



Installing on IBM WebSphere Application Server



Installing on IBM WebSphere Application Server

This edition applies to version 7, release 2, modification 0 of IBM Tivoli Asset Management for IT and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2002, 2009.**

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

Contents

Figures	vii
--------------------------	------------

Tables	ix
-------------------------	-----------

Chapter 1. Introduction 1

Asset Management for IT components	1
Hardware and software requirements	2

Chapter 2. Planning to deploy IBM Tivoli Asset Management for IT 7

Tivoli Asset Management for IT deployment topologies	7
Planning for Tivoli Asset Management for IT middleware worksheet	8
Reusing existing middleware components	15
Planning for Tivoli Asset Management for IT worksheet	16
Planning for security	18
Planning language support	20
System password policy settings	21

Chapter 3. Preparing to install IBM Tivoli Asset Management for IT 23

DVD layout	23
Before you begin	23
Checking port availability	23
Accessing system directories	24
Disabling the firewall	24
Deleting the TEMP and TMP user environment variables	24
Verifying the required rpm-build package is installed	25
Setting the ulimit	25
Setting the swap size	26
Setting shared memory	26
Enabling remote configuration	26
Preparing UNIX systems for Tivoli Asset Management for IT middleware	27
Increasing AIX file size and number of descriptors	27
Increasing AIX paging space	27
Enabling asynchronous I/O on AIX	28
Checking for required libraries on Linux	29
Configuring the JRE in Linux	29
Tivoli Asset Management for IT Launchpad	29
Starting the Launchpad	30

Chapter 4. Deploying IBM Tivoli Asset Management for IT with automatic middleware configuration. 33

Installing IBM Tivoli Asset Management for IT middleware	33
Process ID	35

Tivoli middleware installer workspace	36
Tivoli Asset Management for IT middleware deployment plan overview	37
Options for invoking the deployment plan	37
Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer	38
Tivoli middleware installer logs	47
Incorrect db2admin password	48
Invalid DB2 password value	50
Configuring IBM Tivoli Directory Server user and group strings	51
Installing middleware silently	52
Silent middleware installation program options	54
IBM Tivoli Asset Management for IT installation program overview	56
Tivoli Asset Management for IT simple install path values	58
Performing IBM Tivoli Asset Management for IT installation	60

Chapter 5. Deploying IBM Tivoli Asset Management for IT automatically reusing existing middleware 77

Reusing middleware	77
Reusing IBM DB2	77
Reusing Oracle	78
Reusing IBM Tivoli Directory Server	79
Reusing Microsoft Active Directory	79
IBM Tivoli Asset Management for IT installation program overview	81
Tivoli Asset Management for IT simple install path values	83
Performing IBM Tivoli Asset Management for IT installation	84

Chapter 6. Installing IBM Tivoli Asset Management for IT with manual middleware configuration 101

Manually configuring the database server	101
Manually configuring DB2 9.x	102
Manually configuring DB2 8.2	106
Manually configuring Oracle 11g	110
Manually configuring Oracle 10g	112
Manually configuring Oracle9i Rel2	114
Manually configuring SQL Server	116
Manually configuring the directory server	118
Manually configuring IBM Tivoli Directory Server	118
Manually configuring Microsoft Active Directory	121
Manually configuring the J2EE server	127

Manually configuring Virtual Member Manager on IBM WebSphere Application Server	128
Manually configuring WebSphere Application Server Network Deployment	131
Manually configuring JMS queues	131

Chapter 7. Installing IBM Tivoli Asset Management for IT without middleware autoconfiguration 143

Chapter 8. Installing IBM Tivoli Asset Management for IT language pack . . . 153

Installing IBM Tivoli Asset Management for IT language pack with the Launchpad	153
Installing language packs with Process Solution Installer	155

Chapter 9. Installing IBM Tivoli Asset Management for IT middleware on Linux on System z 157

Installing and configuring DB2 on Linux on System z	157
Installing and configuring IBM Tivoli Directory Server on Linux on System z	162
Installing and configuring WebSphere Application Server Deployment Manager on Linux on System z	163
Creating profiles using 64-bit WebSphere Application Server Deployment Manager for Linux on System z	164
Installing and configuring IBM HTTP Server on Linux on System z	167
Installing and configuring the WebSphere plug-in on Linux on System z	168
Installing and configuring Virtual Member Manager on WebSphere on Linux on System z	169

Chapter 10. Installing middleware on Solaris and HP-UX 171

Operating system preparation	171
Solaris 10.	171
HP-UX 11i	171
Installing the components	171
Installing DB2	172
Installing DB2 fix packs	174
Installing IBM Tivoli Directory Server	174
Installing WebSphere Application Server Network Deployment	175
Creating WebSphere Application Server Network Deployment profiles	176
Installing the WebSphere update installer	178
Installing and configuring IBM HTTP Server	179
Installing and configuring the WebSphere Plug-in	181
Configuring Virtual Member Manager on WebSphere Application Server.	183
Configuring the authentication service in IBM WebSphere Network Deployment	184

Chapter 11. Starting IBM Tivoli Asset Management for IT middleware on Windows 187

Chapter 12. Starting IBM Tivoli Asset Management for IT middleware on UNIX 189

Chapter 13. Uninstalling IBM Tivoli Asset Management for IT middleware . 191

Chapter 14. IBM WebSphere Application Server management . . . 193

Starting the MXServer application server from the command line	193
Starting the MXServer application server from the administrative console	194
Securing WebSphere Administrative Console	195
Configuring the WebSphere Application Server to run as a Windows service	196
Configuring the WebSphere node agent to run as a Windows service	198
Creating a WebSphere Application Server Network Deployment cluster	199

Chapter 15. IBM WebSphere Portal Server overview 201

Tivoli Asset Management for IT deployed on WebSphere Portal Server	201
--	-----

Chapter 16. Installing IBM Tivoli Integration Composer 205

IBM Tivoli Integration Composer overview	205
Integration Composer backward compatibility	206
Hardware and software requirements	207
Installation prerequisites.	208
Performing the Tivoli Integration Composer installation	209
Installing Tivoli Integration Composer on 32-bit Windows using the launchpad	209
Installing IBM Tivoli Integration Composer on 64-bit Windows operating systems	211
Installing Tivoli Integration Composer on UNIX operating systems	213
Confirming the installation.	216
Post-installation tasks.	216
Verifying the settings in the Integration Composer fusion.properties file	216
Changing the memory allocation in the startFusion file (optional)	217
Changing the memory allocation in the commandLine file (optional)	218
Uninstalling Integration Composer	219
Uninstalling Integration Composer on Windows operating systems	219
Uninstalling on UNIX operating systems	219

Chapter 17. IBM Tivoli Asset Management for IT post installation tasks 221

Performing post installation tasks for the J2EE server	221
Initial data configuration	223
Signing in using a default user ID	223
Configuring SMTP	224
Create currency codes	225
Create item and company sets	225
Create an organization	225
Create a general ledger account component	226
Applying changes to the database	226
Create a general ledger account	227
Update General Ledger Component Type Authorization	227
Create default insert site	228
Create a Work Type	228
Specify a top-level class for IT assets and software	228
Create a classification structure for IT assets	229
Signing out and signing in	230
Manually configuring the VMMSYNC cron task for Microsoft Active Directory	230
Tuning DB2	231
Process solution package installation methods	232
Software life cycle operations	233
Process solution packages	233
Package types	234
Aggregation packages	235
Determining which process solution installation program to use	235
Supported operations for the process solution installation programs	236
Before using the process solution installation programs	237
Managing process solution deployment from the IBM Tivoli Asset Management for IT administrative workstation	237
Typical deployment operation	237
Selectable features	238
Deferring J2EE and database related configuration	242
Manually completing deployment	244
Pre-deployment system check	244
Installing process managers using the Process Solution Installation wizard	246
Process solution installation client command-line interface	247

Invoking the process solution installation client CLI	248
Process solution command line interface reference	250
Installing and refreshing language support files for a package	261
Deployment for packages with a single special language support feature	262
Deployment for packages with multiple language support features	262
Process Solution Installation logs	263
Post product installation process manager tasks	266
Before working with BIRT reports	266
Generating xml request pages in Asset Management for IT	267
Synchronizing data	267

Chapter 18. Uninstalling IBM Tivoli Asset Management for IT 271

Uninstalling an automatically configured IBM Tivoli Asset Management for IT	271
Running the IBM Tivoli Asset Management for IT uninstall program for automatically configured middleware	272
Uninstalling a manually configured IBM Tivoli Asset Management for IT	273
Running the IBM Tivoli Asset Management for IT uninstall program for a manually configured deployment	273
IBM Tivoli Asset Management for IT database configuration recovery	274
Restoring the DB2 database server	274
Restoring the Oracle database	275
Restoring the Microsoft SQL Server database	276
Troubleshooting the product uninstallation program	277
Error CTG00001 when performing an uninstall	277
Uninstalling IBM Tivoli Asset Management for IT silently	277
Uninstalling the maximo.ear file	278

Notices 279

Trademarks	280
----------------------	-----

Index 283

Figures

1.	Tivoli Asset Management for IT Components	1	6.	Asset Management for IT installation flow- Installing Asset Management for IT language pack.	154
2.	Asset Management for IT Deployed in a Cluster	8	7.	Asset Management for IT installation flow last step - Installing Integration Composer..	205
3.	Asset Management for IT Installation flow - Tivoli middleware installation	34			
4.	Tivoli Asset Management for IT installation flow - Tivoli Asset Management for IT installation.	57			
5.	Tivoli Asset Management for IT installation flow - Tivoli Asset Management for IT installation.	81			

Tables

1. Asset Management for IT hardware and software requirements	2	16. Policy settings and their values.	122
2. List of users and groups created during Asset Management for IT installation. Plan your value here..	9	17. Prerequisite Tasks and their Commands	165
3. Tivoli middleware installer. Plan your value here...	10	18. Profile commands	165
4. DB2 configuration.	10	19. Profile commands	176
5. Oracle configuration	12	20. WebSphere Application Server processes.	194
6. SQL Server configuration	13	21. Administrative Group Roles and their descriptions.	196
7. WebSphere Application Server configuration	14	22. Asset Management for IT EAR and WAR files	201
8. IBM Tivoli Directory Server configuration	15	23. Product compatibility with Integration Composer 7.2 and integration adapters	206
9. Microsoft Active Directory configuration	15	24. Login specifications for the Maximo database	210
10. Settings for a custom installation	16	25. Login specifications for the target (Maximo) database	212
11. Tivoli Asset Management for IT Simple Install Path Values	58	26. Asset Management for IT users and groups	224
12. Asset Management for IT installation prerequisite conditions.	60	27. Operations and package types	235
13. Tivoli Asset Management for IT Simple Install Path Values	83	28. Process solution operations	236
14. Asset Management for IT installation prerequisite conditions.	84	29. Process solution command line interface actions.	248
15. Asset Management for IT required users and groups	121	30. Process solution command line interface supported parameters.	249
		31. Process solution installation logs	264

Chapter 1. Introduction

IBM® Tivoli® Asset Management for IT is a comprehensive suite of products that are built on a single, common platform. Asset Management for IT combines enhanced enterprise asset management functionality with new service management capabilities that together improve the effectiveness of asset management strategies.

Asset Management for IT includes advanced IT asset management, service management, and a full-featured service desk, all based on the IT Infrastructure Library® (ITIL®) guidelines. Each product can be implemented separately as a stand-alone solution or deployed with other products. The solution enhances asset management and ensures service performance of production, facility, transportation, and IT assets.

Asset Management for IT components

Tivoli Asset Management for IT requires multiple software servers that you can either install on separate, dedicated server computers (for best performance), or the same server computer. The diagram included in this topic shows a typical Maximo® configuration.

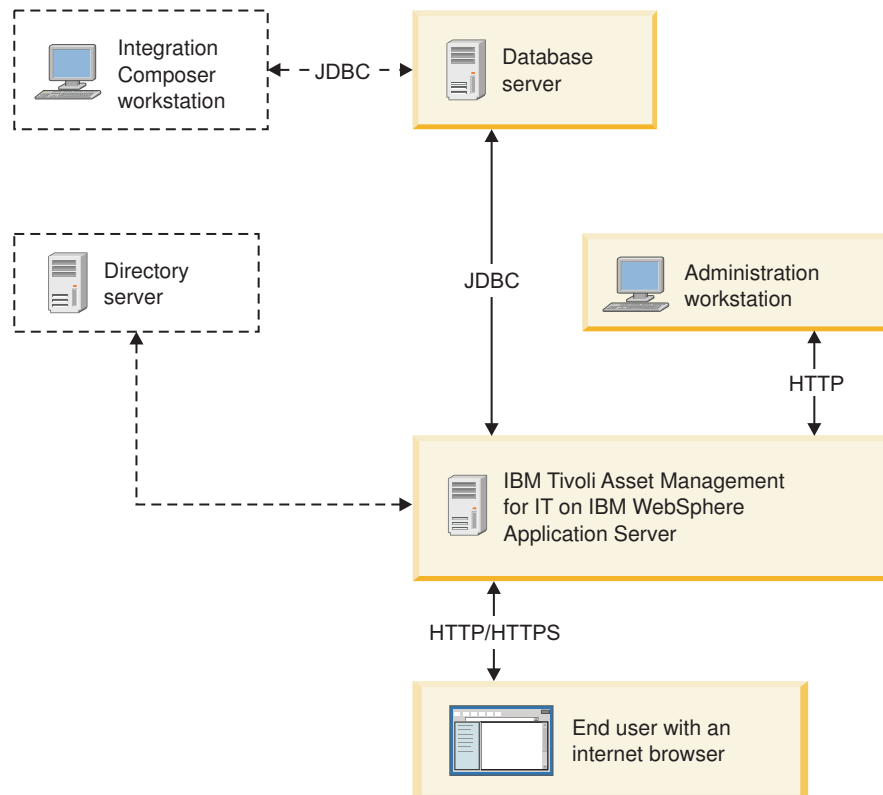


Figure 1. Tivoli Asset Management for IT Components

Database server

Asset Management for IT uses the Maximo database to store details about the attributes and history of each configuration item and the details about the relationships between configuration items.

Application server

Asset Management for IT uses Java™ 2 Enterprise Edition (J2EE) technology, which requires a commercial application server, such as IBM WebSphere® Application Server. The application server consists of Asset Management for IT applications that use JavaServer Pages (JSP), XML, and Asset Management for IT-application-specific business components.

HTTP server

A separate, dedicated HTTP server can be configured to work with the J2EE application server.

Directory server

The directory server is used to secure the Asset Management for IT J2EE application.

The server works with Virtual Member Manager in WebSphere to provide security within Asset Management for IT.

Windows Administrative system

The administrative system is the computer to deploy Asset Management for IT. After the initial deployment, the administrative system is used to make updates or changes to the deployment. Changes to the Asset Management for IT deployment typically require that Asset Management for IT Enterprise Archive (EAR) files be rebuilt, which can only be done from the administrative system.

Related reference

“Hardware and software requirements”

All necessary Asset Management for IT hardware and software requirements are listed in this section. Each product version listed reflects the minimum requirement for use with the product family.

Hardware and software requirements

All necessary Asset Management for IT hardware and software requirements are listed in this section. Each product version listed reflects the minimum requirement for use with the product family.

If available, the Asset Management for IT administrative workstation and systems hosting Asset Management for IT middleware can support Internet Protocol version 6 (IPv6) network configuration. Compare the table with Figure 1 on page 1.

Table 1. Asset Management for IT hardware and software requirements

	Hardware and Software Requirements
Browser	<ul style="list-style-type: none">• Microsoft® Internet Explorer 6 and later.
Windows	<ul style="list-style-type: none">• Mozilla Firefox 3.0.x 9 (Windows® client)

Table 1. Asset Management for IT hardware and software requirements (continued)

Hardware and Software Requirements	
<p>Database products</p>	<ul style="list-style-type: none"> • IBM DB2® Enterprise Edition Version 9.5 for Linux, UNIX®, and Windows fix pack 3a (installed by the Tivoli middleware installer). • IBM DB2 Enterprise Edition Version 9.1 for Linux, UNIX, and Windows (installed by the Tivoli middleware installer) • IBM DB2® Universal Database™ 8.2 with fix pack 14 Note: DB2 8.2 is only supported for manual configuration scenarios. • Oracle Database 11g Release 1 • Oracle Database 10g Release 2 • Oracle Database 9i Release 2 • Microsoft SQL Server 2008 Standard or Enterprise version. • Microsoft SQL Server 2005 service pack 2 and 3, Standard or Enterprise version. Note: If you use Microsoft SQL Server 2005 with Microsoft Windows 2008, make sure you installed service pack 3 to properly install Asset Management for IT. • Microsoft SQL Server 2000 Standard or Enterprise version. <p>Refer to the database product specifications for supported operating systems. For example, see http://www.oracle.com/technology/products/database/oracle10g/index.html for the Oracle databases information.</p>
<p>J2EE application server.</p> <p>This is where you install WebSphere Application Server and where Asset Management for IT runs.</p>	<p>Hardware requirements</p> <ul style="list-style-type: none"> • 2–4 dedicated processors • 2 GB RAM per processor • 1.5 GB or greater of disk space for Maximo and Java/Web Server components <p>Software</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2003 and 2008 (Standard service pack 2, Enterprise, or Datacenter) (32-bit, 64-bit) • IBM AIX® 5.3 • IBM AIX 6.1 (64-bit) • Red Hat Enterprise Linux® 4 and 5 (Enterprise or Advanced) (update 4+5 or later) (Intel®) (32 bit) • SuSE Linux (SLES) 9.0 Enterprise Server System z® service pack 4 or later (manual install only) <p>Note: Asset Management for IT supports the following operating systems. However, if you are using Asset Management for IT with DB2 Enterprise Server Edition, do not use these operating systems on your application server:</p> <ul style="list-style-type: none"> • Sun Solaris 9 or 10 (SPARC processor-based systems) • IBM WebSphere Network Deployment 6.1.0.23 provided by IBM Corporation.

Table 1. Asset Management for IT hardware and software requirements (continued)

	Hardware and Software Requirements
Integration options	<p>Asset Management for IT integration components can be run on any operating system supported by the integration software. The following products can serve as integration options for an Asset Management for IT deployment:</p> <ul style="list-style-type: none"> • IBM Integrated Solutions Console 7.1.1. It is installed as part of IBM WebSphere Application Server Network Deployment 6.1.0.23. • IBM WebSphere Portal Server 6.0 and 6.1.
HTTP server	<p>IBM HTTP Server 6.1 fix pack 23 can serve as the HTTP server component of a deployment. Supported operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2003 SP2 (Standard SP2, Enterprise, or Datacenter) (32-bit, 64-bit) • Microsoft Windows Server 2008 (Standard SP2, Enterprise, or Datacenter) (32-bit, 64-bit) • Microsoft Windows Vista (Business, Enterprise, Ultimate) (32-bit, 64-bit) • Microsoft Windows XP Professional SP2 (32-bit, 64-bit) • Red Hat Enterprise Linux v4 (Enterprise or Advanced) (update 4+5 or later) (Intel) (32-bit) • IBM AIX 5L™ V5.3 TL level 5300-06 (64-bit kernel) • IBM AIX 6.1 (64-bit) • SuSE Linux (SLES) 9.0 Enterprise Server System z SP4 or later (manual install only) • SuSE Linux (SLES) 10 Enterprise Server System z (manual install only)
Directory server	<p>Software</p> <ul style="list-style-type: none"> • IBM Tivoli Directory Server 6.2 fix pack 1 • Microsoft Windows Server 2003 service pack 2 Active Directory • Microsoft Windows Server 2008 Active Directory <p>Microsoft Active Directory Application Mode is not supported.</p> <p>Operating system</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2003 and 2008 (Standard, service pack 2, Enterprise, or Datacenter) (32-bit, 64-bit) • Red Hat Enterprise Linux (Enterprise or Advanced) (update 4+5 or later) Intel (32-bit) • IBM AIX 51 5.3 T1 level 5300-06 (64-bit kernel) • IBM AIX 6.1 • SuSE Linux (SLES) 9.0 Enterprise Server System z SP4 or later (manual install only) • SuSE Linux (SLES) 10 Enterprise Server System z (manual install only)
	<p>Asset Management for IT supports Microsoft Windows Server 2003 service pack 2 Active Directory. Microsoft Active Directory Application Mode is not supported.</p>

Table 1. Asset Management for IT hardware and software requirements (continued)

Hardware and Software Requirements	
Administrative system	<p>Hardware</p> <ul style="list-style-type: none"> • Intel-based Pentium® processor • 1 GB RAM of memory • SVGA 1024 x 768 resolution; if used for Application Designer 1280 x 1024 resolution <p>Software</p> <ul style="list-style-type: none"> • Windows Server 2003 and 2008 (Standard SP2, Enterprise, or Datacenter) (32-bit, 64-bit) • Microsoft Windows Vista (Business, Enterprise, Ultimate) (32-bit, 64-bit) • Microsoft Windows XP Professional service pack 2 (32-bit, 64-bit) • Adobe® Acrobat Reader 6.0 <p>Note: The Asset Management for IT Workflow Designer requires a Java Runtime Environment, 5.0 Service Release 5.</p>
Client system	<p>Hardware</p> <ul style="list-style-type: none"> • Intel based Pentium processor • 1 GB RAM of memory • SVGA 1024 x 768 resolution; if used for Application Designer 1280 x 1024 resolution <p>Software</p> <ul style="list-style-type: none"> • Microsoft Windows Vista (Business, Enterprise, Ultimate) (32-bit, 64-bit) • Microsoft Windows XP Professional service pack 2 (32-bit, 64-bit) • Adobe Acrobat Reader 6.0

Related concepts

“Asset Management for IT components” on page 1

Tivoli Asset Management for IT requires multiple software servers that you can either install on separate, dedicated server computers (for best performance), or the same server computer. The diagram included in this topic shows a typical Maximo configuration.

