

# Migration of Security Artifacts from tWAS to Liberty

—  
Liam Westby  
WebSphere Modernization Development

Gary Picher  
WebSphere Security Architecture



# Migration tools for developers

## Source

```

35 import com.ibm.asphere.samples.jdo.Util;
36
37 //
38 // * Servlet to handle customer account actions.
39 //
40 @Servlet("/servlet/AccountServlet")
41 public class AccountServlet extends HttpServlet
42 {
43     private static final long serialVersionUID=0
44     // Servlet action codes
45     public static final String ACTION_ACCOUNT
46     public static final String ACTION_ACCOUNTIN
47     public static final String ACTION_LOGIN
48     public static final String ACTION_REGISTER
49     public static final String ACTION_SEFLOGST

```

- WebSphere Application Migration Toolkit (<http://ibm.biz/DownloadWASMigTools>)
  - Eclipse-based tooling
  - Version to Version – including Liberty
  - Third-party migration support from JBoss, WebLogic, Oracle, Tomcat
  - Cloud Migration Tool

## Binaries

[illegible]

- Migration Toolkit for Application Binaries (<http://ibm.biz/DownloadWASMigTools>)
  - Command line tooling
  - Version to Version (V85+) and Liberty
  - Cloud migration rules
  - WebSphere configuration to Liberty server config or WebSphere Base edition wsadmin scripts

## Aggregation and Modernization

```

2=<server description="new server">
3
4    <!-- Enable features -->
5    <featureManager>
6        <feature>servlet-3.1</feature>
7        <feature>jsp-2.3</feature>
8        <feature>ejb-3.2</feature>
9    </featureManager>
10
11    <!-- To access this server from a
12    <httpEndpoint id="defaultHttpEndp

```

- Transformation Advisor (<http://ibm.biz/cloudta>)
  - Powered by the Migration Toolkit for Application Binaries
  - Focus on entire cell environment
  - Get estimated developer time cost to modernize
  - More concerned with application modernization than just version to version

# WebSphere Migration Toolkit for Application Binaries

- Command line tooling – download at <https://ibm.biz/DownloadWASmigTools>, use Transformation Advisor, or WebSphere Admin Console.
- Analyzes your application to understand its structure, determine what technologies it uses, and identify specific migration issues in code.
- When specifying an application in a WebSphere cell, generates server configuration for your choice of Liberty or WebSphere base edition.

The screenshot displays the WebSphere Migration Toolkit interface. On the left, a terminal window shows the command line execution of the migration tool. The main window is titled "Application Migration Report" and displays the following information:

**Application Migration Report**  
8/11/21, 2:24 PM  
/Users/liam/Desktop/tls/appDmgr/config/cells/appCell/applications/tls-client\_ear\_server.xml --targetAppServer=liberty --includeSensitiveData --output=tls-migrated/

**Scan options:** --baseEdition --coreEdition --liberty --libertyBuild

**Source options:** --sourceAppServer=was90 --sourceJava=ibm8 --source

**Target options:** --targetAppServer=liberty --targetJava=ibm8

**Excluded packages:** ch.qos, com.fasterxml, com.ibm, com.informix, com.sybase, freemarker, groovy, java, javax, net, oracle, org,

**Technology Evaluation Summary**

This table indicates which IBM platforms fully support the technologies used by your Migration Analysis.

Application	Open Liberty	Liberty for Java on IBM Cloud	Liberty Core
tls-client_ear	✓	✓	✓

**Recommendation:** Address all severe and warning migration issues before deploying.

On the right, the "EXPLORER" pane shows the file structure of the migrated application, including the "tls-client\_ear\_server.xml" file. The "tls-client\_ear\_server.xml" file is selected, and its content is displayed in the main pane. The XML content shows the configuration for the "tls-client\_ear\_server" application, including the "featureManager" section and the "httpEndpoint" configuration.

# Application Security and LDAP Registries

Introduced in the binary scanner in release 20.0.0.4 (available since November 2020).

# Application Security and LDAP Registries

Global security

**Global security > Standalone LDAP registry**

Uses the Lightweight Directory Access Protocol (LDAP) user registry settings when users and groups reside in an external LDAP directory. When security is enabled and any of these properties are changed, go to Security > Global security panel. Click Apply or OK to validate the changes.

