

IBM® Tivoli® Software

Reconfiguring Maximo-based products automatically

Document version 1.0

*Rob Binns
Software Engineer*

IBM

© **Copyright International Business Machines Corporation 2011.**

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

CONTENTS

List of Tables	iv
Revision History	v
1 Introduction.....	1
2 Access the reconfiguration command line interface tool	1
3 Validation.....	2
4 Input properties files	2
5 Command line interface parameters	3
6 Action scenarios	4
6.1 updateDatabaseConfiguration	5
6.2 updateJ2eeConfiguration.....	5
6.3 enableAppSecurity.....	5
6.4 disableAppSecurity	5
7 Properties	5

LIST OF TABLES

Table 1: Command line interface parameters	3
--	---

REVISION HISTORY

Date	Version	Revised By	Comments
10/31/11	1.0	C.E.L.	Initial version

1 Introduction

When you install a fix pack or otherwise upgrade an existing Maximo-based product, the installation program uses values recorded from the previous deployment. These values are stored on the administrative system in the `install.properties` and `maximo.properties` files located under the `maximo_install_location\etc` and `maximo_install_location\maximo\applications\maximo\properties` directories, respectively.

If you have made any environmental changes to any of the systems used for the original deployment, they must be recorded in the `install.properties` and `maximo.properties` files. Typically these types of changes would include changing a host name or updating a password, for example.

You can update these values manually, or you can use the reconfiguration command line interface tool to update configuration values for your existing deployment when they change. Properties specified when using the reconfiguration command line interface tool, either as parameters, or in an input properties file, replace existing properties in the `maximo.properties` and `install.properties` files. Properties are encrypted upon saving.

The reconfiguration command line interface tool can be used in the following scenarios:

- Change the security model chosen for the original deployment. For example, you can migrate from Maximo-based security to WebSphere Application Server security. Note that this option is not available for Oracle WebLogic Server.
- Update database or J2EE server configuration settings without the server being available. Note that these values cannot be validated in this scenario.

2 Access the reconfiguration command line interface tool

The reconfiguration command line interface tool can be downloaded from the Integrated Service Management Library located at:

<http://www.ibm.com/software/ismlibrary/?NavCode=1TW10MA4E>

Once downloaded, uncompress the archive on the administrative workstation. Inside the archive are two additional compressed files. The `Maximo_750x_ReconfigurationTool_for_AdminWorkstation.zip` file includes the reconfiguration command line interface tool that can be used with v7.5 Maximo-based products. The `Maximo_711x_ReconfigurationTool_for_AdminWorkstation.zip` file includes the reconfiguration command line interface tool that can be used with v7.1 and v7.2 Maximo-based products.

Uncompress the appropriate zipped file into the product installation directory. Within the newly created `Reconfig` directory. The reconfiguration command line interface tool are launched on the administrative workstation:

Windows: `reconfigurePae.bat <command-line-parameters>`

UNIX: `reconfigurePae.sh <command-line-parameters>`

3 Validation

The reconfiguration command line interface tool validates input in the same way the product installation program validates input.

The following list details the validation checks performed by the reconfiguration command line interface tool.

- Host names or IP addresses are correctly formatted and are reachable.
- User IDs and passwords meet length and character set criteria.
- Credentials supplied are used to authenticate to WebSphere.
- Port values supplied are listening on the corresponding host, are numeric, and fall into the correct range.
- Pre-configured middleware can authenticate to the product database.
- Required VMM users exist.

4 Input properties files

There are sample input property files that can be used as input for the reconfiguration command line interface tool. These files contain comments and properties you can update and then use as input for the reconfiguration command line interface tool using the `-input` parameter. In addition, there property files contain properties that can only be updated through the use of this input file. Most properties cannot be used as parameters from the command line.

Four input sample files are found in the `reconfig/samples` directory of the reconfiguration command line interface tool packages.

- `DB2_Sample_input.properties`
- `Oracle_Sample_input.properties`
- `SQLServer_Sample_input.properties`
- `WebSphere_App_Server_Sample_input.properties`

Each of these sample files contain properties associated with a specific database or application server type.

All input properties, introduced from either the command line or located in the input properties file, are validated before they are used. Once validation has passed successfully, then the `maximo.properties` and `install.properties` files will be updated.