Chapter 2. Planning to deploy IBM Tivoli Asset Management for IT



Use this information to plan your IBM Tivoli Asset Management for IT deployment, to determine the best deployment option for your environment and business needs. It allows you to better understand and effectively plan your Asset Management for IT product family instances' topologies.

Tivoli Asset Management for IT deployment topologies

A typical deployment lifecycle usually begins with a single-server topology that would move through phases of demonstration, functional proof-of-concept, and testing integration within the existing environment. It then gradually moves towards a pilot multi-server environment before finally implementing a production deployment within the enterprise.

There are two primary strategies to deploy Asset Management for IT within your enterprise.

Single-server (single computer deployment)

The single-server topology consists of loading all Asset Management for IT components onto one computer. This topology is used typically for proof-of-concept purposes, as a demonstration, or as a learning environment. For managing enterprise assets and processes, you would typically implement a multi-server topology.

Multi-server (multiple computer deployment)

The multi-server topology consists of splitting Asset Management for IT components across several different computers (compare with the figure). This strategy is beneficial as it optimizes resource use and decreases the load on each system. This type of deployment would be typical for production use within an enterprise.

When contemplating your deployment strategy, determine whether it includes systems already established in your network. Implementing by installing all new components using the Asset Management for IT middleware and Asset Management for IT installation programs simplifies the deployment. If you plan to reuse or migrate resources that exist in your network, make adjustments to your rollout plan to allow time for things such as bringing the existing resources to version levels that are compatible with Asset Management for IT.

In a disparate environment, the collection of computers in this deployment could be a mixture of Windows and UNIX computers.

Attention: Only the Administrative system must be hosted on a Windows system.

Within Network Deployment you can create deployment managers that provide centralized administration of managed application server nodes and custom nodes as a single cell. WebSphere Application Server Network Deployment provides basic clustering and caching support, including work

balancing, automated performance optimization, and centralized management and monitoring.

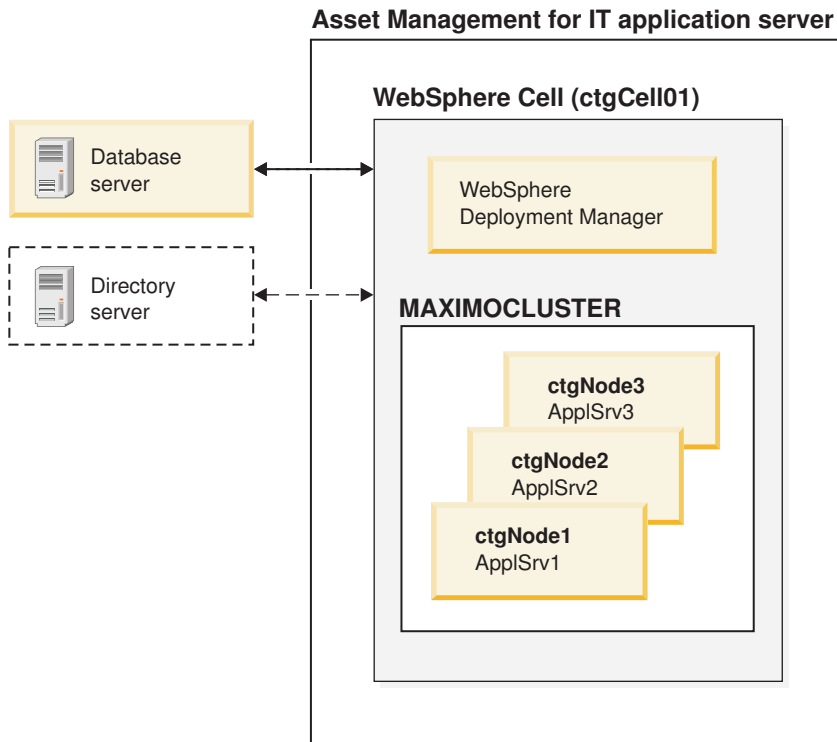


Figure 2. Asset Management for IT Deployed in a Cluster

While Asset Management for IT requires a new WebSphere Application Server Network Deployment application server for deployment, once Asset Management for IT has been deployed, you can add the application server used by Asset Management for IT as a new member of an existing WebSphere Application Server Network Deployment cluster. For more information on adding a new member to an existing WebSphere Application Server Network Deployment cluster, refer to Adding members to a cluster.

Related tasks

“Creating a WebSphere Application Server Network Deployment cluster” on page 199

This section contains information about creating a WebSphere Application Server Network Deployment cluster.

Planning for Tivoli Asset Management for IT middleware worksheet

The tables in this section list the settings for values that you must supply when installing the Asset Management for IT middleware. Although many of the defaults can be accepted when navigating the panels of the middleware installer, you want to review this worksheet if you plan to configure manually or reuse existing middleware. In a multi-computer deployment scenario, you might have multiple values to consider.

Where blanks provided, there are no default values.

Table 2. List of users and groups created during Asset Management for IT installation. Plan your value here..

User, description	Group or groups, Supported platforms
db2admin.	
DB2 administrator. Windows Service User ID.	Windows DB2USERS, DB2ADMNS
This user is created by the middleware installer if it does not exist.	
	Windows Users, Administrators
idscmdb.	
IBM Tivoli Directory Server user.	AIX idldap
This user is created by the middleware installer if it does not exist.	Linux idldap, db2grp1
	Windows Users, Administrators
	AIX Users, Administrators
maximo.	
Used for Maximo database configuration.	Linux Users, Administrators
This user is created by the Asset Management for IT installation program if it does not exist.	Solaris Users, Administrators
ctginst1.	
The system user used as the database instance owner on UNIX platforms. ctginst1 must be a member of db2grp1 with secondary groups of staff and dasadm1 .	AIX Users, Administrators
This user is created by the middleware installer if it does not exist.	Linux Users, Administrators
db2fenc1. UNIX system user used as the fenced user ID for DB2.	AIX db2fgrp1
This user is created by the middleware installer if it does not exist.	Linux db2fgrp1

Table 2. List of users and groups created during Asset Management for IT installation. Plan **your value** here.. (continued)

User, description	Group or groups, Supported platforms
	Windows
	AIX
	Linux
wasadmin. Note: Not a system user. This is a user ID created for use with WebSphere Application Server.	Solaris
This user is created by the middleware installer if it does not exist.	

Table 3. Tivoli middleware installer. Plan **your value** here..

Setting	Default
Workspace directory	<i>user_home</i> \ibm\tivoli\mwi\workspace
Middleware images source directory	
Compressed images directory	
Uncompressed images directory	

Table 4. DB2 configuration.

Setting	Default
Installation directory	Windows <i>SystemDrive</i> \Program Files\IBM\SQLLIB
	Linux /opt/IBM/db2/V9.5
	AIX /opt/IBM/db2/V9.5
DAS user	Windows db2admin
	Linux dasusr1
	AIX dasusr1
Fenced user	Linux db2fenc1
	AIX db2fenc1

Table 4. DB2 configuration. (continued)

Setting	Default
Fenced user group name	Linux db2fggrp1
	AIX db2fggrp1
Fenced user home directory	Linux /home/db2fenc1
	AIX /home/db2fenc1
Instance name	ctginst1
Port	50005
Instance user name home directory	Linux /home/ctginst1
	AIX /home/ctginst1
Database instance user ID	Windows db2admin
	Linux ctginst1
	AIX ctginst1
DB2 administrators group	Windows DB2ADMNS
	Linux db2grp1
	AIX db2grp1
DB2 users group	Windows DB2USERS
Use same user name and p/w for remaining DB2 Services	YES
Database name	ctginst1
Configure Tools Catalog	NO
Enable O/S Security for DB2 objects	YES
	This value is relevant for reuse scenarios only.
DB2 instance port	

Table 4. DB2 configuration. (continued)

Setting	Default
Data table space name	MAXDATA
Data table space size	medium (1000Mb)
	DB2 Medium (5000Mb)
Temporary table space name	MAXTEMP
Temporary table space size	1000Mb

Table 5. Oracle configuration

Setting	Default
Installation directory	<p>Windows</p> <p><i>SystemDrive</i>\oracle\product\10.2.0\oradata</p> <p>Linux</p> <p>/opt/app/oracle/product/10.2.0/oradata</p> <p>AIX</p> <p>/opt/app/oracle/product/10.2.0/oradata</p> <p>Solaris</p> <p>/opt/app/oracle/product/10.2.0/oradata</p>
Administrator User ID	sys
Oracle Software Owner ID	<p>Windows</p> <p>Administrator</p> <p>Linux</p> <p>oracle</p> <p>AIX</p> <p>oracle</p> <p>Solaris</p> <p>oracle</p>

Table 5. Oracle configuration (continued)

Setting	Default
Instance Location	<p>Windows</p> <p>This value might be C:\oracle\product\10.2.0\oradata</p> <p>Linux</p> <p>This value might be /opt/app/oracle/product/10.2.0/ oradata</p> <p>AIX</p> <p>/opt/app/oracle/product/10.2.0/ oradata</p> <p>Solaris</p> <p>/opt/app/oracle/product/10.2.0/ oradata</p>
Oracle database name	ctginst1
Data table space name	MAXDATA
Data table space size	medium (1000Mb) Oracle Medium (1000Mb)
Temporary table space name	MAXTEMP
Temporary table space size	1000Mb

Table 6. SQL Server configuration

Setting	Default
Installation directory	ProgramFiles\Microsoft SQL Server\90
Named instance	maximo
SQL Server administrator	sa
SQL Server administrator password	
Port	1433
Database name	maxdb71
User ID	maximo
User ID password	
Data file name	maxdb71_dat
Log file name	maxdb71_log

Table 7. WebSphere Application Server configuration

Setting	Default
Install location	<p>Windows</p> <p>C:\Program Files\IBM\WebSphere\AppServer</p>
	<p>Linux</p> <p>/opt/IBM/WebSphere/AppServer</p>
	<p>AIX</p> <p>/usr/IBM/WebSphere/AppServer</p>
	<p>Solaris</p> <p>/opt/IBM/WebSphere/AppServer</p>
WebSphere Administration User Name	wasadmin
Deployment Manager profile name	ctgDmgr01
Application server profile name	ctgAppSrv01
Profile directory	<p>Linux</p> <p>/opt/IBM/WebSphere/AppServer/profiles</p>
	<p>AIX</p> <p>/usr/IBM/WebSphere/AppServer/profiles</p>
	<p>Solaris</p> <p>/opt/IBM/WebSphere/AppServer/profiles</p>
Cell name	ctgCell01
Deployment Manager node name	ctgCellManager01
Application server node name	ctgNode01
HTTP server install location	<p>Windows</p> <p>C:\Program Files\IBM\HTTPServer</p>
	<p>Linux</p> <p>/opt/IBM/HTTPServer</p>
	<p>AIX</p> <p>/usr/IBM/HTTPServer</p>
	<p>Solaris</p> <p>/opt/IBM/HTTPServer</p>
HTTP port	<p>80</p> <p>Note: On Windows, this port might already be in use. Ensure that you either free up this port, or use another port that is unassigned.</p>
HTTP admin server port	8008
HTTP plugin profile name	ctgAppSvr01

Table 8. IBM Tivoli Directory Server configuration

Setting	Default
Install location	Windows C:\Program Files\IBM\LDAP\V6.1
	Linux /opt/IBM/ldap/V6.1
	AIX /opt/IBM/ldap/V6.1
Administrator distinguished name	cn=root
Organizational unit	ou=SWG
Organization and country suffix	o=IBM,c=US
Directory server port	389
Directory server secure port	636
Administration port	3538
Administration secure port	3539
Database name	security
Instance name	idscmdb
Instance port	50006
Instance user name	idscmdb

Table 9. Microsoft Active Directory configuration

Setting	Default
Directory server port	389
LDAP base entry	DC=ism71,DC=com
User suffix	CN=Users,DC=ism71,DC=com
Group suffix	DC=ism71,DC=com
Organization container suffix	DC=ism71,DC=com
Bind distinguished name	CN=Administrator,CN=Users, DC=ism71,DC=com

Reusing existing middleware components

You can reuse some existing middleware installations as Tivoli Asset Management for IT components. If you plan to do so, ensure that they are at the level supported by Asset Management for IT. The middleware and Asset Management for IT installation programs do not provide a mechanism for patching unsupported servers, nor do these programs provide remote prerequisite checks to ensure they are at the right level.

For example, you probably have an instance of DB2 or Oracle in an existing database server farm which already has established access policies, redundancy measures, and backup plans in place.

Middleware configuration options

You are presented with the option of either allowing the Asset Management for IT installation program to configure middleware automatically, or configuring each middleware component manually.

Auto-configure

The Asset Management for IT installation program automatically configure middleware to work together with Asset Management for IT. This option is recommended if you are installing new instances of middleware components, or if you have existing middleware instances that are not governed by policies that restrict programmatic configuration.

Manual

You can manually configure middleware that exists in your environment, or has been installed by the middleware installer. This configuration must be completed prior to running the Asset Management for IT installation program. If you have policies in place that dictate certain procedures and guidelines when configuring systems in your environment, you can choose this deployment path.

Related tasks

Chapter 4, “Deploying IBM Tivoli Asset Management for IT with automatic middleware configuration,” on page 33

The automatic IBM Tivoli Asset Management for IT installation consists of subsequent tasks that need to be performed in a specified order. You are guided through the tasks by the Asset Management for IT Launchpad.

Chapter 5, “Deploying IBM Tivoli Asset Management for IT automatically reusing existing middleware,” on page 77

Use this information to use IBM Tivoli Asset Management for IT installation programs and tools to automatically configure existing middleware within your enterprise during the Asset Management for IT deployment process.

Chapter 6, “Installing IBM Tivoli Asset Management for IT with manual middleware configuration,” on page 101

You can have one or more IBM Tivoli Asset Management for IT middleware components configured automatically by the Asset Management for IT installation program. Alternatively, you can choose to manually configure one or more of the middleware servers to work with Asset Management for IT. Configure the components before you install the product.

Planning for Tivoli Asset Management for IT worksheet

These tables list the settings whose values that you must supply when using the Asset Management for IT installation program.

Table 10. Settings for a custom installation

Setting	Default
Installation directory	C:\IBM\SMP
API port	9530
DB2 host name	
DB2 port	50005
Maximo database name	maxdb71
Maximo database instance	ctginst1
Maximo database user ID	maximo

Table 10. Settings for a custom installation (continued)

Setting	Default
DB2 installation directory	Windows C:\Program Files\IBM\SQLLIB
	Linux /opt/IBM/db2/V9.5
	AIX /opt/IBM/db2/V9.5
DB2 instance administrator user ID	Windows db2admin
	Linux ctginst1
	AIX ctginst1
Windows DB2 service user ID	db2admin
Oracle installation directory	Windows C:\oracle\product\10.2.0\oradata
	Linux /opt/app/oracle/product/10.2.0/oradata
	AIX /opt/app/oracle/product/10.2.0/oradata
	Solaris /opt/app/oracle/product/10.2.0/oradata
Oracle administrator user ID	sys
Oracle software owner user ID	oracle
SQL installation directory	C:/ProgramFiles/Microsoft SQL Server/90
Data table space name	MAXDATA
Data table space size	medium
	DB2 Medium (5000Mb)
	Oracle Medium (1000Mb)
	SQL Server (Initial data file size) Medium (1000Mb)
Temporary table space name	MAXTEMP
Temporary table space size	1000Mb
WebSphere host name	
WebSphere SOAP port	8879

Table 10. Settings for a custom installation (continued)

Setting	Default
WebSphere server home directory	<div style="background-color: #800000; color: white; padding: 2px; display: inline-block; margin-bottom: 5px;">Windows</div> C:\Program Files\IBM\WebSphere\AppServer <div style="background-color: #800000; color: white; padding: 2px; display: inline-block; margin-bottom: 5px;">Linux</div> /opt/IBM/WebSphere/AppServer <div style="background-color: #800000; color: white; padding: 2px; display: inline-block; margin-bottom: 5px;">AIX</div> /usr/IBM/WebSphere/AppServer <div style="background-color: #800000; color: white; padding: 2px; display: inline-block; margin-bottom: 5px;">Solaris</div> /opt/IBM/WebSphere/AppServer
WebSphere admin user ID	wasadmin
WebSphere profile name	ctgDmgr01
Web server port	80
Web server name	webserver1
Node name	ctgNode01
Cluster name	MAXIMOCLUSTER
Application server	MXServer Note: This value cannot be changed.
JMS Data Source name	
JMS database name	maxsibdb
JMS server name	
Database server port	50000
Database user ID	MAXADMIN
Directory server host name	
Directory server port	389
Directory server administrator DN	cn=root
Bind password	
Maximo installation folder	<div style="background-color: #800000; color: white; padding: 2px; display: inline-block; margin-bottom: 5px;">Windows</div> C:\IBM\SMP Note: Maximo can only be installed on the Asset Management for IT administrative system, which must be a Windows system.
SMTP server	
Workflow Admin E-mail	
Admin E-mail	

Planning for security

Planning for security includes choosing a security option, deciding which users will work with each application in Asset Management for IT, and optionally which users can work with which configuration items.

Each service management process defines its own *roles*. If you install more process managers, additional roles for those processes will be added.

The roles are based on those defined in the Information Technology Infrastructure Library (ITIL). IBM implements ITIL using IBM Tivoli Unified Process. Refer to the IBM Tivoli Unified Process content for more detailed information on roles and their responsibilities.

You must decide whether to use the roles defined by the service management processes, or define your own.

The roles defined by the processes are implemented as *security groups*. You can assign each user defined to one or more security groups, which enables them to perform the responsibilities assigned to those roles. You can modify the applications that members of each security group can use in the Security Groups application.

Choosing a security option

Asset Management for IT offers three options for managing your users and their memberships in security groups.

When you install Asset Management for IT, you must choose one of three options for managing users and groups. This choice will apply to all products that you install together. If you are installing Asset Management for IT with another product already installed, the choice you made when installing the first product will be used for Asset Management for IT as well.

The security option you choose will determine how your system performs *authentication*, which is the validation of a user signing in to Asset Management for IT, and *authorization*, which uses security groups to control which users can work with each application.

Choose one of these security options:

Use WebSphere application security for authentication and authorization

This is the option that was required on previous releases of Asset Management for IT. With this option, you create all your users and security groups in your directory (LDAP) server, and this information is updated in your Maximo database using a cron task.

When you install Asset Management for IT, if you choose automatic configuration of your directory server, the roles for change management and configuration management are defined.

The directory server containing the user and group definitions is configured to work with Virtual Member Manager within WebSphere Application Server.

Use WebSphere application security for authentication only

With this option, you create all your users in your directory server, but you manage their membership in security groups in the base services Security Groups application.

Use Maximo security for authentication and authorization

With this option, a directory server is not required. You create and manage users and groups in the base services Users and Security Groups applications, separately from any corporate user data you might have.

This is the only security option available if you are using WebLogic for your J2EE server.

With this option, you cannot configure single sign-on to launch in context to the Asset Management for IT interface without providing credentials.

Controlling access to configuration items

By default, any authenticated user can work with any configuration item (CI), using any application to which the user's role gives access. If you want, you can control which users can work with selected configuration items. You do this by organizing the configuration items into *access collections*.

Configuring security

You will configure your security environment by creating users and assigning them to security groups, defining the applications that members of each security group can use, and optionally by creating access collections, after you have finished installing Asset Management for IT.

Related tasks

"Signing in using a default user ID" on page 223

User management is managed through the application server or the directory server you have configured to use with Asset Management for IT. When first installed, Asset Management for IT contains the following default user IDs, which are members of the specified security groups described in this section.

"Manually configuring Virtual Member Manager on IBM WebSphere Application Server" on page 128

This procedure provides task information for manually configuring Virtual Member Manager (VMM) to secure Tivoli Asset Management for IT.

"Manually configuring Microsoft Active Directory" on page 121

Windows You can choose to configure a Microsoft Active Directory resource manually for better use with Tivoli Asset Management for IT.

"Securing WebSphere Administrative Console" on page 195

You can secure the Administrative Console so that only authenticated users can use it. Virtual Member Manager must have been configured on the WebSphere server prior to securing the console.

Planning language support

Language support refers to the languages you plan to support in the product user interface.

IBM Tivoli Asset Management for IT includes language support for languages supported by UTF-8 and UCS-2.

When deployed using Microsoft SQL Server, Asset Management for IT does not support UTF-8. Language support is limited to those supported by the current Windows system code page. Supported language set choices are either all Latin 1 languages and English or one double-byte character set language and English.

Important: If you plan to add language support to Asset Management for IT, you **must** use the Asset Management for IT language pack installation program to define the base language to use **before** you perform post-installation steps described in Chapter 17, "IBM Tivoli Asset Management for IT post installation tasks," on page 221. You can add additional languages at a later date, but the base language must be set either during or directly after the Asset Management for IT installation.

