Link-OS™
Profile Manager

Installation Guide

ZEBRA TECHNOLOGIES

P1065697-002

Proprietary Statement This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies Corporation.

Product Improvements Continuous improvement of products is a policy of Zebra Technologies Corporation. All specifications and designs are subject to change without notice.

Liability Disclaimer Zebra Technologies Corporation takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies Corporation reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability In no event shall Zebra Technologies Corporation or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies Corporation has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Contents

Notes •

About This Document

This section provides you with contact information, document structure, and organization.

Contents

Who Should Use This Document

This is intended for use by any person who needs to perform routine maintenance, upgrade, or troubleshoot problems with the printer.

How This Document Is Organized

The is set up as follows:

Section	Description
Installation on page 9	This chapter includes the procedure to install Profile Manager.
Adding the Zebra Certificate Authority on page 63	This chapter includes the procedure to add the Zebra Certificate Authority to the Trusted Root Certifications Authorities Store.
Changing Permissions on page 93	This chapter includes the procedure to change permissions to allow the Zebra Certificate Authority (CA) successfully.
Getting Started Using Profile Manager on page 97	This chapter provides an overview and description of the steps necessary to set up and begin to use Profile Manager. For additional details, please see the help system contained within the Profile Manager application.

Document Conventions

The following conventions are used throughout this document to convey certain information.

Alternate Color (online only) Cross-references contain hot links to other sections in this guide. If you are viewing this guide online in.pdf format, you can click the cross-reference (blue text) to jump directly to its location.

Command Line Examples Command line examples appear in `Courier New` font. For example, type `ZTools` to get to the Post-Install scripts in the `bin` directory.

Files and Directories File names and directories appear in `Courier New` font. For example, the `Zebra<version number>.tar` file and the `/root` directory.

Icons Used

Important • Advises you of information that is essential to complete a task.

Note • Indicates neutral or positive information that emphasizes or supplements important points of the main text.

Example • Provides an example, often a scenario, to better clarify a section of text.

Notes •

Installation

This chapter includes the procedure to install Profile Manager.

Contents

System Requirements

Supported Operating Systems

Windows:

- 64-bit Windows 7 or Windows Server 2008 R2
  - Tomcat version 7.0.42 64-bit for Windows: http://www.us.apache.org/dist/tomcat/tomcat-7/v7.0.42/bin/apache-tomcat-7.0.42-windows-x64.zip
  - Java Virtual Machine (JVM) Version 6.0.43 Download: http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-javase6-419409.html#jre-6u43-oth-JPR
    - You must accept the license agreement.
    - For Windows 64-bit, choose: Windows x64 (11MB) jre-6u43-windows-x64.exe

Linux:

- 64-bit Red Hat Enterprise Linux version 6.4 and higher
  - Tomcat version 7.0.42 Core for Linux: http://www.us.apache.org/dist/tomcat/tomcat-7/v7.0.42/bin/apache-tomcat-7.0.42.zip
  - Java Virtual Machine (JVM) Version 6.0.43 Download: http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-javase6-419409.html#jre-6u43-oth-JPR
    - You must accept the license agreement.
    - For Linux 64-bit choose: Linux x64 (19.82 MB) jre-6u43-linux-x64-rpm.bin

Browsers

- Chrome browser version 29 and higher
- Internet Explorer version 10 and higher

Before You Begin

1. Which operating system are you installing?

If you are installing...	Then
Windows OS	Continue with *Installation for Windows*.
Linux OS	Go to *Installation for Red Hat Enterprise Linux* on page 37.

Installation for Windows

1. Install Java JRE version 6. For more details about how to install Java for Windows, go to http://www.java.com/en/download/help/download_options.xml#windows

2. Once Java is installed, the JRE_HOME environment variable needs to be set.

Note • The CATALINA_OPTS environment variable change listed here is recommended based upon a 50 user, 500 printer configuration. As more printers or users are required the individual memory values may need to be adjusted. Please contact your Reseller for details on how to do this.

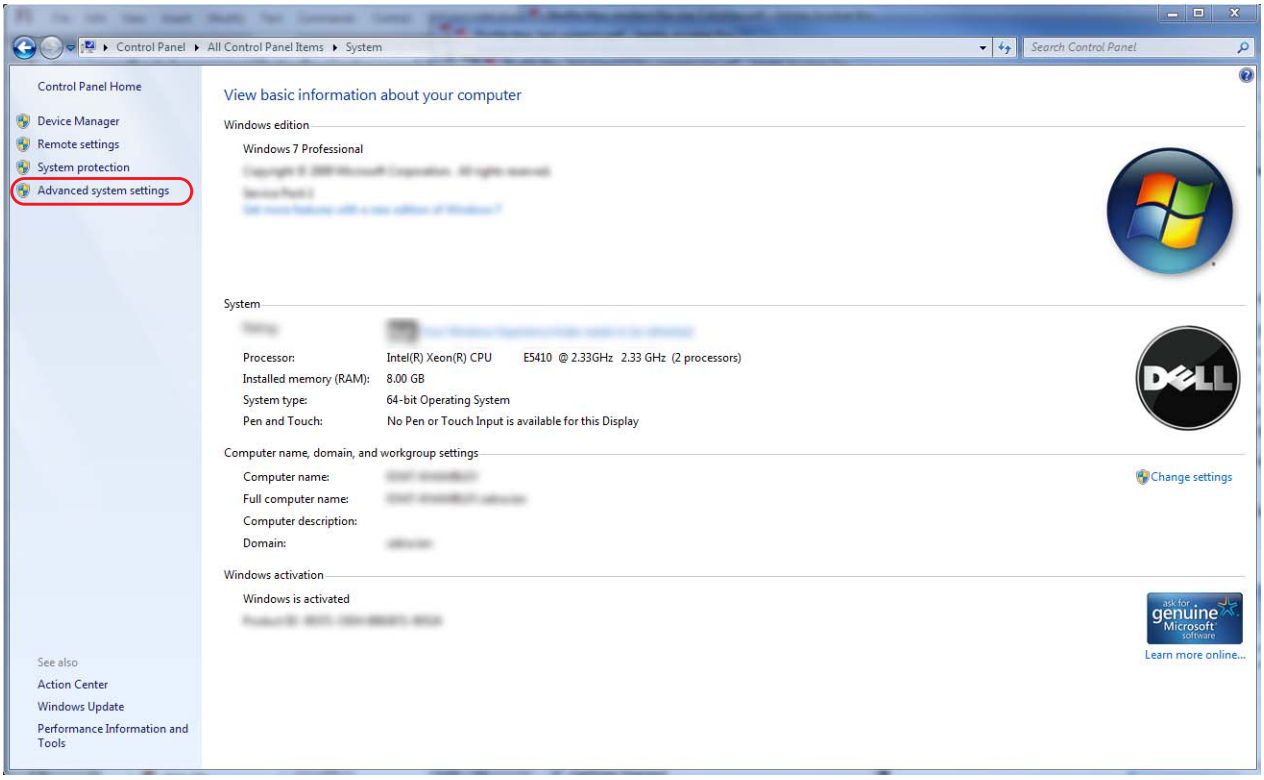
Note • A 64-bit Java Virtual Machine (JVM) is required to support the CATALINA_OPTS parameters.

a. Open the Control Panel.

b. Select **System**.

c. See Figure 1. Click on **Advanced system settings**.

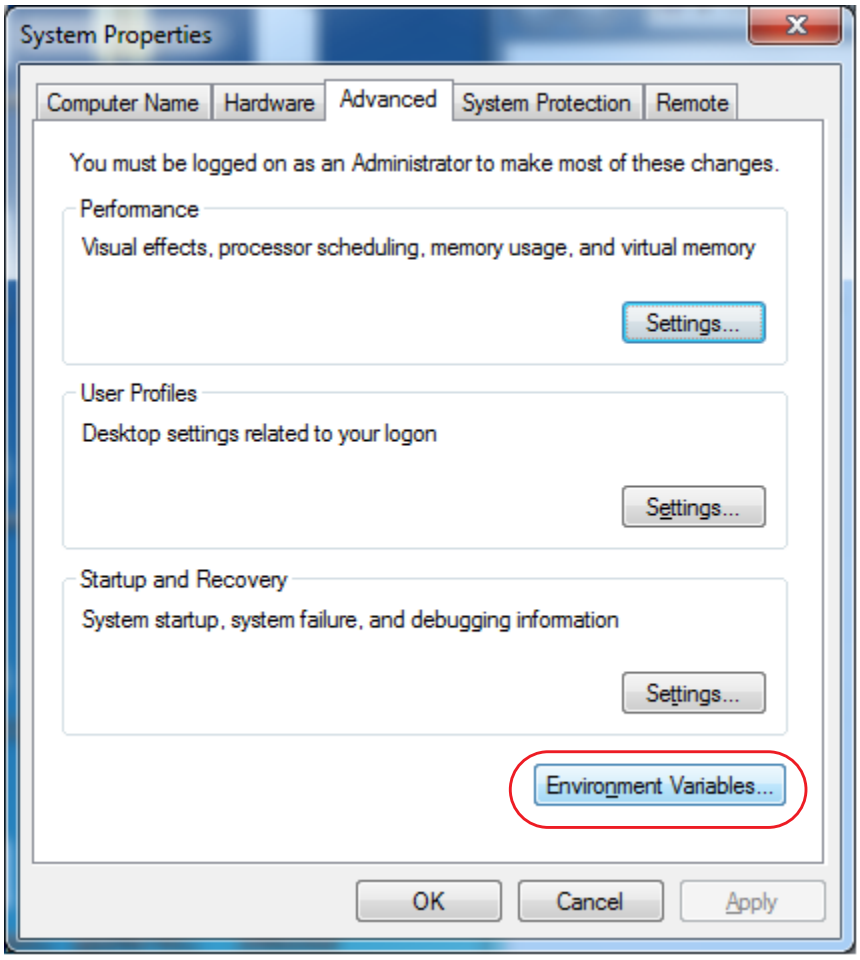
Figure 1 • Control Panel > System



d. See Figure 2. Click on the **Advanced** tab.

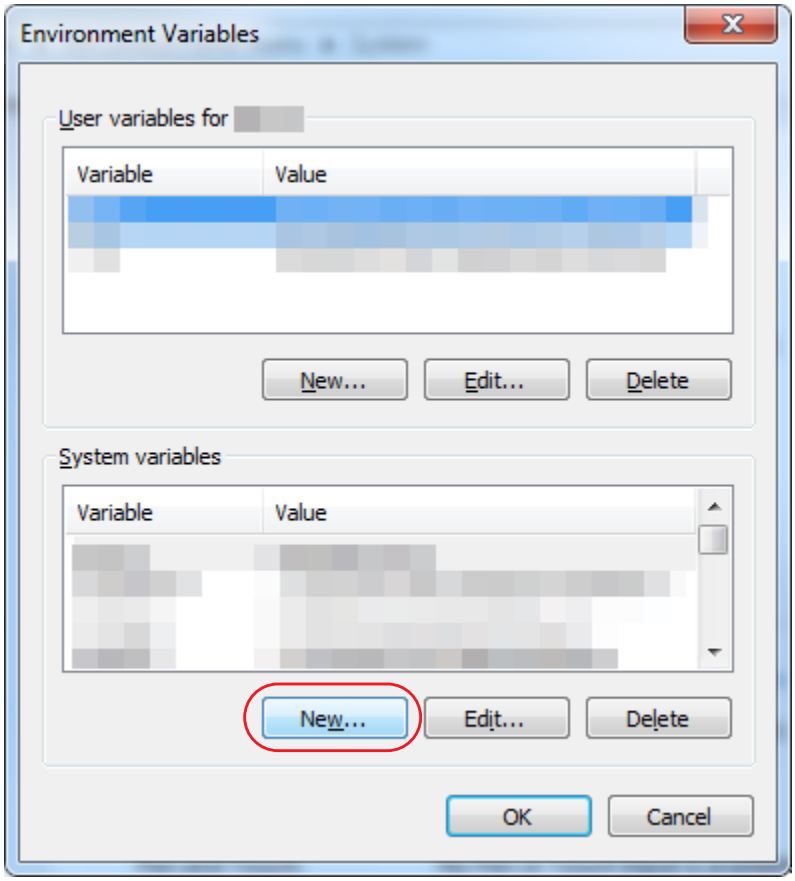
e. Click on **Environment Variables**.

Figure 2 • Advanced Tab



f. See Figure 3. To create a new environment variable under System variables, click on **New...**.

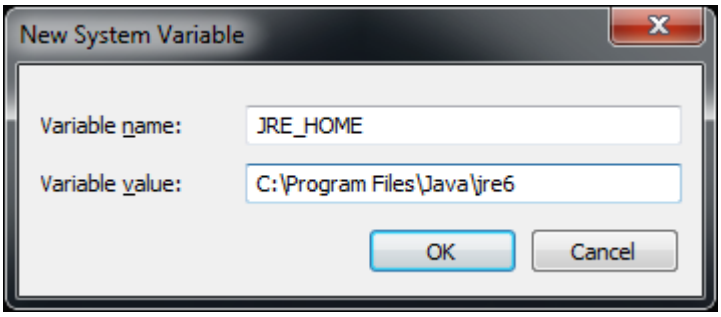
Figure 3 • Environment Variables Dialog



g. See Figure 4. Enter the Variable name and Variable value shown below in the appropriate boxes.

Note • When entering the variable name and variable value, do not enter surrounding quotes.

Figure 4 • New System Variable

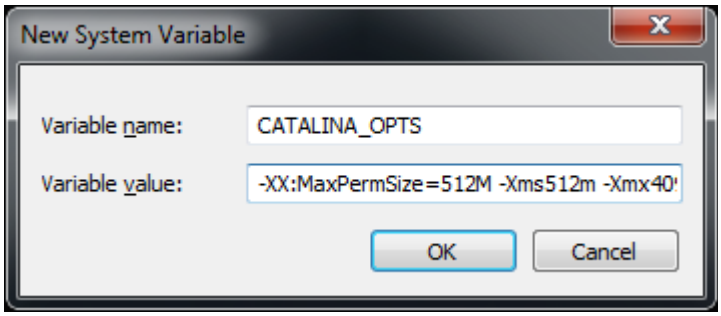


h. See Figure 3. To create a new environment variable under System variables, click on **New...**.

i. See Figure 5. Enter the Variable name and Variable value in the appropriate boxes. Variable value should be set to:
`-XX:MaxPermSize=512M -Xms512m -Xmx4096m`

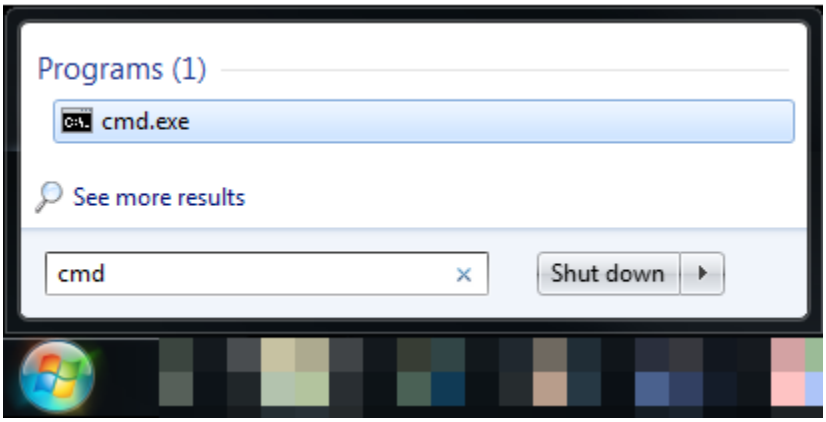
Note • When entering the variable name and variable value, do not enter surrounding quotes.

Figure 5 • Setting the CATALINA_OPTS Environment Variable



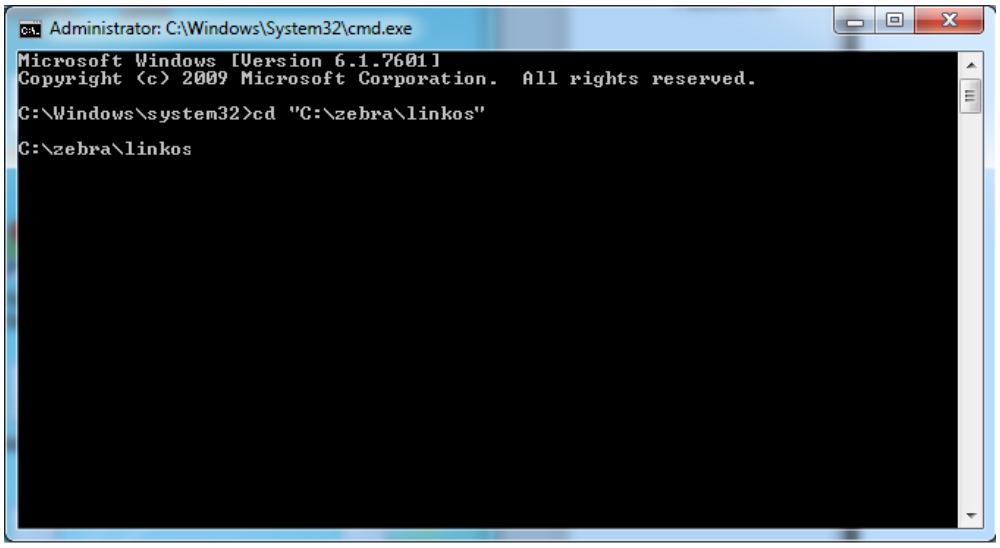
3. Download the Zebra Link-OS Application Server zip file: www.zebra.com/profilemanager
4. Extract the Zebra Link-OS Application Server zip file contents to: `C:\zebra\linkos`
5. Download the Tomcat zip file: http://www.us.apache.org/dist/tomcat/tomcat-7/v7.0.42/bin/apache-tomcat-7.0.42-windows-x64.zip
6. Extract the Tomcat zip to `C:\zebra\linkos\tomcat`
7. See Figure 6. Open a command prompt.

Figure 6 • Command Prompt



8. See Figure 7. Change the current directory to the `C:\zebra\linkos`

Figure 7 • Change Directory from Command Line



9. See Figure 8 and Figure 9. The JVM Certificate Authority keystore must be updated in order to trust the Zebra Weblink Certificate Authority and the GeoTrust™ Subordinate CA.

Note • Omitting or incorrectly performing this step could lead to several issues.

- If the GeoTrust certificate is not added, it will not be possible to successfully register the product and will prevent printers from being connected.
- If the ZebraCAChain certificate is not added correctly, the printer will not be able to connect successfully.

To update the keystore, execute the following keytool command (running command prompt as admin).

```
"%JRE_HOME%\bin\keytool.exe" -importcert -file ZebraCAChain.cer ^
-keystore "%JRE_HOME%\lib\security\cacerts" -alias "ZebraCAChain"
```

Note • The default keytool password is *changeit*

Figure 8 • Add ZebraCAChain to Keystore

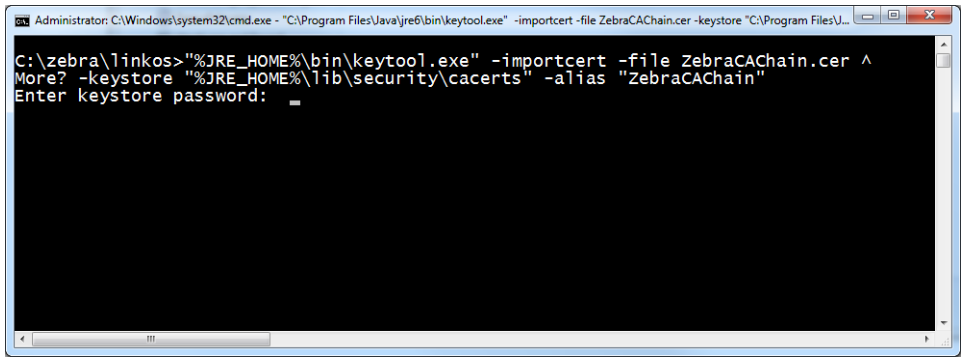
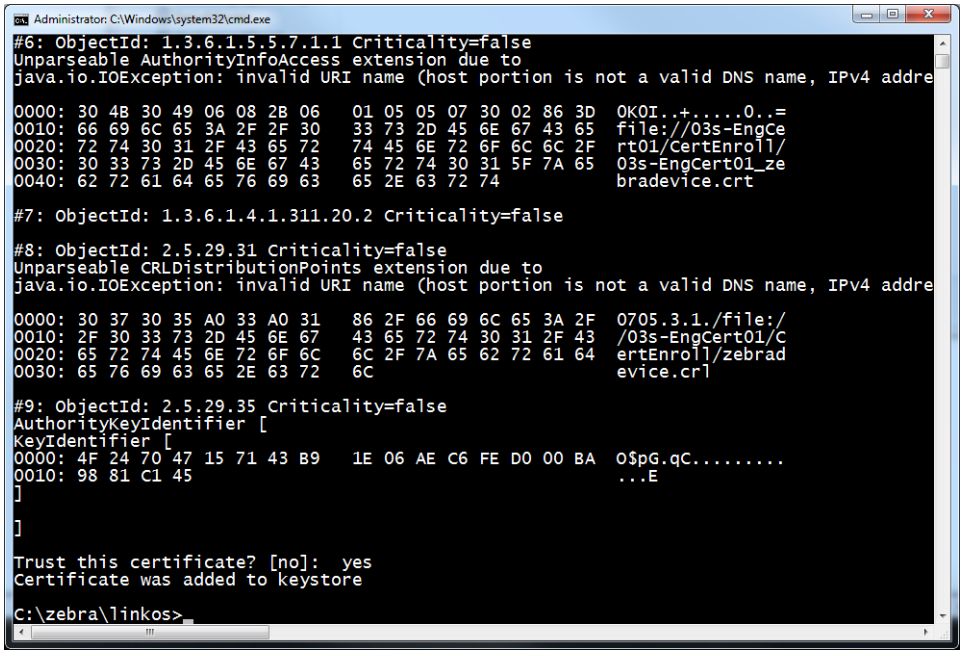


Figure 9 • Confirm Certificate



a. See Figure 10. To update the keystore, execute the following keytool command (running command prompt as admin).

```
"%JRE_HOME%\bin\keytool.exe" -importcert -file ^
GeoTrustSSLCA.cer -keystore ^
"%JRE_HOME%\lib\security\cacerts" -alias "GeoTrustSSLCA"
```

Note • The default keytool password is *changeit*

Figure 11 shows the results after the keystore is updated.

