

Configuring your browser for trusted HTTPS connections to IBM Content Navigator and Box

The information in this web doc guides you through adding the IBM® Content Navigator server's certificate to the desktop browser for Internet Explorer, Firefox, and Chrome. This document is an associated web doc for the web doc *How to Successfully Integrate IBM Content Navigator with Box Repository*, TIPS1350, found at:

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

Use the web server administrative console to check that the server that is 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. It is important that you are not presented with a certificate error.

Figure 1 shows an example of an IBM WebSphere® root certificate in the IBM WebSphere Application Server administrative console.

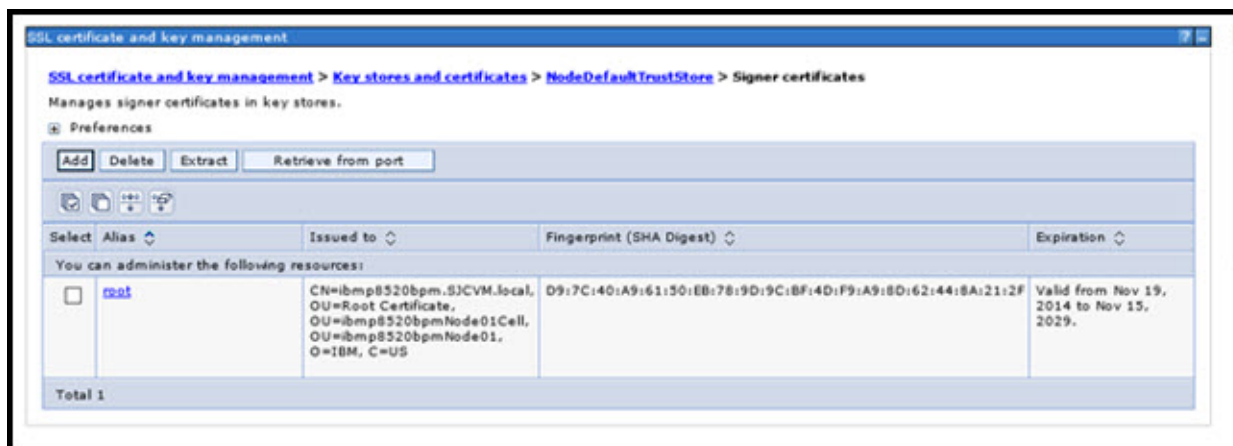


Figure 1. Example WebSphere root certificate

Configuring Internet Explorer

To configure Internet Explorer, complete these steps:

1. Add the HTTPS connection URL host name to the Internet Explorer Trusted Sites.
2. Connect to IBM Content Navigator by using HTTPS and the HTTPS port (use the application server default 9443 and the front-end proxy default 443).

3. If the root certificate is not imported into Internet Explorer, you get a security warning. Continue to the site and you see a red certificate error on the address bar.
4. Click the certificate error, view the certificate, view the Certificate chain path, and install the root certificate into the Certificate store: Trusted Root Certification Authorities.
5. Restart the browser and check that the connection to IBM Content Navigator completes without any certificate security warnings.

Figure 2 shows where to add the IBM Content Navigator URL host to the Internet Explorer Trusted Sites list.



Figure 2. Adding the IBM Content Navigator host to the trusted sites

Figure 3 shows an HTTPS browser connection with a non-existent or invalid certificate.