Related tasks

“Deployment for packages with multiple language support features” on page 262
Packages can be deployed with a multiple language support.

“Installing language packs with Process Solution Installer” on page 155

The Process Solution Installer guides you through the installation of a process manager product (PMP) or Integration Module. Use the Process Solution Installer to refresh languages to synchronize them with Maximo languages.

Chapter 8, “Installing IBM Tivoli Asset Management for IT language pack,” on page 153

“Generating xml request pages in Asset Management for IT” on page 267

Perform this task after you installed Asset Management for IT and before you run request pages. This procedure needs to be performed for every language that is enabled on your system.

“Installing process managers using the Process Solution Installation wizard” on page 246

To install a process solution package into your Asset Management for IT instance, you might use the Process Solution Installer wizard.

System password policy settings

Be familiar with the password policies of systems you are using as part of an Asset Management for IT deployment.

Before deploying Asset Management for IT, be sure you are familiar with the password policies of systems used in the deployment, or you might experience errors during installation.

For example, Microsoft Windows Server 2008 systems have a stricter set of password requirements than previous versions configured by default. If you are not familiar with these stronger password requirements, you might experience an error during the installation of Asset Management for IT when creating users on a Microsoft Windows Server 2008 system.

Password values that you provide during the Asset Management for IT installation should be compliant with the password policies set for the target system.

Go to the sections “Incorrect db2admin password” on page 48 and “Invalid DB2 password value” on page 50 to read about potential problems with system password policy settings while installing Asset Management for IT middleware.

Chapter 3. Preparing to install IBM Tivoli Asset Management for IT

These topics provide information on product media, preinstallation considerations, overview of the installation procedure, and instructions on using the IBM Tivoli Asset Management for IT Launchpad.

DVD layout

Tivoli Asset Management for IT ships on a set of DVDs that contain the prerequisite middleware, Quick Start Guide, and the product code. Alternatively, you can download Asset Management for IT files containing these same images from IBM Passport Advantage®.

The following DVDs contain files for the Asset Management for IT product:

- Tivoli Asset Management for IT Quick Start
- Tivoli Asset Management for IT for Multiplatforms
- **Windows** Tivoli Middleware Installer Images for Windows Server x86-32
- **Windows** Tivoli Middleware Installer Images for Windows Server x86-64
- **Linux** Tivoli Middleware Installer Images for Linux x86-32
- **Linux** Tivoli Middleware Installer Images for Linux x86-64
- **Linux** Tivoli Middleware Installer Images for Linux on System z
- **AIX** Tivoli Middleware Installer Images for AIX PPC-64
- **Solaris** Tivoli Middleware Installer Images for Solaris SPARC-64
- **HP-UX** Tivoli Middleware Installer Images for HP-UX x86-64
- Tivoli Software Knowledge Base Toolkit
- Maximo eCommerce Adapter

Related tasks

“Starting the Launchpad” on page 30

All the Tivoli Asset Management for IT components can be installed using the Asset Management for IT Launchpad.

Before you begin

This section describes the steps that you must take before you install middleware or Tivoli Asset Management for IT. To perform any of the steps, you must be logged in as a user with administrator privileges on Windows or as root on UNIX.

Attention: Make a copy of the image of the system on which you are planning to install the product. An automated uninstall feature is not supplied with Asset Management for IT. If the installation fails, restore the system to its previous working state using the copy of the disk image prior to attempting the installation again.

Checking port availability

You need to ensure certain ports are available before using the product installation programs.

About this task

You must manually check to see if port 50000 is in use for the system you are using to host DB2. This is the default port value used by DB2. If you intend to use this value, ensure the port is not already assigned before you run the middleware installation program.

1. Open the appropriate port checking utility on the host system.
2. Check the availability of port 50000. If you find that port already assigned, ensure you choose another value for DB2 when prompted by the middleware installation program.

Accessing system directories

Linux Before using the middleware installation directory, you need to assign access permission to particular directories.

Before you begin

Before using the middleware installation directory, you need to assign access permission for the /tmp and /home directories on Linux systems.

About this task

The product installation programs require *read*, *write* and *execute* permissions for the /tmp and /home directories. If one of these directories uses a symbolic link, for example, /products/home, ensure that symbolic link directory also has the proper access.

1. Log into the system as a user with root authority on the system.
2. Enter the following commands:

```
#chmod 777 /tmp
#chmod 777 /home
```

Disabling the firewall

Prior to the installation, disable the firewall for the system to which you are installing Asset Management for IT middleware.

About this task

See the documentation that comes with your Operation System for information on disabling the firewall.

Deleting the TEMP and TMP user environment variables

Windows The existence of the TEMP and TMP user variables can cause errors with the installation of DB2 on a Windows system. Prior to installing DB2, remove these variables for the user ID that performs the installation.

Before you begin

Note: The TEMP and TMP user variables are user environment variables that must be deleted, not system variables.

About this task

To remove the TEMP and TMP user variables on a Windows system, complete the following steps:

1. Access the System Properties dialog by right-clicking the My Computer icon on your desktop and selecting **Properties**.
2. From the System Properties dialog, first select the **Advanced** tab, and then click **Environment Variables**.
3. In the **User variables** section, select **TEMP**, and then click **Delete**. Repeat the process for the TMP variable.
4. Click **OK**.
5. Exit the System Properties dialog by clicking **OK**.

Verifying the required rpm-build package is installed

Linux This procedure describes how to verify that the rpm-build package is installed on Linux. This package must be installed before you install the Tivoli Asset Management for IT middleware. This procedure applies only if you are installing on Linux.

About this task

To verify that the rpm-build package is installed, perform the following steps:

1. Run `rpm -qa | grep build` command.
2. If the command returns a value like `rpm-build-4.3.3.-18_nonpt1`, the rpm-build package is installed. If nothing is returned, install the rpm-build package which is located on disk 3 (of 5) of the Red Hat Enterprise Advanced Server version 4 installation CDs using the rpm tool with the `-i` option.

Setting the ulimit

Linux This section details how to set the ulimit in Linux, which is used to define user system and process resource limits.

About this task

Set the ulimit for the system prior to installing Tivoli Asset Management for IT middleware. To set the ulimit, complete the following steps:

1. From a command line, type `ulimit -f unlimited`.
2. From a command line, type `ulimit -n 8192`.

Results

If you set the ulimit in the `.profile` for root, the ulimit setting will apply to all processes.

AIX For AIX systems, refer to “Increasing AIX file size and number of descriptors” on page 27.

Setting the swap size

Linux Tivoli Asset Management for IT can be a resource-intensive application. It is recommended that you configure and tune your system for maximum performance. This section details how to set the size of the swap space used in Linux systems.

About this task

Typically, the swap size set for Linux systems must be equivalent to twice the amount of physical RAM in the computer.

Additional swap space can be made available to the system by:

- increasing the size of the existing swap partition
- creating an additional swap partition
- creating a swap file

What to do next

Refer to the product documentation for your Linux distribution for more information.

AIX For AIX systems, refer to “Increasing AIX paging space” on page 27.

Setting shared memory

Linux This section details how to set a minimum shared memory value in Linux before you start to install Asset Management for IT

Before you begin

Set a minimum shared memory value for the system prior to installing the Tivoli Asset Management for IT middleware.

About this task

To set the minimum shared memory value, complete the following steps:

1. From a command line, type `sysctl -w kernel.shmmax` and determine if the value is less than 268,435,456 bytes (256Mb).
2. If you want to increase the value, from a command line, type `sysctl -w kernel.shmmax=268435456`.
3. Update the value in `/etc/sysctl.conf`.

Enabling remote configuration

If you plan to take advantage of the Tivoli Asset Management for IT installation program feature that automates the configuration of Asset Management for IT middleware, enable a *Remote Execution and Access (RXA)* service for each system on which you intend to install Asset Management for IT middleware.

RXA requires that the target system enable at least one of the protocols supported by RXA, which include rsh, rexec, SSH, and Windows SMB. Before you start the Asset Management for IT installation program, ensure that one of these protocols is running and accepts remote logins using a user name and password configured on the target computer.

- **Windows** If the remote system is a Windows computer, configure RXA to work over SMB. For Windows computers, you cannot use Cygwin ssh. If Cygwin is present on the Windows computer, the installation will fail.
- **AIX** Default installations of AIX systems might not include a suitable protocol and need to have RXA compatible protocols enabled.

RXA does not support accessing network drives on the local or remote system.

Preparing UNIX systems for Tivoli Asset Management for IT middleware

UNIX Certain UNIX parameters must be set to specific values to create an environment on the system that can accommodate Asset Management for IT and its associative middleware.

Increasing AIX file size and number of descriptors

AIX To make Tivoli Asset Management for IT function correctly, you need to increase the default number of file descriptors allowed for the root user, and also set the maximum allowable file size to unlimited.

About this task

To increase the allowable file size and number of allowable descriptors for the root user in AIX, complete the following steps:

1. Edit the `/etc/security/limits` file by opening it in a text editor.
2. Locate the section for the root user, and then make changes to the parameters below using the values listed.

```
root:
    fsize = -1
    nofiles = 8192
```

A value of -1 for the `fsize` parameter indicates no limit.

3. Save and exit the file. You must log out as root and log back in for these changes to take effect.

What to do next

Verify the settings from a command window by issuing the following command:
`ulimit -a`

Output from the `ulimit` command should be similar to the following:

```
time(seconds)          unlimited
file(blocks)           unlimited
data(kbytes)           2097152
stack(kbytes)          32768
memory(kbytes)         unlimited
coredump(blocks)      2097151
nofiles(descriptors)  8192
```

Increasing AIX paging space

AIX To successfully install and run Tivoli Asset Management for IT, you need to increase the default paging space for the AIX system to a minimum of 4 GB, or, preferably, the total amount of physical memory in the system.

- To determine the current amount of paging space available to the server, issue the following command

```
lspv -a
```

This command will result in output similar to the following:

Page Space	Physical Volume	Volume Group	Size	%Used
hd6	hdisk0	rootvg	5632MB	2

- To determine the size of a logical partition, issue the following command:

```
lslv hd6
```

This command will result in output that will include partition information similar to the following:

```
LPs:                44
PP SIZE:            128 megabyte(s)
```

In the example output, there are a total of 44 Logical Partitions that are each 128 Mb in size. This results show a total of 5632 Mb of paging space available to the system.

- In order to add more paging space, you will add more logical partitions to the system. To add more logical partitions, use the following command:

```
chps -s xx yyy
```

Where *xx* is the number of logical partitions to add and *yyy* identifies the logical volume.

For example,

```
chps -s 10 hd6
```

adds 10 logical partitions to the logical volume *hd6*, which results in adding 1280 Mb to the paging space.

Enabling asynchronous I/O on AIX

AIX Tivoli Directory Server requires asynchronous I/O be enabled on AIX systems. Without asynchronous I/O, DB2 and Oracle database instances cannot be started successfully. It is an operational requirement, not an installation requirement so this step can be run at any time before full operation of the product.

About this task

You only need to perform this step if the system will host the IBM Tivoli Directory Server.

To turn asynchronous I/O on follow these steps:

1. Log into the system as root.
2. Open a terminal and run the following command:

```
smit chgaio
```
3. From the System Management Interface Tool (SMIT) dialog box, change STATE to be configured at system restart from defined to available, and then click **OK**.
4. Exit SMIT.
5. Run the following command from the command line:

```
smit aio
```
6. From the System Management Interface Tool dialog box, select **Configure Defined Asynchronous I/O**, and then click **Enter**.
7. Reboot the system to enable the changes.

Checking for required libraries on Linux

Linux The Tivoli Asset Management for IT middleware installation program requires the `libstdc++.so.5` system library to be present on a Linux system in order to launch the middleware installation program user interface.

About this task

If you do not have this library installed, you will receive an error indicating that the Asset Management for IT middleware installation program is unable to run in graphical mode.

If you receive this error, check the `/usr/lib/` directory to determine if you have the `libstdc++.so.5` library installed. This library is included as part of Red Hat Enterprise Linux v4 update 4. If you cannot locate this library on your system, locate the RPM package for your system that contains this library and install the package.

Configuring the JRE in Linux

Linux In some cases, the Tivoli middleware installer will fail on RHEL 5 systems, or other systems with SELinux enabled. In one failure scenario, the middleware installer will fail with an error message stating that the Java Runtime Environment (JRE) could not be found on the system.

About this task

If this is the case, implement one of the following solutions:

- Temporarily disable SELinux by using the `setenforce 0` command, run the install, and then re-enable SELinux by using the `setenforce 1` command.
- Edit the `/etc/selinux/config` file and set **SELINUX** to either `permissive` or `disabled`. This solution, however, affects the level of security for the entire system.

In another failure scenario, middleware installer will fail stating that it cannot find the VM. If this is the case, implement one of the following solutions:

- Manually issue the command:

```
chcon -R -t textrel_shlib_t install_dir/jvm/jre
```
- Edit the `/etc/selinux/config` file and set **SELINUX** to either `permissive` or `disabled`. This solution, however, affects the level of security for the entire system.

Tivoli Asset Management for IT Launchpad

The Tivoli Asset Management for IT Launchpad serves as a centralized interface for launching a collection of installation programs and product information.

The Launchpad application assists you in choosing which product installation programs to install and indicates the order in which they must be installed.

Note: Use the Launchpad for 32-bit Windows only.

Use the Asset Management for IT Launchpad to:

- Plan the installation (**Installation Planning**) using the installation documentation:
 - Release notes for technical information

- Quick Start Guide for available features and deployment options
- Planning installation guides for system requirements and deployment options
- Install software. The Launchpad guides you through the installation to perform the following tasks in the right order:
 1. “Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer” on page 38
 2. Installing Tivoli Asset Management for IT 7.2 and the appropriate Language Pack
 3. “Installing Tivoli Integration Composer on 32-bit Windows using the launchpad” on page 209
- Access the information center.
- Exit the installer.

Starting the Launchpad

All the Tivoli Asset Management for IT components can be installed using the Asset Management for IT Launchpad.

About this task

To start the Asset Management for IT Launchpad, complete the following steps:

1. Log on to an account with system administration privileges on the computer where Asset Management for IT components are to be installed.
2. Start the Launchpad from the root directory of the product DVD:
 - **Windows** Windows: Start the Launchpad by using the launchpad.exe program if the Windows autorun feature is disabled.
 - **AIX** AIX: Start the Launchpad from the root directory by using the launchpad.sh program.

The Launchpad program uses the system default browser to run. If the default browser on AIX is Firefox, it is likely that the Launchpad program will not run properly due to the ksh shell interface. If you want to use the Launchpad with the Firefox browser, follow these steps to modify it.

- a. Copy all of the files from disk1 to a local directory (for example, */your_dir*). If you have downloaded the product images rather than using physical media, download and extract the Launchpad images as described in the download document.
- b. Modify */your_dir/launchpad/Firefox.sh* and remove the following lines:


```
typeset +r LOGNAME 2>/dev/null
LOGNAME=lp_user_$$; export LOGNAME
```
- c. Run the Launchpad from */your_dir*
- **Linux** Linux: Start the Launchpad from the root directory by using the launchpad.sh program.

For example,

```
./media/cdrecorder/launchpad.sh
```

Running the Launchpad from the root directory avoids complications that would arise if you ran it inside the mounted directory and you wanted to swap disks. If you changed directory to the mounted DVD and launched the Launchpad from that directory, at a certain point in the deployment process you would need to swap to another DVD, but you would not be able to

because Launchpad was still running from the directory on DVD you have mounted. You would not be able to unmount the disk without terminating the Launchpad.

- **Solaris** Sun Solaris: Start the Launchpad from the root directory by using the `launchpad.sh` program.

What to do next

For more information about installation and configuration parameters you might encounter while installing Asset Management for IT, refer to “Planning for Tivoli Asset Management for IT middleware worksheet” on page 8 and “Planning for Tivoli Asset Management for IT worksheet” on page 16.

Related reference

“DVD layout” on page 23

Tivoli Asset Management for IT ships on a set of DVDs that contain the prerequisite middleware, Quick Start Guide, and the product code. Alternatively, you can download Asset Management for IT files containing these same images from IBM Passport Advantage.

Chapter 4. Deploying IBM Tivoli Asset Management for IT with automatic middleware configuration

The automatic IBM Tivoli Asset Management for IT installation consists of subsequent tasks that need to be performed in a specified order. You are guided through the tasks by the Asset Management for IT Launchpad.

About this task

Installation and deployment of Asset Management for IT involves:

1. Installing and configuring required Asset Management for IT middleware software products. Refer to “Installing IBM Tivoli Asset Management for IT middleware.”
2. Installing and configuring Asset Management for IT components:
 - a. Installing and configuring Asset Management for IT.
 - b. Optionally, installing and configuring additional language support. Refer to Chapter 8, “Installing IBM Tivoli Asset Management for IT language pack,” on page 153.
3. Optionally, installing and configuring Tivoli Integration Composer. See “Installing Tivoli Integration Composer on 32-bit Windows using the launchpad” on page 209 in the Chapter 16, “Installing IBM Tivoli Integration Composer,” on page 205.
4. Configuration of optional Asset Management for IT middleware software products, such as WebSphere Portal Server. Refer to Chapter 15, “IBM WebSphere Portal Server overview,” on page 201.

What to do next

The installation programs for these Asset Management for IT components can be initiated through the Launchpad, where you can also access product information. If you decide to deploy Asset Management for IT automatically or manually, pay special attention to Step 18 on page 70 in “Performing IBM Tivoli Asset Management for IT installation” on page 60.

Related concepts

“Reusing existing middleware components” on page 15

You can reuse some existing middleware installations as Tivoli Asset Management for IT components. If you plan to do so, ensure that they are at the level supported by Asset Management for IT. The middleware and Asset Management for IT installation programs do not provide a mechanism for patching unsupported servers, nor do these programs provide remote prerequisite checks to ensure they are at the right level.

Installing IBM Tivoli Asset Management for IT middleware

Before you can install IBM Tivoli Asset Management for IT, there are several Asset Management for IT middleware products that must be deployed. The middleware installer provides an interface for installing and deploying Asset Management for IT middleware in a reliable and repeatable fashion.

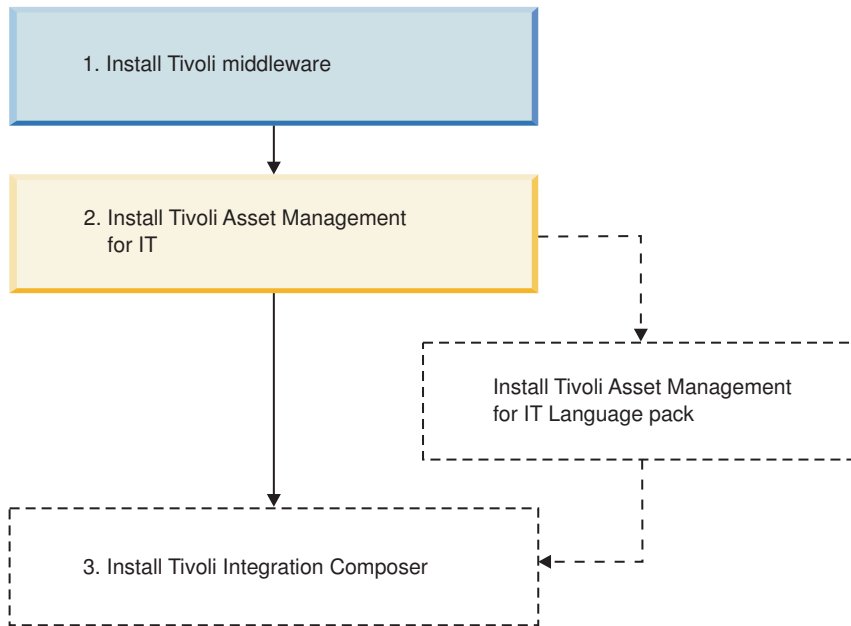


Figure 3. Asset Management for IT Installation flow - Tivoli middleware installation

The middleware installer records choices you make about your Asset Management for IT deployment and configuration parameters associated with those choices, and then installs and deploys the middleware based upon the information you entered.

The middleware installer installs and deploys the following software (compare with Figure 1 on page 1)::

Database server

Asset Management for IT uses the Maximo database to store details about the attributes and history of each configuration item and the details about the relationships between configuration items.

You will have the choice of installing a new instance of IBM DB2 9.5 , or using a preexisting instance of IBM DB2 8.2 or 9.1. If you choose to use Microsoft SQL Server or Oracle for your Asset Management for IT deployment, you will have to install and configure them separately.

Directory server

The directory server is used to secure the Asset Management for IT J2EE application.

You will have the choice of installing a new instance of IBM Tivoli Directory Server 6.2, or using a preexisting Directory Server or Microsoft Active Directory server. If you choose to install a new version of Directory Server, you must choose to install a new IBM DB2 instance or reuse an existing DB2 server. If you choose to use Microsoft Active Directory Server for your directory server, you will have to install and configure it separately.

J2EE server

The J2EE server is the application server used to serve and manage the Asset Management for IT application.

A directory server can be configured to secure the J2EE server deployment. You can use a local or remote IBM Tivoli Directory Server or Microsoft Active Directory Server.

The J2EE component includes the following subcomponents:

IBM HTTP Server

The server is used as the primary HTTP server. You will install a new instance of IBM HTTP Server.

IBM HTTP Server Plugin

The IBM HTTP Server Plug-in is used as the interface between the HTTP Server and the J2EE server. You will install a new instance of HTTP Server Plug-in.