5 Command line interface parameters

The following table contains a list of parameters that can be used with the reconfiguration command line interface tool.

Table 1: Command line interface parameters

Parameter name	Description
-validateUsers	Used in conjunction with the enableAppSecurity action to validate users exist in the LDAP repository. If the users do not exist, the existing security model is not modified.
-action	The type of configuration action being performed by the tool. Possible values are: <ul style="list-style-type: none"> • updateDatabaseConfiguration – Used to update existing database configuration values. • updateJ2eeConfiguration - Used to update existing application server configuration values. • enableAppSecurity – Enables application security for the application. This action sets the mxe.useAppServerSecurity property to a value of 1, and updates the mxe.IdapUserManagement flag. This value is written to the database when updated. • disableAppSecurity - Disables application security for the application. Security is handled entirely through Maximo. This action sets the mxe.useAppServerSecurity property to a value of 0. This value is written to the database when updated. <p>The actions that modify the security setting used by Maximo also updates Maximo web.xml files.</p>
-force	The -force option updates the properties file and skips the validation of parameters input to the command line tool through an input properties file. When using this parameter, you are not prompted for confirmation of the property update task.
-buildAndDeployEAR	Rebuilds and deploys application EAR files. Application EAR files must be rebuilt and redeployed for configuration changes to take effect in the application.
-dbserverhost	Host name of the database server.
-dbserverport	Port name of the database server.
-dbname	Name of the database.
-dbuser	User ID that accesses the database.
-dbpwd	Password for the user ID that accesses the database.
-dbrxouser	User ID used to access a remote middleware server.
-dbrxapwd	Password for the user ID used to access a remote middleware server.
-j2eeserverhost	Host name of the J2EE domain manager server. If deployment manager host name or server port is specified the

	thinwsadmin scripts will be updated accordingly.
-j2eeserverport	Port name of the J2EE domain manager server. If deployment manager host name or server port is specified the thinwsadmin scripts will be updated accordingly.
-wasuser	WebSphere administrator user ID. This is the User ID that is used to log into the WebSphere administrative client application. Typically, this user ID is defined as wasadmin.
-waspwd	WebSphere administrator user ID password.
-wasrxouser	Operating system user ID used to access remote WebSphere server host. Typically this user ID is defined either as Administrator or root.
-wasrxapwd	Password for user ID to access remote WebSphere server host.
-applicationServerNode	Name of the application server node.
-applicationServerName	Name of the application server.
-installDir	Installation directory of the application server deployed in the runtime server. Typically this directory is c:\Program Files\IBM\Websphere on Windows systems.
-truststore	Fully-qualified path to the truststore file on the application server. The -truststore is argument is required if the host name is updated. The specified trust store will be copied into the <installation_home>\wasclient\etc directory as trust.p12.
-usermanagement	Used to change the security configuration of the existing Maximo deployment. Possible values are: <ul style="list-style-type: none"> • j2ee – Use this value to change the security setting in Maximo so that both Maximo users and Maximo groups are managed through application server security mechanisms. • mixed – Use this value to manage users through application server security mechanisms, and manage groups using Maximo.
-inputfile	Fully-qualified path to the properties file being used to set properties in a cloned environment. Values specified as command line parameters for the reconfiguration command line interface tool supersede those from the input file.

Processing will stop and tool exits with an error message if the application server type is configured as Oracle Weblogic Server. This tool does not allow you to change database types.

6 Action scenarios

The following sections detail various scenarios for the reconfiguration command line interface tool supported actions.

6.1 updateDatabaseConfiguration

The updateDatabaseConfiguration action is used to update existing database configuration values.

```
-action updateDatabaseConfiguration [-force] [-buildAndDeployEAR] [-dbserverhost hostname] [-dbserverport port] [-dbname name] [-dbuser dbuser] [-dbpwd dbpassword] [-dbrxouser remoteuser] [-dbrxapwd remotepassword] [-inputfile fullyqualifiedpath]
```

6.2 updateJ2eeConfiguration

The updateJ2eeConfiguration action is used to update existing application server configuration values.

```
-action updateJ2eeConfiguration [-force] [-j2eeserverhost fullyqualifiedDMgrhostname] [-truststore fullyqualifiedpathtotruststore] [-j2eeserverport port] [-wasuser WebSphereAdminuser] [-waspwd WebSphereAdminuserpassword] [-wasrxouser WebSphereRemoteuser] [-wasrxapwd WebSphereRemoteuserpassword] [-applicationServerNode NodeName] [-applicationServerName applicationserverhostname] [-installDir WebSphereinstallDir] [-inputfile fullyqualifiedpath]
```

6.3 enableAppSecurity

The enableAppSecurity action enables application security for the application. This action sets the mxe.useAppServerSecurity property to a value of 1, and updates the mxe.IdapUserManagement flag according to the setting of the `-usermanagement` parameter. This value is written to the database when updated. The maximouiweb, maxrestweb, meaweb, and mboweb web.xml files are updated during this action.