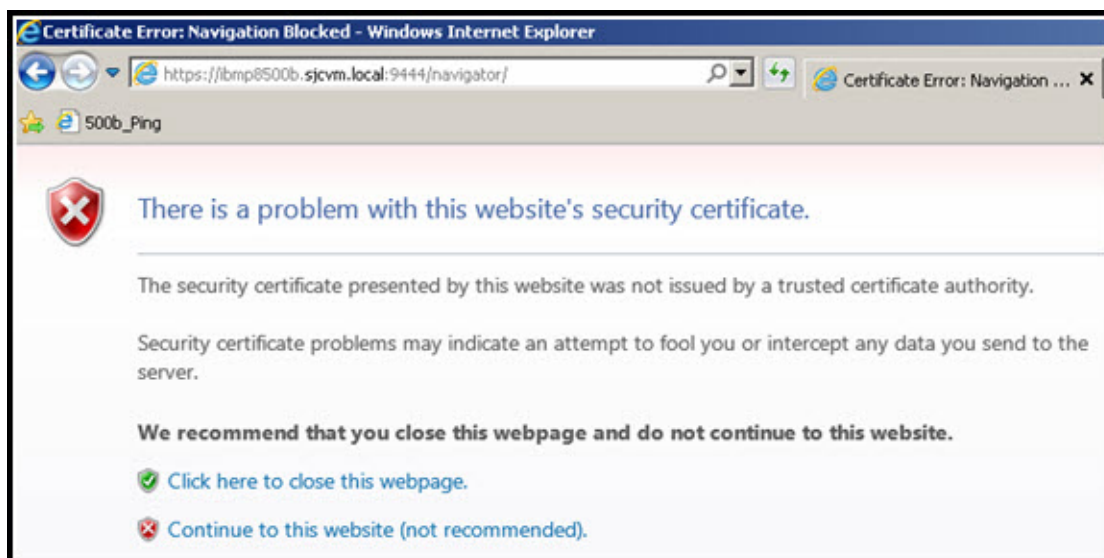


Figure 3. Connecting to IBM Content Navigator and clicking “Continue to this website” if prompted

Figure 4 shows a certificate error that is reported by Internet Explorer.

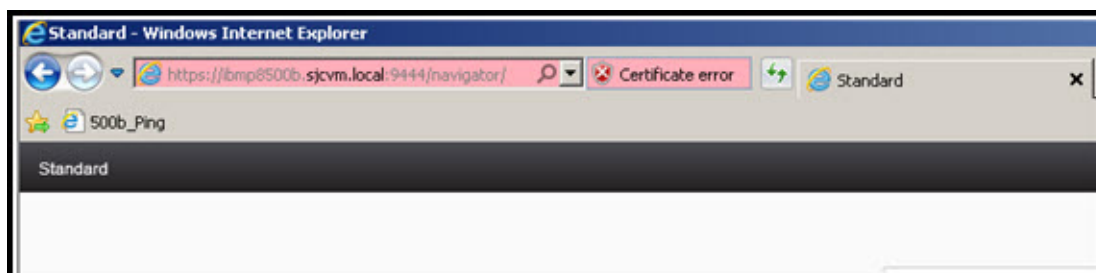


Figure 4. Clicking the “Certificate error” message on the address bar

Figure 5 shows an example of an untrusted root certificate in the certificate chain path.



Figure 5. Viewing the certification path to select the root certificate and clicking View Certificate

Figure 6 shows clicking **Install Certificate** and installing the root certificate into the Trusted Root Certification Authorities store.