The middleware installer deploys software on a single computer. To deploy Asset Management for IT middleware on multiple computers, the middleware installer must be invoked on each computer in the topology configuration you have chosen. Ensure you have a strategy for deploying product middleware for each system you plan to use in your Asset Management for IT deployment. If you deploy a Asset Management for IT component using the middleware installer on a system, for example, DB2, and then later decide you would also like to add Directory Server to that same system, you will have to undeploy DB2 before redeploying it in the same middleware installer deployment plan that included Directory Server. When installing Asset Management for IT middleware on a system, you must install all of the middleware intended for that system at one time.

In addition to installing and configuring Asset Management for IT middleware, the middleware installer performs additional tasks. If you choose to not run the middleware installer because you intend to perform the necessary configuration on existing middleware resources manually, you will need to configure Virtual Member Manager after the J2EE server and the Directory Server have been installed and configured. Refer to “Manually configuring Virtual Member Manager on IBM WebSphere Application Server” on page 128 for more information.

Process ID

Every time you use Tivoli middleware installer to install or uninstall middleware products, a *process ID* is generated.

A process ID:

- Appears on the file system in various places related to logs and generated files, such as file names, directory names, and log messages.
- It is used to group logs and other generated files that are related to the same invocation of the middleware installer.
- It also separates logs and other generated files that are related to different invocations of the middleware installer.

The process ID is a string of the format
`[operation_MMdd_HH.mm]`,

where

operation

is a string indicating the operation being performed, such as “INSTALL” or “UNINSTALL”,

MM

is a two-digit number (1-12) indicating the current month,

dd is a two-digit number (1-31) indicating the current day in the month,

HH

is a two-digit number (0-23) indicating the current hour,

mm

is a two-digit number (0-59) indicating the current minute.

Here are some examples of process ID values:

- [INSTALL_0924_15.45]
An installation started on September 24 at 3:45pm
- [UNINSTALL_1216_09.59]
An uninstallation started on December 16 at 9:59am

Tivoli middleware installer workspace

The Tivoli middleware installer is designed to record the options you select during install in a directory referred to as the *workspace*, and then configure the components selected as a single deployed application. Once a plan has been deployed, the middleware installer cannot subsequently deploy additional features and products onto the computer at a later time.

The existing plan must first be completely undeployed through the middleware installer before a different set of features and products can be deployed.

The composition and details of the deployment, as well as any logs generated by the middleware installer process are located in the workspace.

By default, the middleware installer workspace is defined as:

Windows

Windows:

C:\ibm\tivoli\mwi\workspace

UNIX

UNIX:

/ibm/tivoli/mwi/workspace

The workspace can be defined on a shared resource that is made available to all the systems that will run the middleware installer. Locating the workspace on a shared resource avoids the need to copy files such as the topology file manually from one computer to another.

The workspace contains the following items:

Deployment Plan

The deployment plan is a collection of installation steps, configuration parameters for those steps, and target computer information. It is generated through the middleware installer and it resides in the workspace directory.

When deployment steps are changed, the existing deployment plan is deleted and replaced with the new deployment plan.

The deployment plan configuration files contain information on the deployment plan itself. Whenever a deployment plan is modified, which

includes reconfiguring existing deployment choices, the deployment plan configuration files will be deleted and regenerated when the deployment plan is redeployed.

Topology File

The topology file is a properties file that describes the configuration parameters of the Asset Management for IT middleware deployment. This file is created and then updated after every deployment or undeployment. If you have not defined a workspace that is centrally located and accessible to all the systems that will be receiving Asset Management for IT middleware, this file will have to be copied to the workspace of each computer where Asset Management for IT middleware is being deployed. The contents of this file can be used by the Asset Management for IT installation program to populate its panels with meaningful default values.

This file is saved in *workspace_dir/topology.xml*.

Logs Log files that contain information on the deployment can be found in the workspace directory. In addition, log files native to the Asset Management for IT middleware itself are also contained in this directory.

Tivoli Asset Management for IT middleware deployment plan overview

The deployment plan resides in the workspace directory and is generated from deployment choices selected in the middleware installer. The plan is a series of deployment steps and configuration parameters.

Each step is responsible for installing and uninstalling one portion of the middleware. When deployment choices are changed, the existing deployment plan is deleted and replaced with the new deployment plan.

Once the deployment plan has been generated using the information you entered in the middleware installer, you have the option to have the middleware installer execute it. This method of executing the deployment plan is recommended in most instances.

Options for invoking the deployment plan

Once the deployment plan has been generated using the information you entered in the Tivoli middleware installer, you have several options for executing it.

Have the Tivoli middleware installer execute the deployment plan after it has been generated

This is the most common method of implementing the deployment plan. Create the plan using the middleware installer and then have it execute the plan by installing and configuring the middleware selected. This option also includes configuring existing instances of middleware present in your environment that will be used with Tivoli Asset Management for IT.

This method of executing the deployment plan is recommended in most instances.

Have the Tivoli middleware installer create the deployment plan and then componentize and distribute it

The deployment plan consists of a collection of XML files that can be used to deploy middleware either through the middleware installer or by Apache Ant. Ant is an open source software tool used to automate the software build process. Ant uses XML to describe build tasks and dependencies.

You need to have Ant 1.6.5 and the Java 1.5 JRE installed in order to execute a deployment plan outside of the middleware installer.

This method of executing the deployment plan should be reserved for advanced users that have a need to modify deployment plan parameters that are not configurable through the middleware installer.

Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer

This procedure explains how to use the middleware installer to create a deployment plan that is responsible for installing and configuring prerequisite middleware products. The instructions provided are for a typical installation using default values, and assume you are using the middleware installer to install a complete set of middleware for use with Asset Management for IT on a single computer.

Before you begin

If you intend to deploy middleware products across an array of computers, you will have to run the middleware installer on each computer, choosing which piece of middleware to install on that each particular computer. In this case, you will encounter a subset of the panels included in these instructions that are relevant to the middleware you have chosen to install on a computer.

The middleware installer can also configure existing middleware products. If you intend to reuse existing middleware products for your Asset Management for IT deployment, refer to “Reusing middleware” on page 77. Refer to the Asset Management for IT planning information to learn about using custom values during a custom installation.

In some cases, fields and labels displayed within the middleware installer are not correctly displayed on the panel when installing through remote sessions. It is recommended that you use the middleware installer locally on the system that will host the middleware. If you do experience this phenomenon, first minimize and then maximize the install wizard to force it to redisplay the panel.

Avoid using localhost for host name values in the installation program. Specify the actual fully-qualified host name of the system on which you are installing.

- **Linux** For Linux systems, ensure that the command `hostname -f` returns a fully-qualified host name. If it does not, consult the appropriate documentation for your operating system to ensure that the host name command returns a fully qualified host name.
- **Windows** For Windows systems, ensure a Windows Primary DNS suffix is defined.

To verify a fully qualified host name, complete the following steps:

1. On the desktop, right-click **My Computer**.
2. Select **Properties**. The System Properties panel is displayed.
3. From the Computer Name tab, click **Change**. The Computer Name Changes panel is displayed.
4. Enter your fully qualified host name in the **Computer name** field, and then click **More**. The DNS Suffix and NetBIOS Computer Name panel is displayed.

5. Verify that the Primary DNS suffix field displays a domain name, and then click **OK**.
6. From the Computer Name Changes panel, click **OK**.
7. Click **Apply** and close the System Properties panel.

Important: When entering LDAP values for Asset Management for IT installation panel fields, entries in LDIF files, or values you enter directly into an directory instance using the directory server's own tools, be aware of the product-specific syntax rules for using special characters in an LDAP string. In most cases, special characters must be preceded by an escape character in order to make it readable by the directory server. Failing to escape special characters contained in an LDAP string used with Asset Management for IT will result in product errors.

Many directory server products consider a blank space as a special character that is part of the LDAP string. Therefore, if you mistakenly enter an LDAP string that contains a blank, at the end of a field value, for example, and you do not precede the blank character with an escape character, you will encounter Asset Management for IT errors that will be difficult to troubleshoot. Refer to the product documentation for your directory server for more information on special characters in LDAP strings.

About this task

To install the prerequisite middleware products for Asset Management for IT, follow these steps:

1. Login as a user with administrative authority.
2. Launch the middleware installer from the Launchpad.
 - a. Start the Launchpad:

Windows For Windows

On the DVD titled "Tivoli Asset Management for IT 7.2", navigate to the root directory of the product disc or the downloaded installation image, and run the command: `launchpad.exe`.

UNIX For UNIX operating systems

On the DVD titled "Tivoli Asset Management for IT 7.2", navigate to the root directory of the product disc or the downloaded installation image, and run the following command: `launchpad.sh`.

AIX AIX

On the DVD titled "Tivoli Asset Management for IT 7.2", navigate to the root directory of the product disc or the downloaded installation image, and run the following command: `launchpad.sh`.

- b. In the Launchpad navigation pane, click **Install the Product**.
 - c. Click the **Middleware** link under **Install the middleware**.
3. Select a language for the installation and click **OK**.
4. From the Welcome panel, click **Next**. The middleware installer license agreement window is displayed. Read the license information and select **I accept both the IBM and the non-IBM terms** if you agree with the terms. Click **Next**.
5. From the Choose Workspace panel, specify the directory you will use as the middleware installer workspace, and then click **Next**.

The default location for the workspace will be the last workspace location used by this user, as specified in the middleware user preferences node. If no

previous workspace location exists in the middleware user preferences node, then the default location for the workspace will be

- **Windows** Windows: C:\ibm\tivoli\mwi\workspace
- **UNIX** UNIX: /ibm/tivoli/mwi/workspace

If the selected directory does not exist, it will be created.

After deployment, the middleware installer also generates a topology file in this directory. This topology file can be manually copied by the user to the workspace of the next computer in the topology, so that information on the deployment of middleware will be available to the middleware installer when it is executed on the next computer.

6. From the Install IBM Autonomic Deployment Engine panel, click **Next** to install the IBM Autonomic Deployment Engine.
7. From the Deployment Choices panel, select the features to deploy on this computer, and then click **Next**.

Choices include:

Database Server

The Database Server is used to store details about the attributes and history of each configuration item and the details about the relationships among configuration items.

Directory Server

The directory server is used to secure the J2EE Server. This feature should be selected to either install a new directory server locally or reuse a local directory server.

J2EE Server

The J2EE server is the application server used to serve and manage the application.

If you choose to only install the J2EE server portion of the Asset Management for IT middleware, you will be prompted to supply the directory server you will use to secure it. Your choices will be to secure with an existing instance of Directory Server, or an existing instance of Microsoft Active Directory.

Secure the J2EE Server using the Directory Server.

This option allows you to use a directory server to secure the J2EE server. By default this option is selected. It must remain selected in order for you to enable the Directory Server option. If you select to opt out of maintaining J2EE server through the use of the directory server, you will be unable to install the directory server through the Asset Management for IT middleware installation program.

8. From the Deployment Plan Summary window, click **Next** to configure the parameters displayed. The deployment plan is generated and you will be provided details about the plan.

The example modules of a full deployment look like this:

```
IBM Rational Agent Controller Version 7.0.3.3
DB2 Enterprise Server Edition Version 9.5.1
Configuration for DB2 Enterprise Server Edition
IBM Tivoli Directory Server Version 6.2
Configuration for IBM Tivoli Directory Server
WebSphere Application Server ND Version 6.1.0.23
Configuration for WAS ND
IBM HTTP Server Version 6.1.0.23
Embedded Security Services
```

9. In the Configuration Parameters window, the default discovered host name is displayed. You might want to override it, and then click **Next**.
10. From the Credentials panel, enter the Username and Password you will use to deploy the plan with, and then click **Next**. You can choose to enable the option of using the same password as the default user password value in all panels of the middleware installer by enabling the **Use this password as the value for all subsequent passwords** option at the top of this panel.
11. Enter the following configuration parameters for IBM DB2 Enterprise Server Edition 9.5 and then click **Next**.

Install location

Enter the location to install DB2 (*db2_install_dir*).

Windows

Windows :

Default is C:\Program Files\IBM\SQLLIB

Linux

Linux :

Default is /opt/IBM/db2/V9.5

AIX

AIX :

Default is /opt/IBM/db2/V9.5

DB2 Administration Server username

Enter the DB2 administrative account name.

Windows

Windows :

Default is db2admin

Linux

Linux :

Default is dasusr1

AIX

AIX :

Default is dasusr1

DB2 Administration Server password

Enter the password for the DB2 administrative account. If you marked in Step 10 to use the password in all subsequent windows, this password will be used.

Linux

AIX

Fenced user

Enter a system user ID that can be used as a DB2 fenced user account. Default fenced user is db2fenc1.

12. Enter the following configuration parameters for **the Default Database Instance** and click **Next**:

Default Instance name

Enter the name of the Asset Management for IT database instance.

Default for is DB2.

Default Instance Port

Enter the port that the Asset Management for IT database instance will use.

Default for all platforms is 50000.

Default Instance Username

Enter the user name for the Asset Management for IT database instance.

Windows **Windows :**
Default is db2admin

Linux **Linux :**
Default is ctginst1

AIX **AIX :**
Default is ctginst1

Default Instance user password

Enter the password for the Asset Management for IT database instance user name. If you marked in Step 10 on page 41 to use the password in all subsequent windows, this password will be used.

13. Enter the following configuration parameters for the Asset Management for IT Database Instance, and then click **Next**.

Instance name

Enter the name of the Asset Management for IT database instance.

Default for all platforms is ctginst1.

Port Enter the port that the Asset Management for IT database instance will use.

Default for all platforms is 50005.

Instance username

Enter the user name for the Asset Management for IT database instance.

Windows **Windows :**
Default is db2admin

Linux **Linux :**
Default is ctginst1

AIX **AIX :**
Default is ctginst1

Instance user password

Enter the password for the Asset Management for IT database instance user name. If you marked in Step 10 on page 41 to use the password in all subsequent windows, this password will be used.

14. Enter information on the DB2 user groups (**DB2 Enterprise Server Edition**).

DB2 administrators group

Enter the name of the DB2 administrators group.

Windows **Windows :**
Default is DB2ADMNS

Linux **Linux :**
Default is db2grp1

AIX **AIX :**
Default is db2grp1

Windows **DB2 users group**

Enter the name of the DB2 users group.

Default is DB2USERS

15. Enter the following configuration parameters for **IBM Tivoli Directory Server Version 6.2**, and then click **Next**.

Install location

Enter the location to install Directory Server.

Windows

Windows :

Default is C:\Program Files\IBM\LDAP\V6.2

Linux

Linux :

Default is /opt/IBM/ldap/V6.2

AIX

AIX :

Default is /opt/IBM/ldap/V6.2

Administrator distinguished name

Enter the distinguished name of the Directory Server administrator.

Default for all platforms is cn=root.

Administrator password

Enter the password for the Directory Server administrator.

16. Enter the following configuration parameters for **IBM Tivoli Directory Server Version 6.2**, and then click **Next**.

Organizational unit

Enter the name of the Directory Server organizational unit to use with Asset Management for IT.

Default for all platforms is ou=SWG.

Organization and country suffix

Enter the name of the Directory Server organization and country suffix to use with Asset Management for IT.

Default for all platforms is o=IBM,c=US.

Directory server port

Enter the port number of the Directory Server.

Default for all platforms is 389.

Directory server secure port

Enter the secure port number of the Directory Server.

Default for all platforms is 636.

Administration port

Enter the administration port number of the Directory Server.

Default for all platforms is 3538.

Administration secure port

Enter the secure administration port number of the Directory Server.

Default for all platforms is 3539.

17. Enter the following configuration parameters for **IBM Tivoli Directory Server Database Instance**, and then click **Next**.

Database name

Enter the name of the DB2 database you are using to hold Directory Server data.

Default for all platforms is security.

Instance name

Enter the name of the Directory Server database instance.

Default for all platforms is `idsccmdb`.

Port Enter the port number used by the Directory Server database instance.

Default for all platforms is `50006`.

Instance user password

Enter the password for the instance user ID.

18. Enter the following configuration parameters for **WebSphere Application Server security**, and then click **Next**.

LDAP HostName

Enter the host name of the system hosting the LDAP instance to use for WebSphere security.

Directory server port

Enter the port number used by the LDAP server to use for WebSphere security.

Default is `389`.

LDAP base entry

Enter the LDAP base entity of the LDAP instance to use for WebSphere security.

Default is `ou=SWG,o=IBM,c=US`

User suffix

Enter the user suffix of the LDAP instance to use for WebSphere security.

Default is `ou=users,ou=SWG,o=IBM,c=US`

Group suffix

Enter the group suffix of the LDAP instance to use for security.

Default is `ou=groups,ou=SWG,o=IBM,c=US`

Organization container suffix

Enter the organizational container suffix of the LDAP instance to use for security.

Default is `ou=SWG,o=IBM,c=US`.

19. Enter the following configuration parameters for WebSphere Application Server security, and then click **Next**.

Bind distinguished name

Enter the bind distinguished name for binding to the LDAP instance.

Default is `cn=root`

Bind password

Enter the password for the bind distinguished name.

20. Enter the following configuration parameters for WebSphere Application Server Network Deployment 6.1.0.23, and then click **Next**.

Install location

Enter the location to install WebSphere (*was_install_dir*)

Windows

Windows :

Default is `C:\Program Files\IBM\WebSphere\AppServer`

Linux

Linux :

Default is /opt/IBM/WebSphere/AppServer

AIX

AIX :

Default is /usr/IBM/WebSphere/AppServer

Administrator username

Enter the WebSphere administrative account name.

Default for all platforms is wasadmin.

Administrator password

Enter the password for the WebSphere administrative account.

21. Enter the following configuration parameters for WebSphere Application Server, and then click **Next**.

Deployment Manager profile name

Enter the WebSphere profile name of the deployment manager server.

Default for all platforms is ctgDmgr01.

Application server profile name

Enter the WebSphere profile name of the application server.

Default for all platforms is ctgAppSrv01.

22. Enter the following configuration parameters for WebSphere Application Server, and then click **Next**.

Cell name

Enter the WebSphere Cell name.

Default for all platforms is ctgCell01.

Deployment Manager node name

Enter the name of the WebSphere deployment manager node.

Default for all platforms is ctgCellManager01.

Application server node name

Enter the name of the WebSphere application server node.

Default for all platforms is ctgNode01.

Update Installer install location

Enter the location where the WebSphere update installer will be installed.

Windows

Windows :

Default is C:\Program Files\IBM\WebSphere\UpdateInstaller

Linux

Linux :

Default is /opt/IBM/WebSphere/UpdateInstaller

AIX

AIX :

Default is /usr/IBM/WebSphere/UpdateInstaller

23. Enter the following configuration parameters for IBM HTTP Server, and then click **Next**.

Install location

Enter the location to install HTTP Server (*http_server_install_dir*).

Windows

Windows :

Default is C:\Program Files\IBM\HTTPServer

Linux

Linux :

Default is /opt/IBM/HTTPServer

AIX

AIX :

Default is /usr/IBM/HTTPServer

HTTP port

Enter the port used by the HTTP Server.

Default for all platforms is 80.

Admin Server port

Enter the port to use to administer HTTP Server.

Default for all platforms is 8008.

24. Enter the configuration parameter **Profile name** for WebSphere Application Server plug-in for the IBM HTTP Server, and then click **Next**. Default for all platforms is ctgAppSvr01, and this value cannot be changed.
25. Enter the following configuration parameters for **IBM Rational Agent Controller Version 7.0.3.3**, and then click **Next**.

Install location

Enter the location to install Agent Controller.

Windows

Windows :

Default is C:\Program Files\IBM\AgentController

Linux

Linux :

Default is /opt/IBM/AgentController

AIX

AIX :

Default is /opt/IBM/AgentController

26. Specify the location of the Asset Management for IT middleware images, and then click **Next**.

Copy the middleware install images from the source media to a specified directory

Select this option to copy the Asset Management for IT middleware images from the product media to a directory that you will specify.

Specify a directory containing all the required middleware install images

Select this option if you intend to specify a file system directory that already contains all of the Asset Management for IT middleware installation images.

- If you selected the option to copy install images from the source media, specify the source and destination directories, and then click **Next**.
- If you selected the option to specify a directory that already contained the middleware images, specify that directory, and then click **Next**.

Note: Make sure you specified all the required files. If you did not, an error message is displayed.

27. Specify a directory to use for middleware installer temporary files and extracted middleware installation images, and then click **Next**.
28. From the Deployment Plan Operation panel, select **Deploy the plan**, and then click **Next**. You can also choose to make changes to the deployment plan or parameters you have previously configured from this panel.

29. From the Deployment Plan and Parameter Configuration summary panel, review the contents of the summary, and then click **Deploy** to initiate the installation and configuration of the middleware you selected. The installation might take up to 2 hours.
30. Once the deployment completes successfully, click **Finish** to exit. All the installed components are displayed in the deployment summary window.

Tivoli middleware installer logs

Tivoli middleware installer log files are located in the workspace directory (*workspace_dir*) that was defined in the middleware installer. Compare the different types of log files described in this section.

User interface logs

The logs generated by the middleware installer user interface are located in the workspace directory.

The *mwi.log* file is the high-level log file that was generated by the most recent invocation of the middleware installer. If an error occurs, examine this log file first. An entry in this log file might direct you to a lower-level log file.

