Deltek Know more. Do more.™

Deltek Costpoint® 7.1.1

Post-Installation Hardening Guide

April 22, 2019

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This edition published April 2019.

Contents

Overview

Deltek went a long way to build effective application security into Costpoint 7. The following major security elements are already in place when you install the product:

- **Custom authentication realm for Oracle® WebLogic®**: This custom security realm is used to verify that all valid Costpoint users, not only the administrator, can be authenticated to an application server.
- **Pre-defined security policies for Oracle WebLogic**: When you first start an application server, its internal database of users and rights is initialized with authentication and authorization information necessary to run Costpoint. The list of built-in users and security policies were carefully designed to minimize access to each application server resource.
- **Defense against cross-site scripting attacks:** Both HTML and JavaScript sent from the server to the client computer are monitored for special characters that may be used to set up cross-site scripting attacks.
- **Defense against SQL injections:** Special SQL parsers are used to verify SQL queries for potential SQL injections.

These security features are part of what is called “application security.”

But application security needs to be complemented with “infrastructure security,” recognizing that overall system security is only as good as its weakest link.

Because every Costpoint client has a more or less unique infrastructure, Deltek cannot ship the system correctly pre-packaged for your individual infrastructure needs. Therefore, this guide covers common principles and considerations that system administrators should review and consider for post-installation hardening of the server environment.

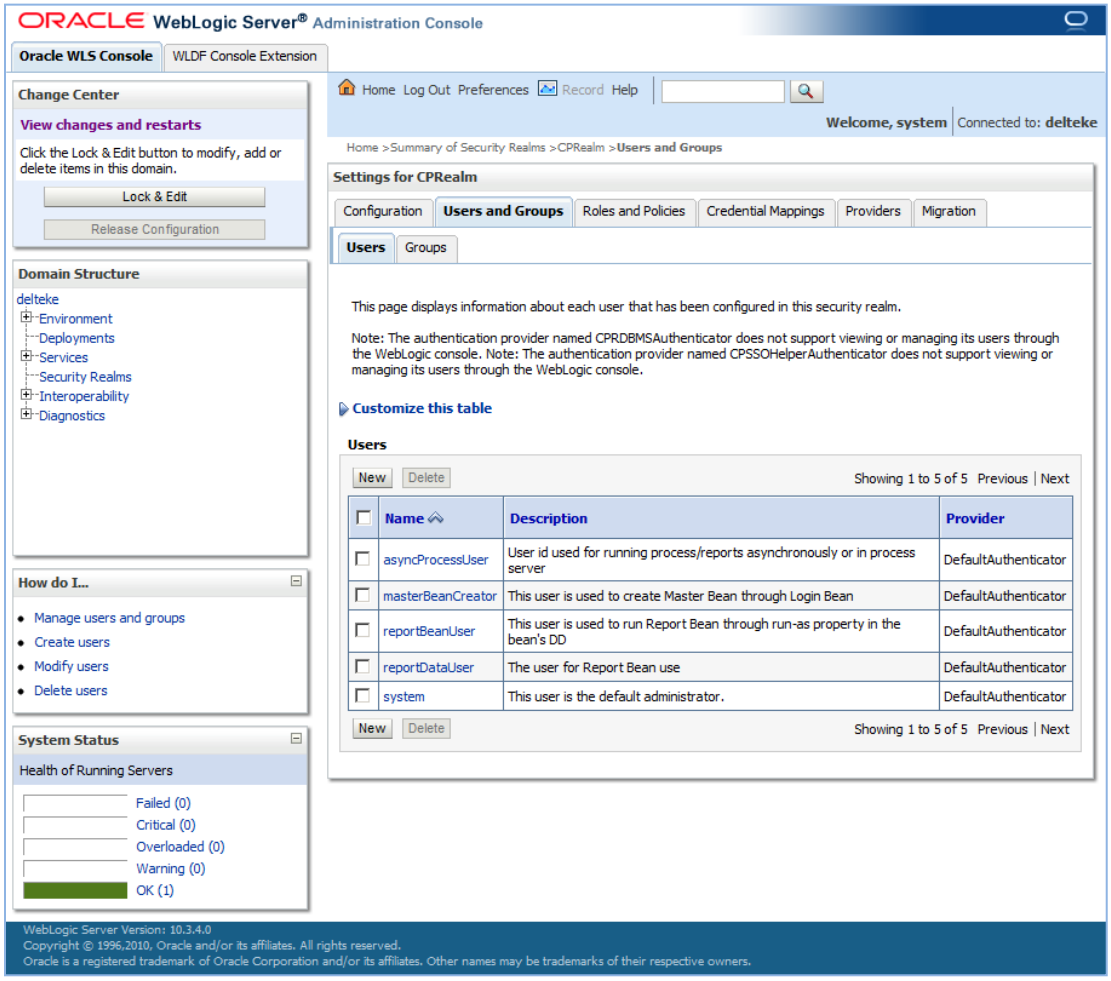
Deltek also recommends the following Oracle documentation about best practices for securing WebLogic servers:

http://docs.oracle.com/cd/E24329_01/web.1211/e24418/practices.htm

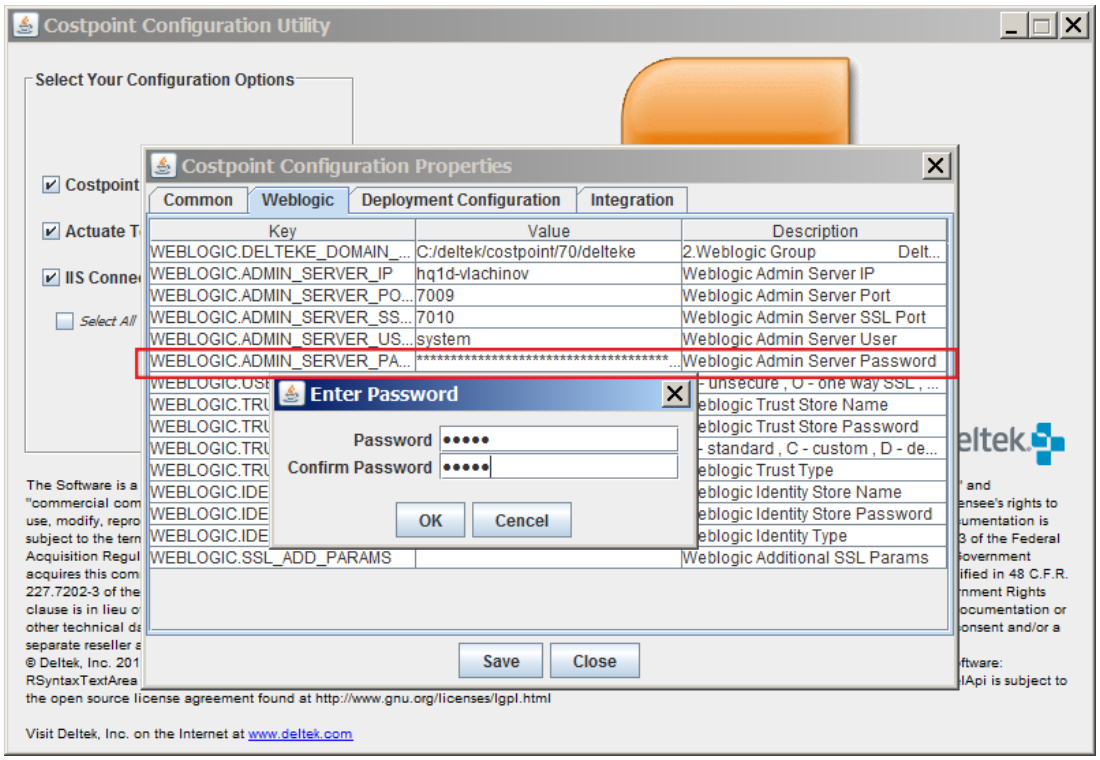
Costpoint-Specific Recommendations for Securing the WebLogic Server

Deltek recommends that you perform the steps and consider the tips described below to secure your WebLogic server environment.