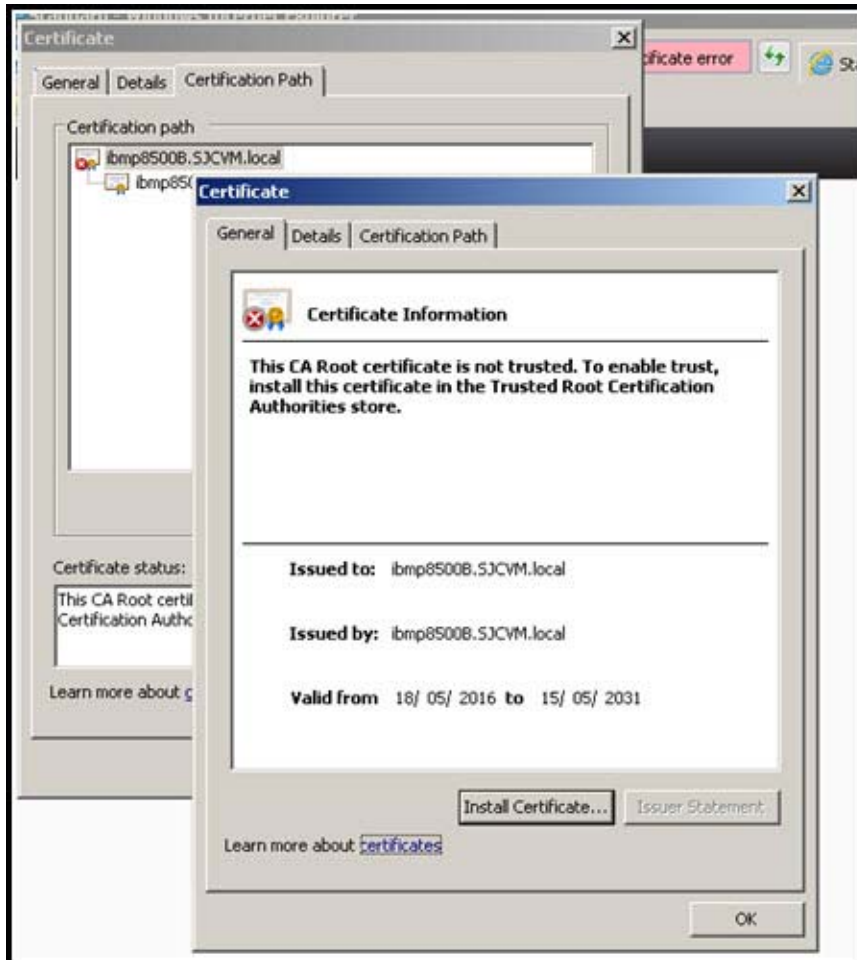


Figure 6. Clicking Install Certificate and installing the root certificate in the Trusted Root Certification Authorities store

Figure 7 shows the selection of the Trusted Root CA store.

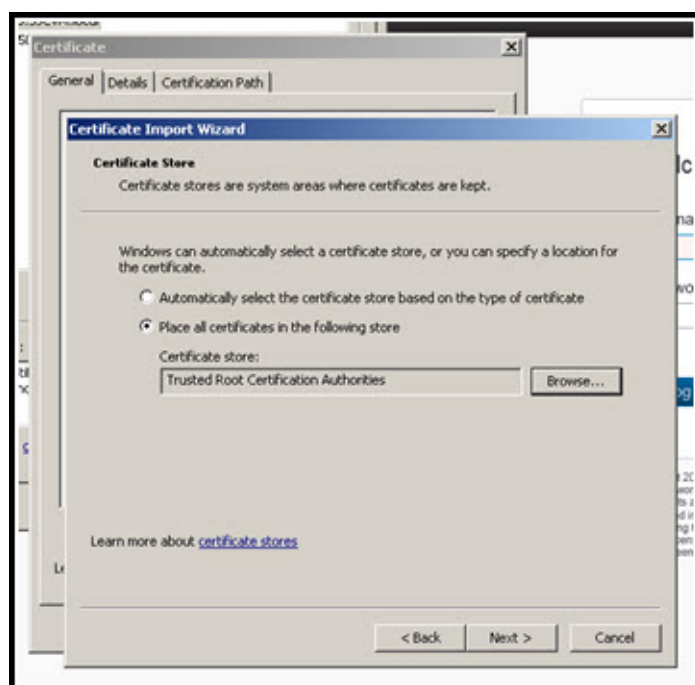


Figure 7. Choosing the option to store the certificate in the Trusted Root CA store

Figure 8 shows a successful trusted connection after restarting the browser.

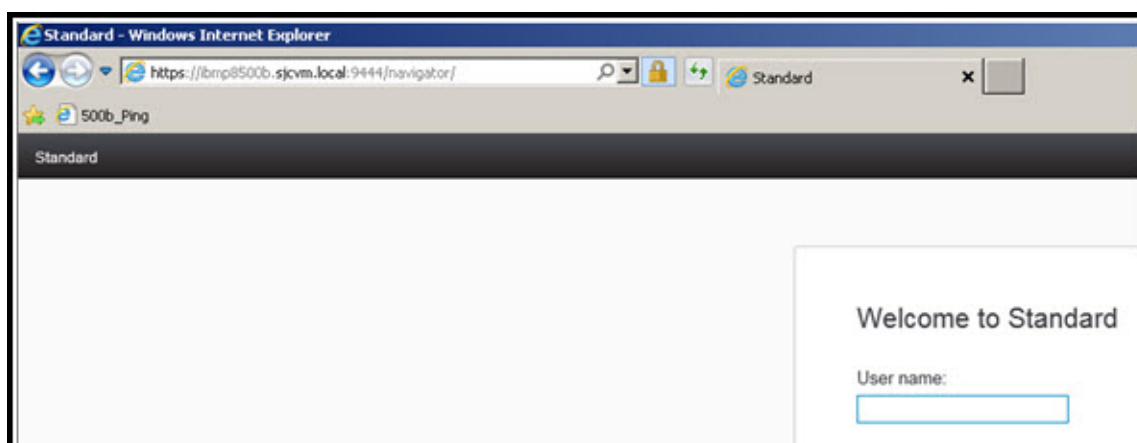


Figure 8. Restarting the browser, connecting to IBM Content Navigator, and checking that there are no certificate warnings

If the certificate is created for a named host, ensure that you use the same host name format for the host name in your IBM Content Navigator URL. If the certificate uses the host short name, your IBM Content Navigator URL must use the host short name. If the certificate uses the FQDN, your IBM Content Navigator URL must use the FQDN.