Log files named *mwi.logX*, where *X* is a number, are copies of the *mwi.log* file from earlier invocations of the middleware installer. So, for example, *mwi.log0* is produced after the first invocation of the middleware installer, *mwi.log1* is produced after the second invocation of the middleware installer, and so on.

Logs for steps run by the user interface

In addition to collecting input from the user, the user interface of the middleware installer also performs several system checks. Examples of system checks run by the user interface runs include:

- dependency checking to ensure the operating system meets the deployment requirements
- inventorying the software on the system to locate existing instances of middleware products deployed by the middleware installer
- checking the available disk space to ensure there is enough for the deployment

Each of these checks is produced in the form of a step so that it can also be run as part of the deployment plan. When the user interface runs a step, it copies the step into a subdirectory of the workspace directory. The log files generated by a step are located in the same subdirectory and follow the same pattern as a step that is run as part of the deployment plan.

Logs for the deployment plan

The deployment plan is located in the directory *workspace_dir/host_name/deploymentPlan*, where *host name* is the host name of the current system. Each time the deployment plan is used to install or uninstall middleware products, a process ID is assigned and log files are generated.

The log files for the deployment plan are located in the subdirectory *logs/process_ID*. The primary log file for the deployment plan is *DeploymentPlan.log*, a high-level log file that lists the steps invoked as part of the deployment plan.

Logs for the computer plan

The computer plan is located in the directory *workspace_dir/host_name/deploymentPlan/computerPlan_host_name*. The log files for the computer plan are located in the logs subdirectory. The primary log files for the

computer plan are named `computerPlan_host_name_process_ID`. These log files contain the output generated by ANT when running the computer plan ANT script.

Logs for steps in the deployment plan

Each step in the deployment plan is located in a directory named `workspace_dir/host_name/deploymentPlan/MachinePlan_host_name/step_num_step_ID`, where `step_num` is the sequence number of this step in install processing order of the deployment plan and `step_ID` identifies the step. The log files for the step are located in the logs subdirectory.

Some steps might provide a message log file named `step_ID_process_ID.message`, which contains a few entries that summarize the result of invoking the step. All steps will provide a trace log file named `step_ID_process_ID.log`, which contains many entries, usually including information about the input parameters and the substeps invoked.

Logs for substeps

Each step contains one or more substeps. The substeps perform the actual install, uninstall and checking work for the middleware installer.

Each substep is located in the directory `workspace_dir/hostname/deploymentPlan/MachinePlan_host_name/step_num_step_ID/operation/substep_num_substep_ID`, where `operation` is the ANT target in the step ANT script that invokes this substep.

- `substep_num` is the sequence number of this substep in the processing order of the step
- `substep_ID` identifies the substep

Typical values for `operation` are `install`, `uninstall`, and `check`.

The log files for the substep are usually located in a subdirectory named `process_ID/logs`.

Log files generated by the native middleware installation programs will also be kept here.

Incorrect db2admin password

If you encounter error CTGIN9042E Errors were encountered during the execution of the step DB2 Enterprise Server Edition Version 9.1.4. through the normal use of the middleware installation program, it might be related to the fact that there is an existing user named `db2admin` on the system, but with a different password than the one entered in the middleware installation program.

Check the `db2_91_inst.log` file for an error similar to the following:

```
ERROR:The password specified is invalid. Enter a valid password.
```

The `db2_91_inst.log` file is located at: `Workspace\computer_name\deploymentPlan\MachinePlan_computer_shortcode\00004_DB2_9.1\install\01_BASE\ [INSTALL_processing.req.id]\logs\ db2_91_inst.log`

So, for example, if the workspace is located at: `C:\ibm\tivoli\workspace`, the machine name is `mymachine`, and the `processing.req.id` is created as a `date_timestamp`, then the `db2_91_inst.log` file would be located in: `C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\MachinePlan_mymachine\00004_DB2_9.1\install\01_BASE\ [INSTALL_0424_09.32]\logs`

Check the `de_processreq.log` file for an error similar to the following:

```

<errorMessages>
  <errorMessage>[com.ibm.ac.si.ap.action.ExternalCommandActionException:
ACUOSI0050E External command action failed with return code 87. Invocation
string: [C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\DB2-ESE_9.1.0/ESE/setup.exe,
/f, /1, C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\INSTALL_0424_09.32]/db2_91_inst.log,
/u, C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\INSTALL_0424_09.32]/
Decrypted_ResponseFile.txt],
com.ibm.ac.common.hosts.CreationFailedException: : ]</errorMessage>
  <errorMessage>[com.ibm.ac.common.hosts.CreationFailedException: : ]
</errorMessage>
</errorMessages>
<actionErrorEvents>
  <actionErrorEvent actionID="InstallProduct" actionName="externalCommand">
    ACUCME1100E
  </actionErrorEvent>
</actionErrorEvents>

```

The de_processreq.log file is located at: *Workspace\computer_name\deploymentPlan\MachinePlan_computer_shortcode\00004_DB2_9.1\install\01_BASE\INSTALL_processing.req.id\logs\ de_processreq.log*

So, for example, if the workspace is located at: *C:\ibm\tivoli\workspace*, the machine name is *mymachine*, and the *processing.req.id* is created as a *date_timestamp*, then the de_processreq.log file would be located in: *C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\MachinePlan_mymachine\00004_DB2_9.1\install\01_BASE\INSTALL_0424_09.32\logs*

These errors indicate that the existing system user db2admin has different password than the one entered in the middleware installation program.

To resolve this issue, complete the following steps:

1. If you have not done so, click **Finish** to exit out of the of the middleware installation program install wizard.
2. Resolve the issue using one of the following methods:
 - If you are the Administrator for that machine/user and if you know the password for the user db2admin you can use the same password for the middleware installation program installation.
 - You can delete the user db2admin and restart the middleware installation program .
 - You can set or change the password for existing DB2 user db2admin.

To set the password follow these steps

 - a. Right click the My Computer icon and select **Manage**.
 - b. From the Computer Management console, select Local Users and Groups in System Tools.
 - c. Expand Local Users and Groups and then select **Users**
 - d. Right-click the db2admin user and then click **Set password**.
 - e. Enter the password, confirm it, and then click **OK**
 - f. Click **OK** once again.
3. Navigate to the directory containing the middleware installation program DVD image and restart the middleware installation program.
4. Select **Restart the Plan** and click **Next**.
5. Specify the directory for the middleware install images and click **Next**.
6. Specify the temporary directory and click **Next**.

7. After disk space checks are completed, click **Deploy** to start the install.
8. After install completes click **Finish** to exit the wizard.

Invalid DB2 password value

While installing the middleware, you might encounter a problem with the DB2 password that is not compliant with the password policy of the system.

If you encounter the following error while using the middleware installation program:

```
CTGIN9042E: Errors were encountered during the execution of the step DB2
Enterprise Server Edition Version 9.1
```

it could be attributed to the use of a password value entered for the DB2 user in the middleware installation program that is incompatible with the password policy of the system.

Check the db2_91_inst.log file for an error similar to the following:

```
1: ERROR:The installation program has been unable to create the user
"db2admin" on computer "mymachine" because the password specified is too short.

1: ERROR:The response file specified "C:\WINNT\TEMP\2\_INSTA~1.18_/DECryp~1.TXT"
is not valid.
```

The db2_91_inst.log file is located at: <Workspace>\<machine name>\deploymentPlan\MachinePlan_<machine shortname>\00004_DB2_9.1\install\01_BASE\[INSTALL_<processing.req.id>]/logs/ db2_91_inst.log

So, for example, if the workspace is located at: C:\ibm\tivoli\workspace, the machine name is mymachine, and the processing.req.id is created as a date_timestamp, then the db2_91_inst.log would be located in:C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\MachinePlan_mymachine\00004_DB2_9.1\install\01_BASE\[INSTALL_0424_09.32]\logs.

Also check the de_processreq.log file for an error similar to the following:

```
<errorMessages>
  <errorMessage>[com.ibm.ac.si.ap.action.ExternalCommandActionException:
    ACUOSI0050E External command action failed with return code 87.
    Invocation string: [C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\DB2-ESE_9.1.0/
    ESE/setup.exe, /f, /1, C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\
    [INSTALL_0424_09.32]/db2_91_inst.log, /u, C:\DOCUME~1\ADMINI~1\LOCALS~1\
    Temp\1\[INSTALL_0424_09.32]\Decrypted_ResponseFile.txt],
    com.ibm.ac.common.hosts.CreationFailedException: : ]</errorMessage>
  <errorMessage>[com.ibm.ac.common.hosts.CreationFailedException: : ]
</errorMessage>
</errorMessages>
<actionErrorEvents>
  <actionErrorEvent actionID="InstallProduct"
    actionName="externalCommand">ACUCME1100E
  </actionErrorEvent>
</actionErrorEvents>
```

The de_processreq.log file is located at: *Workspace\computer_name\deploymentPlan\MachinePlan_computer_shortname\00004_DB2_9.1\install\01_BASE\[INSTALL_processing.req.id]/logs/ de_processreq.log.*

So, for example, if the workspace is located at: C:\ibm\tivoli\workspace, the computer name is mymachine, and the processing.req.id is created as a date_timestamp, then the de_processreq.log would be located in:

C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\
MachinePlan_mymachine\00004_DB2_9.1\install\01_BASE\
[INSTALL_0424_09.32]\logs.

This would indicate that the password provided for the DB2 user db2admin in the middleware installation program is not supported by the policy of the operating system.

To resolve this issue, complete the following steps:

1. If you have not done so, click **Finish** to exit out of the of the middleware installation program install wizard.
2. Check the system rules defined for passwords by navigating to **Start** → **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Account Policies** → **Password Policy**.
3. Restart the middleware installation program, by running the `launchpad.[exe|sh]` command.
4. Proceed through the panels until you reach the option to select **Undeploy the Plan** and then click **Finish** to exit the wizard.
5. Restart the middleware installation program.
6. Select **Edit the Configuration parameters**.
7. Enter a valid password for the DB2 user based upon the password policy rules you observed earlier.
8. Specify the directory for the middleware install images and click **Next**.
9. Specify the temporary directory and click **Next**.
10. After disk space checks are completed, click **Deploy** to start the install.
11. After install completes, click **Finish** to exit the wizard.

Configuring IBM Tivoli Directory Server user and group strings

Use this information to configure directory server user and group strings post installation, on systems that only host Directory Server.

About this task

If you need to configure Directory Server user and group strings for a system that only hosts the Directory Server, it is necessary to manually create properties in the `input.properties` file of the `ITDS_CONFIGURATION` step of the deployment plan.

1. Edit the `input.properties` file located in the directory server folder at: `Workspace\computer_name\deploymentPlan\MachinePlan_computer_shortname\00006_ITDS_Configuration`

Windows

For example, in Windows, if the workspace is located at: `C:\ibm\tivoli\workspace` and the machine name is `mymachine`, then the `input.properties` would be located in: `C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\MachinePlan_mymachine\00006_ITDS_Configuration`

Linux

For example, in Linux, if the workspace is located at: `/root/ibm/tivoli/mwi/workspace` and the machine name is `mymachine`, then the `input.properties` would be located in: `/root/ibm/tivoli/mwi/`

workspace/mymachine.ibm.com/deploymentPlan/
MachinePlan_mymachine.ibm.com/00006_ITDS_Configuration

AIX AIX

For example, in AIX, if the workspace is located at: /ibm/tivoli/mwi/workspace, the machine name is *mymachine*, then the input.properties would be located in: /ibm/tivoli/mwi/workspace/mymachine.ibm.com/deploymentPlan/MachinePlan_mymachine.ibm.com/00006_ITDS_Configuration

2. Create properties in the input.properties file that are like the following sample property:

```
was_nd.secure.GroupSuffix=ou\=groups,ou\=SWG,o\=IBM,c\=US  
was_nd.secure.UserSuffix=ou\=users,ou\=SWG,o\=IBM,c\=US
```

These group and user strings are default strings. These strings can be customized.

Example

For example, if you want to change the strings groups to grpous and users to usarious, the properties are like the following sample strings:

```
was_nd.secure.GroupSuffix=ou\=grupos,ou\=SWG,o\=IBM,c\=US  
was_nd.secure.UserSuffix=ou\= usarious,ou\=SWG,o\=IBM,c\=US
```

So, in the configuration parameters panel for Directory Server, if you have given custom values instead of default values for Organizational unit, such as ou=SWG1 and an Organization country suffix such as o=IBM1,c=US1 then you have to manually replace all the occurrences of ou=SWG with ou=SWG1 and o=IBM,c=US with o=IBM1,c=US1 in the input.properties file.

In this example, the properties are like the following sample properties:

```
was_nd.secure.GroupSuffix=ou\= grpous,ou\=SWG1,o\=IBM1,c\=US1  
was_nd.secure.UserSuffix=ou\= usarious,ou\=SWG1,o\=IBM1,c\=US1
```

Installing middleware silently

provides the option of installing middleware silently. The middleware silent installation option allows you to interface with the middleware installation program using a command prompt (not the), and a response file. It can be used to deploy, undeploy, or restart the deployment of an existing deployment plan. It can also be used to select deployment choices, generate a deployment plan and enter configuration parameters provided you have a valid response file with the appropriate entries.

Before you begin

The middleware installation program includes a record option that allows you to record the responses entered when installing, and then produces a response file. By providing a text-based response file and invoking the middleware installation program silently, a deployment plan can be processed without the use of the middleware installation program user interface and without requiring user interaction.

You need to create a separate silent installation response file for each combination of the features that you want deployed. For example, you can create one silent response file for an all inclusive installation which includes the deployment and

configuration of a database, J2EE server, and directory server, or you can create one silent response file for each piece of middleware, where only one server type is selected to be deployed and configured.

Note: Passwords are encrypted strings in response files. If you are modifying password values in a response file, you enter clear text values. The middleware installation program silent installation feature can work with either encrypted or clear text values.

An error can occur when reinstalling middleware silently after it has been uninstalled. This error occurs if you use the same command window you used to uninstall middleware to reinstall using the middleware installation program. To avoid this error, after a successful uninstall operation, close the command window you used to invoke the installation program and use a new command window to run the middleware installation program.

About this task

To install middleware silently, complete the following steps:

1. Create a response file by generating a deployment plan and making configuration choices using the middleware installation program.
 - a. Open a command window, and invoke the middleware installation program user interface using the following command:

Windows **Windows:**

- 32-bit
`mwi-console.exe -options -record`
- 64-bit
`mwi-AMD64.exe -options -record`

Linux **Linux:**

```
mwi.bin -options -record
```

AIX **AIX:**

```
mwi_aix.bin -options -record
```

- b. Navigate the middleware installation program user interface, making deployment and configuration choices.
- c. When you reach the Deployment Preview Panel, select one of the following:

Finish The **Finish** button generates a response file containing the choices you made.

Cancel

The **Cancel** button quits the installation.

The middleware installation program executable files are located in the middleware directory of the “ ” product DVD.

2. Open the response file in a text editor and make any necessary changes. Changes might include supplying different passwords or installation paths.
3. Copy the response file to the target system.
4. Launch the middleware installation program silently and identify the response file to be used.

Windows **Windows:**

- 32-bit:
`mwi-console.exe -options -silent`

- 64-bit
mwi-AMD64.exe -options -silent

Linux:
mwi.bin -options -silent

AIX:
mwi_aix.bin -options -silent

The value for needs to contain the fully qualified path and name of the response file being used.

The middleware installation program executable files are located in the middleware directory of the “ ” product DVD.

What to do next

When the installation is complete, you receive a success message output to the console.

Silent middleware installation program options

Response files contain a number of options that you can edit before invoking the middleware installation program silent installation program.

Response file options are detailed in comments contained in the response file itself.

Each option exists as an entry in the middleware installation program response file, in the following format:

-V option_name option_value

The following text is an excerpt of a response file:

```
#####
date time
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Has the license been accepted
#-----
LICENSE_ACCEPTED=TRUE

#Choose Install Folder
#-----
USER_INSTALL_DIR=C:\\IBM\\SMP

#Choose Deployment
#-----
SIMPLE=0
ADVANCED=1

#Import Middleware Configuration Information
#-----
MWI_IMPORT_DATA=1
MWI_HOSTNAME=127.0.0.1
MWI_USER_ID=Administrator
MWI_PASSWORD=
MWI_LOCATION=C:\\ibm\\tivoli\\mwi\\workspace

#Database Type
```

```

#-----
DB_TYPE_DB2=1
DB_TYPE_ORACLE=0
DB_TYPE_SQLSERVER=0

#Database
#-----
DB_HOST_NAME=127.0.0.1
DB_PORT=50005
DB_NAME=maxdb71
DB_INSTANCE=ctginst1
DB_SCHEMA=maximo
DB_USER=maximo
DB_PASSWORD=

#Automate Database Configuration
#-----
AUTOMATE_DB=1
DO_NOT_AUTOMATE_DB=0

#Remote Access Authorization
#-----
DB_RXA_USER=administrator
DB_RXA_PASSWORD=

#DB2 Administration
#-----
DB_INSTALL_DIR=C:\\Program Files\\IBM\\SQLLIB
DB_ADMIN_USER=db2admin
DB_ADMIN_PASSWORD=
DB_WIN_SERVICE_USER=db2admin
DB_WIN_SERVICE_PASSWORD=

#DB2 Tablespace
#-----
DB_TABLE_SPACE_NAME=MAXDATA
DB_TABLE_SPACE_SIZE=5000
DB_TEMP_TABLE_SPACE_NAME=MAXTEMP
DB_TEMP_TABLE_SPACE_SIZE=1000
DB_INDEX_TABLE_SPACE_NAME=MAXDATA
DB_INDEX_TABLE_SPACE_SIZE=5000

#Application Server Type
#-----
APPLICATION_SERVER_TYPE_WAS=1
APPLICATION_SERVER_TYPE_BEA=0

#WebSphere Connectivity
#-----
WAS_HOSTNAME=127.0.0.1
WAS_SOAP_PORT=8879

#Automate WebSphere Configuration
#-----
AUTOMATE_WAS_CLIENT=1
DO_NOT_AUTOMATE_WAS_CLIENT=0

#WebSphere Remote Access Authorization
#-----
WAS_CLIENT_RXA_USER=administrator
WAS_CLIENT_RXA_PASSWORD=

#WebSphere Deployment Manager Configuration
#-----
WAS_HOME_DIR=C:\\Program Files\\IBM\\WebSphere\\AppServer
WAS_USER=wasadmin
WAS_PASSWORD=

```

```

WAS_PROFILE=ctgDmgr01

#WebSphere Application Server Configuration
#-----
WAS_VIRTUAL_HOST_PORT=80
WAS_WEB_SERVER_NAME=webserver1
WAS_NODE_NAME=ctgNode01
WAS_CLUSTER_NAME=MAXIMOCLUSTER
WAS_APPLICATION_SERVER_NAME=MXServer

#Security
#-----
LDAP_OPTION1=0
LDAP_OPTION2=0
LDAP_OPTION3=1

#Integration Adapter JMS Configuration
#-----
WAS_SIB_DS_NAME=intjmsds
WAS_JMS_PERSIST_DATASTORE=0
WAS_JMS_DO_NOT_PERSIST_DATASTORE=1

#SMTP Configuration
#-----
SMTP_SERVER=
ADMIN_EMAIL=

#Run Configuration Step
#-----
RUN_CONFIG_YES=1
RUN_CONFIG_NO=0
DEPLOY_EAR_YES=1
DEPLOY_EAR_NO=0

#Choose Shortcut Folder
#-----
USER_SHORTCUTS=C:\\Documents and Settings\\All Users\\Start Menu\\Programs\\Tivoli Asset Management

#Language Support
#-----
INSTALL_LANGUAGE_VALUE=0
DO_NOT_INSTALL_LANGUAGE=1

```

IBM Tivoli Asset Management for IT installation program overview

The IBM Tivoli Asset Management for IT installation program provides an interface for installing and deploying Asset Management for IT. The installation program records choices you make about your Asset Management for IT deployment and configuration parameters associated with those choices, and then installs and deploys Asset Management for IT based upon the information you entered.

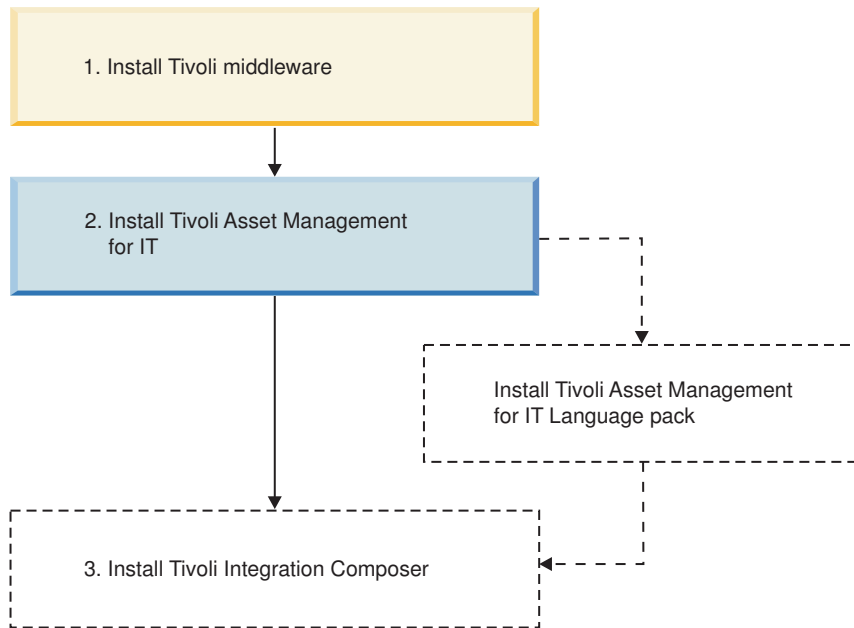


Figure 4. Tivoli Asset Management for IT installation flow - Tivoli Asset Management for IT installation.