- Change the passwords of all standard, pre-configured users that ship with the system. Make this change through the WebLogic administrative console, under **Security Realms 》 CPRealm » Users and Groups » Users**.



- If you change the password for the **system** user, you will need to re-enter and confirm the new password the next time you log into the Configuration Utility.



After changing the **system** user password you would also need to update boot.properties files for all your WebLogic servers (see Appendix A) .

- If the Metadata schema is in the same database as the Transactional schema, do not give the DELTEK account (the owner of the Transactional schema) access to the Metadata schema.
- Disable the IIOP protocol, using the WebLogic Console (DEServer\Protocols\IIOP tab).
- For production environments, Deltek recommends using IIS.
- For production environments, Deltek recommends placing the WebLogic in the DMZ.

Manage SSL Certificates

WebLogic SSL Certificate

WebLogic is preconfigured with a Demo certificate to support SSL communication. This certificate is mainly for testing purposes. Users accessing the server with a browser will get security exceptions stating that the certificate is untrusted. They need to accept the certificate as trusted and then the browser will successfully access the WebLogic server. For production purposes or for when the server is exposed to external clients or interfaces, Deltek recommends replacing the Demo certificate with a real certificate that is issued by a trusted certificate authority.

For more information, refer to the WebLogic documentation:

https://oracle-base.com/articles/11g/weblogic-configure-ssl-for-a-managed-server

http://www.oracle.com/webfolder/technetwork/tutorials/obe/fmw/wls/12c/12_2_1/01-38-001-ConfiguringSSL/ConfiguringSSL.html

Managing Third-Party SSL Certificates

WebLogic uses java keystore to maintain the list of trusted SSL certificates. This keystore is pre populated with a number of widely trusted CA certificates. If you configure LDAP authentication over SSL or interface the Costpoint WebLogic server with other servers—such Microsoft Exchange or SharePoint—you may encounter security exceptions. This could happen if the other server is using a Demo SSL certificate that is not trusted by WebLogic. You should use the java keytool utility to import the CA certificate of other servers as trusted certificates into the default keystore used by the WebLogic server. This keystore is located under the Java installation folder:

C:\Oracle\<jdk folder>\jre\lib\security\cacerts

For example: C:\Oracle\jdk1.8.0_152\jre\lib\security\cacerts

Run **C:\Oracle\<javafolder>\bin\keytool –help** to get usage information for the utility, or refer to https://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html.

Upgrading Costpoint

Costpoint comes bundled with WebLogic and JDK software. After upgrading Costpoint, previous SSL certificates stored in the WebLogic and JDK files are no longer accessible. This will require the SSL stores to be reconfigured.

In most cases, you would probably upgrade your hardware or operating system to install the new Costpoint version, and this in itself would render the old certificate invalid, thus requiring the certificate to be regenerated and deployed onto the WebLogic server. Third-party certificates such as LDAP, SharePoint, and Exchange Server (which were imported as trusted certificates) are also lost during this upgrade process. Depending on the number of certificates to be maintained, you can choose to either re import them after every upgrade or you can save the certificate store to an alternate location that is accessible even after upgrading Costpoint.

To move the WebLogic SSL certificate to an alternate location:

1. Open the WebLogic Admin Console, and navigate to **delteke » Environment » Servers » DEServer » Configuration tab**.
2. On the Key Stores tab and the SSL tab, edit the **Identity** properties to change the location of the DemoIdentity.jks file from:

C:\oracle\Middleware<xx>\wlserver<..>\server\lib to a location outside the WebLogic installation folder.