Configuring the Firefox browser

When using Firefox with an untrusted certificate, you see the window that is shown in Figure 9.

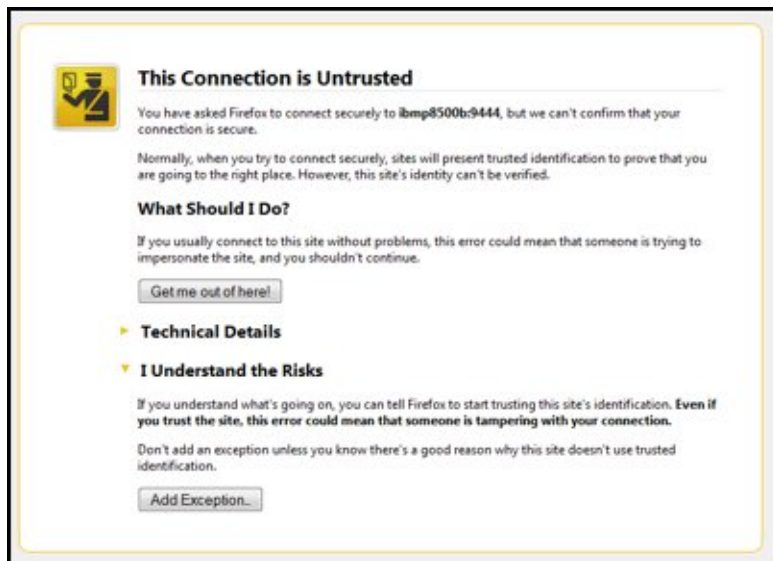


Figure 9. Example of an untrusted connection with Firefox

To configure the Firefox browser, complete the following steps:

1. Click **Add Exception**, and then in the window that opens, which is shown in Figure 10, click **Get Certificate**. Click **View**.

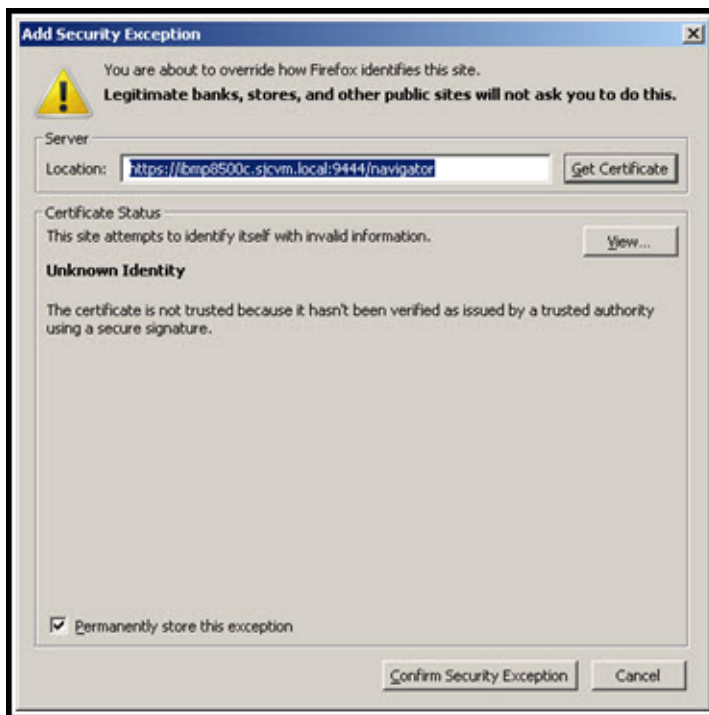


Figure 10. Firefox Security Exception window

-
2. In the Certificate Viewer, which is shown in Figure 11, click the **Details** tab and select the root certificate.