There are two installation paths available to you when installing Asset Management for IT.

Simple

A simple deployment consists of installing all middleware on one system. You will not have the option of using existing middleware within your organization with Asset Management for IT. All middleware used with Asset Management for IT must have been installed on the system using the middleware installer using default values. Asset Management for IT will be installed using default values provided by the middleware and Asset Management for IT installation programs.

For a list of values being set when using this option, refer to “Tivoli Asset Management for IT simple install path values” on page 58. If you intend to override default values used by the simple deployment path, you will have to use the custom deployment path instead.

Note: On choosing a simple deployment, you might encounter this error message:

CTGIN2375E: J2EE application security non enabled in J2EE application server

Make sure you have the WebSphere Application Server security switched on. Refer to the WebSphere Application Server Information Center for instructions.

<http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp>.

Custom

A custom deployment typically involves deploying Asset Management for IT across several systems, some of which probably already host middleware products that you wish to use with your Asset Management for IT deployment. Deploying through the custom installation path also allows you to modify default installation values.

This deployment option does not require you to spread the Asset Management for IT deployment across several systems. You can enter the name of the local host as the destination for all Asset Management for IT components that are to be installed using the middleware installer and the Asset Management for IT installation program.

The Asset Management for IT installation program can automate the configuration of middleware for use with Asset Management for IT. If you choose not to have the Asset Management for IT installation program automatically configure middleware, configure that piece of middleware manually prior to the installation of Asset Management for IT.

Important: While you can deploy Asset Management for IT in a distributed environment consisting of predominately UNIX systems, the Asset Management for IT installation program must be run from a Windows system.

Important: When entering LDAP values for Asset Management for IT installation panel fields, entries in LDIF files, or values you enter directly into a directory instance using the directory server tools, be aware of the product-specific syntax rules for using special characters in an LDAP string. In most cases, in order to make them readable by the directory server, special characters must be preceded by an escape character. Failing to escape special characters contained in an LDAP string used with Asset Management for IT result in Asset Management for IT errors.

Many directory server products consider a blank space as a special character that is part of the LDAP string. Therefore, if you mistakenly enter an LDAP string that contains a blank, at the end of a field value, for example, and you do not precede the blank character with an escape character, you will encounter Asset Management for IT errors that are difficult to troubleshoot.

Refer to the product documentation for your directory server for more information on special characters in LDAP strings.

Information that you input into the Asset Management for IT installation program is stored in the `maximo.properties` file and the Maximo database. These values are populated into the panel fields of the Asset Management for IT installation program on subsequent uses of the program. Therefore, if you cancel the installation program after entering values across several installation panels, the installation program will recall the values the next time you start up the Asset Management for IT installation program (except for the Asset Management for IT install directory and the shortcut option chosen). You can restore the default values in the Asset Management for IT installation program by deleting `tamit_install_dir/maximo/applications/maximo/properties/maximo.properties`.

Tivoli Asset Management for IT simple install path values

If you choose to install Tivoli Asset Management for IT using the *simple* install path, the values listed in this section are set. You will be able to provide values where indicated.

Table 11. Tivoli Asset Management for IT Simple Install Path Values

Category	Field	Value	Provided by User?
Deployment Option	Deployment	Simple	

Table 11. Tivoli Asset Management for IT Simple Install Path Values (continued)

Category	Field	Value	Provided by User?	
Database Configuration	Database Type	DB2		
	Host name		Yes	
	Port	50005		
	Database Name	maxdb71		
	Instance	ctginst1		
	User ID		Yes	
	Automate Database Configuration	yes		
	Remote Access User ID		Yes	
	Database Install Directory			
		Windows		
		Windows	C:\Program Files\IBM\SQLLIB	
		UNIX		
		UNIX	/opt/IBM/db2/V9.5	
	Instance Administrator User ID			Yes
		Windows		
		Windows	db2admin	
	UNIX			
	UNIX	ctginst1		
Windows Service User ID	db2admin			
Data table space name	maxdata			
Data table space size (Mb)	5000			
Temporary table space name	MAXTEMP			
Temporary table space size (Mb)	1000			
Index table space name	MAXDATA			
Index table space size (Mb)	3000			
WebSphere Deployment Manager Configuration	Host name		Yes	
	SOAP Port	8879		
	WebSphere installation directory (<i>was_install_dir</i>)			
		Windows		
		Windows	C:\Program Files\IBM\WebSphere\AppServer	
		Linux		
		Linux	/opt/IBM/WebSphere/AppServer	
		AIX		
		AIX	/usr/IBM/WebSphere/AppServer	
		Solaris		
		Sun Solaris	/opt/IBM/WebSphere/AppServer	
	User ID	wasadmin		Yes
	Profile name	ctgDmgr01		
	Automate WebSphere Configuration	yes		
	Remote Access User ID			Yes
	WebSphere Application Server configuration	Web server port	80	
Web server name		webservice1		
Node name		ctgNode01		
Cluster name		MAXIMOCLUSTER		
Application server		MXServer Note: This value cannot be changed.		
Integration Adapter JMS Configuration	JMS DataSource name	intjmsds		
	Persist JMS messages	no		

Table 11. Tivoli Asset Management for IT Simple Install Path Values (continued)

Category	Field	Value	Provided by User?
Security Server Configuration	Configure J2EE Server application security	yes	
	Use WebSphere application security for authentication and authorization	yes	
	User base entry	ou=users,ou=SWG,o=IBM,c=US	
	Group base entry	ou=groups,ou=SWG,o=IBM,c=US	
	Create the required users	yes	
Maximo Configuration	Install directory	C:\IBM\SMP	Yes
Configuration Step	Perform installation configuration now	yes	

Performing IBM Tivoli Asset Management for IT installation

In addition to configuring new instances of IBM Tivoli Asset Management for IT middleware products installed by the middleware installer, the Asset Management for IT installation program can configure existing instances of prerequisite products, including those from other vendors, that you want to use with Asset Management for IT. The instructions provided are for a *multiple computer* installation using default values and assume that you choose to have the Asset Management for IT installation program automatically configure middleware across multiple computers to work with Asset Management for IT.

Before you begin

If you do not allow the Asset Management for IT installation program to configure middleware automatically, it still performs programmatic checks to verify that the documented manual steps were performed properly. If any errors are encountered, a dialog box detailing the error appear. You will not be permitted to continue in the Asset Management for IT installation task until the errors are resolved.

Attention: Windows The Asset Management for IT installation program can only be run from a Windows-based system.

Before you begin, ensure you have addressed the following prerequisite conditions:

Table 12. Asset Management for IT installation prerequisite conditions.

Operating system or database management system	Requirements
Linux	Ensure that the command <code>hostname -f</code> returns a fully qualified host name. If it does not, consult the appropriate documentation for your operating system to ensure that the <code>hostname</code> command returns a fully qualified host name.

Table 12. Asset Management for IT installation prerequisite conditions. (continued)

Operating system or database management system	Requirements
	<p data-bbox="857 275 1446 323">If the remote system is a Windows computer, configure RXA to work over SMB.</p> <p data-bbox="857 350 1446 453">If you are using DB2 with Asset Management for IT, and you want to use the fully automated database configuration capabilities of the Asset Management for IT installation program, ensure that the following conditions are met:</p> <ul data-bbox="857 464 1463 842" style="list-style-type: none"> <li data-bbox="857 464 1463 594">• The user ID specified as the Instance administrator user ID that you enter on the DB2 Administration panel of the Asset Management for IT installation program must have DB2 administration authority, which is referred to as SYSADM authority in the DB2 product documentation. <li data-bbox="857 604 1463 842">• The user ID specified on the Remote Access Authorization panel of the Asset Management for IT installation program must have DB2 administration authority. It is used to create the DB2 instance, database, and schema. It must have SYSADM authority, as defined by DB2. This requires the ID to be a member of the group defined by the sysadm_group configuration parameter for the DB2 instance you plan to use. For example, on Windows, the user must belong to the DB2ADMNS group. <p data-bbox="883 877 992 905">Windows</p> <p data-bbox="883 926 1446 1056">If you are using Microsoft Active Directory to secure WebSphere Application Server, ensure the users and groups listed in “Manually configuring Microsoft Active Directory” on page 121 have been manually created in the Microsoft Active Directory instance.</p> <p data-bbox="857 1083 1446 1136">For more information on creating DB2 users, refer to the IBM DB2 product documentation:</p> <p data-bbox="456 1163 565 1190">Windows</p> <p data-bbox="857 1163 1414 1213">http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp</p>

Table 12. Asset Management for IT installation prerequisite conditions. (continued)

Operating system or database management system	Requirements
	<p>If you are using DB2 with Asset Management for IT, and you want to use the fully automated database configuration capabilities of the Asset Management for IT installation program, ensure that the following conditions are met:</p> <ul style="list-style-type: none"> • For DB2 UNIX installations, create the instance user on the DB2 server before starting the Asset Management for IT installation program. For example if you plan to create the Maximo database in a DB2 instance (ctginst1 is recommended), create a user (including the home directory for the user) on the UNIX DB2 server prior to starting the install. • The user ID specified as the Instance administrator user ID that you enter on the DB2 Administration panel of the Asset Management for IT installation program must have DB2 administration authority, which is referred to as SYSADM authority in the DB2 product documentation. • The user ID specified on the Remote Access Authorization panel of the Asset Management for IT installation program must have DB2 administration authority. It is used to create the DB2 instance, database, and schema. It must have SYSADM authority, as defined by DB2. This requires the ID to be a member of the group defined by the sysadm_group configuration parameter for the DB2 instance you plan to use. • The fenced user must be db2fenc1. • Add root to the DB2GRP1 group prior to starting the Asset Management for IT installation program. <p>For more information on creating DB2 users, refer to the IBM DB2 product documentation:</p> <p>http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp</p>
UNIX	
AIX	<p>Default installations of AIX systems might not include a suitable protocol and must have RXA compatible protocols enabled.</p> <p>If you plan to take advantage of the Asset Management for IT installation program feature that automates the configuration of Asset Management for IT middleware, enable a Remote Execution and Access (RXA) service for each system on which you intend to install the middleware. RXA requires that the target system enable at least one of the protocols supported by RXA, which includes rsh, REXEC, SSH, and Windows SMB. Before you start the Asset Management for IT installation program, ensure that one of these protocols is running and accepting remote logins using a user name and password configured on the target computer.</p>
	<p>The middleware environment is installed and running properly.</p>
	<p>Avoid using localhost for host name values in the install program. Specify the actual fully qualified host name of the system for all host name values.</p>
All DB2 installations	<p>You might encounter ever increasing system memory usage linked with DB2. If you experience this behavior, set the following DB2 property and then restart the DB2 server:</p> <pre>db2 update dbm cfg using KEEPFCENCED NO</pre>
Oracle installations	<p>Ensure that Oracle 9i, 10g or 11g are installed (see "Hardware and software requirements" on page 2 for comparison).</p>

Table 12. Asset Management for IT installation prerequisite conditions. (continued)

Operating system or database management system	Requirements
Microsoft SQL Server installations	<p>Ensure:</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2008 is installed. • Asset Management for IT uses port 1433 when configured with SQL Server. By default, this port is not enabled. Enable this port. Refer to http://msdn.microsoft.com/en-us/library/ms177440.aspx for instructions.

For WebSphere Application Server Network Deployment, ensure that the Cell and all related nodes are actively running.

About this task

To install Asset Management for IT, follow these steps:

1. Log in as Administrator on the Asset Management for IT administrative system.
2. Launch the Asset Management for IT installation program from the Launchpad:
 - a. Start the Launchpad: On the DVD titled "Tivoli Asset Management for IT 7.2", navigate to the root directory of the product disk or the downloaded installation image, and run the following command: `launchpad.exe`.
 - b. In the launchpad navigation pane, click **Install the Product**.
 - c. Click **Tivoli Asset Management for IT**.
3. Select a language for the installation and click **OK**.
4. From the Introduction panel, click **Next**. The Pre-installation Progress window is displayed.

Note: This is the moment the installer analyzes whether to install or upgrade the IBM Autonomic Computing Deployment Engine and detects the existing instances.

5. In the Package Summary window, there are **Packages Analyzed** displayed and their status. When installing for the first time, the status **Not installed** shows up. If there were any other Asset Management for IT instances detected, they would be marked **Installed** along with their version.
6. From the License Agreement panel, choose the **I accept both the IBM and non-IBM terms**, if you agree with them, and then click **Next**.
7. From the Choose Install Folder panel, specify the directory you use to install Asset Management for IT, and then click **Next**.

Where Would You Like to Install?

Enter the path to install Asset Management for IT.

By default, this value is `C:\IBM\SMP`.

The path you specify must not contain spaces.

8. From the Choose Deployment panel, select the **Custom** deployment topology, and then click **Next**.

Simple

Select **Simple** if you want to deploy all Asset Management for IT components on a single system. This deployment option is typically

only used for demonstration, proof-of-concept, or training purposes. The default values are displayed in Table 11 on page 58.

Custom

Select custom if you want to deploy Asset Management for IT components across several systems. This deployment option is typically used in a production environment. This option is recommended.

As a result, the Asset Management for IT configuration for your system processing window is displayed.

9. From the Import Middleware Configuration Information panel, specify that you want to use field values you input into the middleware installer as default values for those same fields in the Asset Management for IT installation program.

Import Middleware Configuration Information

Select this check box if you want to allow the Asset Management for IT installation program to reuse values entered for DB2 in the middleware installer.

Note that if you select this feature while installing Asset Management for IT by way of RXA, the **Workspace Location** that you specify cannot be located on a networked drive of the remote system. It must reside locally on the remote system.

The middleware default information will not be used if you select the Simple deployment path.

Host name

Enter the fully qualified host name of the system where the middleware installer was run.

User ID

Enter the User ID that was used to run the middleware installer.

Password

Enter the password of the User ID that was used to run the middleware installer.

Workspace Location

Enter the location of the topology file that contains the values entered for the middleware installer. This file is found in the workspace that was defined during the Asset Management for IT middleware installation task. For example, C:\ibm\tivoli\mwi\workspace.

10. From the Maximo Database Type panel, select the product that you use for the Maximo database, and then click **Next**.

DB2 Select this choice to use DB2 as the Maximo database.

Oracle Select this choice to use Oracle as the Maximo database.

SQL Server

Select this choice to use Microsoft SQL Server 2008 as the Maximo database.

Each database will have its own unique set of configurable parameters and values.

11. From the Maximo Database panel, enter configuration information on the database, and then click **Next**.

DB2

Host name

Enter the host name of the computer hosting DB2.

The host name must be fully qualified.

Port Enter the port being used by DB2 instance.

The default is *50005*.

Database name

Enter the name of the database to use with Maximo.

The default database name is *maxdb71*. The database is created if it does not exist.

Instance

Enter the name of the database instance to be used with Maximo.

The default instance name is *ctginst1*. This instance is created if it does not exist, however, the user and its associated home directory must exist on the DB2 server.

Database user ID

Enter the user ID used for Maximo to access DB2.

Default for all platforms is *maximo*.

This user ID is created if it does not exist.

This user ID cannot be the same one used as the instance administrator user ID.

Database password

Enter the password for the user ID used to access DB2.

Oracle**Host name**

Enter the host name of the computer hosting Oracle.

The host name must be fully qualified.

Port Enter the port being used by Oracle.

The default is *1521*.

Instance

Enter the name of the database instance to be used with Maximo.

The default instance name is *ctginst1*.

Database user ID

Enter the user ID used for Maximo to access Oracle.

Default for all platforms is *maximo*.

This user ID is created if it does not exist.

Database password

Enter the password for the user ID used to access Oracle.

SQL Server**Host name**

Enter the host name of the computer hosting SQL Server.

The host name must be fully qualified.

Port Enter the port being used by SQL Server.
The default is 1433.

Database Name
Enter the name of the database to use with Maximo.
The default database name is maxdb71.

Database user ID
Enter the user ID used to access SQL Server.
Default for all platforms is maximo.
This user ID is created if it does not exist.

Database password
Enter the password for the user ID used to access SQL Server.

12. From the Automate Database Configuration panel, select **Automate database configuration**, and then click **Next**.

This step allows the Asset Management for IT installation program to configure the database automatically for use by Asset Management for IT. Examples of automated tasks include creating table spaces, creating database tables, creating database schemas, creating users, and so on.

If you choose not to have the Asset Management for IT installation program automatically configure the database, you must configure a database manually prior to the installation of Asset Management for IT.

If you do not choose to automate the database configuration and you have not manually configured the database prior to selecting Do not automate database configuration from within the Asset Management for IT installation program, the installation will verify that you have not completed these pre-install tasks and you will receive errors. Complete these manual tasks prior to restarting the Asset Management for IT installation program.

13. From the Remote Access Authorization panel, enter authorization information for the automatic database configuration feature, and then click **Next**.

User ID
Enter a valid user ID that gives the Asset Management for IT installation program access to the system that is hosting the database to be used with Asset Management for IT.

This user ID must have administrative rights on the computer you are accessing.

If you are using DB2 for the Maximo database, you need to be a member of the:

- **Windows** Windows: DB2ADMNS group, or the
- **UNIX** UNIX: db2grp1 group.

Password
Enter the password for the user ID.

Refer to Asset Management for IT for details about how to ensure successful remote access between the Asset Management for IT installation program and the remote server.

14. From the Database Administration panel, enter configuration information on the database, and then click **Next**.

DB2

Installation directory (*db2_install_dir*)

Enter the directory where DB2 is installed.

Windows **Windows**

This value might be C:\Program Files\IBM\SQLLIB.

Linux **Linux**

This value might be /opt/IBM/db2/V9.5.

AIX **AIX**

This value might be /opt/IBM/db2/V9.5.

Instance administrator user ID

Enter the administrator user ID for the DB2 instance.

Windows **Windows**

This value might be db2admin.

Linux **Linux**

This value might be ctginst1.

AIX **AIX:**

This value might be ctginst1.

This user ID cannot be the same one as is as the database user ID.

Instance administrator password

Enter the password for the DB2 instance administrator user ID.

Windows **Windows service user ID**

Enter the user ID used to start the DB2 service. The default is db2admin. This user ID must have administrative authority on the system.

Windows **Windows service password**

Enter the password for the user ID used to start the DB2 service.

Oracle

Installation directory (*oracle_install_dir*)

Enter the directory where Oracle is installed.

Windows **Windows**

This value might be C:\oracle\product\10.2.0\oradata.

Linux **Linux**

This value might be /opt/app/oracle/product/10.2.0/oradata.

AIX **AIX**

This value might be /opt/app/oracle/product/10.2.0/oradata.

Solaris **Sun Solaris**

This value might be /opt/app/oracle/product/10.2.0/oradata.

Administrator User ID

Enter the administrator user ID for Oracle. For all platforms, the default is `issys`.

Administrator Password

Enter the password for the administrator user ID for Oracle.

Oracle Software Owner ID

Enter the user ID of the user that was used to install Oracle. For all platforms, the default is `oracle`.

Oracle Owner Password

Enter the password for the user ID of the user that was used to install Oracle.

SQL Server**SQL Server administrator**

Enter the administrator user ID for Microsoft SQL Server. Default is `sa`.

SQL Server administrator password

Enter the password for the administrator user ID for SQL Server.

Data file name

Enter the name of the SQL Server data file. Default value is `maxdb71_dat`.

Data file initial size

Select the initial size of the SQL Server data file. Default is set to Medium (1000 MB).

Log file name

Enter the name for the SQL Server log file. Default is `maxdb71_log`.

15. From the Database Tablespace panel, enter information on the table space of the database, and then click **Next**.

DB2**Data tablespace name**

Enter the name of the table space that will be created in DB2 for Maximo.

For all platforms, the default is `MAXDATA`.

If the table space does not exist, it is created.

Data tablespace size

Enter a size for the table space by selecting one of the following values:

- *small* (3000Mb)
Select this size if supporting between 1-20 users
- *medium* (5000Mb)
Select this size if supporting between 20-100 users
- *large* (8000Mb)
Select this size if supporting 100+ users

Table space size is measured in Mb.

Temporary tablespace name

Enter the name for the temporary table space to be created for DB2.

Temporary table spaces hold data during sorting or collating actions.

For all platforms, the default is MAXTEMP.

If the table space does not exist, it is created.

Temporary tablespace size

Enter a size for the temporary table space.

Temporary table space size is measured in Mb.

This value must be set to 1000Mb.

Oracle

Instance Location

Enter the path where the database instance is loaded.

Windows Windows

This value might be C:\oracle\product\10.2.0\oradata\db.

Linux Linux

This value might be /opt/app/oracle/product/10.2.0/oradata.

AIX AIX

This value might be /opt/app/oracle/product/10.2.0/oradata.

Solaris Sun Solaris

This value might be /opt/app/oracle/product/10.2.0/oradata.

tablespace name

Enter the name of the table space that is created in Oracle for Maximo.