The action

```
-action enableAppSecurity -usermanagement {j2ee,mixed} [-buildAndDeployEAR] [-validateUsers] [-force]
```

6.4 disableAppSecurity

The disableAppSecurity action disables application security for the application. This action sets the mxe.useAppServerSecurity property to a value of 0. This value is written to the database when updated. Using this action reverts the security implementation to Maximo-based security for users and groups. The maximouiweb, maxrestweb, meaweb, and mboweb web.xml files are updated during this action.

```
-action disableAppSecurity [-buildAndDeployEar] [-force]
```

7 Properties

The following table contains a list of properties that can be modified using the reconfiguration command line interface tool through the use of an input.properties file.

Table 2 Properties available to be reconfigured through the reconfiguration command line interface tool

Category	Property	Definition
DB2 Properties	mxe.db.schemaowner	Owner of the database schema. This value is written to the database when updated.
	Database.DB2.ServerHostName	Host name of the DB2 server. For example, mymachine.mydomain.com. This value is written to the database when updated.
	Database.DB2.ServerPort	Database server port. For example, 50005. This value is written to the database when updated.
	Database.DB2.InstanceName	Name of the database instance. For example, ctginst1. This value is written to the database when updated.
	Database.DB2.DatabaseName	Name of the database. For example, maxdb75. This value is written to the database when updated.
	Database.DB2.InstallLocation	Install location of the database. For example, /opt/IBM/db2/V9.7
	Database.DB2.LogFileSize	Set the size for transaction logs. For example, 4096
	Database.DB2.AppCtlHeapSize	Application control heap size. For example, 1024
	Database.DB2.ApplHeapSize	Application heap size. For example, 1024
	Database.DB2.LockListSize	Size allocated to the lock list. For example, 30000
	Database.DB2.LogSecond	Number of secondary log files allowed. For example, 4
	Database.DB2.ServiceUser	User ID used to autostart.
	Database.DB2.ServicePassword	Password for Database.DB2.ServiceUser.
	Database.DB2.PageSize	Page size setting. Measured in kb. For example, 32
	Database.DB2.ExtentSize	Number of pages per extent (group of pages). For example, 32
	Database.DB2.FencedUser	Fenced user ID for DB2 on Linux® or UNIX

		systems. For example, db2fenc1.
	Database.DB2.AuthType	Method DB2 uses to authenticate users. For example, server.
	Database.DB2.DataTablespaceName	DB2 table space name for the product database. For example, maxdata.
	Database.DB2.BufferPoolName	DB2 buffer pool name. For example, MAXBUFPOOL.
	Database.DB2.BufferPoolLocation	Location of the buffer pool.
	Database.DB2.BufferPoolSize	Size of the buffer pool. For example, 32
	Database.DB2.DataTablespaceLocation	Location of DB2 database table space.
	Database.DB2.DataTablespaceSize	Table space size, measured in Mb. For example, 1000.
	Database.DB2.DataTablespaceMaxSize	Maximum size of the table space, measured in Mb. For example, 8000.
	Database.DB2.TempTablespaceName	Temporary table space name. For example, maxtemp.
	Database.DB2.TempTablespaceLocation	Location of temporary table space.
	Database.DB2.TempTablespaceSize	Temporary table space size, measured in Mb. For example, 1000.
	Database.DB2.TempTablespaceMaxSize	Maximum size of the table space, measured in Mb. For example, 8000.
	Database.DB2.IndexTablespaceName	Index table space name. For example, maxdata.
	Database.DB2.IndexTablespaceLocation	Location of index table space.
	Database.DB2.IndexTablespaceSize	Index table space size, measured in Mb. For example, 1000.
	Database.DB2.IndexTablespaceMaxSize	Maximum size of the index table space, measured in Mb. For example, 8000.
	Database.DB2.InstanceAdminUserName	Administrative user or the database instance.
	Database.DB2.InstanceAdminPassword	Password for the user ID specified for Database.DB2.InstanceAdminUserName
	Database.RemoteAccessUserName	Database server system user ID that is used for configure the database remotely.
	Database.RemoteAccessPassword	Password for user ID named in Database.RemoteAccessUserName.
Oracle	Database.RemoteAccessUserName	Database server system user ID that is used for