Figure 10 • Add GeoTrustSSLCA to Keystore

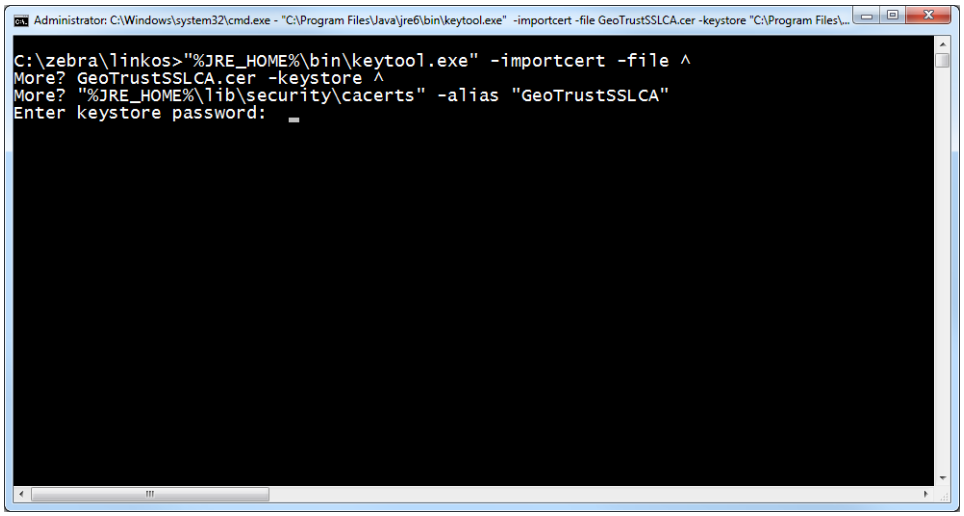
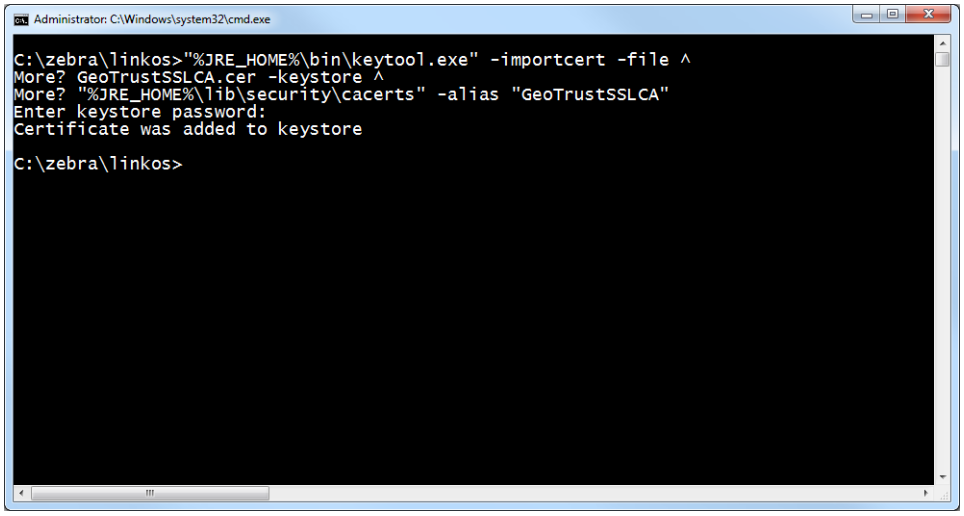


Figure 11 • Successful Addition to Keystore



10. See Figure 12. Verify the certificates were correctly installed by entering the following command:

```
"%JRE_HOME%\bin\keytool.exe" ^
-keystore "%JRE_HOME%\lib\security\cacerts" ^
-alias "ZebraCAChain" -list
```

a. Enter keystore password (default password is *changeit)*.
The console will show the following:
`ZebraCAChain, Feb 18, 2013, trustedCertEntry,`
Certificate fingerprint (MD5):
ED:D2:75:F3:84:5E:32:E7:82:5A:3C:4D:1A:B4:73:2C

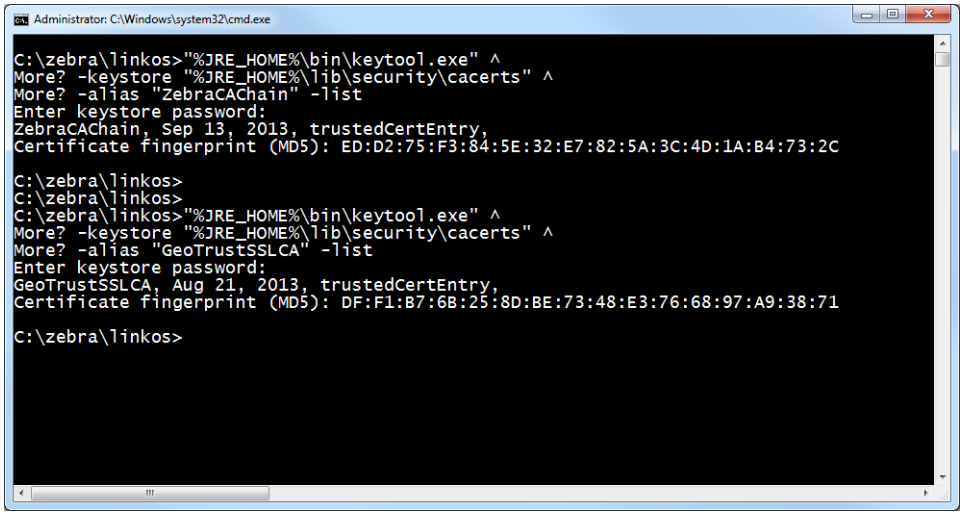
b. Enter the following command:

```
"%JRE_HOME%\bin\keytool.exe" ^
-keystore "%JRE_HOME%\lib\security\cacerts" ^
-alias "GeoTrustSSLCA" -list
```

c. Enter keystore password (default password is *changeit)*.
The console will show the following:

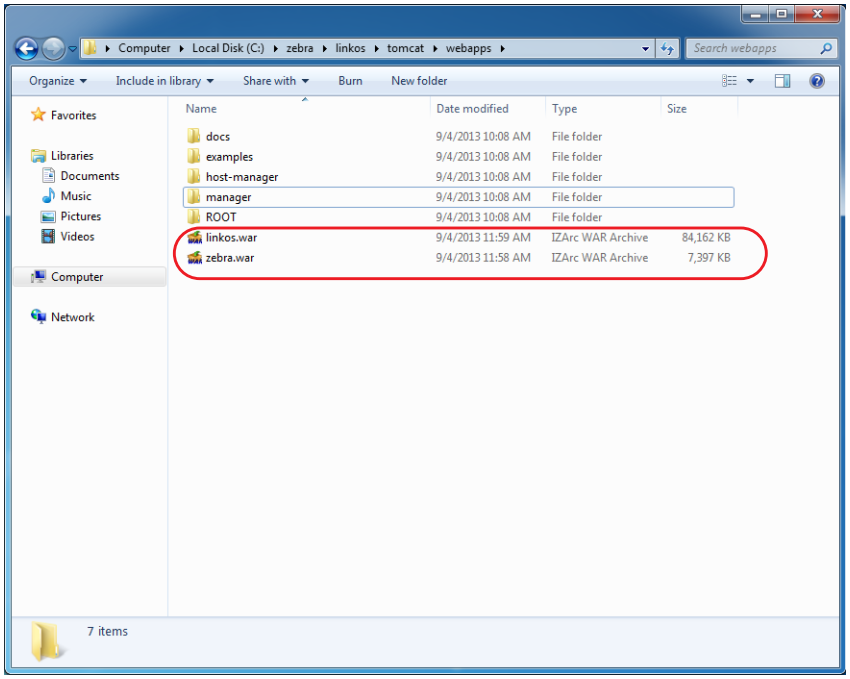
```
GeoTrustSSLCA, Aug 5, 2013, trustedCertEntry,
Certificate fingerprint (MD5):
DF:F1:B7:6B:25:8D:BE:73:48:E3:76:68:97:A9:38:71
```

Figure 12 • Verifying the Certificate Installation



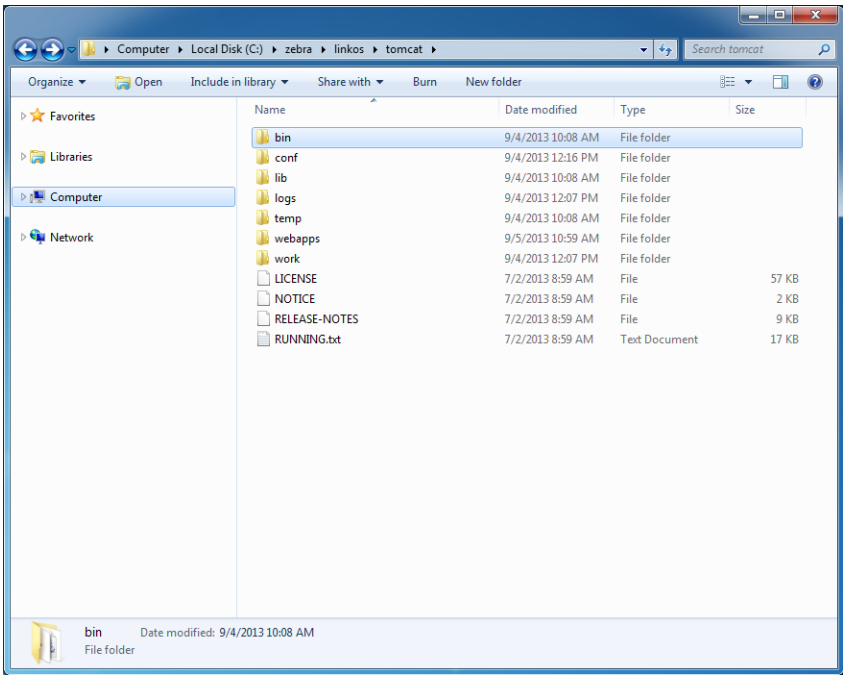
11. See Figure 13. Copy the `zebra.war` and `linkos.war` files from the into the `C:\zebra\linkos\tomcat\webapps` directory.

Figure 13 • Webapps Directory for Tomcat



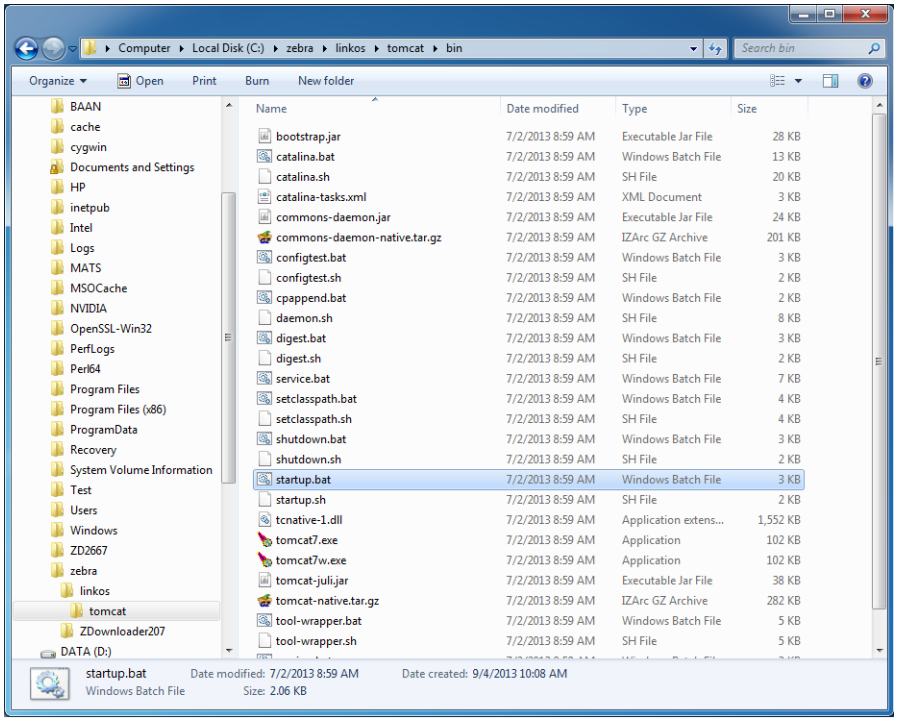
12. See Figure 14. Navigate to the `C:\zebra\linkos\tomcat\bin\` folder.

Figure 14 • C:\Tomcat\bin Directory



a. See Figure 15. Start the Tomcat server by double-clicking on `startup.bat`.

Figure 15 • Startup.bat File for Tomcat

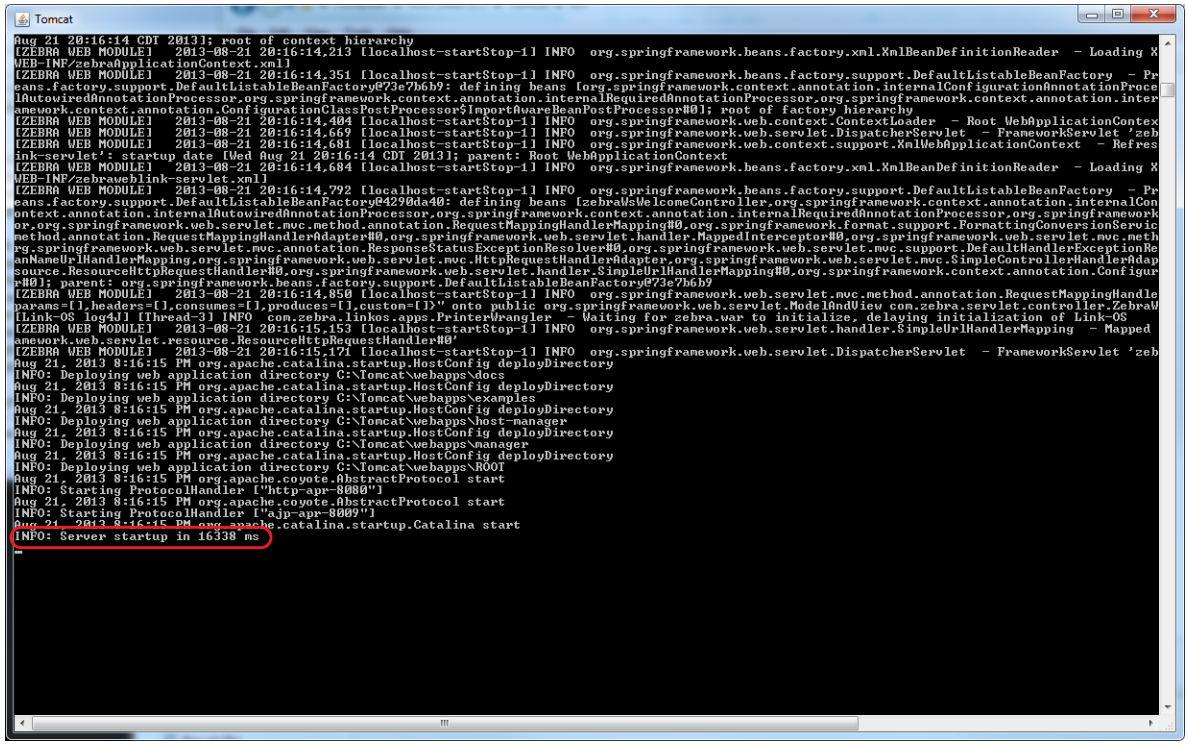


13. See Figure 16. Verify that Tomcat started correctly.

a. Look for the line that starts:

```
INFO: Server startup in xxxxx ms
```

Figure 16 • Tomcat Server Start



14. See Figure 17. Open a web browser to: http://localhost:8080/linkos/register.

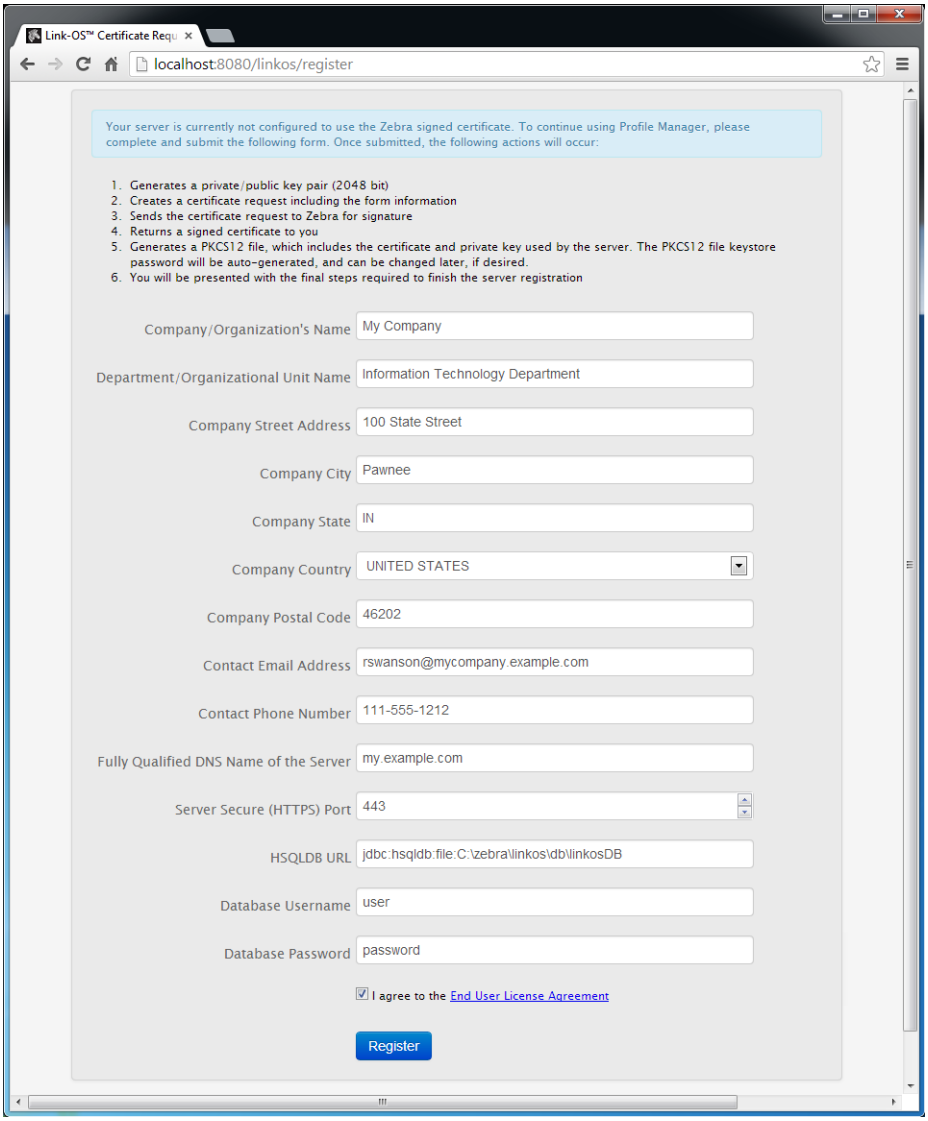
15. See Figure 17. Fill in the registration form completely.

Note • The entry in the **Company Street Address** field must be limited to 30 characters.

a. Read and check the box to accept the End User License Agreement.

Note • The port specified will be the SSL port used by printers and browsers to securely connect to your server. Confirm that it is not currently in use (by your server) or ask your IT department to confirm.

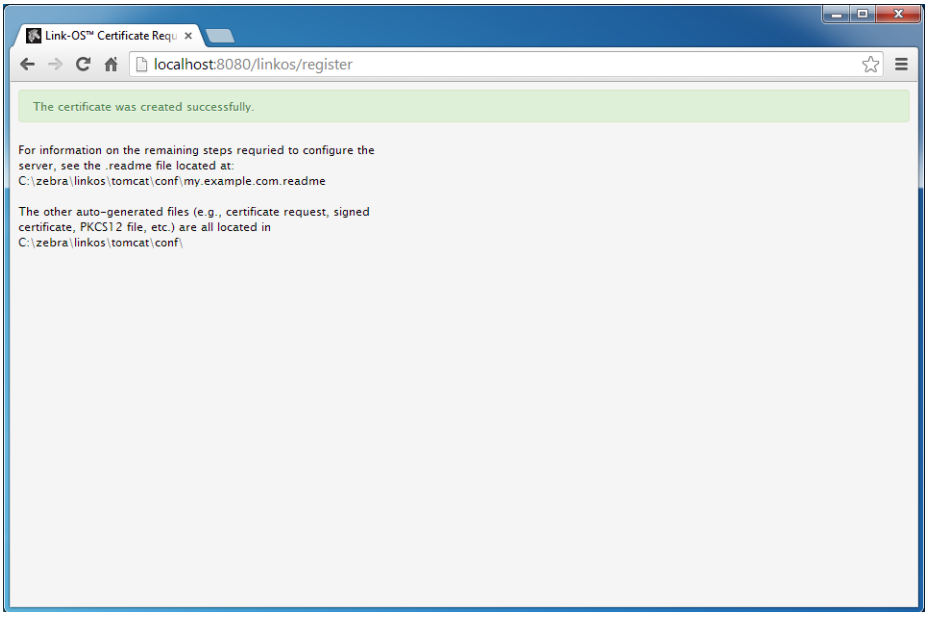
Figure 17 • Registration Form



b. Click **Register**.

See Figure 18. The registration is successfully completed and your SSL certificate has been created.

Figure 18 • Registration Successful



16. See Figure 19 and Figure 20. Using a text editor, like Notepad, open the specified `.readme` instructions file in the `C:\zebra\linkos\tomcat\conf\` directory.

Figure 19 • Directory for Readme File

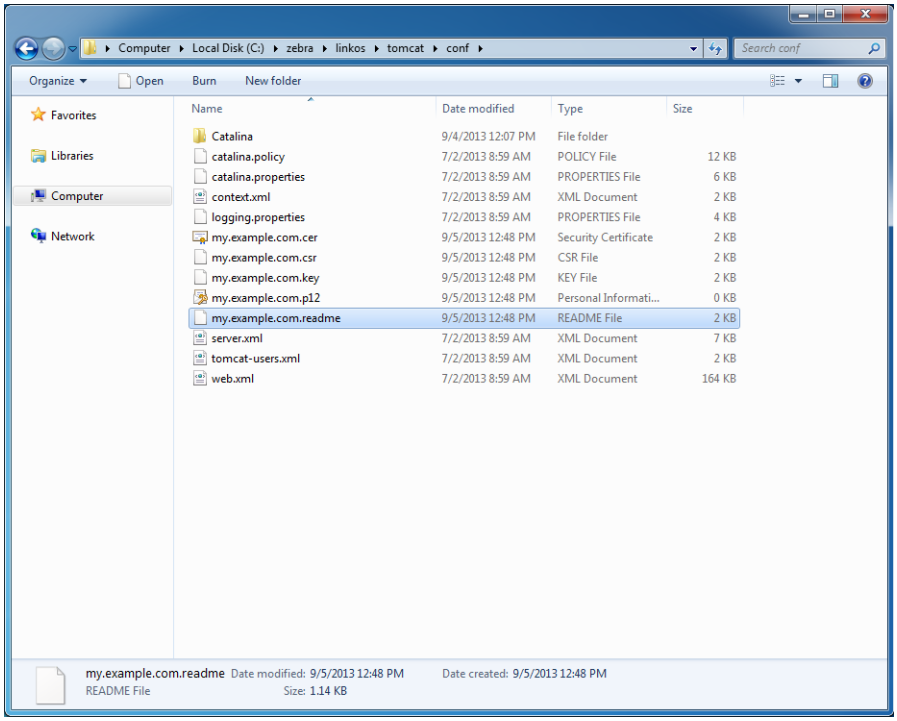
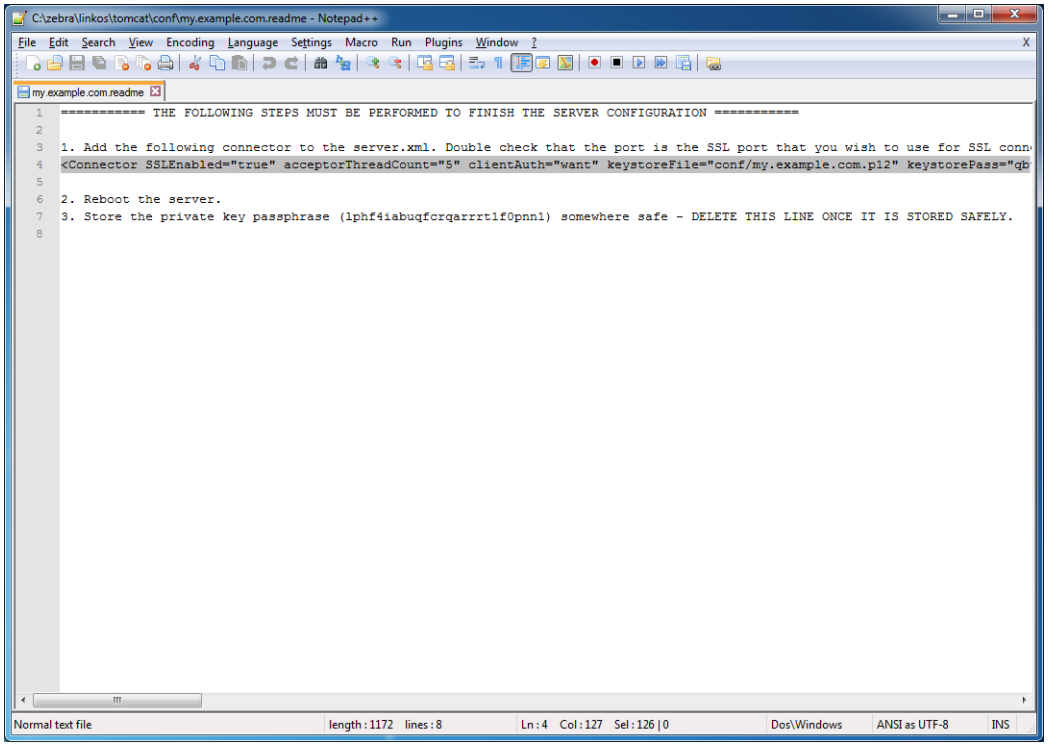


Figure 20 • Readme File Contents



17. Copy line 4 (highlighted in Figure 20).

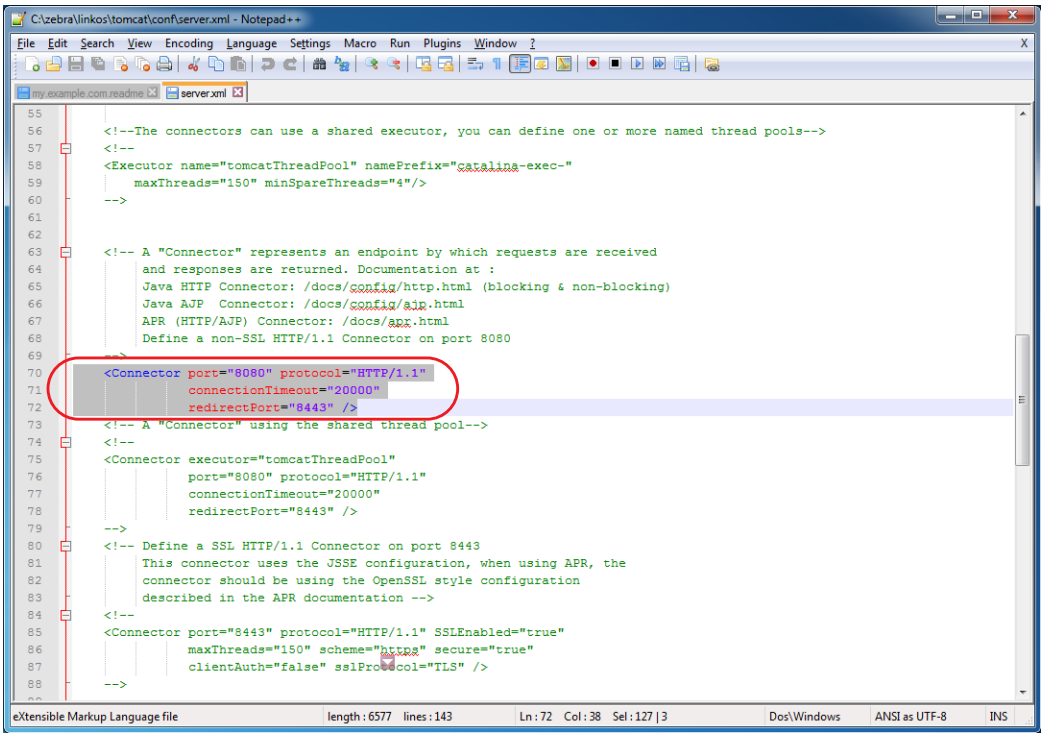
    The auto-generated connector is the configuration for the HTTPS port that printers and browsers will use to connect to your server.