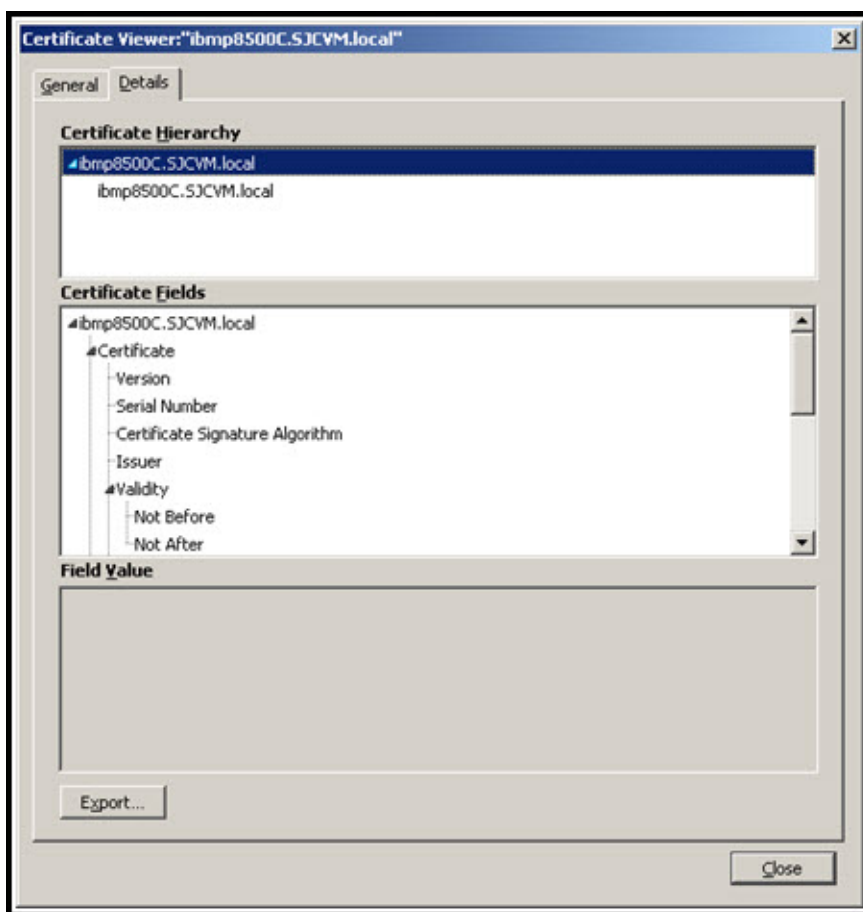


Figure 11. Firefox Certificate Viewer

-
-
3. Click **Export** at the lower left of the Certificate Viewer window (Figure 11).
4. Save the file with a `.crt` or `.pem` extension, then close the Certificate Viewer and Security exception windows. Open the Firefox Options menu, as shown in Figure 12.