		configure the database remotely.
	Database.RemoteAccessPassword	Password for user ID named in Database.RemoteAccessUserName.
	Database.Oracle.InstanceName	Oracle instance name. This value is written to the database when updated.
	Database.Oracle.SoftwareOwner	Owner of the software installation. For example, oracle.
	Database.Oracle.SoftwareOwnerPassword	Password for the user ID listed in Database.Oracle.SoftwareOwner.
	Database.Oracle.InstallLocation	Oracle installation location. For example, /opt/app/oracle/product/10.2.0/db_1.
	Database.Oracle.DataTablespaceName	Oracle table space name for the product database. For example, maxdata.
	Database.Oracle.InstanceLocation	Oracle instance location. For example, /opt/app/oracle/product/10.2.0/db_1.
	Database.Oracle.DataTablespaceLocation	Location of Oracle database table space.
	Database.Oracle.DataTablespaceSize	Tablespace size, measured in Mb. For example, 1000.
	Database.Oracle.DataTablespaceMaxSize	Maximum size of the table space, measured in Mb. For example, 8000.
	Database.Oracle.TempTablespaceName	Temporary table space name. For example, maxtemp.
	Database.Oracle.TempTablespaceLocation	Location of temporary table space.
	Database.Oracle.TempTablespaceSize	Temporary table space size, measured in Mb. For example, 1000.
	Database.Oracle.TempTablespaceMaxSize	Maximum size of the temporary table space, measured in Mb. For example, 8000.
	Database.Oracle.IndexTablespaceName	Index table space name. For example, maxdata.
	Database.Oracle.IndexTablespaceLocation	Location of index table space.
	Database.Oracle.IndexTablespaceSize	Index table space size, measured in Mb. For example, 1000.
	Database.Oracle.IndexTablespaceMaxSize	Maximum size of the index table space, measured in Mb. For example, 8000.
	Database.Oracle.ServerHostName	Host name of the Oracle server.
	Database.Oracle.ServerPort	Port number used by Oracle.

		For example, 1521. This value is written to the database when updated.
	Database.DBAUserName	Oracle DBA user name. For example, sys.
	Database.DBAPassword	Password for user ID listed for Database.DBAUserName.
SQL Server	Database.SQL.DatabaseName	Name of the database. For example, maxdb75. This value is written to the database when updated.
	Database.SQL.InstallLocation	Microsoft SQL Server installation location. For example, C:\Program Files\Microsoft SQL Server\90.
	Database.SQL.DataFileLocation	Location for database data file.
	Database.SQL.DataFileName	A way to specify the name of the data file used for the database. For example, maxdb75_dat.
	Database.SQL.DataFileMaxSize	Maximum size for data file for database.
	Database.SQL.DataFileSize	Initial size for data file for database.
	Database.SQL.LogFileName	A way to specify the name for the database transaction log file. For example, maxdb75_log.
	Database.SQL.LogFileSize	Microsoft SQL Server Database transaction log file size.
	Database.SQL.DataFilegroupName	Database logical name file group. For example, PRIMARY.
	Database.SQL.ServerHostName	Host name of the database server. For example, myhost.mydomain.com.
	Database.SQL.ServerPort	Database server port. For example, 1433. This value is written to the database when updated.
	Database.SQL.InstanceAdminUserName	Administrative user for the Microsoft SQL Server instance. used during install for creating database, creating database user, and modifying the database.
	Database.SQL.InstanceAdminPassword	Administrative users password.
WebSphere	WAS.InstallLocation	Installation location for WebSphere Application Server Network Deployment. For example, C:\IBM\WebSphere\AppServer
	WAS.DeploymentManagerHostName	Host name of the WebSphere Application Server Network Deployment deployment manager. This value is written to the database when updated.
	WAS.CellName	WebSphere Application Server Network Deployment CELL name. For example, ctgCell01.