18. See Figure 21. Open the `server.xml` file located in `C:\zebra\linkos\tomcat\conf\.`

19. See Figure 21. Locate the Connector xml element that looks as follows:

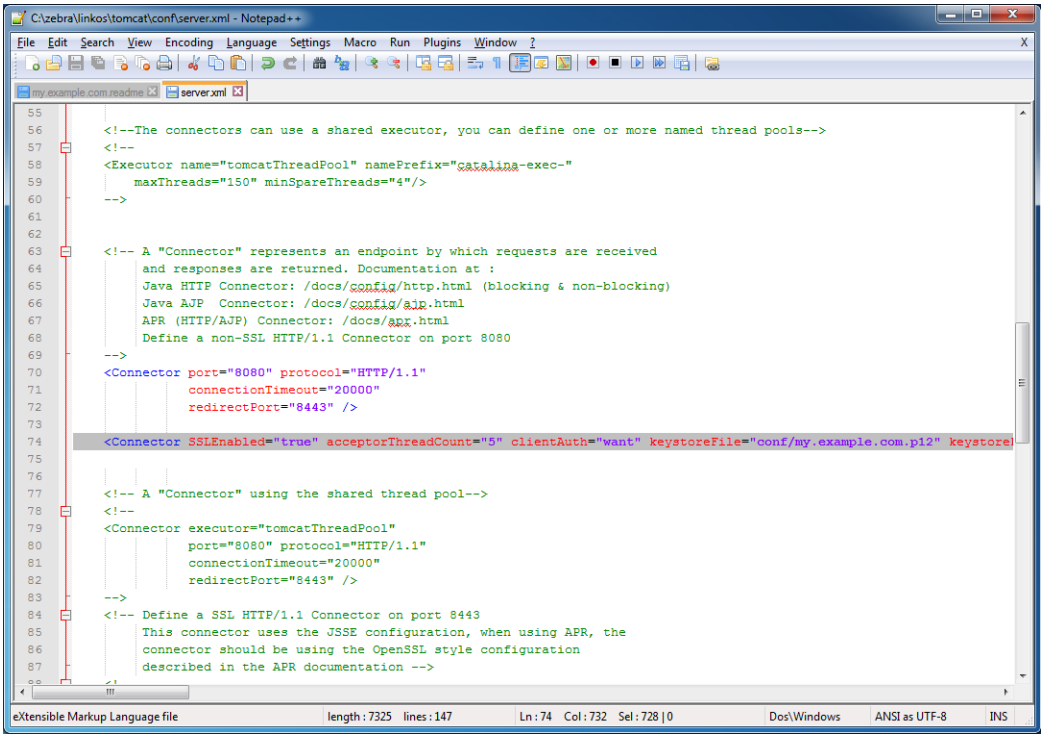
<Connector connectionTimeout="20000" port="8080" protocol="HTTP/1.1" redirectPort="8443"/>

Figure 21 • Locate the Connector Element in the server.xml File



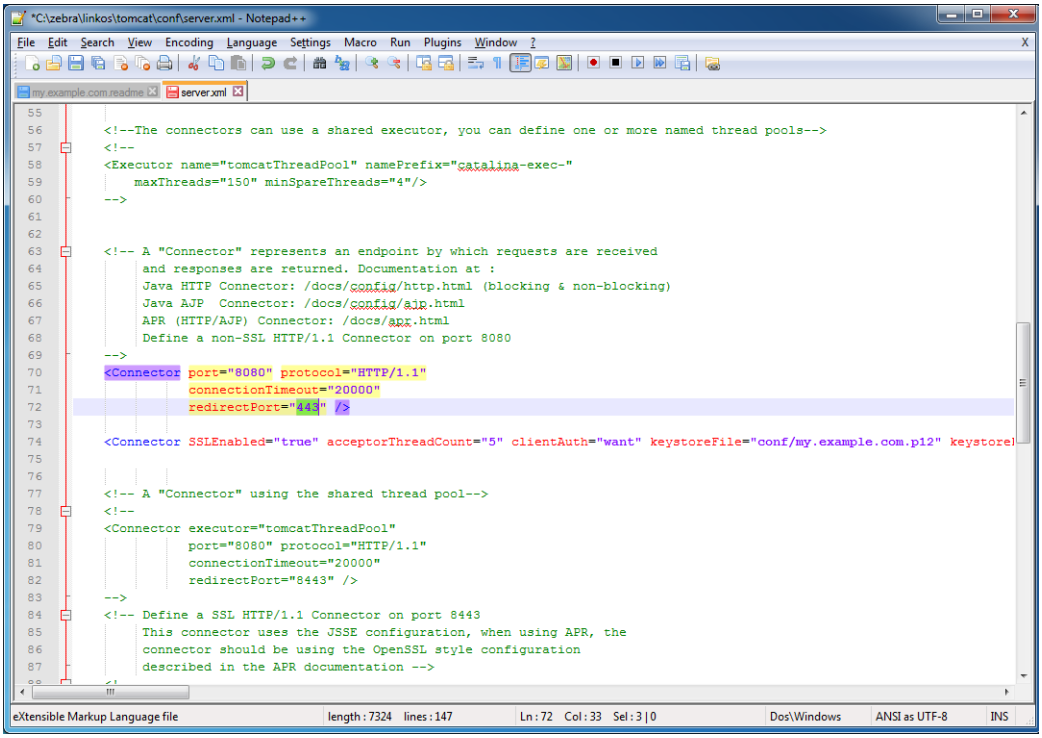
20. See Figure 22. Paste the contents of the clipboard (copied in step 17) after the line located in step 19.

Figure 22 • SSL Connector Added to server.xml File



a. See Figure 23. Change `redirectPort="8443"` to `redirectPort="443"` (The default value is 443. The redirect port should match the value specified in step 15).

Figure 23 • Change the Redirect Port Attribute



21. Close the Tomcat console window.

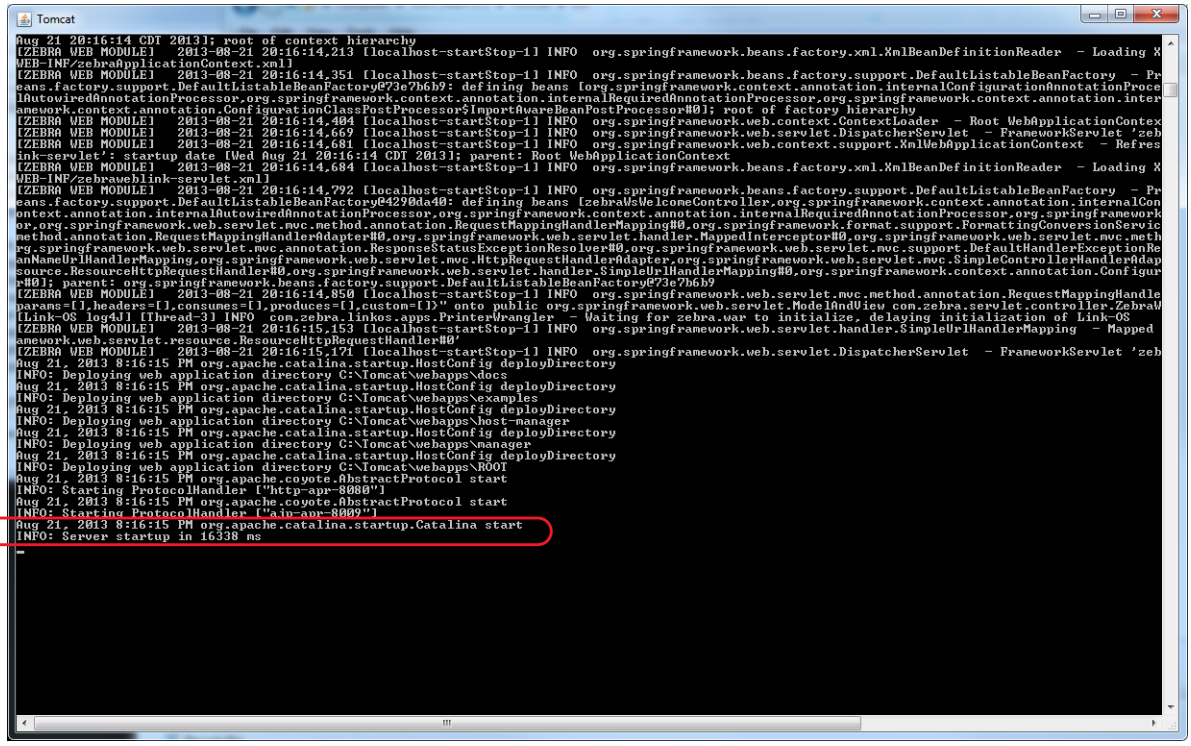
22. See Figure 24. Start the Tomcat server by double-clicking on `startup.bat`.

Note • This will start the web application. In the future, when your server is rebooted, the application will not automatically restart.

If you require the application to start automatically when the server is rebooted, you can use the Windows Task Scheduler to run the `startup.bat` and `shutdown.bat` scripts at the appropriate times. Alternatively, you can use the Tomcat Windows Service Installer package.

For assistance with this, please contact your IT organization, or Zebra Development Services at DevelopmentServices@zebra.com.

Figure 24 • Tomcat Server Start



23. Open the Chrome browser and go to https://localhost/linkos/.

Note • If the port is something other than 443, it must be specified (e.g., https://localhost:4443/linkos).

24. Which browser are you using?

If you are using a(n)…	Then…
Chrome browser	**a.** See Figure 25. Click on **Proceed anyway.** **b.** To avoid this message in the future, please see *Adding the Zebra Certificate Authority* on page 63.
Internet Explorer	**a.** See Figure 26. Click on **Continue to this website (not recommended).** **b.** To avoid this message in the future, please see *Adding the Zebra Certificate Authority* on page 63.

Figure 25 • Site Security Certificate for Chrome

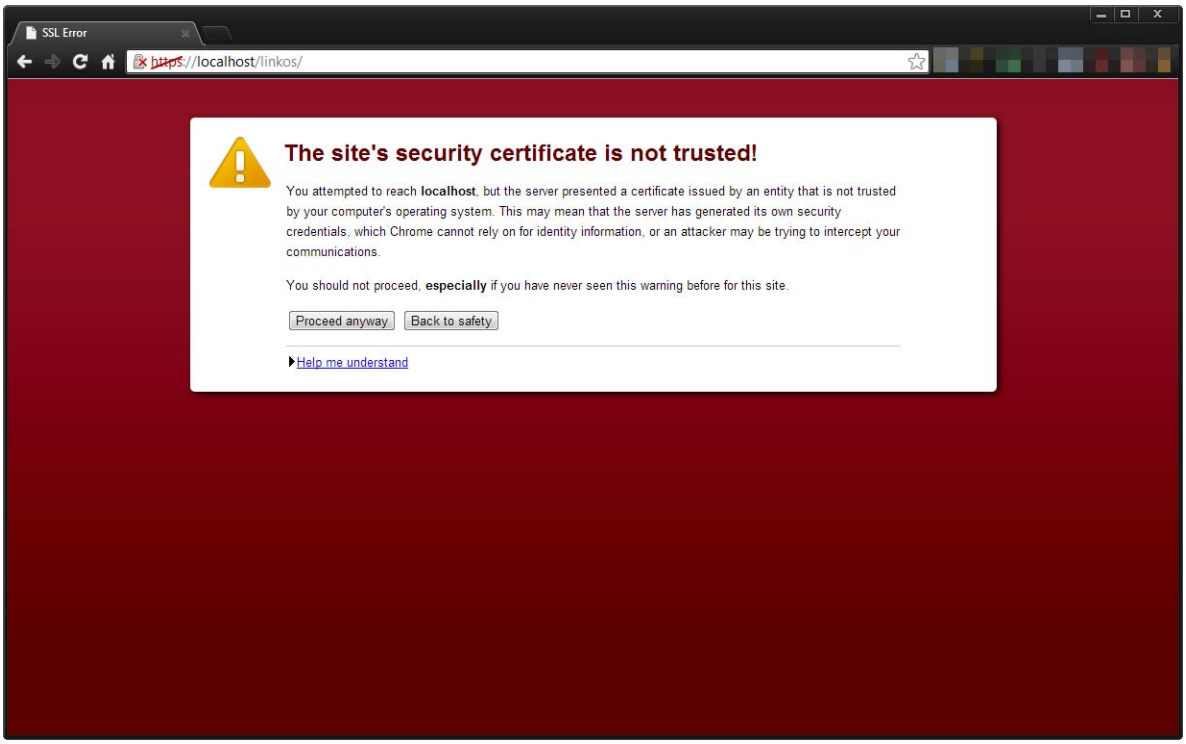
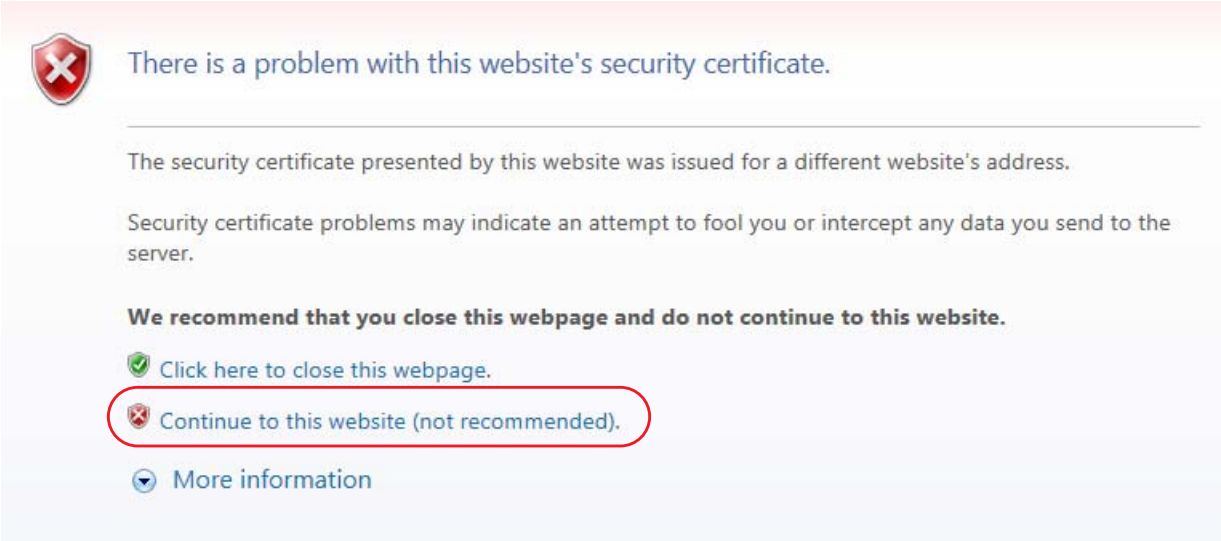


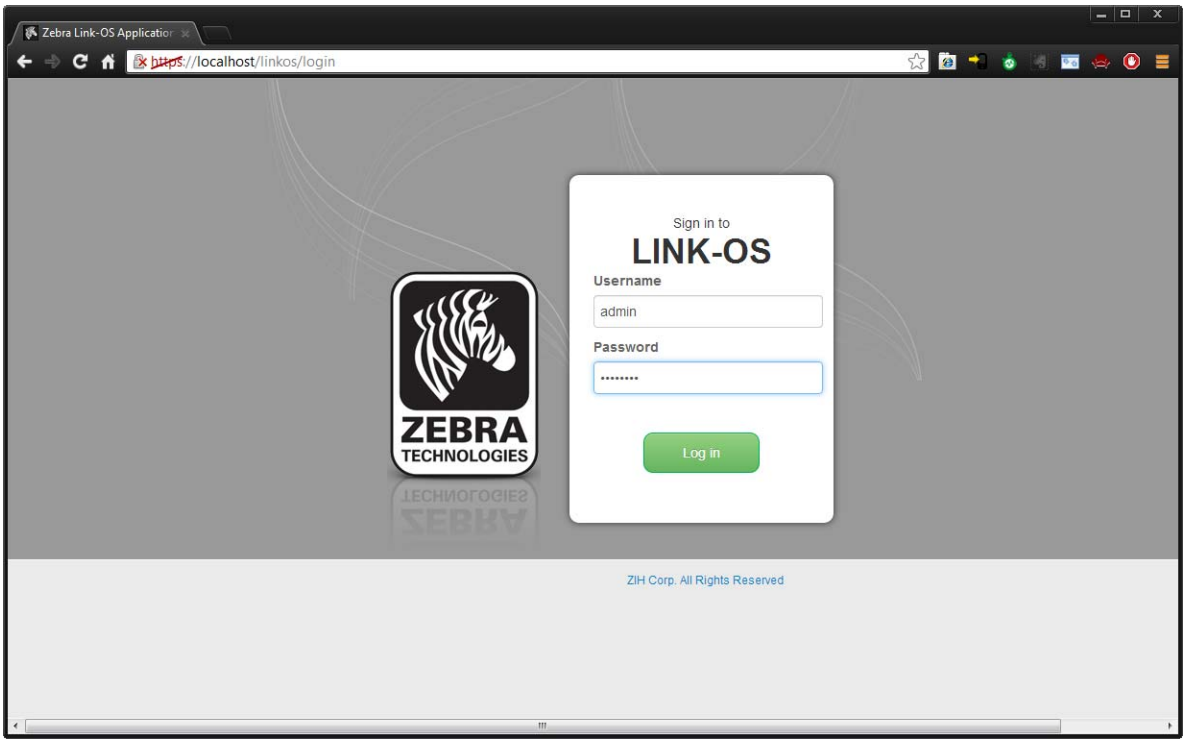
Figure 26 • Site Security Certificate for Internet Explorer



25. See Figure 27. Log into the Link-OS Application Server.

Note • The default username is *admin* and the default password is *password*.

Figure 27 • Login Screen



26. The first time you log into the Link-OS Application Server, change your password. Go to **User and Settings** > **Change password**.

Installation for Red Hat Enterprise Linux

Before You Begin

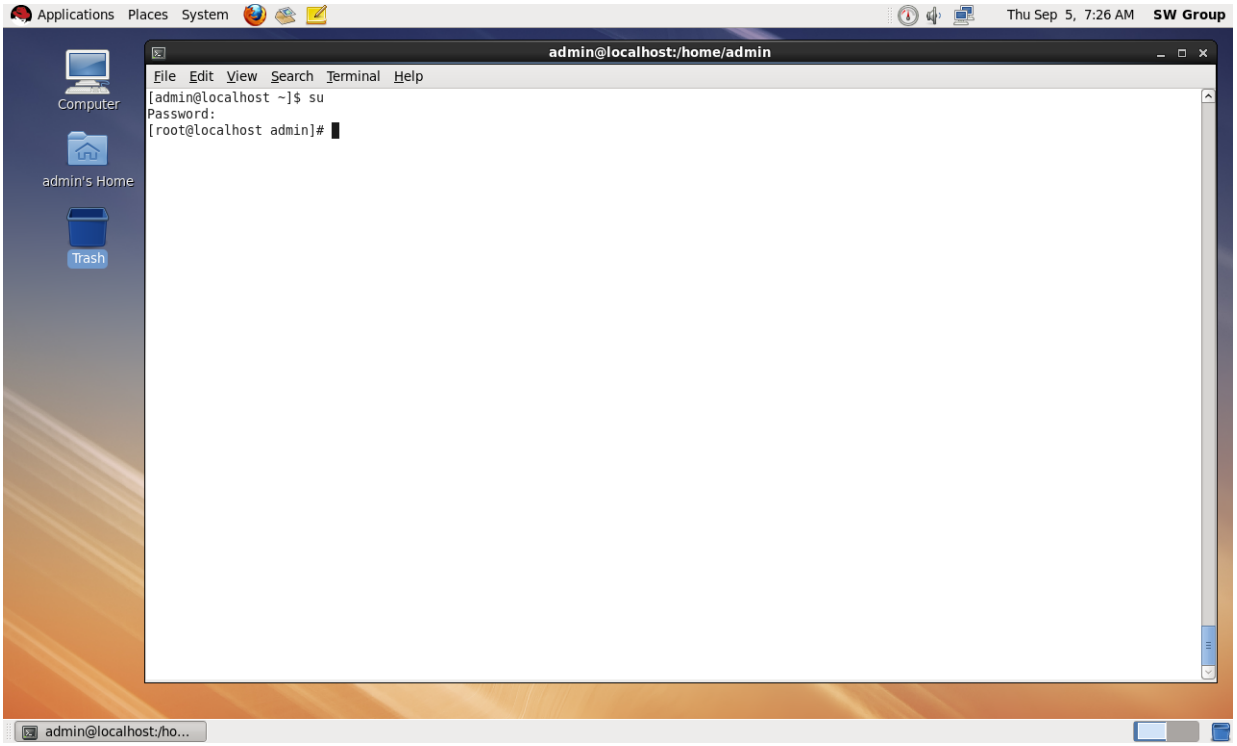
A note about root access: Installing applications, such as Java and Tomcat, require that you have the proper permissions. Typically, applications like Java and Tomcat modify the /`usr/local` or `/opt/` directories, and therefore, you must have write and execute permissions for those directories. Tomcat will also require permission to listen on two network ports. The default ports for HTTP and HTTPS are 80 and 443, respectively. These two ports typically require root access and the user will need to be given access to run the Tomcat server.

For the purposes of this document, it is assumed that the user is either running as root or the user has the proper permissions to access the operations described below. This document will provide directions and examples to run as root. For gaining access to a root console or creating an admin account that has the proper permissions, please see the documentation for your version of Linux.

1. Install Java JRE version 6. For more details about how to install Java for Linux, go to http://www.java.com/en/download/help/linux_install.xml

2. See Figure 28. Once Java is installed, the JRE_HOME environment variable needs to be set.
   a. Open a command prompt.
   b. Elevate to root by typing '`su`'

Figure 28 • Elevate to “root”



   c. Edit the file `etc/profile` by typing:
   `nano /etc/profile`

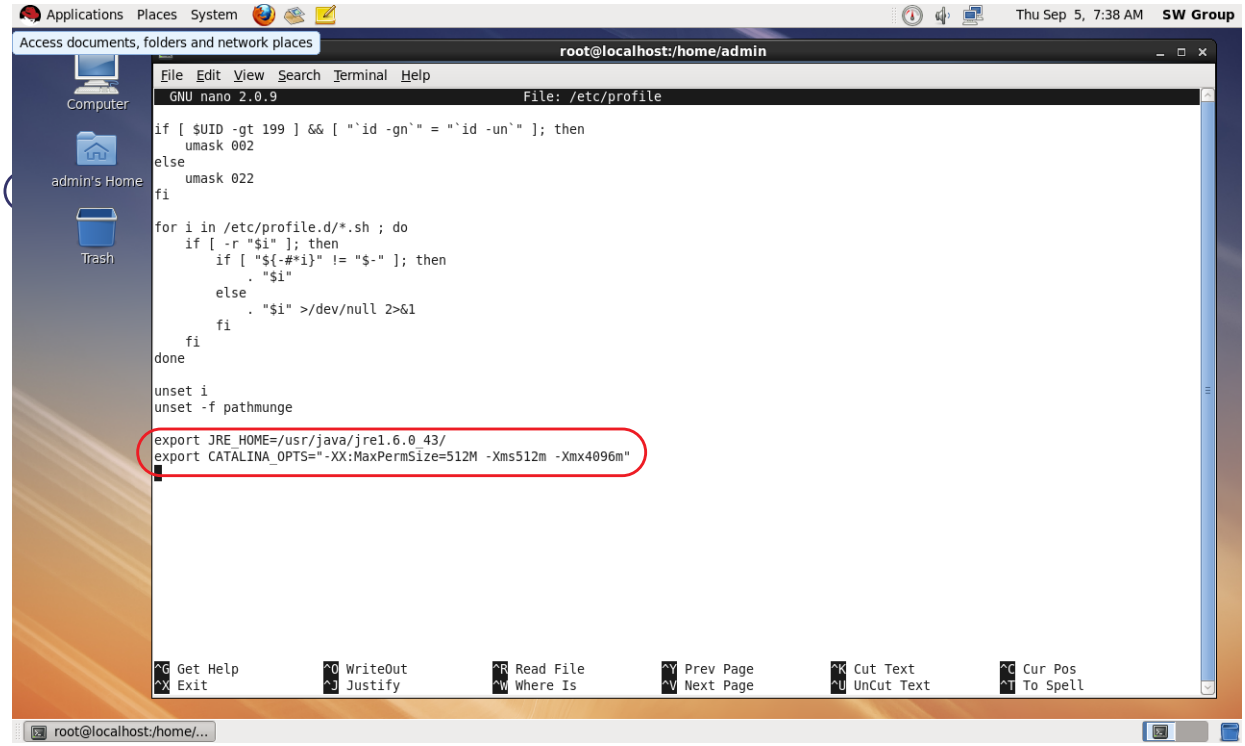
d. See Figure 29. Go to the bottom of the file, add the following 2 lines

```
export JRE_HOME=/usr/java/default/
export CATALINA_OPTS="-XX:MaxPermSize=512M -Xms512m -Xmx4096m"
```

Note • The CATALINA_OPTS environment variable change listed here is recommended based upon a 50 user, 500 printer configuration. As more printers or users are required the individual memory values may need to be adjusted.

Note • A 64-bit Java Virtual Machine (JVM) is required to support the CATALINA_OPTS parameters.

Figure 29 • Adding Environment Variables



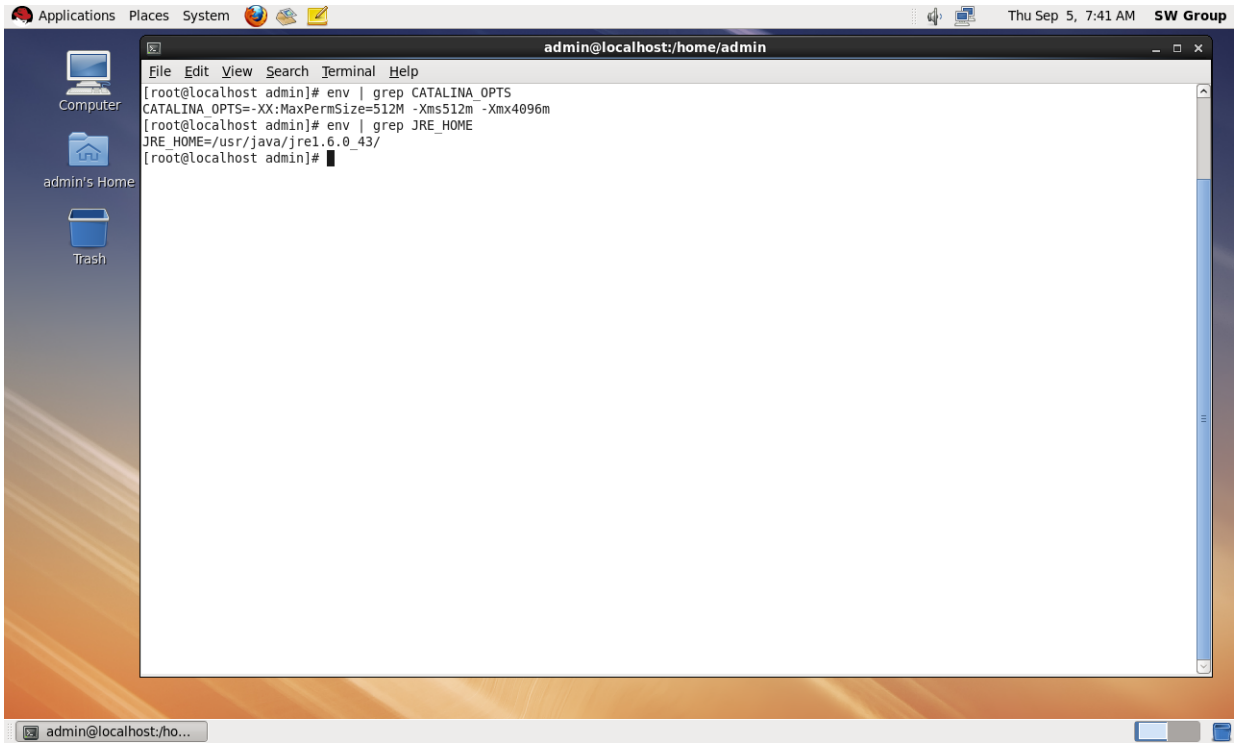
e. Press CTRL+O and press Enter to save. Press CTRL+X to exit the editor.

f. Restart the Red Hat Enterprise server for these options to take effect.

g. See Figure 30. Verify that the environment variables are present by typing and verifying that both commands print the environment variable name and value

```
env | grep CATALINA_OPTS
env | grep JRE_HOME
```

Figure 30 • Verify Environment Variables are Set



3. Download the Zebra Link-OS Application Server zip file
www.zebra.com/profilemanager

4. Extract the Zebra Link-OS Application Server zip file contents to:
`/opt/zebra/linkos`

5. Download the Tomcat zip file:
http://www.us.apache.org/dist/tomcat/tomcat-7/v7.0.42/bin/apache-tomcat-7.0.42.zip

6. Extract the Tomcat zip to:
`/opt/zebra/linkos/tomcat`

7. Open a command prompt as root.

8. Change the current directory to:
`/opt/zebra/linkos`

9. The JVM Certificate Authority keystore must be updated in order to trust the Zebra Weblink Certificate Authority and the GeoTrust™ Subordinate CA.