For all platforms, the default is maxdata.

tablespace Size

Enter a size for the table space by selecting one of the following values:

- *small* (500Mb)
Select this size if supporting between 1-2 users
- *medium* (1000Mb)
Select this size if supporting between 20-100 users
- *large* (5000Mb)
Select this size if supporting 100+ users

Table space size is measured in Mb.

Temporary tablespace name

Enter the name for the temporary table space to be created for Oracle.

Temporary table spaces hold data during sorting or collating actions.

For all platforms, the default is maxtemp.

Temporary tablespace size

Enter a size for the temporary table space, which will be used for sort operations.

Temporary table space size is measured in Mb.

For all platforms, the default is 100Mb.

Index tablespace name

For all platforms, the default is MAXDATA.

Index tablespace size

For all platforms, the default is 3000Mb.

The Asset Management for IT installation program now connects to the database server and validate all of the information you have entered.

16. From the Application Server Type panel, select **IBM WebSphere Application Server**.
17. From the WebSphere Connectivity panel, enter host information on the WebSphere Application Server, and then click **Next**.

Host name

Enter the fully qualified host name of the system hosting WebSphere Application Server.

Alternatively, you can provide the IP address for the system.

SOAP port

Enter the SOAP port of the WebSphere Application Server system.

The default value for this field is 8879.

18. From the Automate WebSphere Remote Configuration panel, select whether you would like to automate the WebSphere Application Server configuration, and then click **Next**.

Automate WebSphere Configuration

This option is recommended. Ensure you have a remote access protocol enabled.

Windows

Windows :

The SSH or SMB protocol is required.

UNIX

UNIX :

The SSH or rsh REXEC protocol is required.

Do not automate WebSphere configuration

If you choose this option, you need to configure WebSphere Application Server manually before you start to install Asset Management for IT.

19. From the WebSphere Remote Access Authorization panel, enter authorization information for WebSphere Application Server configuration, and then click **Next**.

Operating system user ID

Enter a valid user ID that gives the Asset Management for IT installation program access to the system that is hosting WebSphere Application Server.

This user ID must have administrative rights on the computer you are accessing.

Operating system password

Enter the password for the system user ID.

20. From the Automate WebSphere Configuration panel, select **Automate WebSphere configuration**, and then click **Next**.

This allows the Asset Management for IT installation program to configure WebSphere Application Server automatically for use by Asset Management for IT.

If you choose not to have the Asset Management for IT installation program automatically configure WebSphere Application Server, you will have to configure WebSphere Application Server manually prior to the installation of Asset Management for IT. Configuration tasks include creating a profile, running WebSphere Application Server as a Windows service, copying WebSphere Application Server keystore file from the computer where WebSphere Application Server is installed to the administrative workstation, setting up JMS queues, and so on. For more information, see “Manually configuring the J2EE server” on page 127.

21. From the WebSphere Deployment Manager Configuration panel, enter values for the following fields, and then click **Next**.

WebSphere installation directory (*was_install_dir*)

Enter the directory where WebSphere Application Server is installed on the host system.

Windows

Windows :

This value might be C:\Program Files\IBM\WebSphere\AppServer.

Linux

Linux :

This value might be /opt/IBM/WebSphere/AppServer.

AIX

AIX :

This value might be /usr/IBM/WebSphere/AppServer

Solaris

Sun Solaris:

This value might be /opt/IBM/WebSphere/AppServer.

User ID

Enter the administrative user ID used to access the WebSphere Application Server server.

Default for all platforms is wasadmin.

Password

Enter the password for the administrative user ID used to access the WebSphere Application Server server.

Profile name

Enter the name of the WebSphere Application Server profile.

Default for all platforms is ctgDmgr01.

22. From the WebSphere Application Server Configuration panel, enter the following information, and then click **Next**.

Web server port

Enter the Web server port used by WebSphere Application Server. Default for all platforms is *80*.

Web server name

Enter the name of the Web server. Default for all platforms is *webserver1*.

Node name

Enter the name of the WebSphere Application Server node containing the application server. Default for all platforms is *ctgNode01*.

Cluster name

Enter the name of the WebSphere Application Server cluster containing the application server. Default for all platforms is *MAXIMOCLUSTER*. The cluster name is optional. The cluster and application server will be created if they do not exist.

Application server

Enter the name of the application server. Default for all platforms is *MXServer*.

23. From the Security panel, indicate whether application server security should be enabled automatically, and then click **Next**. If you do not want the WebSphere Application Server security, you might use Maximo security for authentication and authorization.
24. From the Integration Adapter JMS Configuration panel, enter the following information, and then click **Next**.

JMS DataSource name

A JMS server requires a DB2 data repository to be configured to maintain messages. Enter the name of the database to be used by JMS. Default is *intjmsds*.

Select whether the JMS datastore should be persisted.**Persist JMS messages**

Select this option if you want the Asset Management for IT installation program to set the JMS implementation to persist messages.

Do not persist JMS messages

Select this option if you do not want the Asset Management for IT installation program to set the JMS implementation to persist messages automatically. A database will not be used to persist messages. If you later decide that you would like to persist JMS messages, you will have to configure the JMS implementation manually.

Attention: The next several steps of Asset Management for IT installation procedure assume you do not allow Asset Management for IT installation program to configure the JMS implementation to persist messages.

25. From the WebSphere Keystore File panel, enter the location of the keystore file, and then click **Next**.

Attention: This step is only required if you selected **Do not Automate** in Step 18 on page 70.

Note: If you install Asset Management for IT on a remote computer, make sure you copied keystore file from the computer where WebSphere

Application Server is installed. The keystore name is trust.p12 and it will be kept in the *was_install_dir/profiles/your_profile/etc* directory.

26. From the SMTP Configuration panel, enter the **SMTP server** and **Administrator e-mail** . Click **Next**.

SMTP server

Enter the mail server configured to work with Asset Management for IT. This server will be used to send workflow and process notifications. This field is optional.

Administrator e-mail

Enter the e-mail address of the person assigned to the role of Asset Management for IT Administrator. This field is optional.

27. In the Run Configuration Step window, choose whether to perform configuration steps at this point, or to defer them until later, manual configuration.

The configuration values that you enter are stored in the *maximo_install_dir\applications\maximo\properties\maximo.properties* file. You can execute the configuration steps outside of the Asset Management for IT installation program by using the taskrunner utility, located in the *tamit_install_dir\scripts* directory. Simply run the taskrunner utility from the command line, and it will use the configuration values stored in the *maximo.properties* file to configure Asset Management for IT.

tamit_install_dir\scripts\taskrunner

If there is an installation failure, the taskrunner utility can be run again after the error conditions have been rectified. The taskrunner utility will resume the install at the point where the last successfully completed task was recorded in the previous attempt.

The configuration includes:

- database configuration
- application server configuration
- process managers installation

You are also prompted to mark one of these options:

Deploy application files automatically

Mark this radio button if you choose to deploy enterprise archive (EAR) files during this installation.

Deploy applications files manually later

Mark this radio button if you choose to deploy enterprise archive (EAR) files during after the installation completes. For performance reasons, you might want to deploy EAR files later manually.

28. From the Choose Shortcut Folder panel, select the type of shortcut you would like to arrange for Asset Management for IT, and then click **Next**.

In a new Program Group

Select this option and enter the name of a new program group if you would like to create Asset Management for IT shortcuts in a new program group.

In an existing Program Group

Select this option and choose the name of an existing program group to store Asset Management for IT shortcuts.

In the Start Menu

Select this option to create shortcuts for Asset Management for IT in the Start menu.

In order to use the Start Menu shortcut with Microsoft Internet Explorer, ensure that you have added the Asset Management for IT URL to the trusted sites Web content zone and disable the option of requiring server verification for all sites in the zone.

On the Desktop

Select this option to create shortcuts for Asset Management for IT on the desktop.

In the Quick Launch Bar

Do not select this option. Selecting this option does not create a shortcut in the Quick Launch bar.

Other Select this option and use the **Choose...** button to select another location to create Asset Management for IT shortcuts.

Don't create icons

Select this option if you do not want any Asset Management for IT shortcuts created.

Create Icons for All Users

Select this option if you would like Asset Management for IT desktop icons to appear on the desktop for all system users.

29. From the Input Summary panel, review the information you have provided to the Asset Management for IT installation program, and then click **Next**.
Use the **Previous** button to return to previous panels to change anything.
30. From the Pre-Installation Summary panel, review the installation information presented, and then click **Install**. The installation now begins. Progress can be monitored by viewing messages displayed above the progress bar.
31. From the Install Complete panel, click **Done**.
32. From the DB2 Database Server Configuration panel, enter the following information, and then click **Next**:

Note: The JMS data store can only be created as a DB2 database.

Host name

Enter the fully qualified host name of the server hosting the JMS data store.

Port Enter the port used to access the database server. Default for all platforms is *50005*.

Database name

Enter the name of the database serving as the JMS data store.

Default for all platforms is `maxsibdb`.

User ID

Enter the user ID used to access the database server.

Default for all platforms is the database user ID you entered when you selected your database type. If the user does not exist, it will be created for you.

Password

Enter the password for the User ID used to access the database server.

33. From the DB2 Database Server Remote Access Authorization panel, enter authorization information for the automatic configuration feature, and then click **Next**:

User ID

Enter a valid user ID that will allow the Asset Management for IT installation program to access the system that is hosting the JMS database. This user ID should have administrative rights on the computer you are accessing.

Windows **Windows :**

This user must be a member of the DB2ADMNS group.

Windows **UNIX :**

This user must be a member of the db2grp1 group.

Password

Enter the password for the user ID.

34. From the DB2 Database Instance Configuration panel, enter the following information, and then click **Next**.

Installation directory

Enter the installation directory for the DB2 server that is hosting the JMS database that contains the instance to be used with WebSphere Application Server.

Windows **Windows :**

This value might be C:\Program Files\IBM\SQLLIB.

Linux **Linux**

This value might be /opt/IBM/db2/V9.5.

Instance

Enter the JMS database instance to be used with WebSphere Application Server.

For all platforms, the default is ctginst1.

Instance administrator user ID

Enter the administrator's user ID for the JMS database instance.

Windows **Windows**

This value might be db2admin.

Linux **Linux**

This value might be ctginst1.

Instance administrator password

Enter the password for the JMS database instance administrator's user ID.

35. From the Maximo panel, enter the following configuration information, and then click **Next**.

Installation directory

Select the folder where Maximo application will be installed. C:\IBM\maximo is the default value. The path you specify must not contain spaces.

SMTP server

Enter the mail server configured to work with Asset Management for IT. This server will be used to send workflow and process notifications. This field is optional.

Workflow administrator e-mail

Enter the e-mail address of the person assigned to the role of Asset Management for IT Workflow Administrator. This address will be used for workflow notifications. This field is optional.

Administrator e-mail

Enter the e-mail address of the person assigned to the role of Asset Management for IT Administrator. This field is optional.

If you choose to not configure optional properties at this time, you can configure them in the Asset Management for IT user interface using the System Properties application. The relevant properties are:

- **mail.smtp.host**
- **mxe.workflow.admin**
- **mxe.adminEmail**

What to do next

Once the Tivoli Asset Management for IT installation program has completed installation and configuration tasks, it exits. Logs can be found at *tamit_install_dir/logs*.

Chapter 5. Deploying IBM Tivoli Asset Management for IT automatically reusing existing middleware

Use this information to use IBM Tivoli Asset Management for IT installation programs and tools to automatically configure existing middleware within your enterprise during the Asset Management for IT deployment process.

Before you begin

Ensure you have reviewed the following information:

- Chapter 2, “Planning to deploy IBM Tivoli Asset Management for IT,” on page 7
- Chapter 3, “Preparing to install IBM Tivoli Asset Management for IT,” on page 23

About this task

This information provides a high-level overview or road map of tasks you need to complete in order to deploy Asset Management for IT automatically, using middleware already established in your enterprise.

Related concepts

“Reusing existing middleware components” on page 15

You can reuse some existing middleware installations as Tivoli Asset Management for IT components. If you plan to do so, ensure that they are at the level supported by Asset Management for IT. The middleware and Asset Management for IT installation programs do not provide a mechanism for patching unsupported servers, nor do these programs provide remote prerequisite checks to ensure they are at the right level.

Reusing middleware

If you intend to reuse existing middleware servers with the Asset Management for IT instance, they must be configured before running the Asset Management for IT installation program. This section contains information about configuring existing DB2 and IBM Tivoli Directory Server servers for use with Asset Management for IT using the middleware installer.

You cannot use the middleware installer to configure existing Oracle, Microsoft SQL Server, or Microsoft Active Directory servers. Refer to Chapter 6, “Installing IBM Tivoli Asset Management for IT with manual middleware configuration,” on page 101 for more information about those servers. Information found in this section also applies if you decide that you want to reuse existing middleware servers, but you want to configure them to work with Asset Management for IT manually instead of allowing the Asset Management for IT installation program to configure them.

Ensure that all of your middleware is at the level described in “Hardware and software requirements” on page 2.

Reusing IBM DB2

If you have an existing IBM DB2 installation that you would like to reuse for IBM Tivoli Asset Management for IT, run the Tivoli middleware installer on the system.

The middleware installer will identify instances of middleware that already exist on the system that are compatible with Asset Management for IT, and it will configure the existing instance for use with Asset Management for IT.



About this task

To have the middleware installer configure an existing database instance for reuse with Asset Management for IT, complete the following steps:





1. Log in as a user with administrative authority.
2. Launch the middleware installer from the Launchpad.
3. Proceed through the middleware installer panels as instructed in “Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer” on page 38, until you reach the Deployment Choices panel.
4. From the Deployment Choices panel, select **Database Server**, and then click **Next**. The middleware installer will display any instances of DB2 found on the system.
5. From the Installation drop-down menu, select the appropriate instance to reuse, and then click **Next**.
6. Complete the installation by proceeding through the remainder of the middleware installer panels.

Note: If you are reusing an existing DB2 server with Asset Management for IT, the following users and groups must already exist on the system:

Users

- db2admin
-  dasusr1
-  db2fenc1

Groups

-  db2admns
-  dasadm1
-  dbgrp1
-  db2fgrp1

If these users do not exist on the system, you will have to create them prior to running the Asset Management for IT installation program.

Reusing Oracle

If you have an existing Oracle 10g instance that you would like to reuse for Asset Management for IT, configure it manually.

About this task

Refer to

- “Manually configuring Oracle 11g” on page 110
- “Manually configuring Oracle 10g” on page 112 for information.
- For an existing Oracle 9.2 instance, refer to “Manually configuring Oracle9i Rel2” on page 114

Reusing IBM Tivoli Directory Server

If you have an existing IBM Tivoli Directory Server installation that you would like to reuse for Tivoli Asset Management for IT, run the Tivoli middleware installer on the system. The middleware installer will identify middleware that already exists on the system that is compatible with Asset Management for IT, and it will configure it for use with Asset Management for IT.

Before you begin

The middleware installer will create a new instance on the existing Directory Server that you identify. This new instance will contain default Asset Management for IT LDAP information. If you intend to use Asset Management for IT with an existing Directory Server instance that contains your organization's LDAP information, do not run the middleware installer to configure the existing Directory Server.

About this task

To have the middleware installer configure an existing Directory Server instance for reuse with Asset Management for IT, complete the following steps:

1. Log in as a user with administrative authority.
2. Launch the middleware installer from the Launchpad.
3. Proceed through the middleware installer panels as instructed in "Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer" on page 38, until you reach the Deployment Choices panel.
4. From the Deployment Choices panel, select **Directory Server**, and then click **Next**. The middleware installer will display any instances of Directory Server found on the system.
5. From the Installation drop-down menu, select the appropriate instance to reuse, and then click **Next**.
6. Complete the installation by proceeding through the remainder of the middleware installer panels. Refer to "Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer" on page 38 for more information.

Reusing Microsoft Active Directory

Windows If you have an existing Microsoft Active Directory instance, you can use it to secure WebSphere when you install it on the system. The middleware installer will prompt you for LDAP configuration parameters to use with WebSphere.

About this task

To have the middleware installer configure an existing Active Directory instance to secure WebSphere, complete the following steps:

1. Login as a user with administrative authority.
2. Launch the middleware installer from the Launchpad.
3. Proceed through the middleware installer panels as instructed in "Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer" on page 38, until you reach the Deployment Choices panel.

4. From the Deployment Choices panel, deselect the **Directory Server deployment** option, and then click **Next**.

In the next panel, will be given the choice of selecting an existing instance of Directory Server or Active Directory to secure WebSphere.

5. Select **Secure with Active Directory**, and click **Next**.
6. Supply the following configuration values for WebSphere security, and then click **Next**:

LDAP Hostname

Enter the fully qualified name of the computer hosting Active Directory.

Directory server port

389

LDAP base entity

DC=itsm,DC=com

User suffix

OU=Users,OU=SWG,DC=itsm,DC=com

Group suffix

OU=Groups,OU=SWG,DC=itsm,DC=com

Organization container suffix

DC=itsm,DC=com

In this example, *itsm* is the domain name. You need to replace *itsm* with the name of your own domain.

7. Supply the following configuration values for WebSphere security, and then click **Next**:

Bind distinguished name

CN=Administrator,CN=Users,DC=itsm,DC=com

This value assumes that the Administrator user is already a member of the *itsm* domain.

Bind password

Enter the password for the Administrator user on the system hosting Active Directory.

In this example, *itsm* is the domain name. You need to replace *itsm* with the name of your own domain.

8. Complete the installation by proceeding through the remainder of the middleware installer panels. Refer to “Installing and configuring Tivoli Asset Management for IT middleware with the Tivoli middleware installer” on page 38 for more information.

Results

Prior to running the Asset Management for IT installation program, you need to manually create the users and groups. This step can be performed after you have installed middleware using the middleware installer, but it must be completed before you begin using the Asset Management for IT installation program.

IBM Tivoli Asset Management for IT installation program overview

The IBM Tivoli Asset Management for IT installation program provides an interface for installing and deploying Asset Management for IT. The installation program records choices you make about your Asset Management for IT deployment and configuration parameters associated with those choices, and then installs and deploys Asset Management for IT based upon the information you entered.

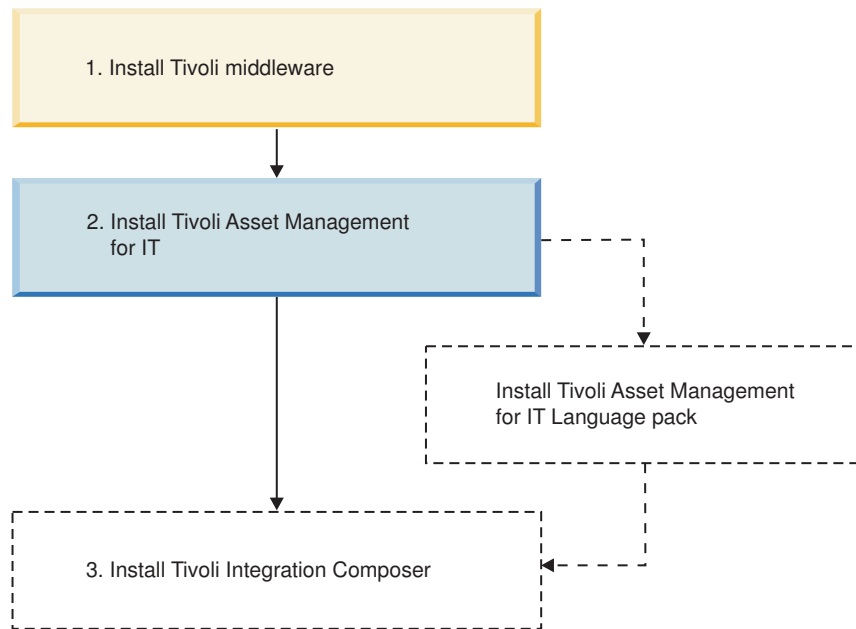


Figure 5. Tivoli Asset Management for IT installation flow - Tivoli Asset Management for IT installation.

There are two installation paths available to you when installing Asset Management for IT.

Simple

A simple deployment consists of installing all middleware on one system. You will not have the option of using existing middleware within your organization with Asset Management for IT. All middleware used with Asset Management for IT must have been installed on the system using the middleware installer using default values. Asset Management for IT will be installed using default values provided by the middleware and Asset Management for IT installation programs.

For a list of values being set when using this option, refer to “Tivoli Asset Management for IT simple install path values” on page 58. If you intend to override default values used by the simple deployment path, you will have to use the custom deployment path instead.

Note: On choosing a simple deployment, you might encounter this error message:

CTGIN2375E: J2EE application security non enabled in J2EE application server

Make sure you have the WebSphere Application Server security switched on. Refer to the WebSphere Application Server Information Center for instructions.

<http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp>.

Custom

A custom deployment typically involves deploying Asset Management for IT across several systems, some of which probably already host middleware products that you wish to use with your Asset Management for IT deployment. Deploying through the custom installation path also allows you to modify default installation values.

This deployment option does not require you to spread the Asset Management for IT deployment across several systems. You can enter the name of the local host as the destination for all Asset Management for IT components that are to be installed using the middleware installer and the Asset Management for IT installation program.

The Asset Management for IT installation program can automate the configuration of middleware for use with Asset Management for IT. If you choose not to have the Asset Management for IT installation program automatically configure middleware, configure that piece of middleware manually prior to the installation of Asset Management for IT.

Important: While you can deploy Asset Management for IT in a distributed environment consisting of predominately UNIX systems, the Asset Management for IT installation program must be run from a Windows system.