Figure 12. Selecting the Firefox Options menu

5. Select **Advanced > Certificates > View Certificates** to access the Certificate Manager, as shown in Figure 13.

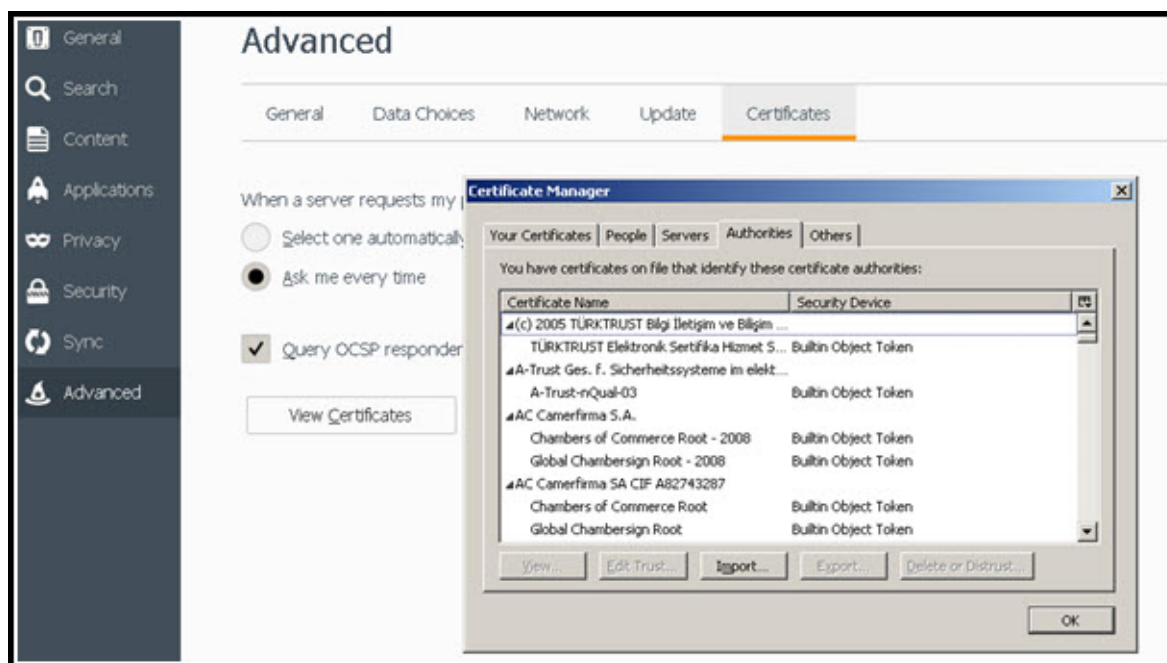


Figure 13. Firefox Certificate Manager

6. Select the **Authorities** tab and click **Import** to import the root certificate that was exported in step 3. Trust the CA certificate to identify websites.
7. Close and restart the browser, and reconnect to the IBM Content Navigator URL.
8. The connection should now be secure and trusted. Click the padlock icon to check the status.

Configuring the Chrome browser

To configure the Chrome browser, complete the following steps:

1. Click **Customize and Control Google Chrome** at the far right of the Chrome address bar and select **Settings**, as shown in Figure 14.

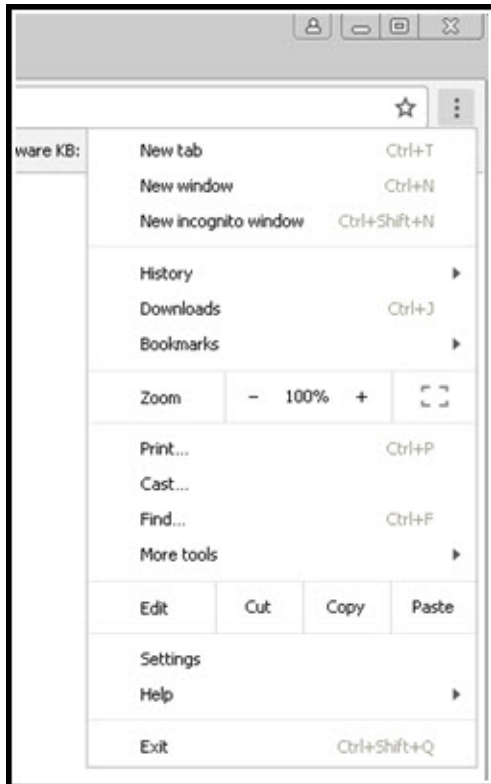


Figure 14. Selecting Settings

2. Type **certificates** into the search box in the Settings window, as shown in Figure 15.

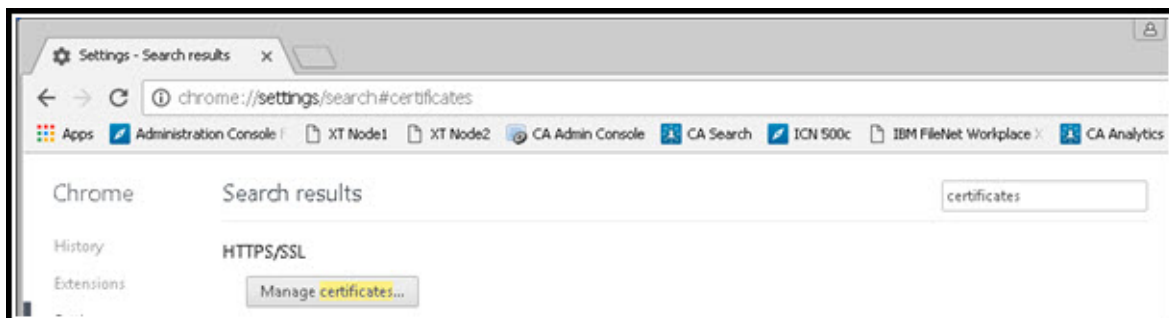


Figure 15. Managing certificates in Chrome

3. Click **Manage certificates**.

Chrome on a Windows PC uses the same local certificate store as Internet Explorer, so if you already imported your Trusted CA certificate for Windows Internet Explorer, it already is available to Chrome. If it is not available, you see what is shown in Figure 16 when you connect to IBM Content Navigator with Chrome.