Test connection

**General Properties**

\* Primary administrative user name  
jwestby@us.ibm.com

**LDAP server**

Type of LDAP server  
IBM Tivoli Directory Server

\* Host Port  
bluepages.ibm.com 389

Failover hosts  
New Delete

Select	Host	Port
<input type="checkbox"/>		

Base distinguished name (DN)  
o=ibm.com

Search timeout  
120 seconds

☒ Reuse connection

☒ Ignore case for authorization

Custom properties  
New Delete

Select	Name	Value
<input type="checkbox"/>		

**Additional Properties**

\* Advanced Lightweight Directory Access Protocol (LDAP) user registry settings

**Security**

**Server user identity**

☒ Automatically generated server identity  
☐ Server identity that is stored in the repository  
Server user ID or administrative user on a Version 6.0.x node  
Password

Bind distinguished name (DN)

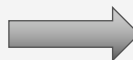
Bind password

☒ SSL enabled  
☐ Centrally managed  
\* Manage endpoint security configurations

☒ Use specific SSL alias  
CellDefaultSSLSettings \* SSL configurations

**Related Items**

\* Trusted authentication realms - inbound  
\* LDAP Test Query



```
<featureManager>
    <feature>appSecurity-
2|3.0</feature>
    <feature>ldapRegistry-
3.0</feature>
</featureManager>

<ldapRegistry
    realm="ldap.example.com:389"
    ldapType="IBM Tivoli
Directory Server"
    baseDN="o=example.com"
    host="example.ibm.com"
    port="389">
</ldapRegistry>
```

# Application Security and LDAP Registries

Security configuration will be migrated for any application deployed to any WebSphere server that has application security enabled.

If the application is part of a security domain, the security domain's configuration will override the global security configuration.

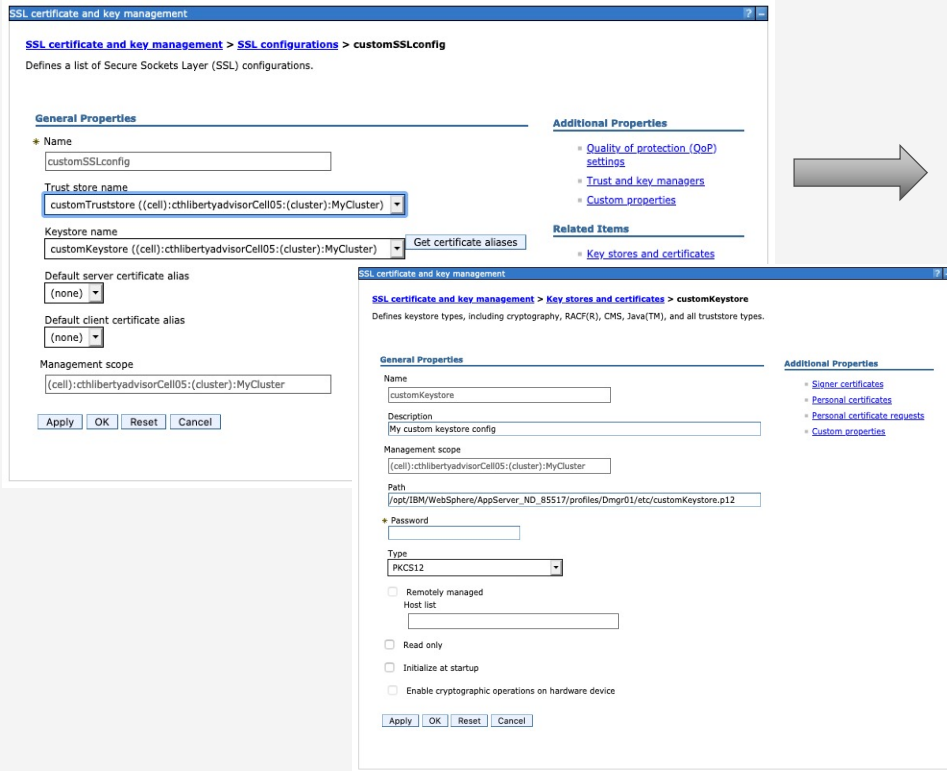
LDAP registry configuration (standalone or federated) and user/group to role mappings will be migrated if configured.

tWAS Function	Liberty Equivalent
Server and application security	appSecurity feature
LDAP – standalone user registry	ldapRegistry configuration element
LDAP – federated user registry	ldapRegistry configuration element(s) and federatedRegistry configuration element
User and group to application role mappings	application-bnd element within application element

# TLS Configuration and Certificate Stores

Introduced in the binary scanner in release 21.0.0.2 (available since June 2021).

# TLS Configuration and Certificate Stores



**SSL certificate and key management**

**SSL certificate and key management > SSL configurations > customSSLconfig**  
Defines a list of Secure Sockets Layer (SSL) configurations.