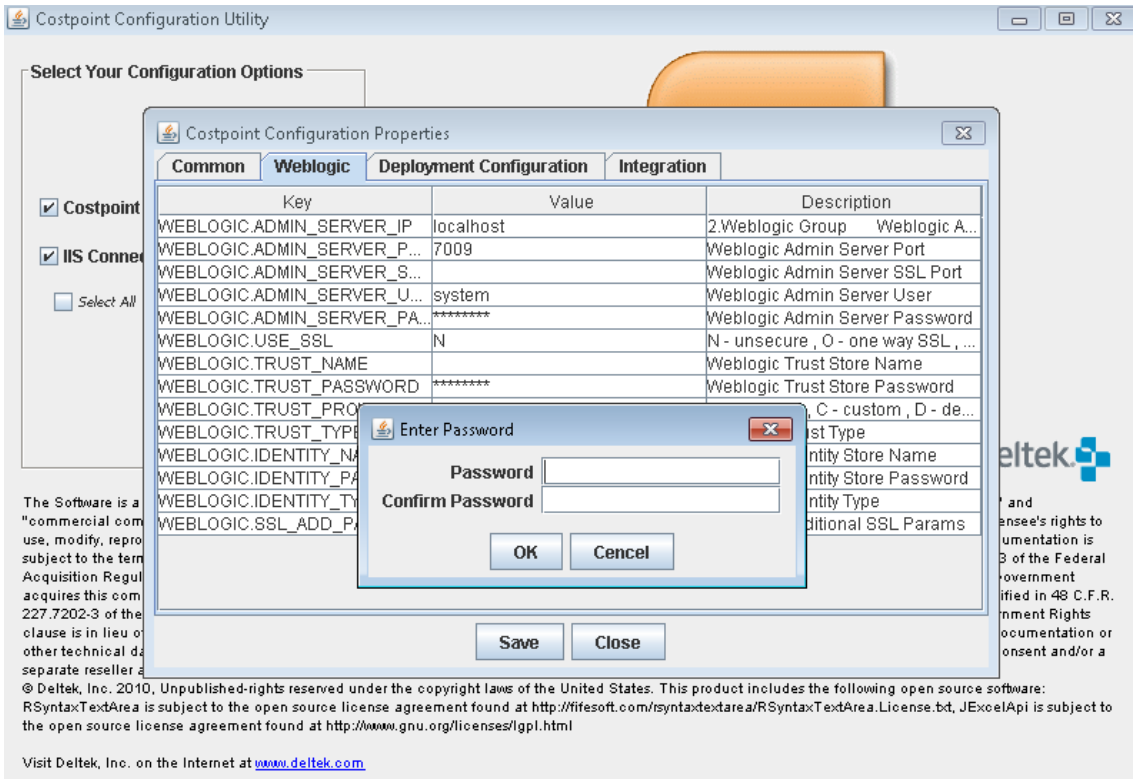
For more information, refer to WebLogic documentation:

https://oracle-base.com/articles/11g/weblogic-configure-ssl-for-a-managed-server#configure-ssl-for-managed-server.

Third party trusted SSL certificates are stored in cacert file of the JDK C:\Oracle\<java folder>\jre\lib\security\cacerts. This location is referenced in two places that need to be updated.

To move the trusted certificate store to an alternate location:

1. Navigate to C:\Oracle\<Java Folder>\jre\lib\security\cacerts where the third-party certificates are stored.
2. Copy the file to an alternate location that will remain accessible after upgrading Costpoint.
3. Open the WebLogic Admin Console, and navigate to **delteke » Environment » Servers » DEServer » Configuration tab**.
4. Click the Key Stores tab, and edit the **Java Standard Trust** properties to point to the new location.
5. Using the Costpoint Configuration Utility, edit the **WEBLOGIC.TRUST_xxx** properties as shown in the following screen shot.



Appendix A: Modifying boot.properties File(s) after Changing the system User Password

Purpose

This step provides instructions for modifying the boot.properties file so that it reflects the WebLogic system user's new password.

Where

This step must be performed on your Costpoint 7.0 WebLogic **application** server.