Note • Omitting or incorrectly performing this step could lead to several issues.

- If the GeoTrust certificate is not added, it will not be possible to successfully register the product and will prevent printers from being connected.
- If the ZebraCAChain certificate is not added correctly, the printer will not be able to connect successfully.

a. See Figure 31 and Figure 32. To update the keystore, execute the following keytool command (running command prompt as root).

```
$JRE_HOME/bin/keytool -importcert -file ZebraCAChain.cer \
-keystore $JRE_HOME/lib/security/cacerts \
-alias "ZebraCAChain"
```

Note • The default keytool password is *changeit.*

b. See Figure 33. To update the keystore, execute the following keytool command (running command prompt as admin).

```
$JRE_HOME/bin/keytool -importcert -file GeoTrustSSLCA.cer \
-keystore $JRE_HOME/lib/security/cacerts \
-alias "GeoTrustSSLCA"
```

Note • The default keytool password is *changeit*

Figure 31 • Adding Zebra CA to the Keystore

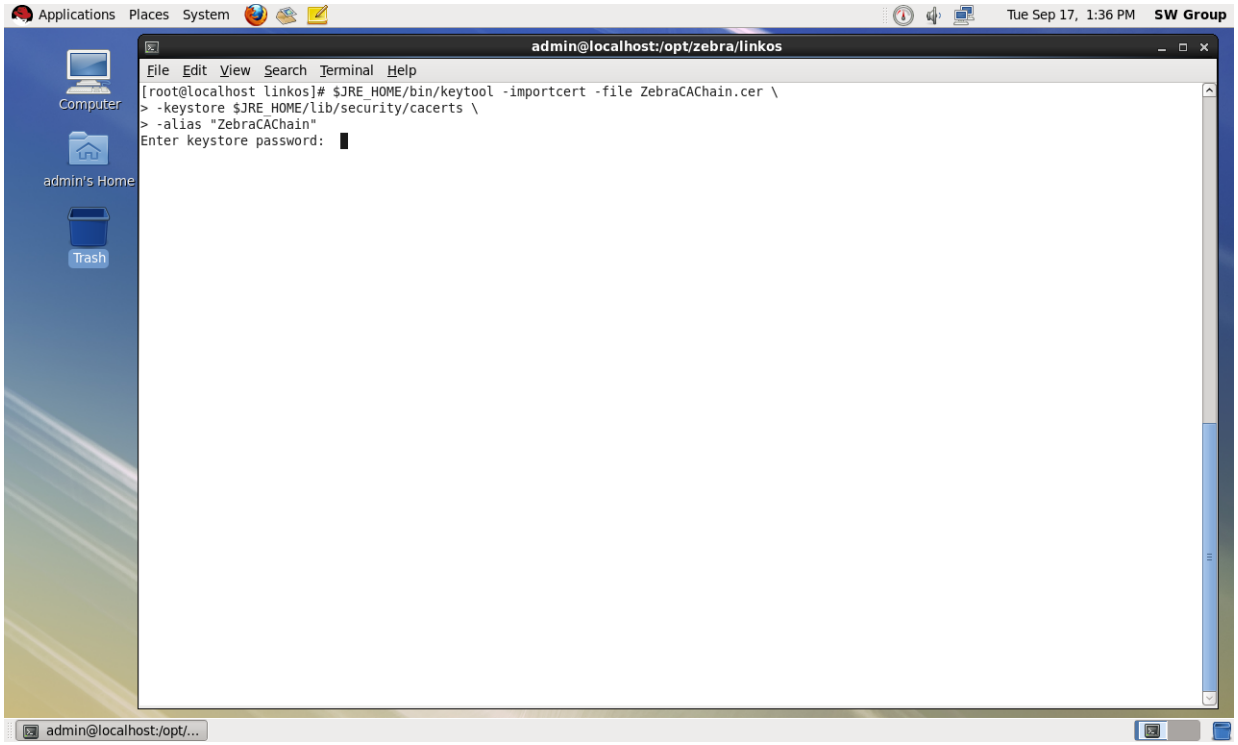


Figure 32 • Trusting the Zebra CA

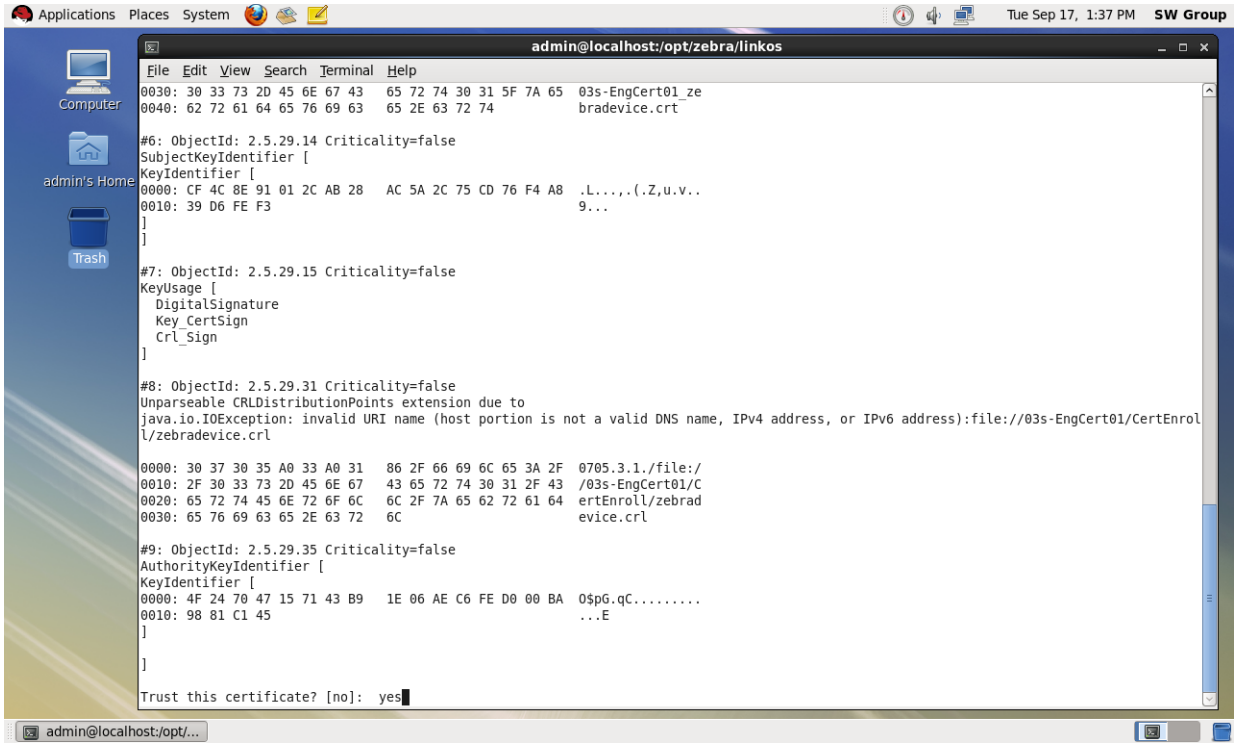
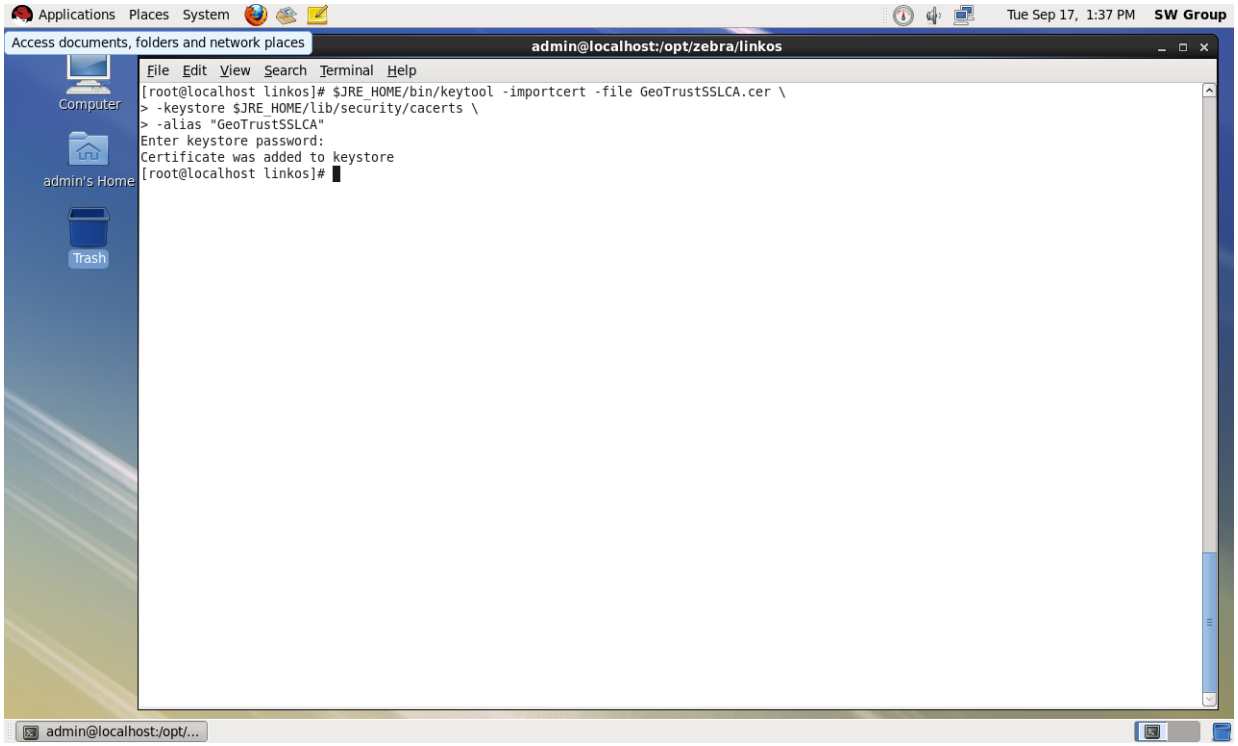


Figure 33 • Adding the GeoTrust CA



10. See Figure 34. Verify the certificates were correctly installed by entering the following command:

```
$JRE_HOME/bin/keytool \
-keystore $JRE_HOME/lib/security/cacerts \
-alias "ZebraCAChain" -list
```

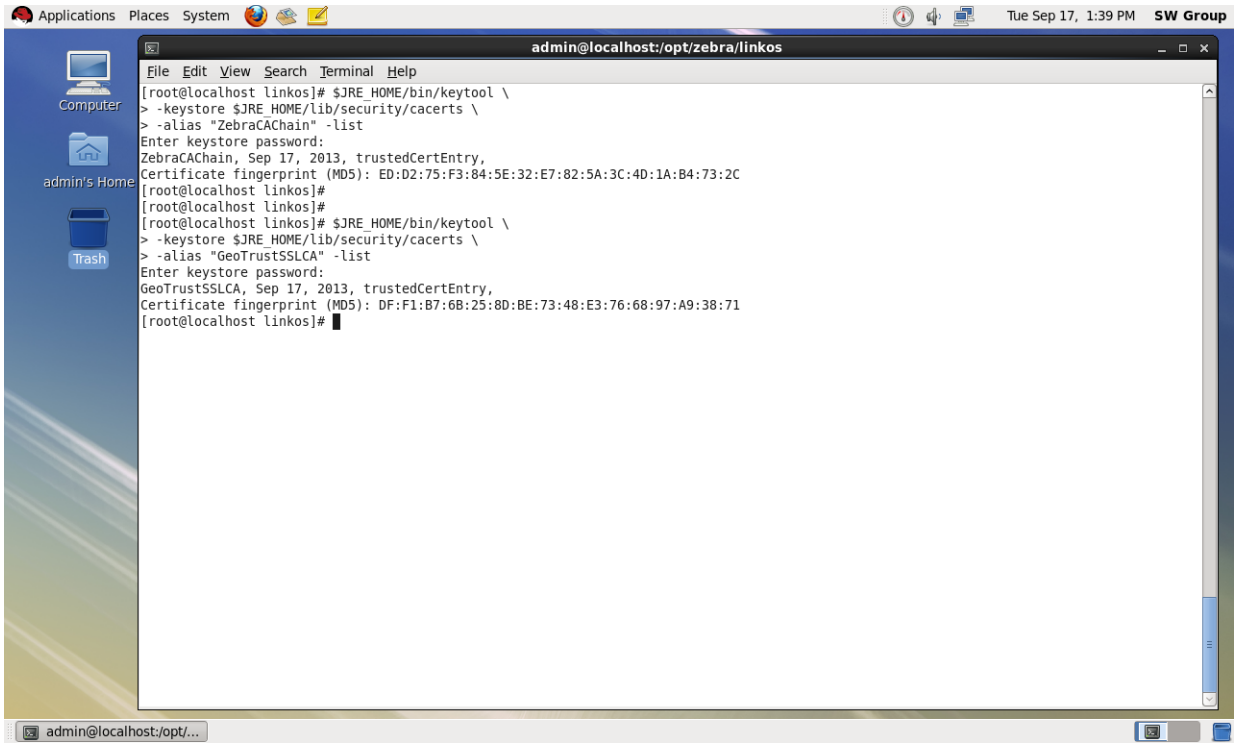
   a. Enter keystore password (default password is *changeit)*.
   The console will show the following:
   `ZebraCAChain, Feb 18, 2013, trustedCertEntry,`
   Certificate fingerprint (MD5):
   ED:D2:75:F3:84:5E:32:E7:82:5A:3C:4D:1A:B4:73:2C

   b. Enter the following command:

```
$JRE_HOME/bin/keytool \
-keystore $JRE_HOME/lib/security/cacerts \
-alias "GeoTrustSSLCA" -list
```

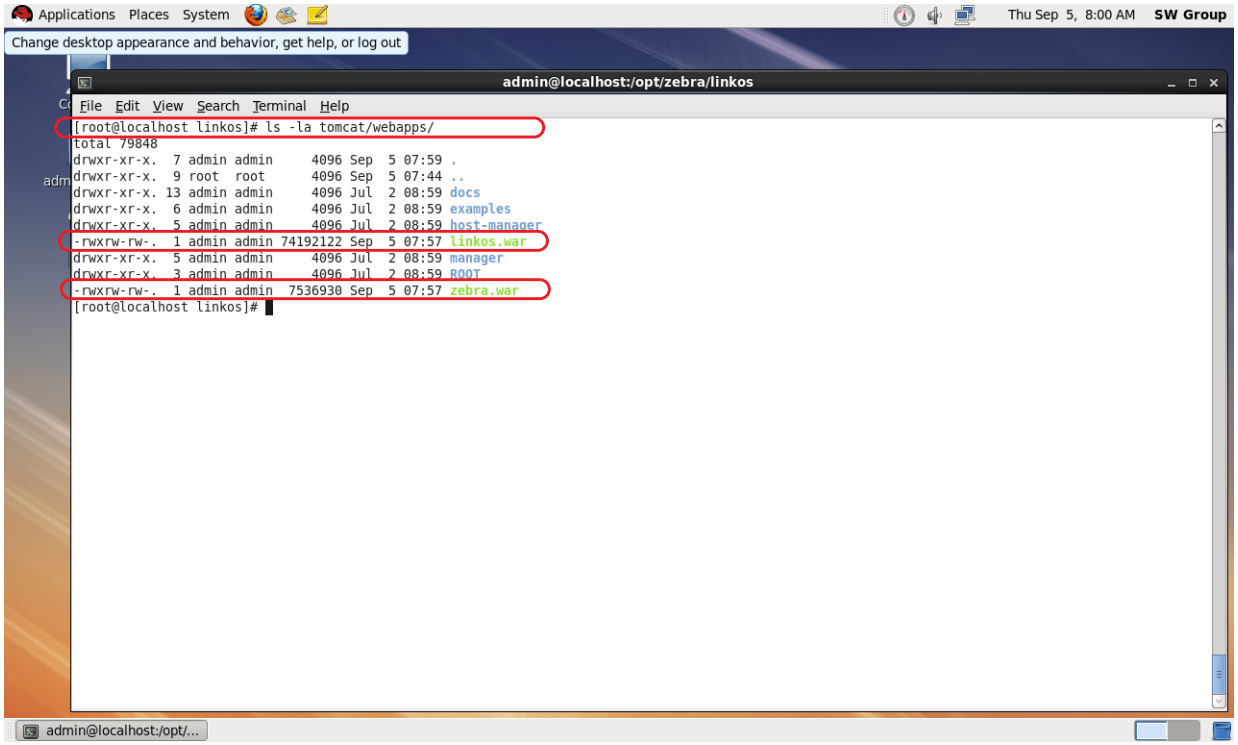
   c. Enter keystore password (default password is *changeit)*.
   The console will show the following:
   `GeoTrustSSLCA, Aug 5, 2013, trustedCertEntry,`
   `Certificate fingerprint (MD5):`
   `DF:F1:B7:6B:25:8D:BE:73:48:E3:76:68:97:A9:38:71`

Figure 34 • Verifying the Certificate Installation



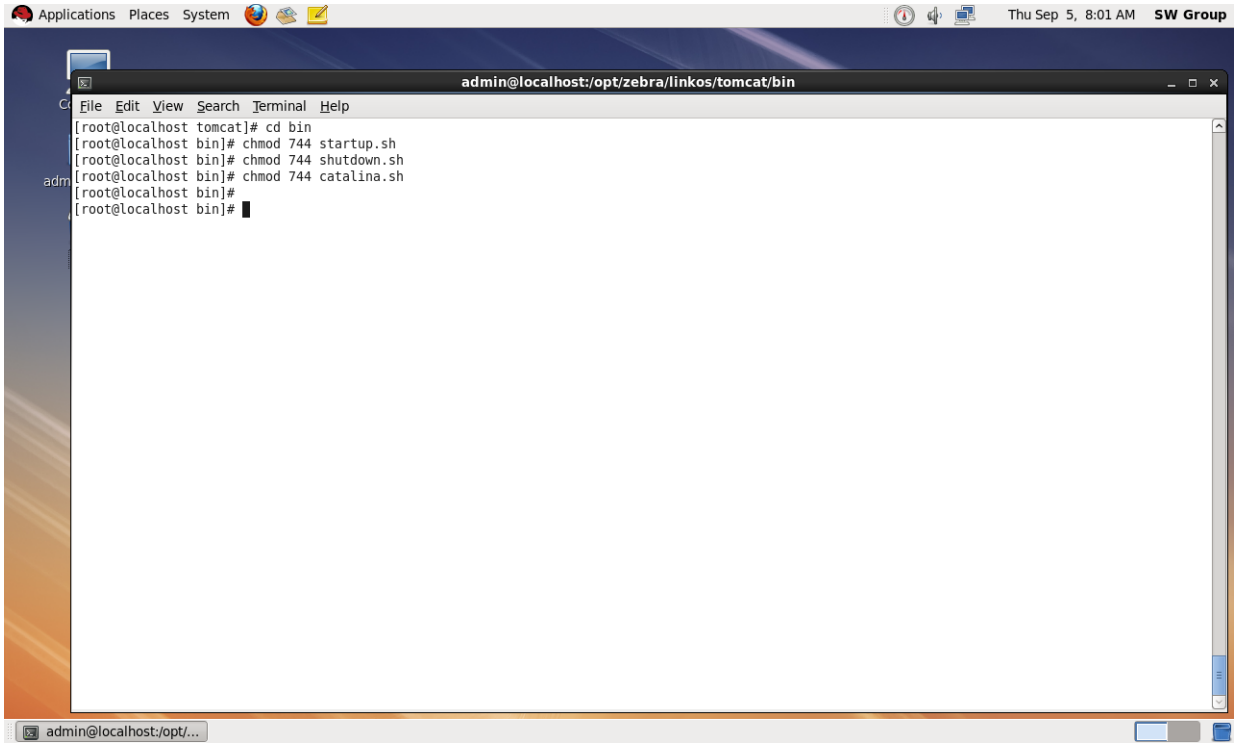
11. See Figure 35. Copy the `zebra.war` and `linkos.war` files from the `/opt/zebra/linkos` directory into the `/opt/zebra/linkos/tomcat/webapps` directory.

Figure 35 • Result of copying the “zebra.war” and “linkos.war” files



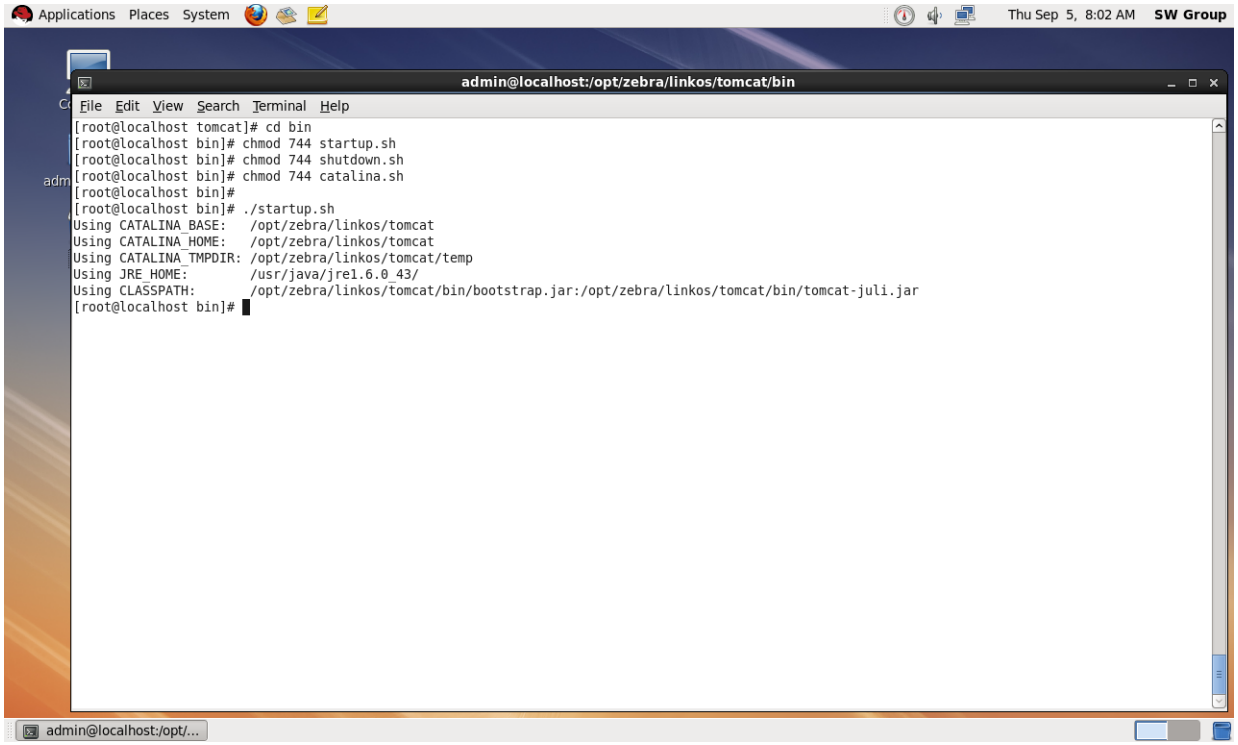
12. See Figure 36. Change the current directory to `/opt/zebra/linkos/tomcat/bin/` and change the permissions of the scripts so that they can be executed.
    a. Enter the following command: `chmod 744 startup.sh`
    b. Enter the following command: `chmod 744 shutdown.sh`
    c. Enter the following command: `chmod 744 catalina.sh`

Figure 36 • Change Script Permissions



13. See Figure 37. Start the Tomcat server by executing ./`startup.sh`

Figure 37 • Starting the Tomcat Server



14. See Figure 38. Verify that Tomcat started correctly by viewing the last 20 lines of the catalina.out log.

    ```
    tail -n20 ../logs/catalina.out
    ```

    a. To view the latest log entries:

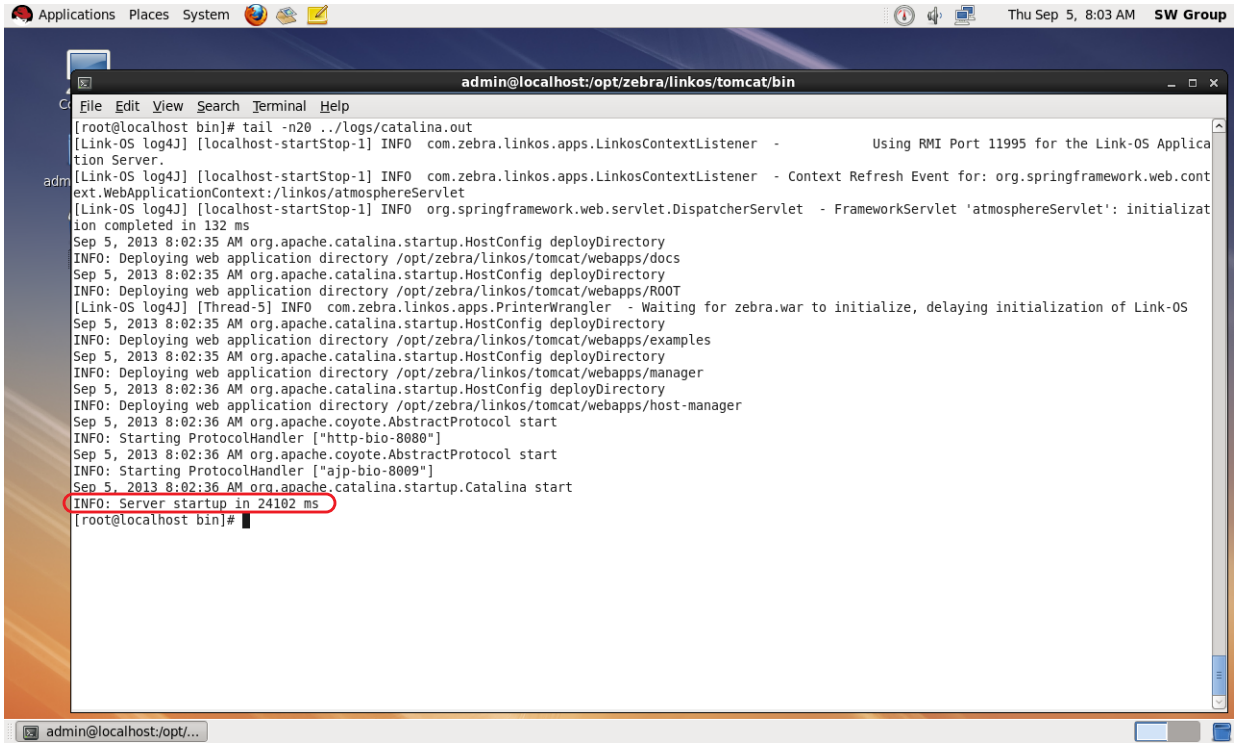
    ```
    tail -f ../logs/catalina.out
    ```

    b. Look for the line that starts:

    ```
    INFO: Server startup in xxxxx ms
    ```

    c. CTRL+C exits the tail command.