**General Properties**

Name: customSSLconfig

Trust store name: customTruststore ((cell):cthlbertyadvisorCell05:(cluster):MyCluster)

Keystore name: customKeystore ((cell):cthlbertyadvisorCell05:(cluster):MyCluster) [Get certificate aliases](#)

Default server certificate alias: (none)

Default client certificate alias: (none)

Management scope: ((cell):cthlbertyadvisorCell05:(cluster):MyCluster)

[Apply](#) [OK](#) [Reset](#) [Cancel](#)

**Additional Properties**

- [Quality of protection \(QoP\) settings](#)
- [Trust and key managers](#)
- [Custom properties](#)
- [Key stores and certificates](#)

**SSL certificate and key management**

**SSL certificate and key management > Key stores and certificates > customKeystore**  
Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

**General Properties**

Name: customKeystore

Description: My custom keystore config

Management scope: ((cell):cthlbertyadvisorCell05:(cluster):MyCluster)

Path: /opt/IBM/WebSphere/AppServer\_ND\_85517/profiles/Dmgr01/etc/customKeystore.p12

★ Password:

Type: PKCS12

☐ Remotely managed

Host list:

☐ Read only

☐ Initialize at startup

☐ Enable cryptographic operations on hardware device

[Apply](#) [OK](#) [Reset](#) [Cancel](#)

```
<featureManager>
  <feature>appSecurity-2.0</feature>
</featureManager>

<ssl id="customSSLconfig">

  <keyStoreRef>customKeystore</keyStoreRef>
  <trustStoreRef>customTruststore
</trustStoreRef>
</ssl>

<keyStore id="customKeystore"
  location="customKeystore.p12"
  type="PKCS12"
  password="${keyStore_password_1}"
</keyStore>

<keyStore id="customTruststore"
  location="customTruststore.p12"
  type="PKCS12"
  password="${keyStore_password_2}"
</keyStore>
```



# TLS Configuration and Certificate Stores

Liberty default TLS configuration will be generated by examining the application's deployment targets and selecting the most specific one – server, cluster, node, cell.

Other TLS configurations will be migrated if they are directly referenced by other configuration elements that are migrated – LDAP over TLS configuration, for example.

When specifying the binary scanner parameter `-includeSensitiveData`, all referenced keystore and truststore files will be copied to the output directory.

## [SSL certificate and key management](#) > Manage endpoint security configurations

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

Local Topology

- [-] [Inbound](#)
  - [-] [bloomers1Cell01\(CellDefaultSSLSettings\)](#)
    - [-] [nodes](#)
      - [+] [bloomers1CellManager01](#)
      - [+] [bloomers1Node01\(NodeDefaultSSLSettings\)](#)
    - [-] [clusters](#)
    - [-] [nodegroups](#)
      - [+] [DefaultNodeGroup](#)
- [-] [Outbound](#)
  - [-] [bloomers1Cell01\(CellDefaultSSLSettings\)](#)
    - [-] [nodes](#)
      - [+] [bloomers1CellManager01](#)
      - [+] [bloomers1Node01\(NodeDefaultSSLSettings\)](#)
    - [-] [clusters](#)
    - [-] [nodegroups](#)
      - [+] [DefaultNodeGroup](#)

# Demo

# Wrap Up

# Modernization Tool References

Read



What's new in Transformation Advisor:

<https://www.ibm.com/docs/en/cta?topic=whats-new>

What's new in Migration Tools:

[ibm.biz/WhatsNewMigTools](https://ibm.biz/WhatsNewMigTools)

Introduction to Mono2Micro:

[ibm.biz/Intro2Mono2Micro](https://ibm.biz/Intro2Mono2Micro)

Watch



Explore subjects related to App Modernization (including demos of Transformation Advisor, Mono2Micro, and the WebSphere Migration Tools)  
[ibm.biz/AppTransformersTV](https://ibm.biz/AppTransformersTV)

Experience



Assess your application estate with Transformation Advisor

[ibm.biz/cloudta](https://ibm.biz/cloudta)

Make changes confidently using WebSphere Migration Toolkit

[ibm.biz/WASmigToolkit](https://ibm.biz/WASmigToolkit)

Test drive the Mono2Micro refactoring experience

[ibm.biz/Mono2Micro](https://ibm.biz/Mono2Micro)

# Thank you

Liam Westby  
WebSphere Modernization Development  
[lwestby@us.ibm.com](mailto:lwestby@us.ibm.com)

Gary Picher  
WebSphere Security Architecture  
[gpicher@us.ibm.com](mailto:gpicher@us.ibm.com)

© Copyright IBM Corporation 2022. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and ibm.com are trademarks of IBM Corp., 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 at [Copyright and trademark information](#).