To modify the WebLogic system user's password in the boot.properties file:

1. Make a backup of the C:\Deltek\Costpoint\71\delteke\servers\DEServer\security\boot.properties file.
2. Open the C:\Deltek\Costpoint\71\delteke\servers\DEServer\security\boot.properties file with a text editor (for example, Notepad).
3. Find **password=** (near the top of the file) and replace the encrypted password (for example, **{AES}GHTVulk923YYpRMrbadNPgjWh55FsmK/EAY/TtP73/w\=**) with your new WebLogic system user's password.

   The clear text password you enter here will automatically get encrypted when you restart your Costpoint Server.

4. Save the **boot.properties** file.
5. Close your text editor.
6. If you have more than one WebLogic server instances - complete steps 1-5 for all WebLogic servers' files.

   For example:

   - C:\Deltek\Costpoint\71\delteke\servers**DEServer1**\security\boot.properties,
   - C:\Deltek\Costpoint\71\delteke\servers**DEServer2**\security\boot.properties
   - And so on

7. Restart all your WebLogic servers.

Mitigating Framesniffing with X-Frame-Options Header in IIS

Framesniffing is an attack technique that takes advantage of browser functionality to steal data from a website. Web applications that allow their content to be hosted in a cross-domain IFRAME may be vulnerable to this attack.

Administrators can mitigate framesniffing by configuring IIS to send an HTTP response header that prevents content from being hosted in a cross-domain IFRAME.

Where

The X-Frame-Options header can be used to control whether or not a page can be placed in an IFRAME. Because the Framesniffing technique relies on being able to place the victim site in an IFRAME, a web application can protect itself by sending an appropriate X-Frame-Options header.

To configure IIS to add an X-Frame-Options header to all responses for a given site:

1. Open Internet Information Services (IIS) Manager.
2. In the Connections pane on the left side, expand the **Sites** folder, and select the site that you want to protect.
3. Double-click the **HTTP Response Headers** icon in the feature list in the middle.
4. In the Actions pane on the right side, click **Add**.
5. In the dialog box that displays, take the following actions:
   - **Name**: Enter **X-Frame-Options** in this field
   - **Value**: Enter **SAMEORIGIN** in this field.
6. Click **OK** to save your changes.

For more information visit http://support.microsoft.com/kb/2694329.

Disable the Server HTTP Response Headers in IIS

Providing verbose HTTP response headers is a form of information disclosure. HTTP response headers can contain detailed information about the Web server that is unneeded for the application to function properly. In most cases, Web servers and frameworks enable these headers by default, opening the application to information disclosure before code has even been written.

An attacker could leverage this vulnerability to determine the exact technological components used by the application. Once identified, an attacker could research these components to discover existing vulnerabilities. Knowledge of the underlying infrastructure also facilitates exploitation of other vulnerabilities, such as OSCI, SQLi, code injection, and so on.

Recommendations

Disable the Server HTTP response headers.

Remove the Server header by creating a DWORD entry called DisableServerHeader in the HKLM\SYSTEM\CurrentControlSet\Services\HTTP\Parameters Windows Server Registry key, and set the value to 1 on every IIS node where Product is deployed.

Additional Resources

This section provides links to relevant online documentation.

Securing WebLogic Servers

- http://docs.oracle.com/middleware/1213/wls/LOCKD/index.html

Securing IIS

- http://www.microsoft.com/technet/security/tools/locktool.mspx

Windows Server 2008 Security Baselines

- 2008: http://technet.microsoft.com/en-us/library/cc514539.aspx

Oracle Recommendations for Securing Multi-Tier Cluster Architecture

- http://download.oracle.com/docs/cd/E12839_01/web.1111/e13709/planning.htm#i1069911
- http://download.oracle.com/docs/cd/E12839_01/web.1111/e13709/planning.htm#insertedID24

Deltek is the leading global provider of enterprise software and information solutions for government contractors, professional services firms and other project- and people-based businesses. For decades, we have delivered actionable insight that empowers our customers to unlock their business potential. 20,000 organizations and millions of users in over 80 countries around the world rely on Deltek to research and identify opportunities, win new business, recruit and develop talent, optimize resources, streamline operations and deliver more profitable projects. Deltek: Know more. Do more.®

deltek.com