Figure 38 • Verifying Tomcat Start



15. See Figure 39. Configure your firewall by performing the following:

a. At the command prompt, type the following commands:

```
service iptables save
nano /etc/sysconfig/iptables
```

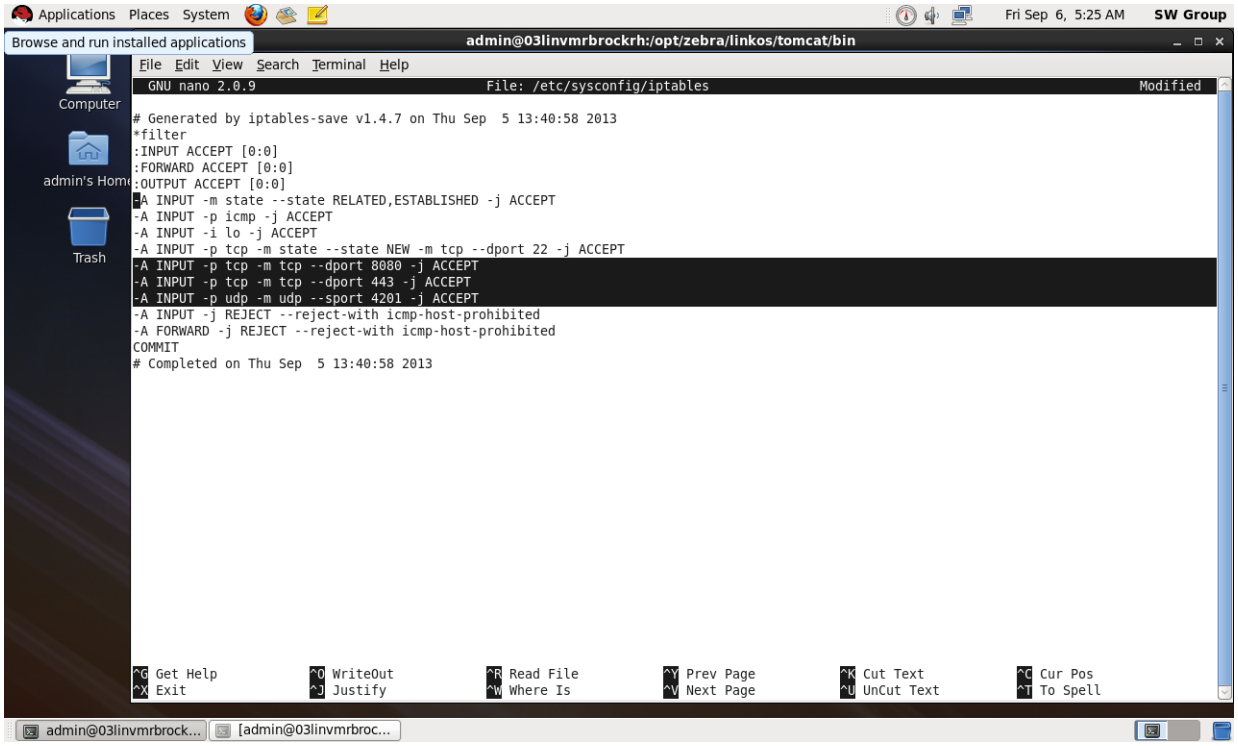
b. Locate this line:

```
–A INPUT –j REJECT –reject-with icmp-host-prohibited
```

c. Above the line, type the following:

```
-A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p udp -m udp --sport 4201 -j ACCEPT
```

Figure 39 • Adding Firewall Rules



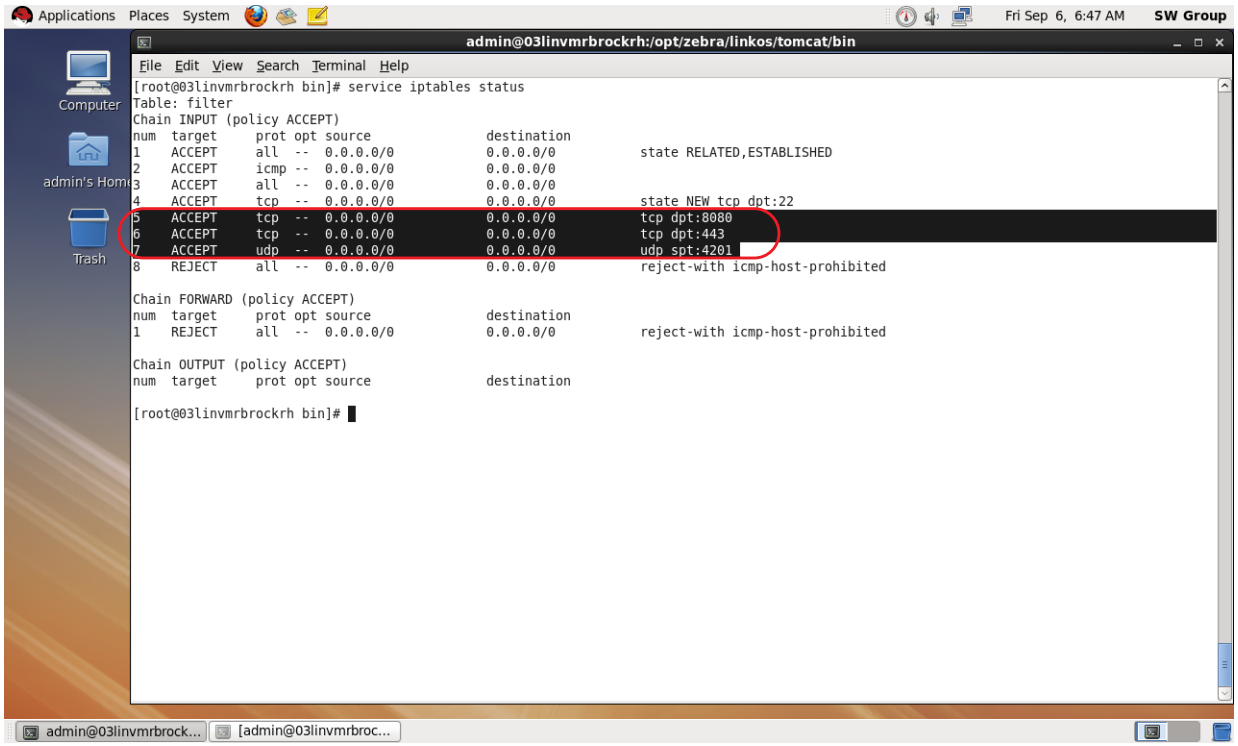
d. Press CTRL + O and press Enter to save. Press CTRL + X to exit.

e. Restart the firewall by typing the following:

```
service iptables stop
service iptables start
```

f. See Figure 40. Double-check that 8080, 443, and 4201 are present .
`service iptables status`

Figure 40 • Verifying the Addition of the Firewall Rules



16. See Figure 41. Open a web browser to:
http://localhost:8080/linkos/register

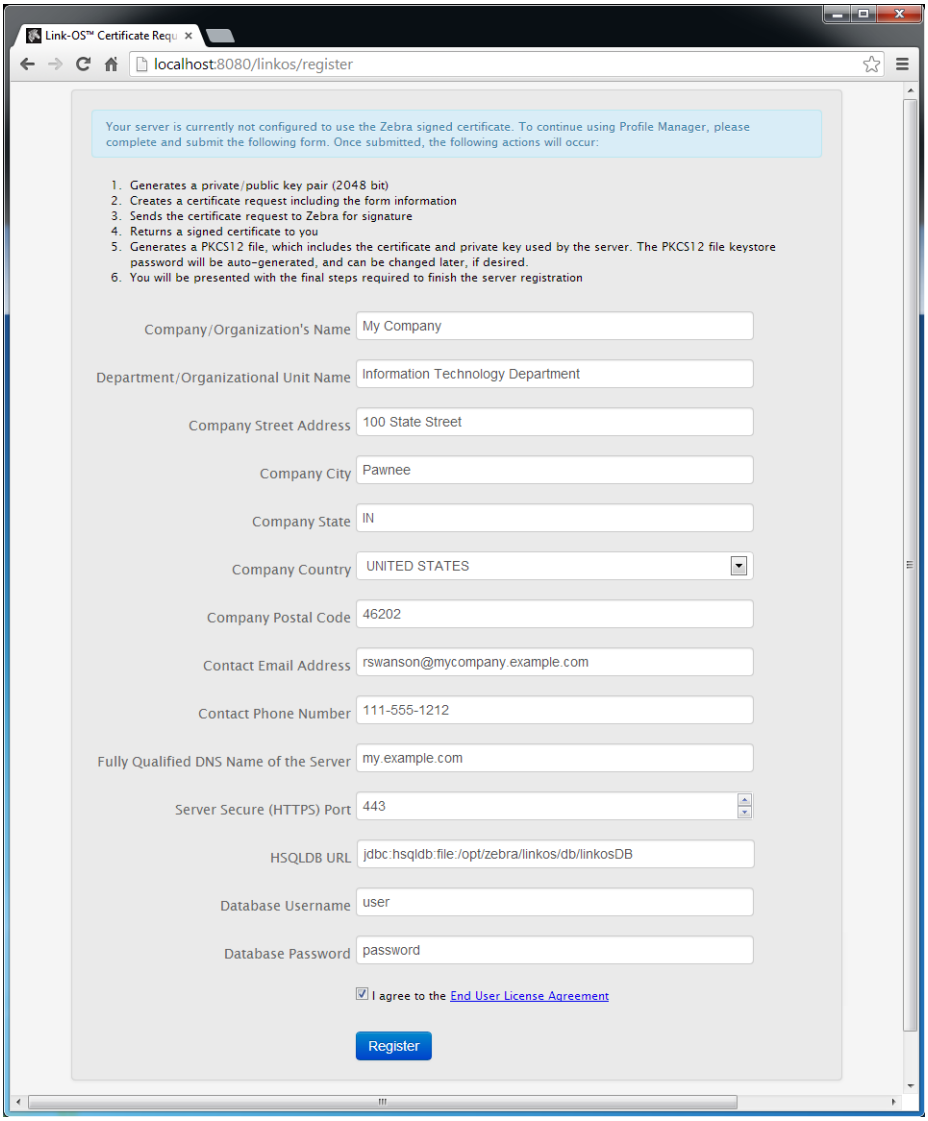
17. Fill in the registration form completely.

Note • The entry in the **Company Street Address** field must be limited to 30 characters.

a. Read and check the box to accept the End User License Agreement.

Note • The port specified will be the SSL port used by printers and browsers to securely connect to your server. Confirm that it is not currently in use (by your server) or ask your IT department to confirm.

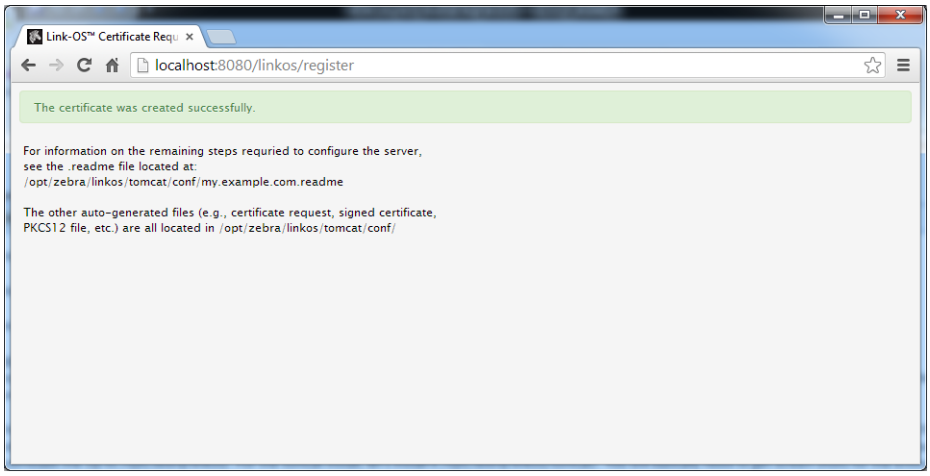
Figure 41 • Registration Form



b. See Figure 42. Click Register.

This step may take up to a minute to complete because of the computational itensity required for the creation of the private key and PKCS12 file.

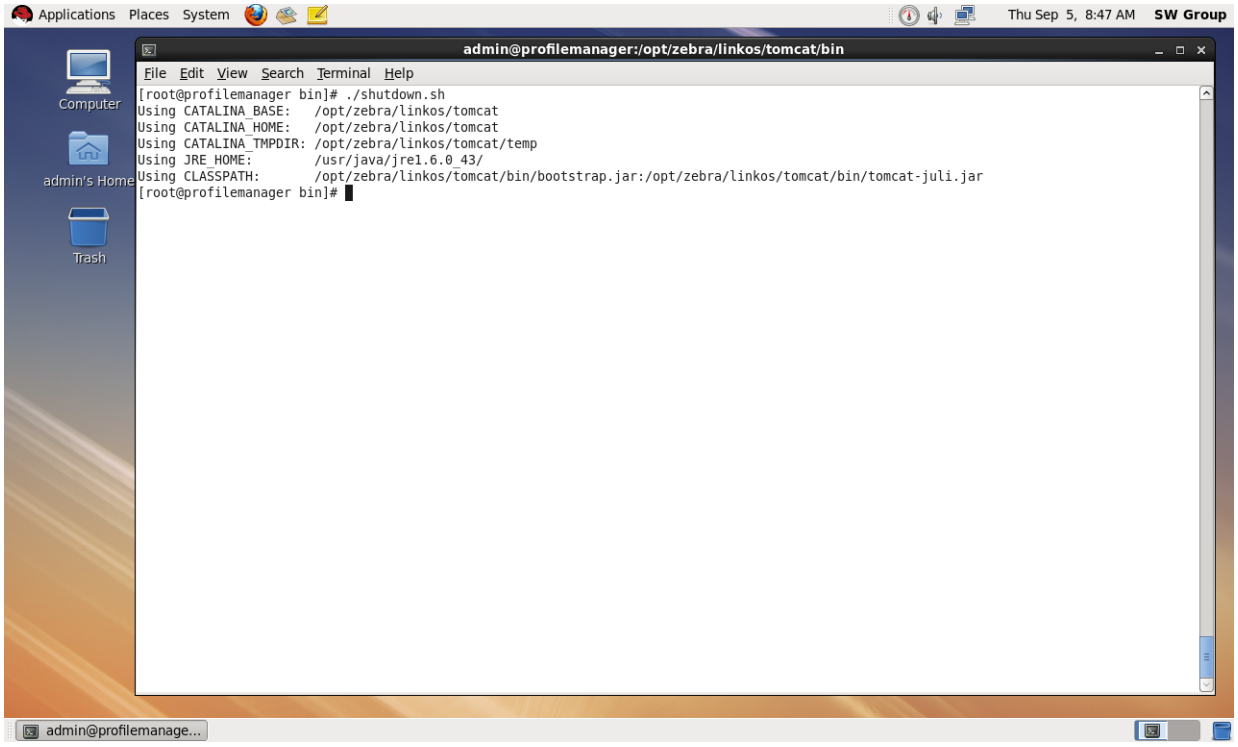
Figure 42 • Registration Successful



18. See Figure 43. Stop the tomcat server from the Tomcat bin directory.

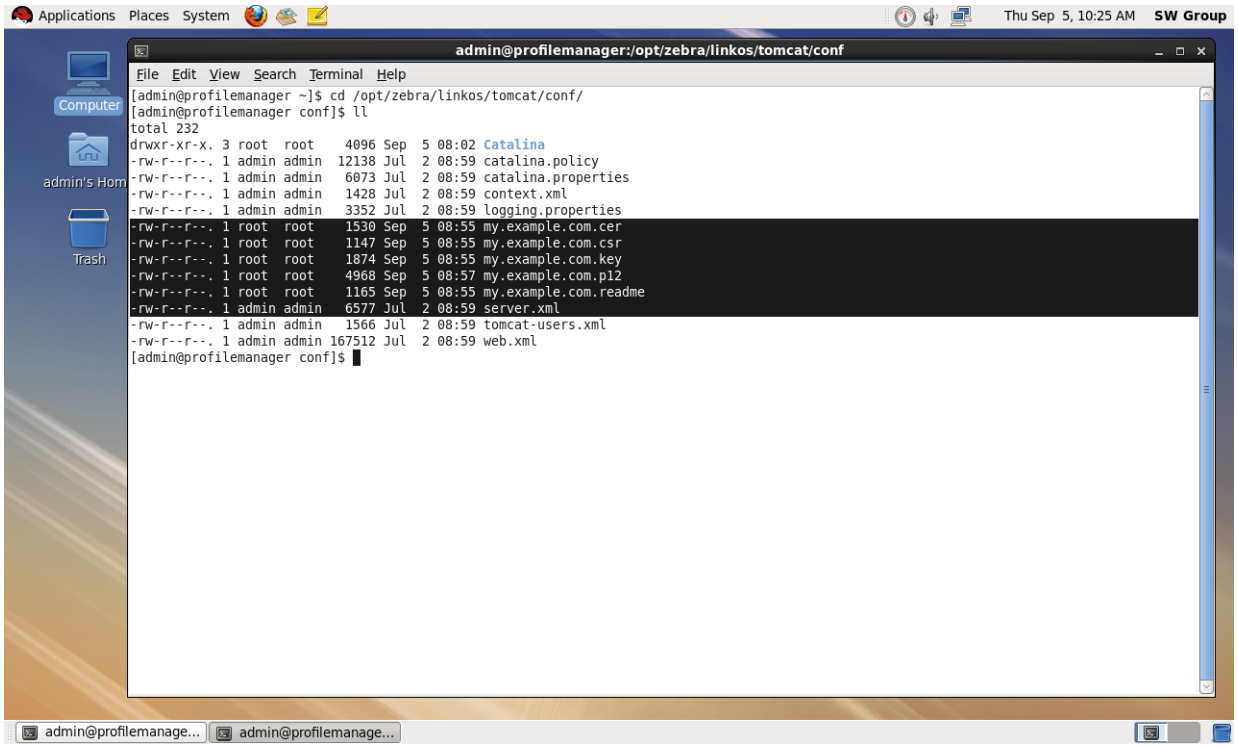
```
./shutdown.sh
```

Figure 43 • Shutting Down Tomcat Server



19. See Figure 44. Using a text editor, like Notepad, open the specified `.readme` instructions file in the `/opt/zebra/linkos/tomcat/conf/` directory.

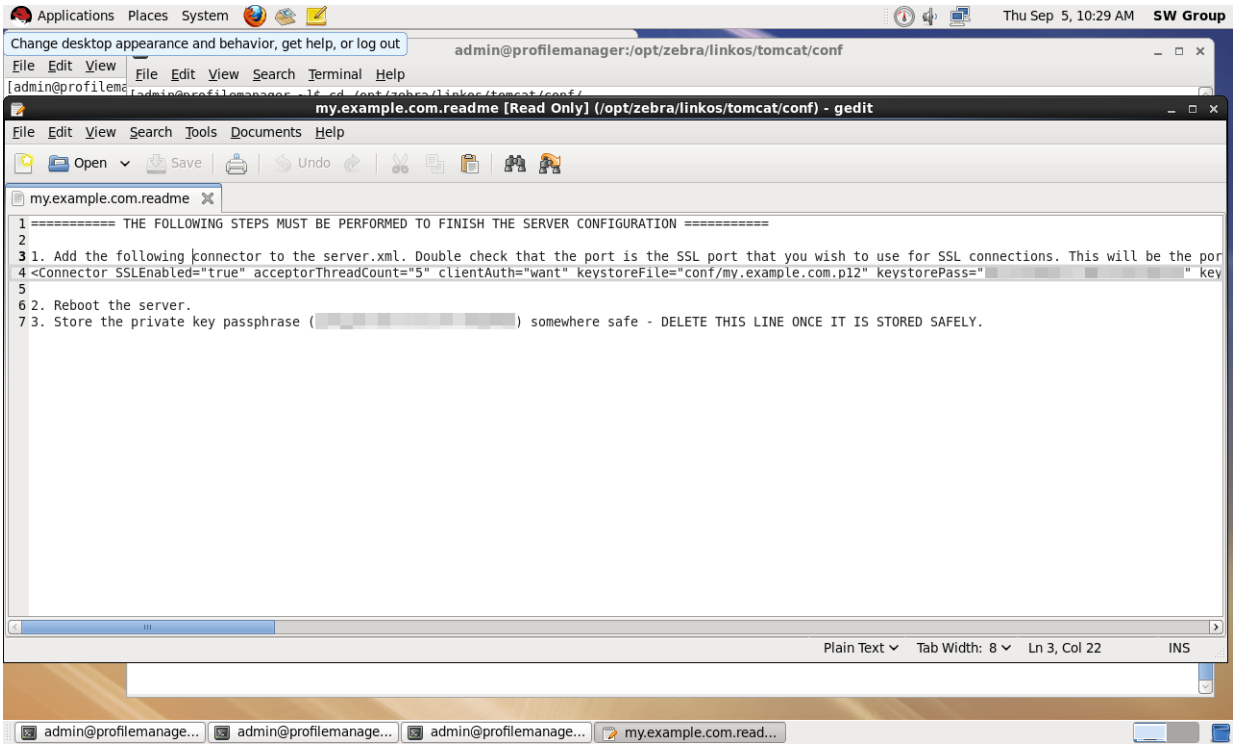
Figure 44 • Directory for Readme File



20. See Figure 45. Copy line 4.

The auto-generated connector is the configuration for the HTTPS port that printers and browsers will use to connect to your server.