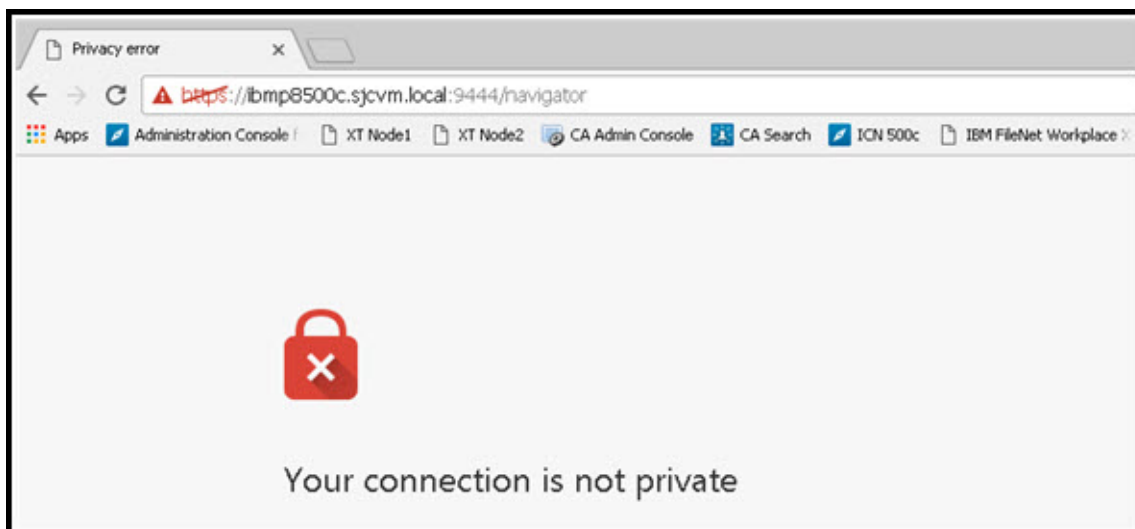


Figure 16. Untrusted connection in Chrome

Either use the earlier instructions for Internet Explorer to add the certificate, or use the following method:

Click the red triangle on the address bar, and then click **Details**. Figure 17 shows the information window that opens.



Figure 17. Chrome connection information window

After clicking **Details**, click **View certificate** in Security Overview. In the Certificate window, select the **Certification Path** tab, as shown in Figure 18.

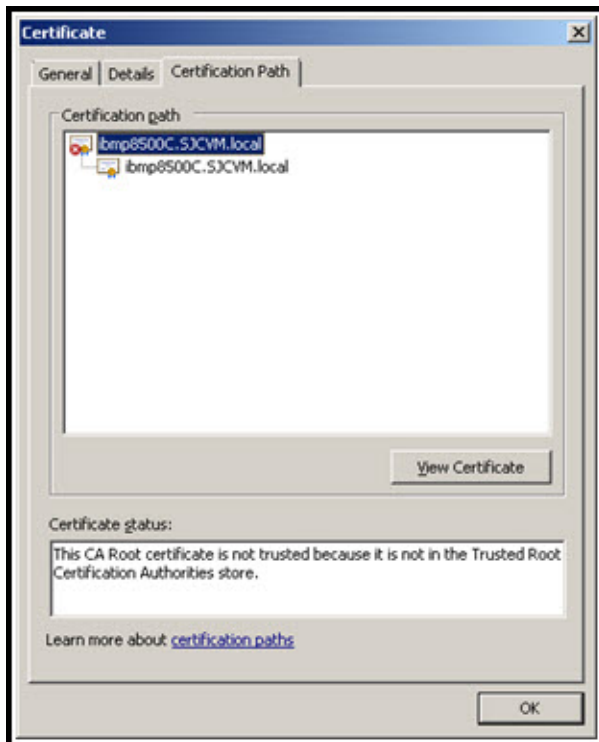


Figure 18. Chrome Certificate Viewer

Select the top-level root certificate and click **View Certificate**. Select the **Details** tab and then **Copy to file**. The Certificate Export Wizard window opens, as shown in Figure 19.



Figure 19. Chrome Certificate Export Wizard

Save the certificate file by clicking **Next**. Save the file with a `.cer` extension, as shown in Figure 20.

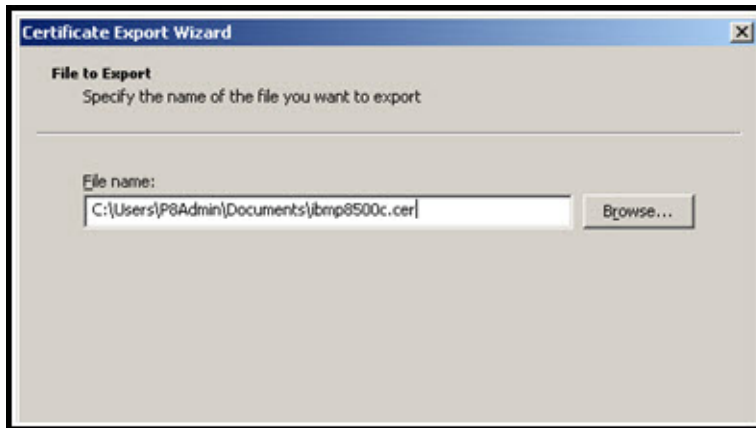


Figure 20. Saving the certificate from the Export Wizard

Click **Next** and then **Finish**. Close Chrome and start the Windows local certificate manager on the desktop by running `certmgr.msc`. Figure 21 shows an example of the certificate manager console window.