	WAS.DeploymentManagerProfileName	WebSphere Application Server Network Deployment profile name. For example, ctgDmgr01
	WAS.DeploymentManagerProfileRoot	Location of the WebSphere Application Server Network Deployment profile. For example, C:/IBM/WebSphere/AppServer/profiles/ctgDmgr01
	WAS.ServerProfileName	WebSphere Application Server Network Deployment application server profile name. For example, ctgAppSrv01
	WAS.NodeName	WebSphere Application Server Network Deployment node name. For example, ctgNode01
	WAS.ApplicationServerName	WebSphere Application Server Network Deployment application server name. For example, MXServer. This value is written to the database when updated.
	WAS.ClusterName	WebSphere Application Server Network Deployment cluster name. For example, MAXIMOCLUSTER. This property is designated for future use.
	WAS.AdminUserName	WebSphere Application Server Network Deployment administrator name. For example, wasadmin
	WAS.AdminPassword	WebSphere Application Server Network Deployment administrator password.
	WAS.RemoteAccessUserName	WebSphere Application Server Network Deployment deployment manager system user ID used for tasks such as copying ISC WAR files and fetching the keystore.
	WAS.RemoteAccessPassword	WebSphere Application Server Network Deployment deployment manager system user password.
	WAS.VirtualHost	Name of the WebSphere Application Server Network Deployment virtual host. For example, maximo_host.
	WAS.VirtualHostPort	Port for virtual host for listening for HTTP server. For example, 80.
	WAS.WebServerHostName	Host name where the HTTP server is located.
	WAS.AppServerJvmHeapMin	Minimum heap size setting for the application server JVM. For example, 512.
	WAS.AppServerJvmHeapMax	Maximum heap size setting for the application server JVM.

		For example, 1024.
	WAS.SibName	Name of the service integration bus. For example, intjmsbus.
	WAS.SibHiMsg	Service integration bus high message count. For example, 500000.
	WAS.SibBusUser	Service integration bus user.
	WAS.SibBusPass	Service integration bus user password.
	WAS.WebServerName	Name of the WebSphere Application Server Network Deployment web server. Used to manage HTTP server from within WebSphere Application Server Network Deployment. For example, webserver1.
	WAS.SibPersistMessages	Binary value that indicates if service integration bus messages are persisted in either the product database or a local derby database. A value of true indicates that the messages are persisted.
	WAS.SibDSName	Service integration bus data source name created to access the service integration bus persistence store. For example, intjmsds.
	WAS.SibDBType	Database type where the service integration bus messages are being stored. For example, DB2.
	WAS.SibDBName	Name of the service integration bus messages database.
	WAS.SibDBInstance	Instance name of the service integration bus database.
	WAS.SibDBServerName	Server name of the system hosting the service integration bus message database.
	WAS.SibDBServerPort	Database server port for the database containing the service integration bus messages. For example, 50005.
	WAS.SibDBUserName	User ID used to access the persistence data store database for service integration bus messages.
	WAS.SibDBUserPass	Password for user ID named in WAS.SibDBUserName.
	WAS.SibDBInstallDir	Where the service integration bus database is installed. For example, C:\Program Files\IBM\SQLLIB.
	WAS.SibDbFencedUser	Fenced user ID for the service integration bus database. This property is only used for databases hosted on UNIX® systems. For example, db2fenc1.
	WAS.SibDbInstanceAdminUser	Instance owner for the service integration bus database.

Properties **Error! Reference source not found.**

	WAS.SibDbInstanceAdminPassword	Password for the instance owner of the service integration bus database.
	WAS.SibDbRemoteAccessUser	Database server system user used to configure the service integration bus remotely.
	WAS.SibDbRemoteAccessPassword	Password for user ID named in WAS.SibDbRemoteAccessUser.



© Copyright IBM Corporation 2011
IBM United States of America
Produced in the United States of America
US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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
Armonk, NY 10504-1785
U.S.A.*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PAPER "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 states 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 may be made periodically to the information herein; these changes may be incorporated in subsequent versions of the paper. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this paper at any time without notice.

Any references in this document to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
4205 South Miami Boulevard
Research Triangle Park, NC 27709 U.S.A.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Other company, product, or service names may be trademarks or service marks of others.