Figure 45 • Readme File Contents

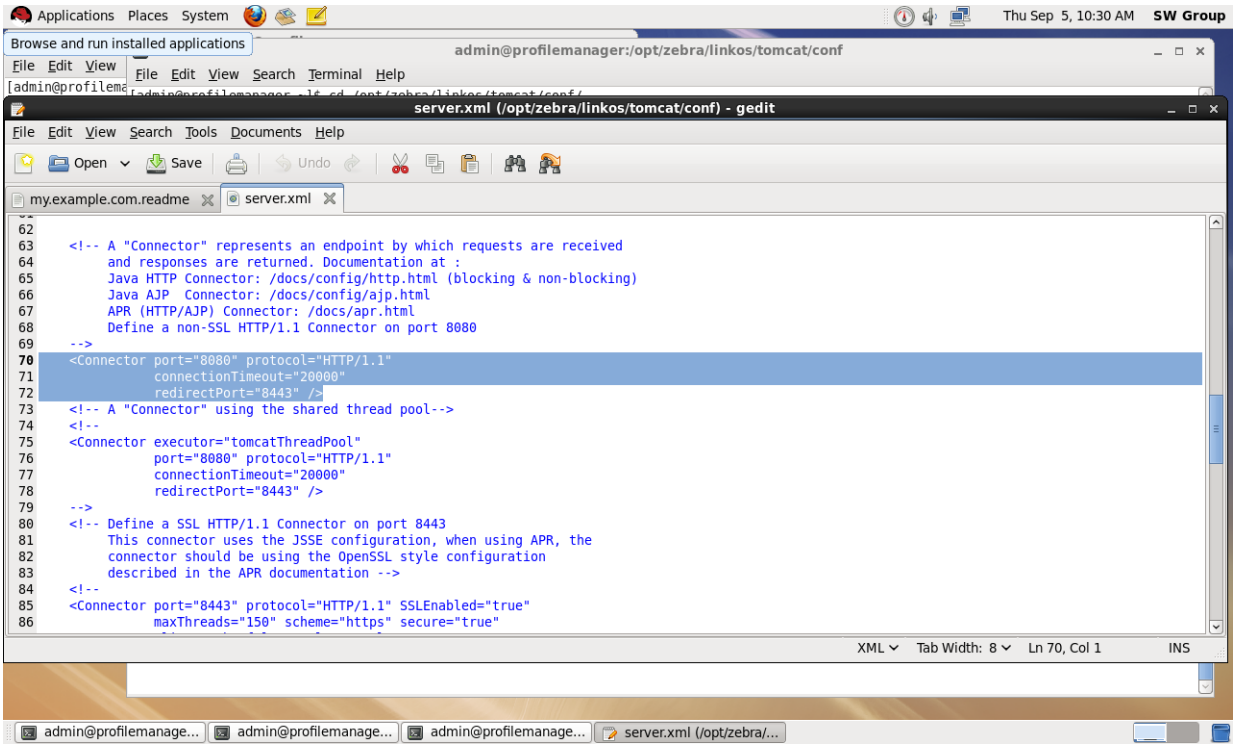


21. Open the `server.xml` file located in:
`/opt/zebra/linkos/tomcat/conf/`

22. See Figure 46. Locate the Connector xml element that looks as follows:

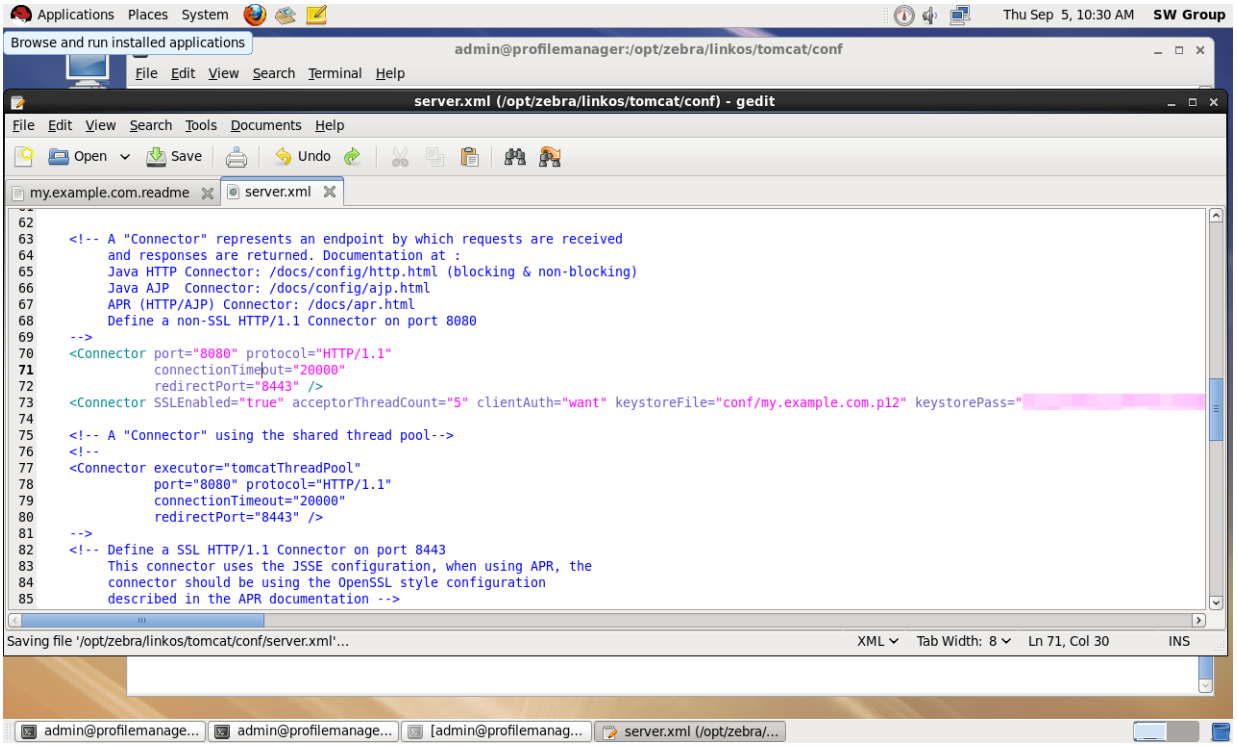
```
<Connector connectionTimeout="20000" port="8080"
protocol="HTTP/1.1" redirectPort="8443"/>
```

Figure 46 • Locate the Connector Element in the server.xml File



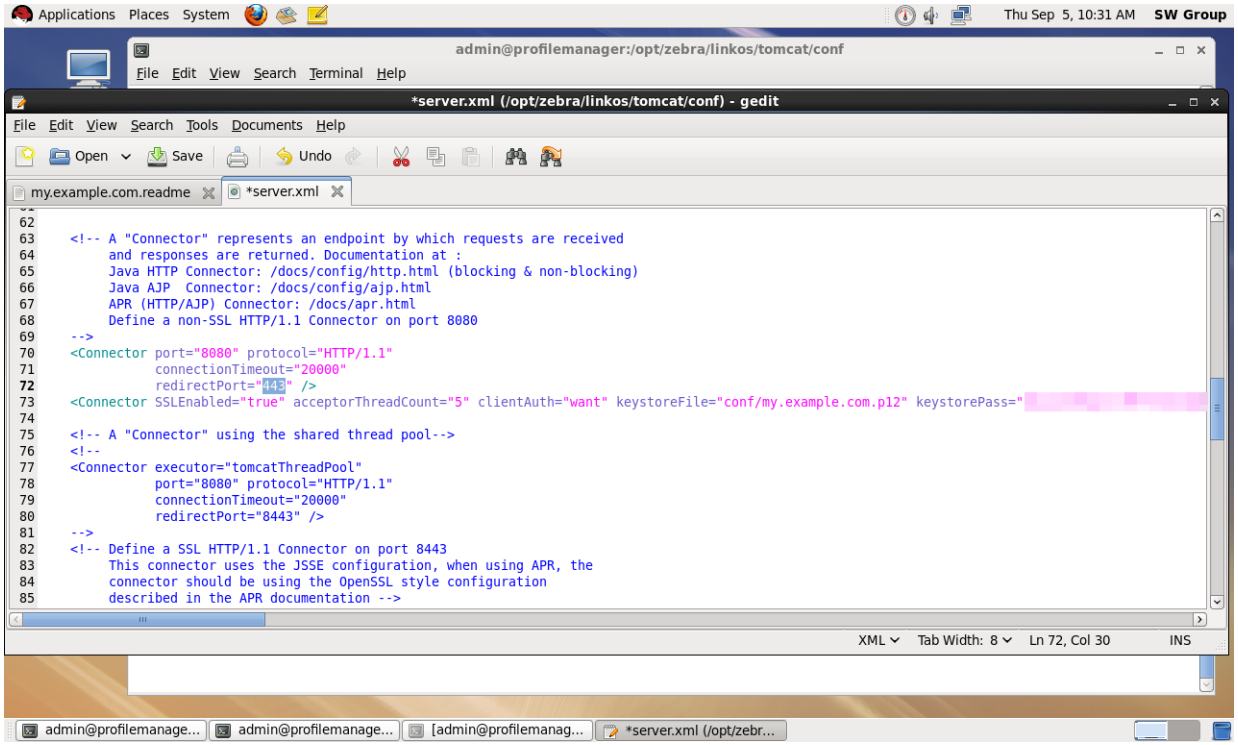
23. See Figure 47. Paste the contents of the clipboard (copied in step 20) after the line located in step 22.

Figure 47 • SSL Connector Added to server.xml File



a. See Figure 48. Change `redirectPort="8443"` to `redirectPort="443"` (The default value is 443. The redirect port should match the value specified in step 17).

Figure 48 • Change the Redirect Port Attribute



24. Start the Tomcat server by typing:

```
./startup.sh
```

Note • This will start the web application. In the future, when your server is rebooted, the application will not automatically restart. If you require the application to start automatically when the server is rebooted, you can configure a System V init script to execute the startup.sh and shutdown.sh scripts at the appropriate times.

For assistance with this, please contact your IT organization, or Zebra Development Services at DevelopmentServices@zebra.com.

25. Open the Chrome browser and go to https://localhost/linkos/.

Note • If the port is something other than 443, it must be specified (e.g., https://localhost:4443/linkos).

26. Which browser are you using?

If you are using a…	Then…
Chrome browser	**a.** See Figure 49. Click on **Proceed anyway.** **b.** To avoid this message in the future, please see *Adding the Zebra Certificate Authority* on page 63.
Internet Explorer	**a.** See Figure 50. Click on **Continue to this website (not recommended).** **b.** To avoid this message in the future, please see *Adding the Zebra Certificate Authority* on page 63.

Figure 49 • Site Security Certificate for Chrome

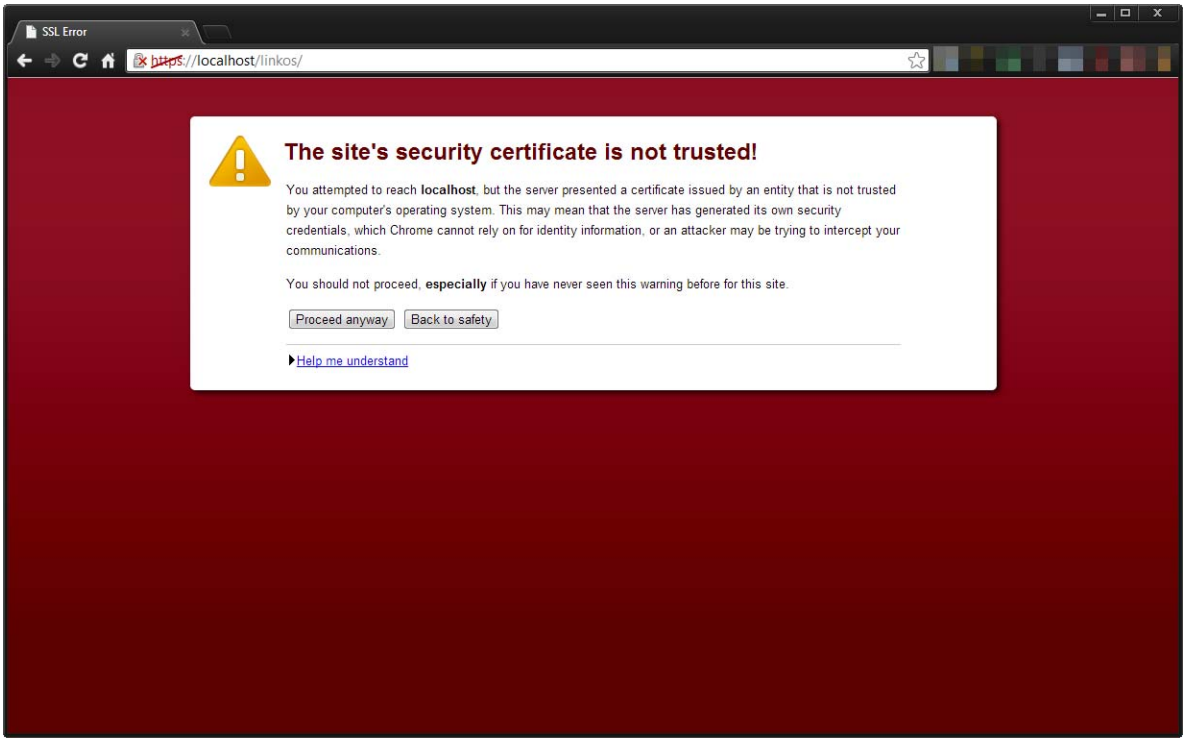
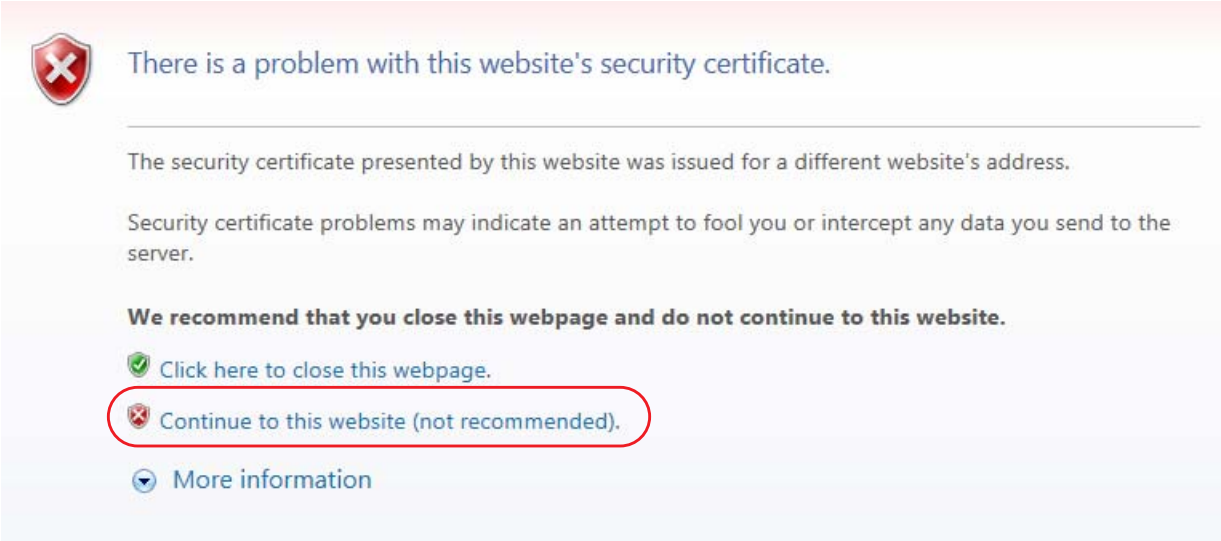


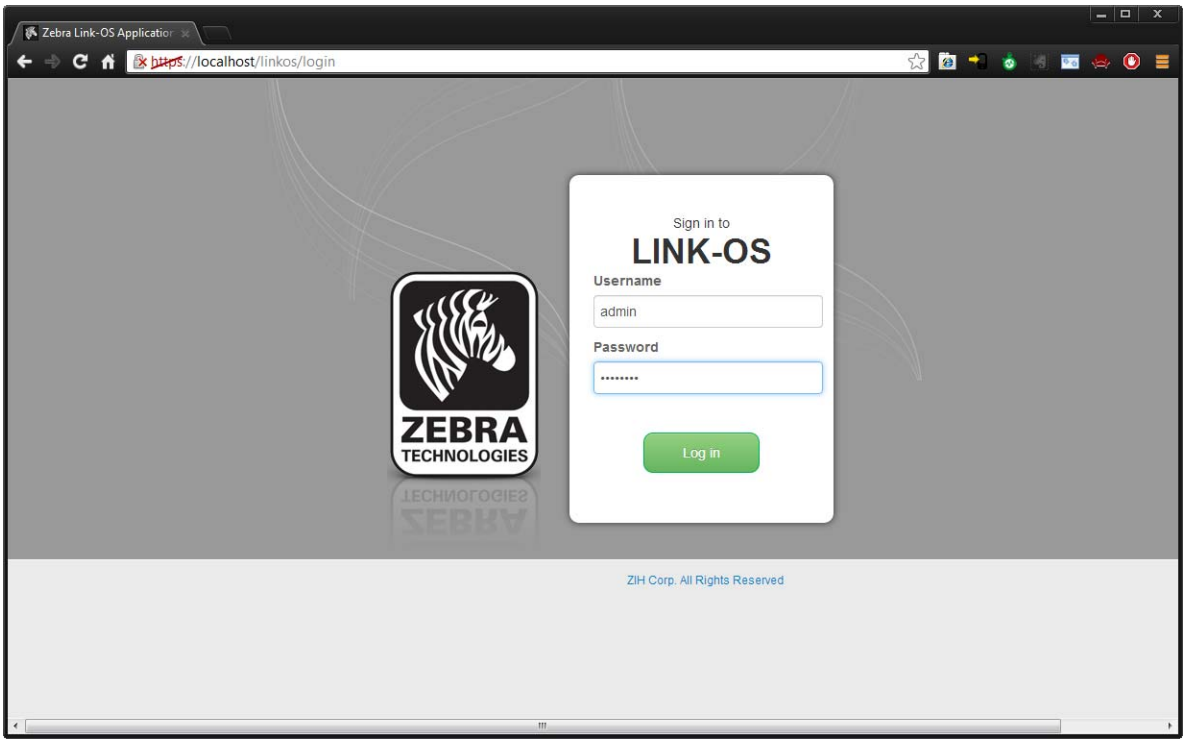
Figure 50 • Site Security Certificate for Internet Explorer



27. See Figure 51. Log into the Link-OS Application Server.

Note • The default username is *admin* and the default password is *password*.

Figure 51 • Login Screen



28. The first time you log into the Link-OS Application Server, change your password. Go to **User and Settings** > **Change password**.

Notes •

Adding the Zebra Certificate Authority

This chapter includes the procedure to add the Zebra Certificate Authority to the Trusted Root Certifications Authorities Store.

Contents

Before You Begin

These instructions include the steps to add the Zebra Certificate Authority (CA) to the Trusted Root Certifications Authorities Store. By adding the Zebra CA to the Trusted Root Certifications Authorities Store, the browser will no longer warn the user that the certificate is not from a trusted authority. These instructions are not required in order to use Profile Manager, however, adding the Zebra CA will improve the overall experience with the Profile Manager application.

Caution • To add the Zebra Certificate Authority (CA) to the Trusted Root Certification Authorities Store and modify the registry, you must have administrator permissions. Additionally, some of the screens and steps may differ slightly depending upon the User Account Control (UAC) level set for your computer, and the version of Windows that you are using. For questions about your version of Windows, administration permissions, or UAC, please contact your local IT department for assistance.

Installation

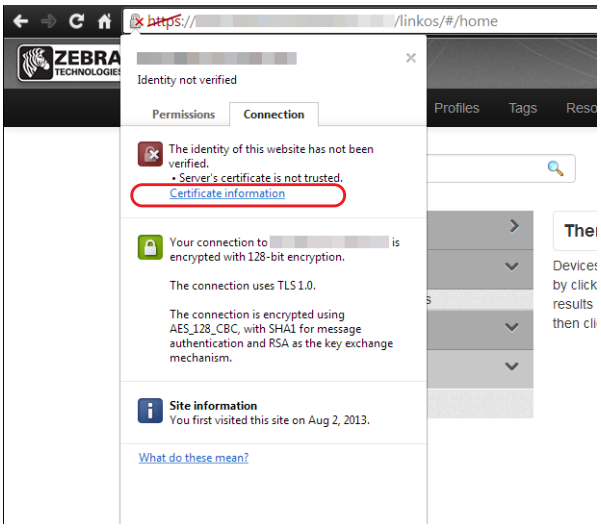
1. Which browser are you using?

If you are installing...	Then
Chrome	Continue with *Installation for Chrome* on page 65.
Internet Explorer	Go to *Installation for Internet Explorer 10* on page 82.

Installation for Chrome

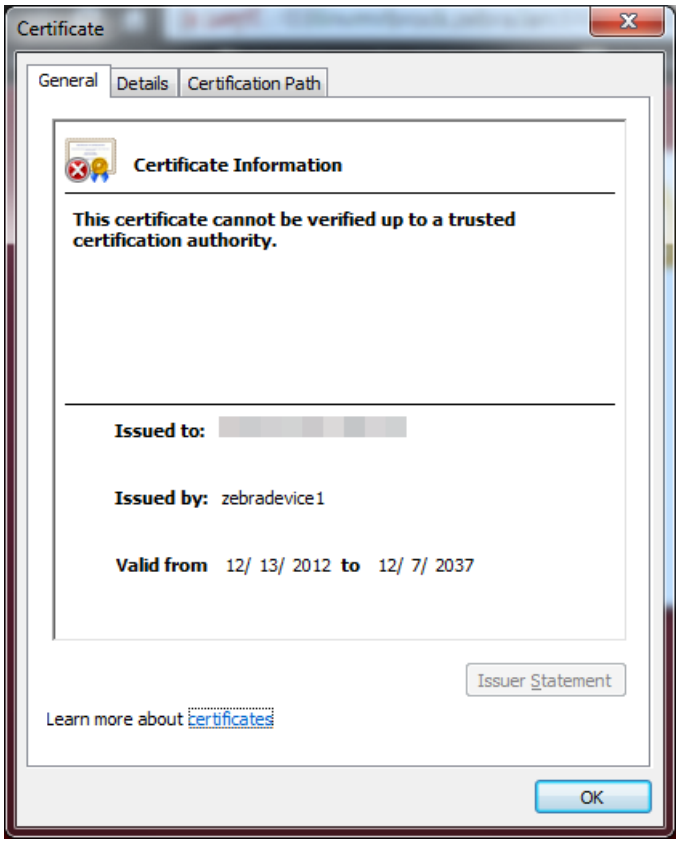
1. Click on the lock icon that has the red '**x**' in the browser location input bar.
2. See Figure 52. Click on the Connection tab and click on the **Certificate Information** link.

Figure 52 • Certificate Information within Chrome Browser



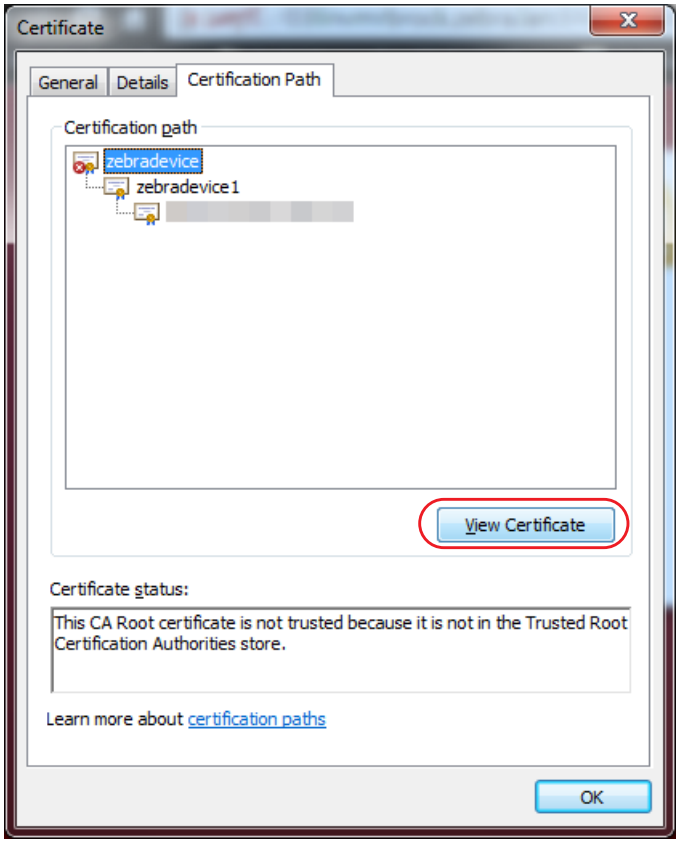
3. See Figure 53. Click on the **Certification Path** tab.

Figure 53 • Certificate Information



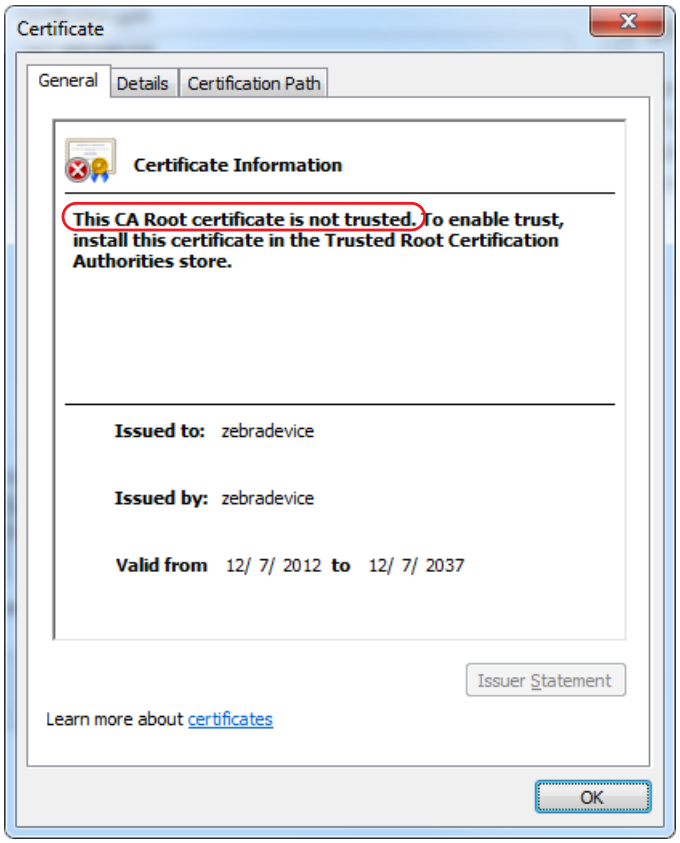
4. See Figure 54. Click on **zebradevice** at the top of the tree and click on **View Certificate**.

Figure 54 • Certificate Path



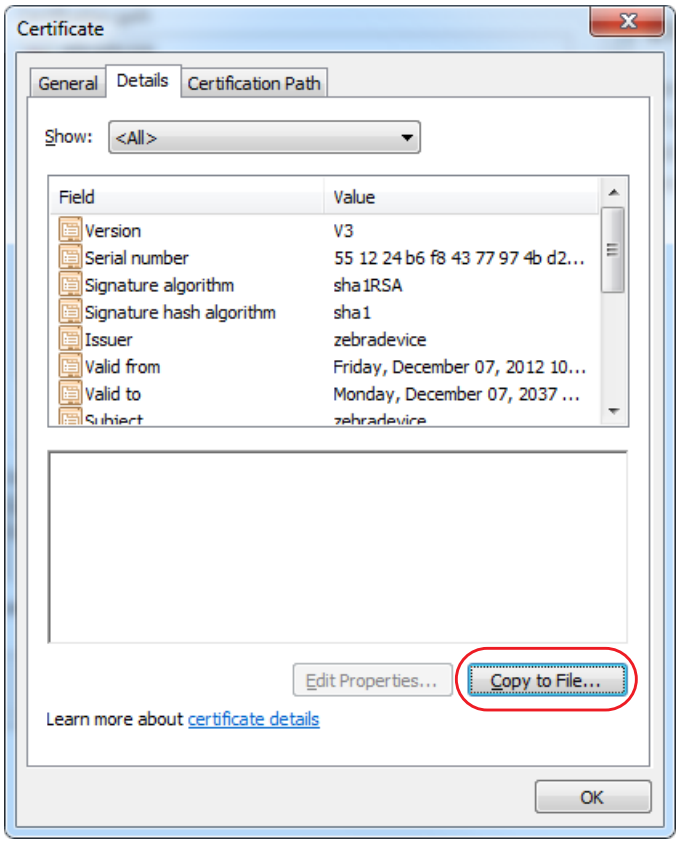
5. See Figure 55. The untrusted Zebra certificate will be shown.