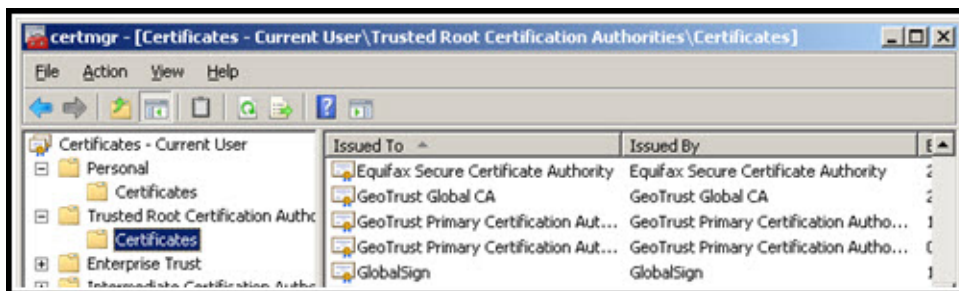


Figure 21. Microsoft Certificate Manager Console

- Expand the **Trusted Root Certification Authorities** folder, right-click the **Certificates** folder, and select **Import**, as shown in Figure 22.

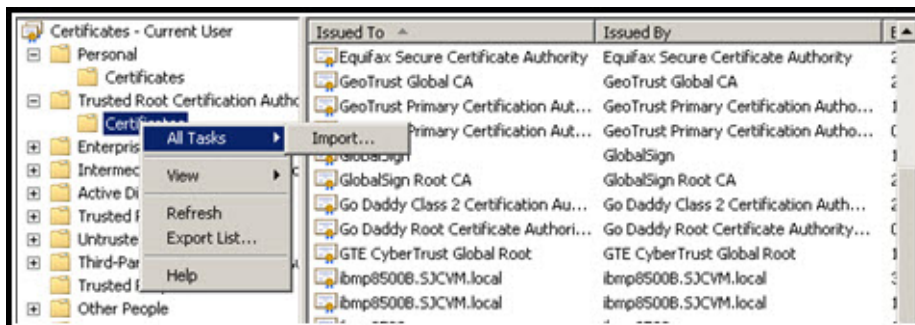


Figure 22. Selecting the Import option

5. Import the .cer file that was exported in step 3 (Figure 23).

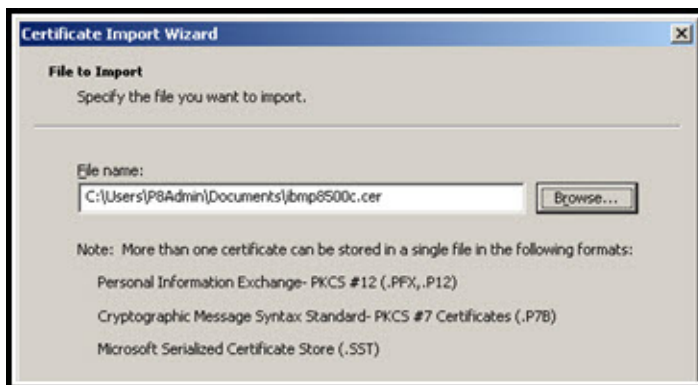


Figure 23. Selecting the certificate file that you want to import

6. Click **Next** and save the certificate in the Trusted Root CA store, as shown in Figure 24.



Figure 24. Saving the certificate in the Trusted Root Certification Authorities store

7. Click **Next** and then **Finish**.

8. To complete the import, accept the security message by clicking **Yes** if prompted with a window that is similar to Figure 25.



Figure 25: Complete the installation of the root certificate

Some versions of Chrome might report an obsolete encryption method. Despite this warning, the connection is still secure and you can continue with Box integration. For more information about how Google Chrome evaluates secure connections in the Chrome browser, see the following website:

<https://www.google.com/transparencyreport/https/faq/#modernconfig>

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 June 30, 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/tips1351.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.

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.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Other company, product, or service names may be trademarks or service marks of others.