the file <code>emailMapping.json</code> or the email is available from the Directory Service. | The email address is displayed, but the user cannot change it to a different email address. |
| No. Do not allow users to update the email address when they share a document. | No. The user ID is not included in the file <code>emailMapping.json</code> and an email is not available from the Directory Service. | An error is returned. The administrator needs to update the file <code>emailMapping.json</code> , rebuild the JAR file, and reload the plug-in. |

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.

© Copyright International Business Machines Corporation 2017. All rights reserved.

This document was created or updated on November 7, 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/tips1355.html> .

Trademarks

FileNet®

IBM®

Redbooks (logo)®

WebSphere®