Figure 55 • Untrusted CA Root Certificate



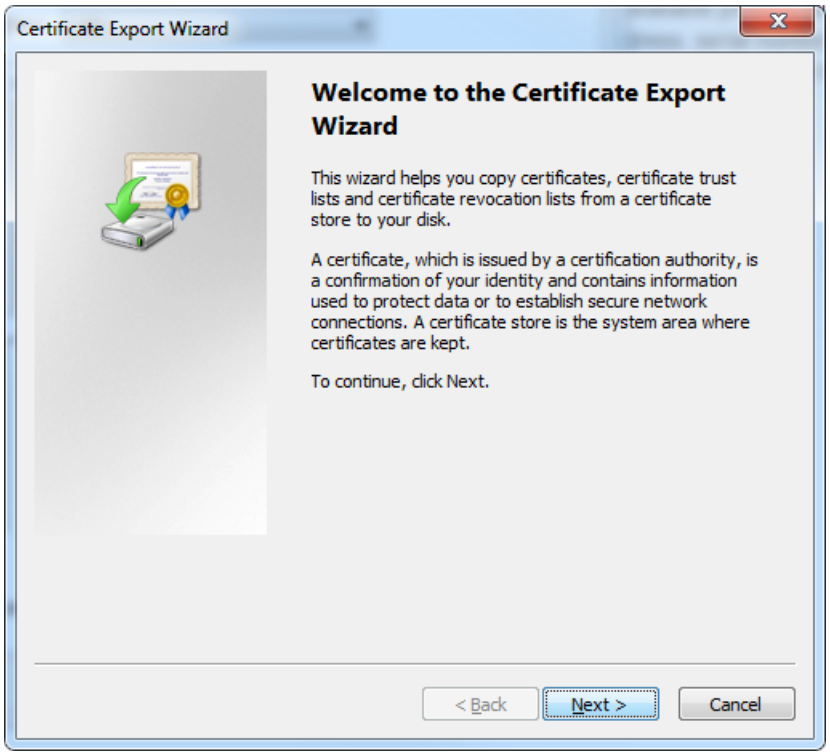
6. See Figure 56. Click on the Details tab and click **Copy to File**.

Figure 56 • Zebra CA Certificate Details Tab



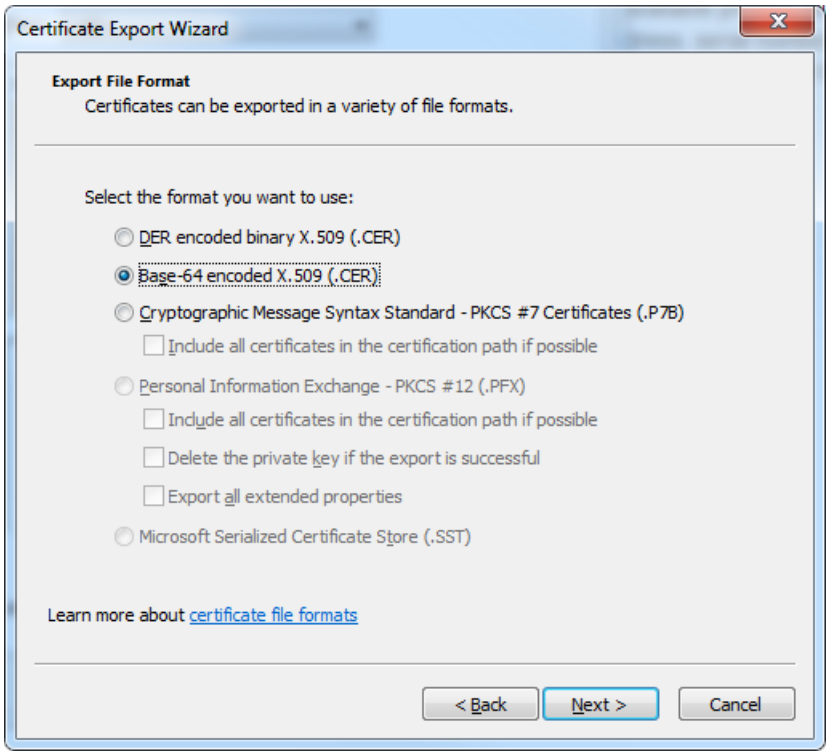
7. See Figure 57. The Certificate Export Wizard will be shown. Click **Next**.

Figure 57 • Certificate Export Wizard



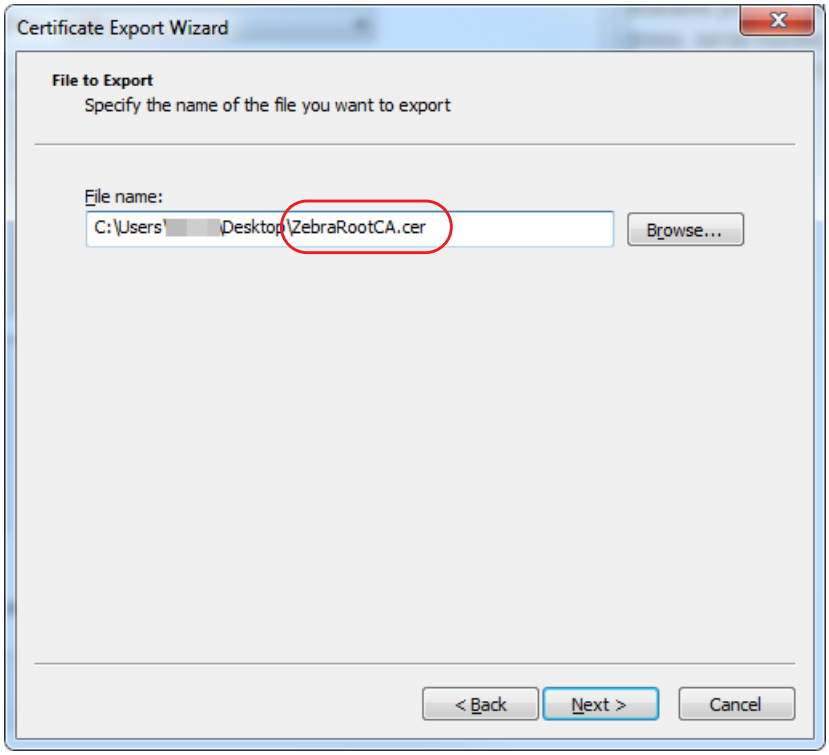
8. See Figure 58. Select Base-64 encoded X.509 (.CER) and click **Next**.

Figure 58 • Certificate Export Format



9. See Figure 59. Select a destination folder that is easily accessible (e.g., the Desktop). Enter the name of the certificate: ZebraRootCA.cer

Figure 59 • Certificate Export Destination



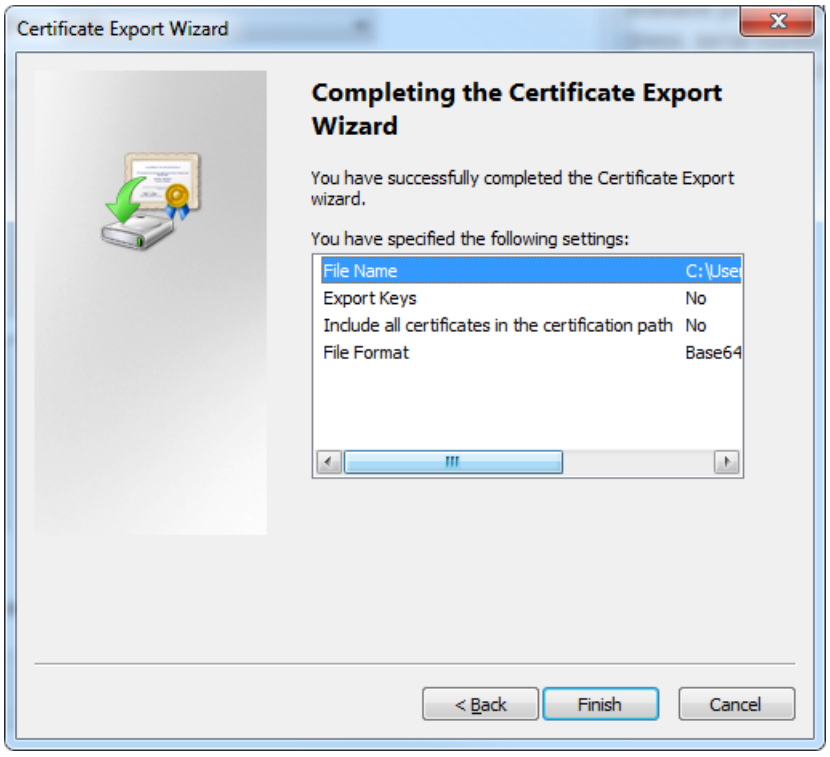
10. Click **Next**.

The Export Success dialog box will appear.

Figure 60 • Export Success Dialog Box

11. See Figure 61. Select **Finish** on the final wizard screen.

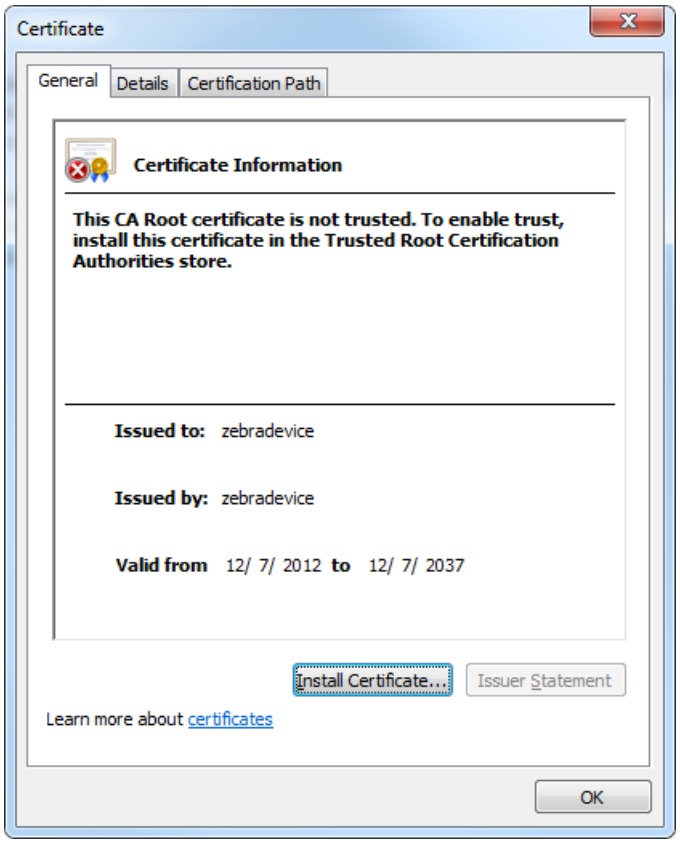
Figure 61 • Completing the Certificate Export Wizard



12. Locate the certificate saved in step 9 and step 11. Double-click on it to open it.

13. See Figure 62. Click on **Install Certificate…**.

Figure 62 • Install Certificate



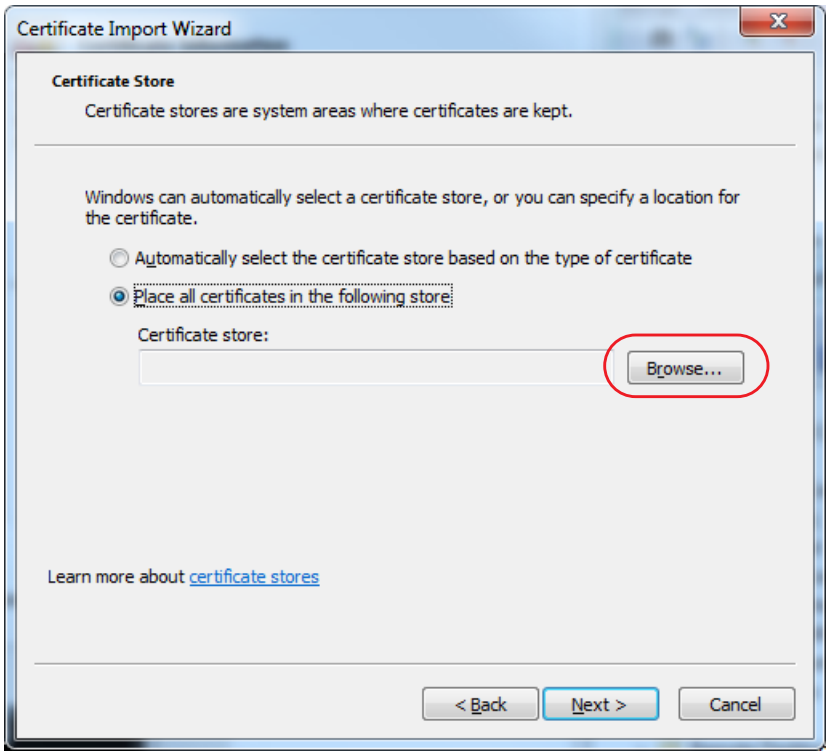
14. See Figure 63. The Certificate Import Wizard will appear.

Figure 63 • Certificate Import Wizard

15. Click **Next**.

16. See Figure 64. Select **Place all certificates in the following store**.

Figure 64 • Certificate Import Wizard Destination Store

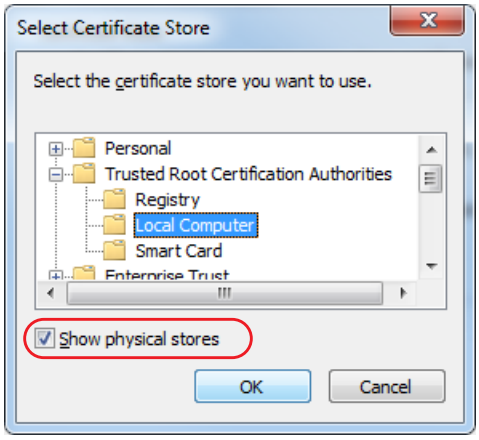


17. Click **Browse**.

18. See Figure 65. Click on the **Show physical stores** and navigate to **Trusted Root Certification Authorities\Local Computer**.

Note • See Figure 65. If 'Local Computer' is not shown under the 'Trusted Root Certification Authorities' entity, please ensure that you have administrator permissions for the computer on which you are attempting to install the Zebra CA. The User Account Control (UAC) on some versions of Windows may also prevent you from seeing the 'Local Computer' option. Please contact your local IT department for more information on administrator permissions and UAC.

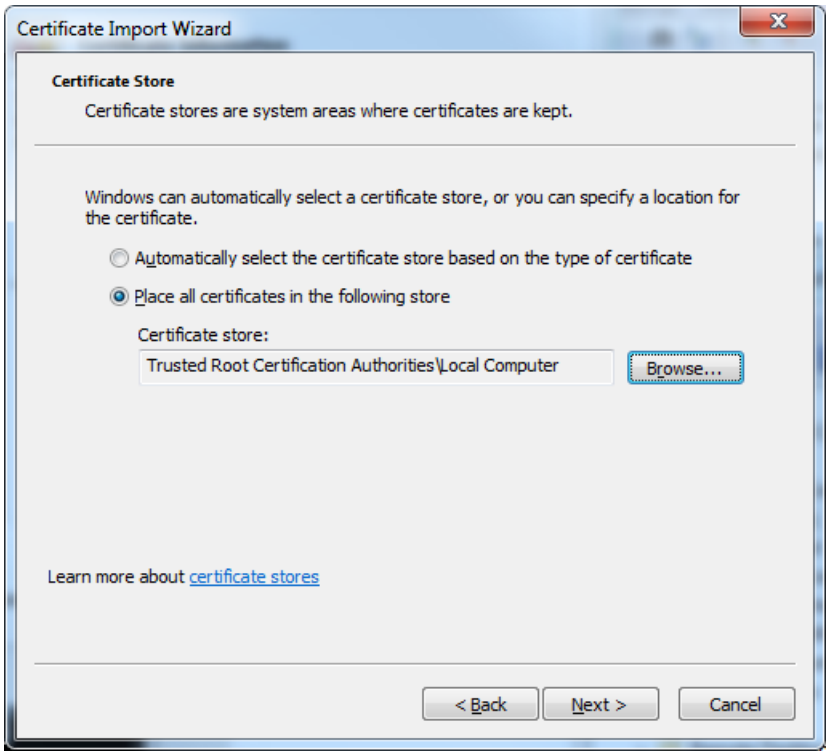
Figure 65 • Certificate Import Wizard Store Selection



19. Click **OK**.

20. See Figure 66. The certificate store should be updated.

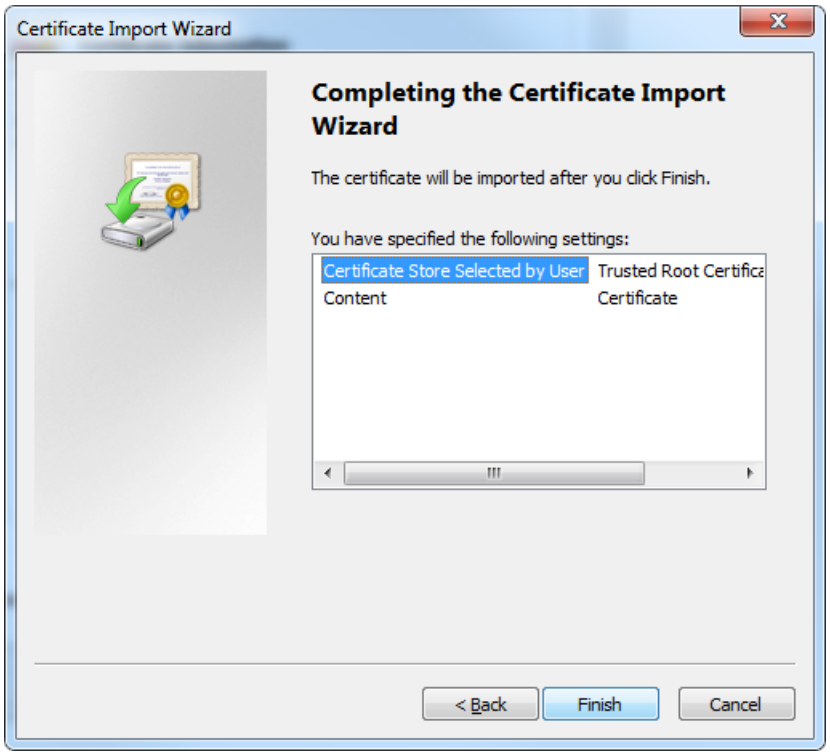
Figure 66 • Certificate Import Wizard Destination Store



21. Click **Next**.

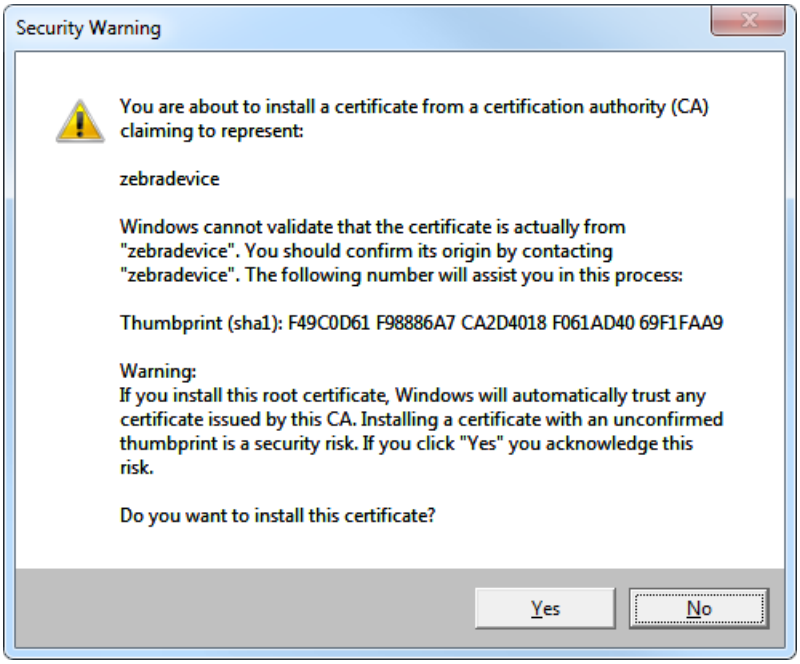
22. See Figure 67. Click **Finish** to install the certificate authority to the local computer.

Figure 67 • Completing the Certificate Import Wizard



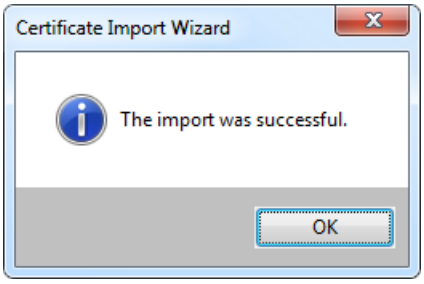
23. You will likely be presented with the Security Warning dialog that indicates the certificate authority origin is unknown. See Figure 68. Click **Yes** to install the Zebra Root Certificate Authority as a Trusted Certificate Authority.

Figure 68 • Agree to Install the Certificate



24. See Figure 69. A dialog box will appear to confim the import's success.

Figure 69 • Import Successful



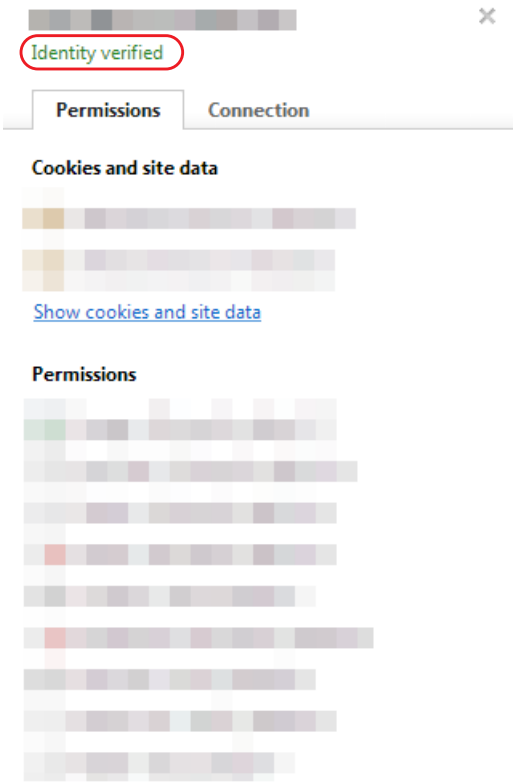
25. Close the Chrome browser and open it again for the new certificate permission to take effect.

26. Return to the Link-OS Profile Manager Application.

27. The lock should no longer have a red 'x' on it. The lock and 'https' portion of the URL should be green.

28. See Figure 70. Clicking on the lock should indicate that the identity of the site is verified.

Figure 70 • Verification of Certificate Installation

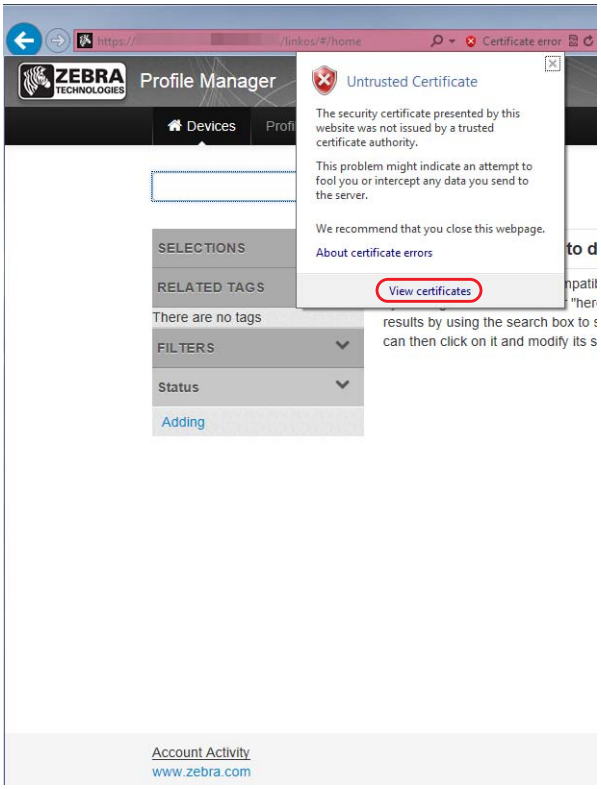


If the lock is not green, it is likely that you do not have permissions to allow the Zebra Root CA. To change your permissions to allow a new certificate authority, see *Changing Permissions* on page 93.

Installation for Internet Explorer 10

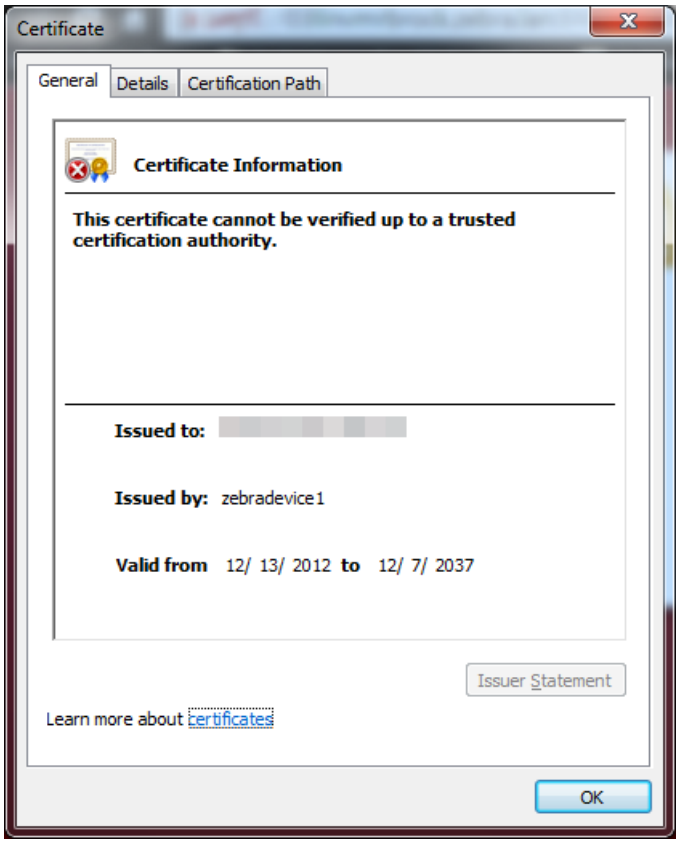
1. Click on the **Certificate error** text in the browser location input bar.
2. See Figure 71. Click on the **View Certificates** link in the dialog box.

Figure 71 • Certificate Information within Internet Explorer



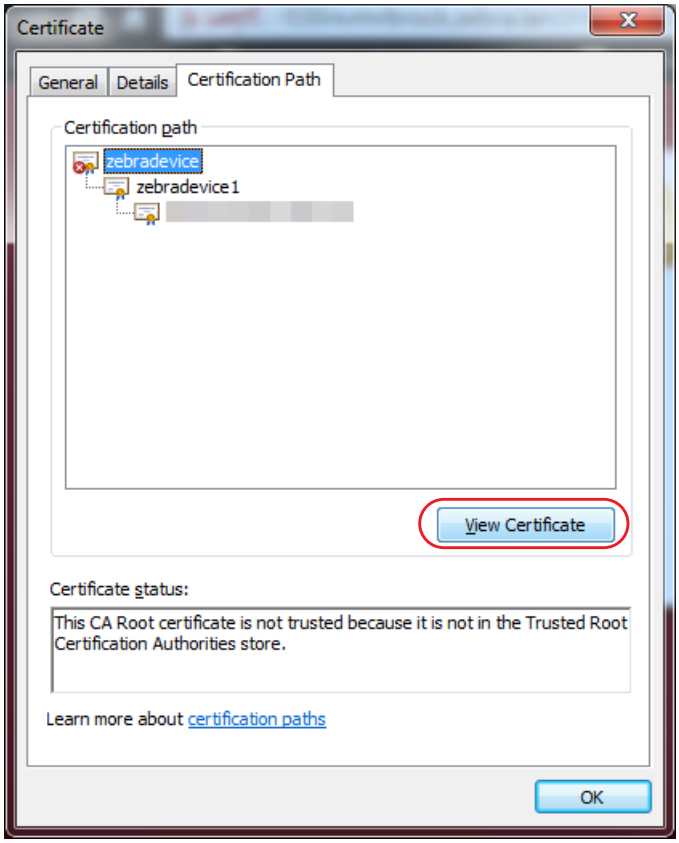
3. See Figure 72. Click on the **Certification Path** tab.

Figure 72 • Certificate Information



4. See Figure 73. Click on **zebradevice** at the top of the tree and click on **View Certificate**.

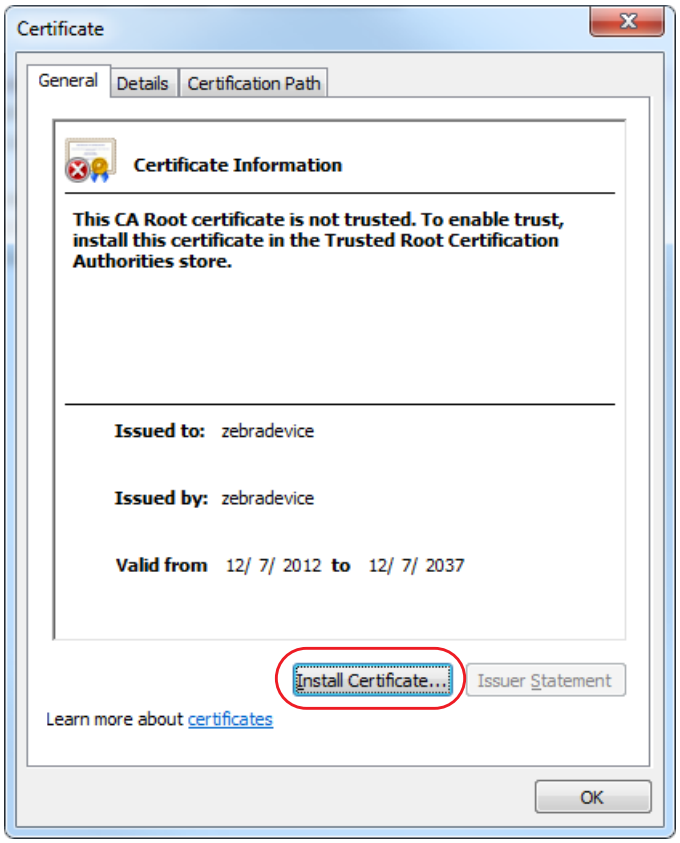
Figure 73 • Certificate Path



The untrusted Zebra certificate will be shown.

5. See Figure 74. Click on **Install Certificate…**.

Figure 74 • Install Certificate



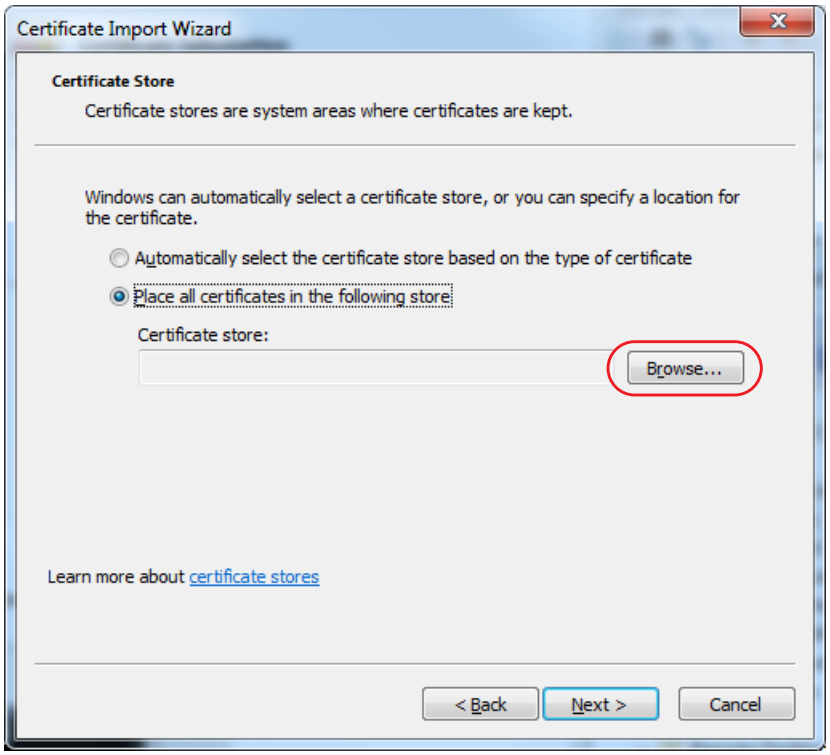
6. See Figure 75. The Certificate Import Wizard will appear.

Figure 75 • Certificate Import Wizard

7. Click **Next**.

8. See Figure 76. Select **Place all certificates in the following store**.

Figure 76 • Certificate Import Wizard Destination Store

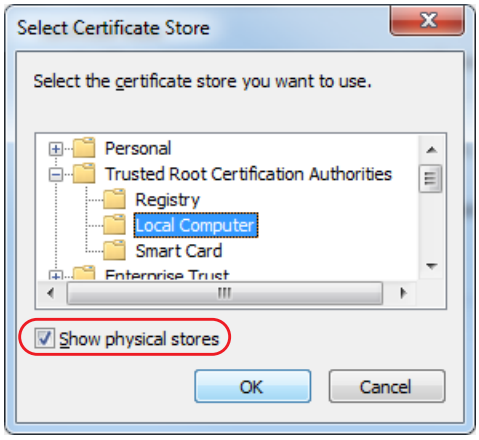


9. Click **Browse**.

10. See Figure 77. Click on the **Show physical stores** and navigate to **Trusted Root Certification Authorities\Local Computer**.

Note • See Figure 77. If 'Local Computer' is not shown under the 'Trusted Root Certification Authorities' entity, please ensure that you have administrator permissions for the computer on which you are attempting to install the Zebra CA. The User Account Control (UAC) on some versions of Windows may also prevent you from seeing the 'Local Computer' option. Please contact your local IT department for more information on administrator permissions and UAC.

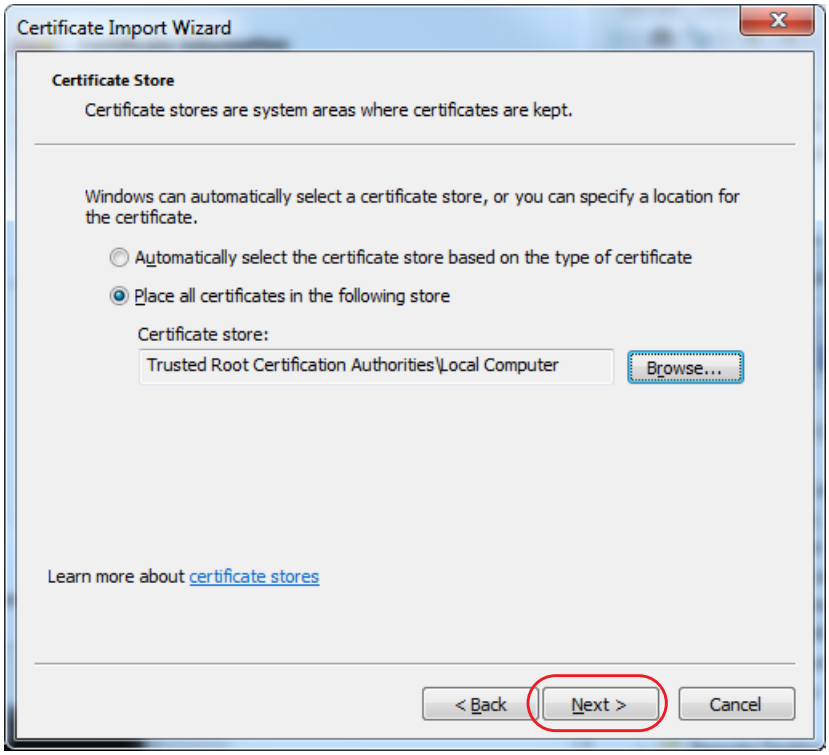
Figure 77 • Certificate Import Wizard Store Selection



11. Click **OK**.

12. See Figure 78. The certificate store should be updated.

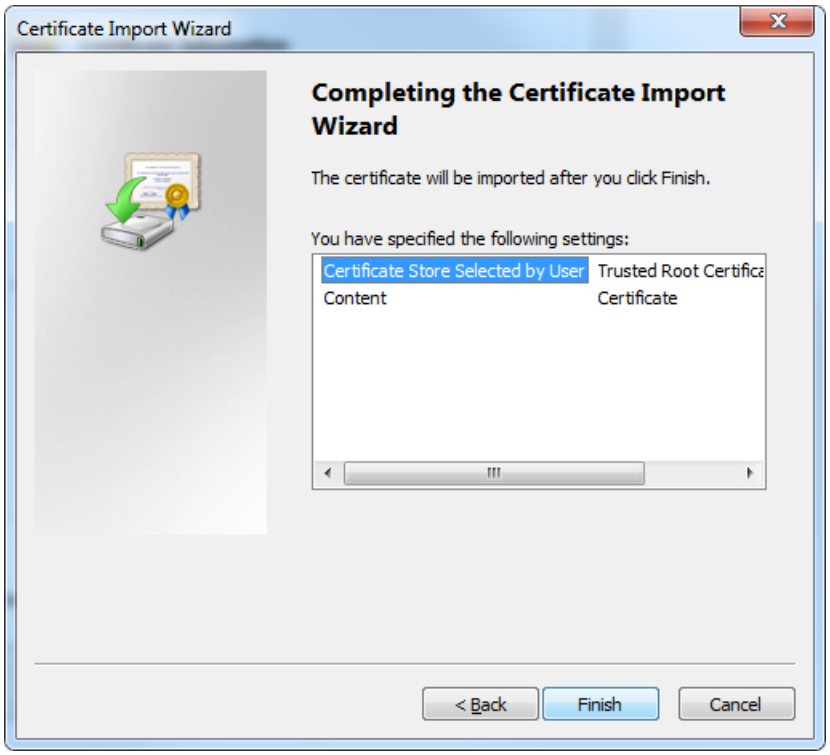
Figure 78 • Certificate Import Wizard Destination Store



13. Click **Next**.

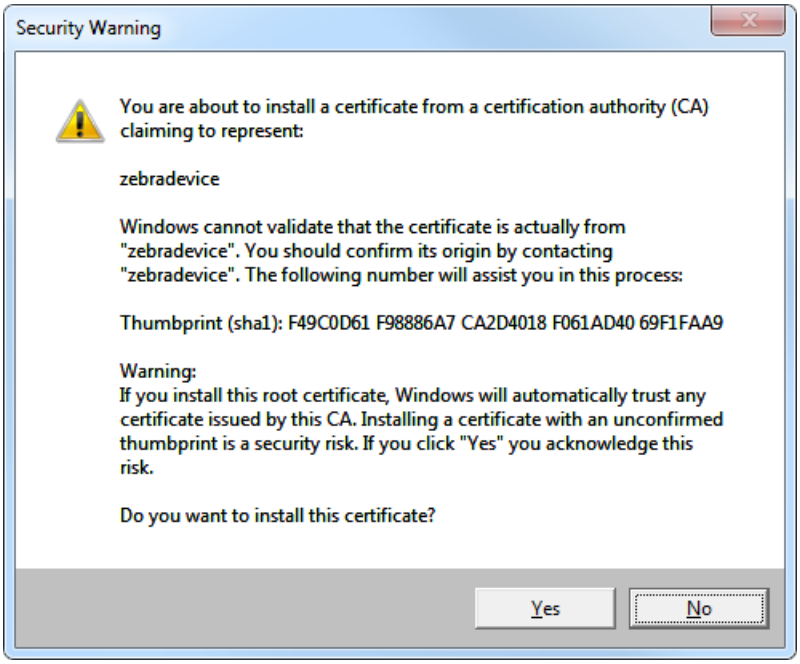
14. See Figure 79. Click **Finish** to install the certificate authority to the local computer.

Figure 79 • Completing the Certificate Import Wizard



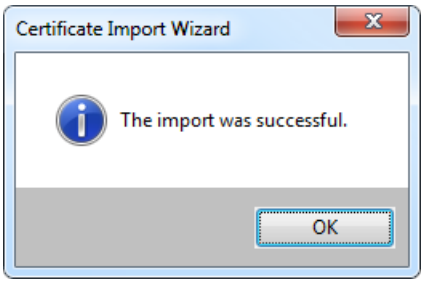
15. You will likely be presented with the Security Warning dialog that indicates the certificate authority origin is unknown. See Figure 80. Click **Yes** to install the Zebra Root Certificate Authority as a Trusted Certificate Authority.

Figure 80 • Agree to Install the Certificate



16. See Figure 81. A dialog box will appear to confim the import's success.

Figure 81 • Import Successful



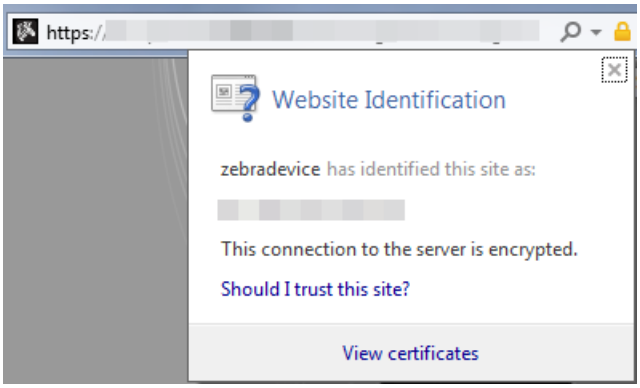
17. Close the Internet Explorer browser and open it again for the new certificate permission to take effect.

18. Return to the Link-OS Profile Manager Application.

    The certificate errors should be resolved and the address bar should be green indicating that the site is trusted.

19. See Figure 82. Clicking on the lock should indicate that the identity of the site is verified.

Figure 82 • Verification of Certificate Installation



If the address bar is not green, it is likely that you do not have permissions to allow the Zebra Root CA. To change your permissions to allow a new certificate authority, see *Changing Permissions* on page 93.

Changing Permissions

This chapter includes the procedure to change permissions to allow the Zebra Certificate Authority (CA) successfully.

Contents

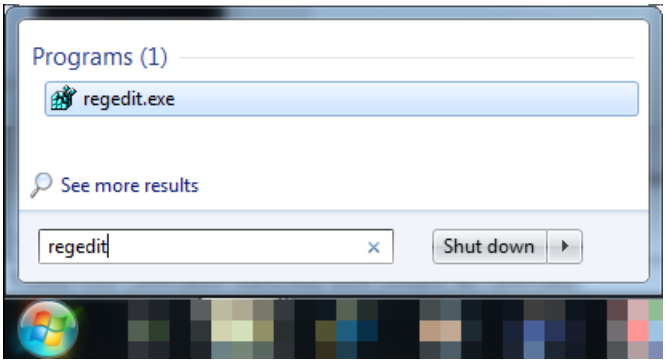
Changing Permissions to Allow a New Certificate Authority

If you encountered difficulties when importing the Zebra CA, you may need to change your permissions to store the CA successfully.

Follow these steps to change your permissions:

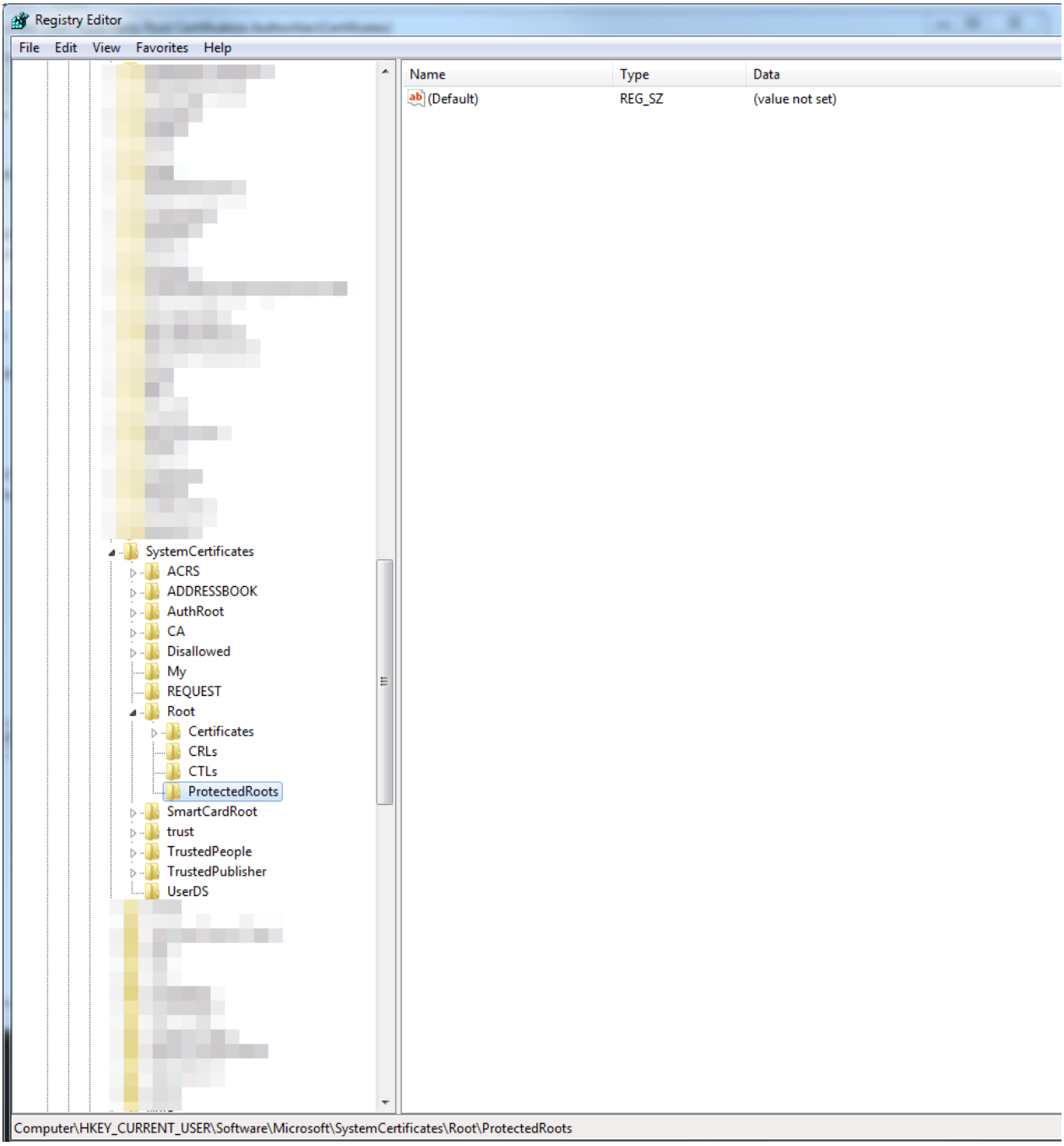
1. See Figure 83. Click on the Windows Logo in the bottom left corner of your screen and type **regedit**.

Figure 83 • Command to Edit the Windows Registry



2. See Figure 84. Navigate to:
`HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\Root\ProtectedRoots`

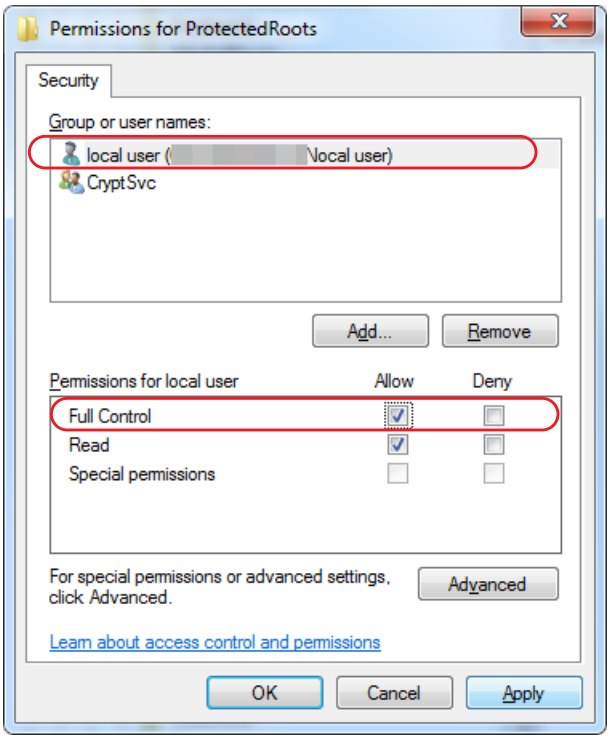
Figure 84 • Location of the ProtectedRoots node



3. Right-click on **Protected Roots and select 'Permissions…**.

4. See Figure 85. Select the **local user** and click **Allow** permission of **Full Control**.

Figure 85 • Permissions for ProtectedRoots



5. Click **Apply** and then, click **OK**.
6. Close the Registry Editor.
7. For Chrome users, repeat step 12 through step 28 in the *Installation for Chrome* on page 65.

   For Internet Explorer users, repeat step 1 through step 19 in the *Installation for Internet Explorer 10* on page 82.
8. Repeat step 1 through step 6 in *Changing Permissions to Allow a New Certificate Authority* on page 94.
9. Click on the Windows Logo in the bottom left corner of your screen and type **regedit**.
10. Navigate to:
    `HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\Root\ProtectedRoots`
11. Right-click on **Protected Roots and select 'Permissions…**.
12. Select the **local user** and uncheck **Allow** permission of **Full Control**.
13. Click **Apply** and then, click **OK**.
14. Close the Registry Editor.

Getting Started Using Profile Manager

This chapter provides an overview and description of the steps necessary to set up and begin to use Profile Manager. For additional details, please see the help system contained within the Profile Manager application.

Contents

Getting Started

After you have completed installation, open Profile Manager. Profile Manager opens to the Devices page.

To set up Profile Manager, follow these steps:

1. *Add Your Devices* on page 98.
2. *Set Tags* on page 98.
3. *Create Base Profile* on page 99.
4. *Deploy Profile to Printers* on page 99.

1. Add Your Devices

Profile Manager automatically detects all the devices on your network. Begin by adding the devices you want to manage.

a. In the Devices tab, click **+Add Device**.
b. In the Add Device field, add your printers by performing ONE of the following:

- Select the device from the ones shown.
- Enter the device name, IP address, or device description.
- Click **View Configured Printers…** and select the device from those shown.

c. Click **Apply** to add the printer.

You can manage your devices individually, or you can filter or group them by status, models, printer types, or media types.

2. Set Tags

Group printers by creating Tags, and adding printers to each Tag.

Begin by creating a Tag to group your devices.

a. On the Tags tab, select **+Add Tag**.
b. Enter Tag Name and Tag Description.
c. Click **Create Tag**.

After you create a Tag, go to the Devices tab to associate one or more devices with your Tag.

a. On the **Devices tab**, select the device you want to associate with your Tag.
b. On the **Tags bar** on your left, click the **Edit** link.

A new dialog box will appear and show all the tags in the system.

c. Click on the tags that you want to assign to the device.

3. Create Base Profile

Copy a printer's "personality profile" and store it for use later to copy to other printers.

a. On the Profiles tab, click **+Create Profile**.
b. On the Filter Devices screen, select a printer and click **Create Profile**.

The profile will be copied and stored for later use.

4. Deploy Profile to Printers

Set up multiple printers at the same time by copying the Base Profile that you set up and sending it out to other printers. Apply these clone files to new printers as needed.

a. On the **Profiles tab**, click on the device whose profile you want to send out to other devices.
b. Click **Send Profile To…**

A list of all your devices will appear.

c. Select the device you want to receive this profile.
d. Click **Apply Profile**.

Zebra Profile Manager setup is now complete.

Notes •

Zebra Technologies Corporation
Zebra Technologies Corporation
475 Half Day Road, Suite 500
Lincolnshire, IL 60069 USA
T: +1 847 634 6700
Toll-free +1 866 230 9494
F: +1 847 913 8766

Zebra Technologies Europe Limited
Dukes Meadow
Millboard Road
Bourne End
Buckinghamshire, SL8 5XF, UK
T: +44 (0)1628 556000
F: +44 (0)1628 556001

Zebra Technologies Asia Pacific, LLC
120 Robinson Road
#06-01 Parakou Building
Singapore 068913
T: +65 6858 0722
F: +65 6885 0838

http://www.zebra.com

P1065697-002