Important: When entering LDAP values for Asset Management for IT installation panel fields, entries in LDIF files, or values you enter directly into a directory instance using the directory server tools, be aware of the product-specific syntax rules for using special characters in an LDAP string. In most cases, in order to make them readable by the directory server, special characters must be preceded by an escape character. Failing to escape special characters contained in an LDAP string used with Asset Management for IT result in Asset Management for IT errors.

Many directory server products consider a blank space as a special character that is part of the LDAP string. Therefore, if you mistakenly enter an LDAP string that contains a blank, at the end of a field value, for example, and you do not precede the blank character with an escape character, you will encounter Asset Management for IT errors that are difficult to troubleshoot.

Refer to the product documentation for your directory server for more information on special characters in LDAP strings.

Information that you input into the Asset Management for IT installation program is stored in the `maximo.properties` file and the Maximo database. These values are populated into the panel fields of the Asset Management for IT installation program on subsequent uses of the program. Therefore, if you cancel the installation program after entering values across several installation panels, the installation program will recall the values the next time you start up the Asset Management for IT installation program (except for the Asset Management for IT install directory and the shortcut option chosen). You can restore the default values in the Asset Management for IT installation program by deleting `tamit_install_dir/maximo/applications/maximo/properties/maximo.properties`.

Tivoli Asset Management for IT simple install path values

If you choose to install Tivoli Asset Management for IT using the *simple* install path, the values listed in this section are set. You will be able to provide values where indicated.

Table 13. Tivoli Asset Management for IT Simple Install Path Values

Category	Field	Value	Provided by User?	
Deployment Option	Deployment	Simple		
Database Configuration	Database Type	DB2		
	Host name		Yes	
	Port	50005		
	Database Name	maxdb71		
	Instance	ctginst1		
	User ID		Yes	
	Automate Database Configuration	yes		
	Remote Access User ID		Yes	
	Database Install Directory			
		Windows		
	Windows	C:\Program Files\IBM\SQLLIB		
	UNIX			
	UNIX	/opt/IBM/db2/V9.5		
Instance Administrator User ID			Yes	
	Windows			
	Windows	db2admin		
	UNIX			
	UNIX	ctginst1		
Windows Service User ID	db2admin			
Data table space name	maxdata			
Data table space size (Mb)	5000			
Temporary table space name	MAXTEMP			
Temporary table space size (Mb)	1000			
Index table space name	MAXDATA			
Index table space size (Mb)	3000			
WebSphere Deployment Manager Configuration	Host name		Yes	
	SOAP Port	8879		
	WebSphere installation directory (<i>was_install_dir</i>)			
		Windows		
		Windows	C:\Program Files\IBM\WebSphere\AppServer	
		Linux		
		Linux	/opt/IBM/WebSphere/AppServer	
		AIX		
		AIX	/usr/IBM/WebSphere/AppServer	
		Solaris		
	Sun Solaris	/opt/IBM/WebSphere/AppServer		
User ID	wasadmin		Yes	
Profile name	ctgDmgr01			
Automate WebSphere Configuration	yes			
Remote Access User ID			Yes	
WebSphere Application Server configuration	Web server port	80		
	Web server name	webserv1		
	Node name	ctgNode01		
	Cluster name	MAXIMOCLUSTER		
	Application server	MXServer Note: This value cannot be changed.		

Table 13. Tivoli Asset Management for IT Simple Install Path Values (continued)

Category	Field	Value	Provided by User?
Integration Adapter JMS Configuration	JMS DataSource name	intjmsds	
	Persist JMS messages	no	
Security Server Configuration	Configure J2EE Server application security	yes	
	Use WebSphere application security for authentication and authorization	yes	
	User base entry	ou=users,ou=SWG,o=IBM,c=US	
	Group base entry	ou=groups,ou=SWG,o=IBM,c=US	
	Create the required users	yes	
Maximo Configuration	Install directory	C:\IBM\SMP	Yes
Configuration Step	Perform installation configuration now	yes	

Performing IBM Tivoli Asset Management for IT installation

In addition to configuring new instances of IBM Tivoli Asset Management for IT middleware products installed by the middleware installer, the Asset Management for IT installation program can configure existing instances of prerequisite products, including those from other vendors, that you want to use with Asset Management for IT. The instructions provided are for a *multiple computer* installation using default values and assume that you choose to have the Asset Management for IT installation program automatically configure middleware across multiple computers to work with Asset Management for IT.

Before you begin

If you do not allow the Asset Management for IT installation program to configure middleware automatically, it still performs programmatic checks to verify that the documented manual steps were performed properly. If any errors are encountered, a dialog box detailing the error appear. You will not be permitted to continue in the Asset Management for IT installation task until the errors are resolved.

Attention: Windows The Asset Management for IT installation program can only be run from a Windows-based system.

Before you begin, ensure you have addressed the following prerequisite conditions:

Table 14. Asset Management for IT installation prerequisite conditions.

Operating system or database management system	Requirements
Linux	Ensure that the command <code>hostname -f</code> returns a fully qualified host name. If it does not, consult the appropriate documentation for your operating system to ensure that the <code>hostname</code> command returns a fully qualified host name.

Table 14. Asset Management for IT installation prerequisite conditions. (continued)

Operating system or database management system	Requirements
	<p data-bbox="857 275 1446 327">If the remote system is a Windows computer, configure RXA to work over SMB.</p> <p data-bbox="857 352 1455 457">If you are using DB2 with Asset Management for IT, and you want to use the fully automated database configuration capabilities of the Asset Management for IT installation program, ensure that the following conditions are met:</p> <ul data-bbox="857 464 1463 863" style="list-style-type: none"> <li data-bbox="857 464 1463 596">• The user ID specified as the Instance administrator user ID that you enter on the DB2 Administration panel of the Asset Management for IT installation program must have DB2 administration authority, which is referred to as SYSADM authority in the DB2 product documentation. <li data-bbox="857 602 1463 842">• The user ID specified on the Remote Access Authorization panel of the Asset Management for IT installation program must have DB2 administration authority. It is used to create the DB2 instance, database, and schema. It must have SYSADM authority, as defined by DB2. This requires the ID to be a member of the group defined by the sysadm_group configuration parameter for the DB2 instance you plan to use. For example, on Windows, the user must belong to the DB2ADMNS group. <li data-bbox="857 848 867 863">• <p data-bbox="883 884 992 909">Windows</p> <p data-bbox="883 930 1455 1062">If you are using Microsoft Active Directory to secure WebSphere Application Server, ensure the users and groups listed in “Manually configuring Microsoft Active Directory” on page 121 have been manually created in the Microsoft Active Directory instance.</p> <p data-bbox="857 1083 1451 1136">For more information on creating DB2 users, refer to the IBM DB2 product documentation:</p> <p data-bbox="456 1167 565 1192">Windows</p> <p data-bbox="857 1161 1414 1213">http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp</p>

Table 14. Asset Management for IT installation prerequisite conditions. (continued)

Operating system or database management system	Requirements
	<p>If you are using DB2 with Asset Management for IT, and you want to use the fully automated database configuration capabilities of the Asset Management for IT installation program, ensure that the following conditions are met:</p> <ul style="list-style-type: none"> • For DB2 UNIX installations, create the instance user on the DB2 server before starting the Asset Management for IT installation program. For example if you plan to create the Maximo database in a DB2 instance (ctginst1 is recommended), create a user (including the home directory for the user) on the UNIX DB2 server prior to starting the install. • The user ID specified as the Instance administrator user ID that you enter on the DB2 Administration panel of the Asset Management for IT installation program must have DB2 administration authority, which is referred to as SYSADM authority in the DB2 product documentation. • The user ID specified on the Remote Access Authorization panel of the Asset Management for IT installation program must have DB2 administration authority. It is used to create the DB2 instance, database, and schema. It must have SYSADM authority, as defined by DB2. This requires the ID to be a member of the group defined by the sysadm_group configuration parameter for the DB2 instance you plan to use. • The fenced user must be db2fenc1. • Add root to the DB2GRP1 group prior to starting the Asset Management for IT installation program. <p>For more information on creating DB2 users, refer to the IBM DB2 product documentation:</p> <p>http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp</p>
UNIX	
AIX	<p>Default installations of AIX systems might not include a suitable protocol and must have RXA compatible protocols enabled.</p> <p>If you plan to take advantage of the Asset Management for IT installation program feature that automates the configuration of Asset Management for IT middleware, enable a Remote Execution and Access (RXA) service for each system on which you intend to install the middleware. RXA requires that the target system enable at least one of the protocols supported by RXA, which includes rsh, REXEC, SSH, and Windows SMB. Before you start the Asset Management for IT installation program, ensure that one of these protocols is running and accepting remote logins using a user name and password configured on the target computer.</p>
	<p>The middleware environment is installed and running properly.</p>
	<p>Avoid using localhost for host name values in the install program. Specify the actual fully qualified host name of the system for all host name values.</p>
All DB2 installations	<p>You might encounter ever increasing system memory usage linked with DB2. If you experience this behavior, set the following DB2 property and then restart the DB2 server:</p> <pre>db2 update dbm cfg using KEEPFCENCED NO</pre>
Oracle installations	<p>Ensure that Oracle 9i, 10g or 11g are installed (see "Hardware and software requirements" on page 2 for comparison).</p>

Table 14. Asset Management for IT installation prerequisite conditions. (continued)

Operating system or database management system	Requirements
Microsoft SQL Server installations	<p>Ensure:</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2008 is installed. • Asset Management for IT uses port 1433 when configured with SQL Server. By default, this port is not enabled. Enable this port. Refer to http://msdn.microsoft.com/en-us/library/ms177440.aspx for instructions.

For WebSphere Application Server Network Deployment, ensure that the Cell and all related nodes are actively running.

About this task

To install Asset Management for IT, follow these steps:

1. Log in as Administrator on the Asset Management for IT administrative system.
2. Launch the Asset Management for IT installation program from the Launchpad:
 - a. Start the Launchpad: On the DVD titled "Tivoli Asset Management for IT 7.2", navigate to the root directory of the product disk or the downloaded installation image, and run the following command: `launchpad.exe`.
 - b. In the launchpad navigation pane, click **Install the Product**.
 - c. Click **Tivoli Asset Management for IT**.
3. Select a language for the installation and click **OK**.
4. From the Introduction panel, click **Next**. The Pre-installation Progress window is displayed.

Note: This is the moment the installer analyzes whether to install or upgrade the IBM Autonomic Computing Deployment Engine and detects the existing instances.

5. In the Package Summary window, there are **Packages Analyzed** displayed and their status. When installing for the first time, the status **Not installed** shows up. If there were any other Asset Management for IT instances detected, they would be marked **Installed** along with their version.
6. From the License Agreement panel, choose the **I accept both the IBM and non-IBM terms**, if you agree with them, and then click **Next**.
7. From the Choose Install Folder panel, specify the directory you use to install Asset Management for IT, and then click **Next**.

Where Would You Like to Install?

Enter the path to install Asset Management for IT.

By default, this value is `C:\IBM\SMP`.

The path you specify must not contain spaces.

8. From the Choose Deployment panel, select the **Custom** deployment topology, and then click **Next**.

Simple

Select **Simple** if you want to deploy all Asset Management for IT components on a single system. This deployment option is typically

only used for demonstration, proof-of-concept, or training purposes. The default values are displayed in Table 11 on page 58.

Custom

Select custom if you want to deploy Asset Management for IT components across several systems. This deployment option is typically used in a production environment. This option is recommended.

As a result, the Asset Management for IT configuration for your system processing window is displayed.

9. From the Import Middleware Configuration Information panel, specify that you want to use field values you input into the middleware installer as default values for those same fields in the Asset Management for IT installation program.

Import Middleware Configuration Information

Select this check box if you want to allow the Asset Management for IT installation program to reuse values entered for DB2 in the middleware installer.

Note that if you select this feature while installing Asset Management for IT by way of RXA, the **Workspace Location** that you specify cannot be located on a networked drive of the remote system. It must reside locally on the remote system.

The middleware default information will not be used if you select the Simple deployment path.

Host name

Enter the fully qualified host name of the system where the middleware installer was run.

User ID

Enter the User ID that was used to run the middleware installer.

Password

Enter the password of the User ID that was used to run the middleware installer.

Workspace Location

Enter the location of the topology file that contains the values entered for the middleware installer. This file is found in the workspace that was defined during the Asset Management for IT middleware installation task. For example, C:\ibm\tivoli\mwi\workspace.

10. From the Maximo Database Type panel, select the product that you use for the Maximo database, and then click **Next**.

DB2 Select this choice to use DB2 as the Maximo database.

Oracle Select this choice to use Oracle as the Maximo database.

SQL Server

Select this choice to use Microsoft SQL Server 2008 as the Maximo database.

Each database will have its own unique set of configurable parameters and values.

11. From the Maximo Database panel, enter configuration information on the database, and then click **Next**.

DB2

Host name

Enter the host name of the computer hosting DB2.

The host name must be fully qualified.

Port Enter the port being used by DB2 instance.

The default is *50005*.

Database name

Enter the name of the database to use with Maximo.

The default database name is *maxdb71*. The database is created if it does not exist.

Instance

Enter the name of the database instance to be used with Maximo.

The default instance name is *ctginst1*. This instance is created if it does not exist, however, the user and its associated home directory must exist on the DB2 server.

Database user ID

Enter the user ID used for Maximo to access DB2.

Default for all platforms is *maximo*.

This user ID is created if it does not exist.

This user ID cannot be the same one used as the instance administrator user ID.

Database password

Enter the password for the user ID used to access DB2.

Oracle**Host name**

Enter the host name of the computer hosting Oracle.

The host name must be fully qualified.

Port Enter the port being used by Oracle.

The default is *1521*.

Instance

Enter the name of the database instance to be used with Maximo.

The default instance name is *ctginst1*.

Database user ID

Enter the user ID used for Maximo to access Oracle.

Default for all platforms is *maximo*.

This user ID is created if it does not exist.

Database password

Enter the password for the user ID used to access Oracle.

SQL Server**Host name**

Enter the host name of the computer hosting SQL Server.

The host name must be fully qualified.

Port Enter the port being used by SQL Server.
The default is 1433.

Database Name
Enter the name of the database to use with Maximo.
The default database name is maxdb71.

Database user ID
Enter the user ID used to access SQL Server.
Default for all platforms is maximo.
This user ID is created if it does not exist.

Database password
Enter the password for the user ID used to access SQL Server.

12. From the Automate Database Configuration panel, select **Automate database configuration**, and then click **Next**.

This step allows the Asset Management for IT installation program to configure the database automatically for use by Asset Management for IT. Examples of automated tasks include creating table spaces, creating database tables, creating database schemas, creating users, and so on.

If you choose not to have the Asset Management for IT installation program automatically configure the database, you must configure a database manually prior to the installation of Asset Management for IT.

If you do not choose to automate the database configuration and you have not manually configured the database prior to selecting Do not automate database configuration from within the Asset Management for IT installation program, the installation will verify that you have not completed these pre-install tasks and you will receive errors. Complete these manual tasks prior to restarting the Asset Management for IT installation program.

13. From the Remote Access Authorization panel, enter authorization information for the automatic database configuration feature, and then click **Next**.

User ID
Enter a valid user ID that gives the Asset Management for IT installation program access to the system that is hosting the database to be used with Asset Management for IT.

This user ID must have administrative rights on the computer you are accessing.

If you are using DB2 for the Maximo database, you need to be a member of the:

- **Windows** Windows: DB2ADMNS group, or the
- **UNIX** UNIX: db2grp1 group.

Password
Enter the password for the user ID.

Refer to Asset Management for IT for details about how to ensure successful remote access between the Asset Management for IT installation program and the remote server.

14. From the Database Administration panel, enter configuration information on the database, and then click **Next**.

DB2

Installation directory (*db2_install_dir*)

Enter the directory where DB2 is installed.

Windows **Windows**

This value might be C:\Program Files\IBM\SQLLIB.

Linux **Linux**

This value might be /opt/IBM/db2/V9.5.

AIX **AIX**

This value might be /opt/IBM/db2/V9.5.

Instance administrator user ID

Enter the administrator user ID for the DB2 instance.

Windows **Windows**

This value might be db2admin.

Linux **Linux**

This value might be ctginst1.

AIX **AIX:**

This value might be ctginst1.

This user ID cannot be the same one as is as the database user ID.

Instance administrator password

Enter the password for the DB2 instance administrator user ID.

Windows **Windows service user ID**

Enter the user ID used to start the DB2 service. The default is db2admin. This user ID must have administrative authority on the system.

Windows **Windows service password**

Enter the password for the user ID used to start the DB2 service.

Oracle

Installation directory (*oracle_install_dir*)

Enter the directory where Oracle is installed.

Windows **Windows**

This value might be C:\oracle\product\10.2.0\oradata.

Linux **Linux**

This value might be /opt/app/oracle/product/10.2.0/oradata.

AIX **AIX**

This value might be /opt/app/oracle/product/10.2.0/oradata.

Solaris **Sun Solaris**

This value might be /opt/app/oracle/product/10.2.0/oradata.

Administrator User ID

Enter the administrator user ID for Oracle. For all platforms, the default is `issys`.

Administrator Password

Enter the password for the administrator user ID for Oracle.

Oracle Software Owner ID

Enter the user ID of the user that was used to install Oracle. For all platforms, the default is `oracle`.

Oracle Owner Password

Enter the password for the user ID of the user that was used to install Oracle.

SQL Server**SQL Server administrator**

Enter the administrator user ID for Microsoft SQL Server. Default is `sa`.

SQL Server administrator password

Enter the password for the administrator user ID for SQL Server.

Data file name

Enter the name of the SQL Server data file. Default value is `maxdb71_dat`.

Data file initial size

Select the initial size of the SQL Server data file. Default is set to Medium (1000 MB).

Log file name

Enter the name for the SQL Server log file. Default is `maxdb71_log`.

15. From the Database Tablespace panel, enter information on the table space of the database, and then click **Next**.

DB2**Data tablespace name**

Enter the name of the table space that will be created in DB2 for Maximo.

For all platforms, the default is `MAXDATA`.

If the table space does not exist, it is created.

Data tablespace size

Enter a size for the table space by selecting one of the following values:

- *small* (3000Mb)
Select this size if supporting between 1-20 users
- *medium* (5000Mb)
Select this size if supporting between 20-100 users
- *large* (8000Mb)
Select this size if supporting 100+ users

Table space size is measured in Mb.

Temporary tablespace name

Enter the name for the temporary table space to be created for DB2.

Temporary table spaces hold data during sorting or collating actions.

For all platforms, the default is MAXTEMP.

If the table space does not exist, it is created.

Temporary tablespace size

Enter a size for the temporary table space.

Temporary table space size is measured in Mb.

This value must be set to 1000Mb.

Oracle

Instance Location

Enter the path where the database instance is loaded.

Windows Windows

This value might be C:\oracle\product\10.2.0\oradata\db.

Linux Linux

This value might be /opt/app/oracle/product/10.2.0/oradata.

AIX AIX

This value might be /opt/app/oracle/product/10.2.0/oradata.

Solaris Sun Solaris

This value might be /opt/app/oracle/product/10.2.0/oradata.

tablespace name

Enter the name of the table space that is created in Oracle for Maximo.

For all platforms, the default is maxdata.

tablespace Size

Enter a size for the table space by selecting one of the following values:

- *small* (500Mb)
Select this size if supporting between 1-2 users
- *medium* (1000Mb)
Select this size if supporting between 20-100 users
- *large* (5000Mb)
Select this size if supporting 100+ users

Table space size is measured in Mb.

Temporary tablespace name

Enter the name for the temporary table space to be created for Oracle.

Temporary table spaces hold data during sorting or collating actions.

For all platforms, the default is maxtemp.

Temporary tablespace size

Enter a size for the temporary table space, which will be used for sort operations.

Temporary table space size is measured in Mb.

For all platforms, the default is 100Mb.

Index tablespace name

For all platforms, the default is MAXDATA.

Index tablespace size

For all platforms, the default is 3000Mb.

The Asset Management for IT installation program now connects to the database server and validate all of the information you have entered.

16. From the Application Server Type panel, select **IBM WebSphere Application Server**.
17. From the WebSphere Connectivity panel, enter host information on the WebSphere Application Server, and then click **Next**.

Host name

Enter the fully qualified host name of the system hosting WebSphere Application Server.

Alternatively, you can provide the IP address for the system.

SOAP port

Enter the SOAP port of the WebSphere Application Server system.

The default value for this field is 8879.

18. From the Automate WebSphere Remote Configuration panel, select whether you would like to automate the WebSphere Application Server configuration, and then click **Next**.

Automate WebSphere Configuration

This option is recommended. Ensure you have a remote access protocol enabled.

Windows

Windows :

The SSH or SMB protocol is required.

UNIX

UNIX :

The SSH or rsh REXEC protocol is required.

Do not automate WebSphere configuration

If you choose this option, you need to configure WebSphere Application Server manually before you start to install Asset Management for IT.

19. From the WebSphere Remote Access Authorization panel, enter authorization information for WebSphere Application Server configuration, and then click **Next**.

Operating system user ID

Enter a valid user ID that gives the Asset Management for IT installation program access to the system that is hosting WebSphere Application Server.

This user ID must have administrative rights on the computer you are accessing.

Operating system password

Enter the password for the system user ID.

20. From the Automate WebSphere Configuration panel, select **Automate WebSphere configuration**, and then click **Next**.

This allows the Asset Management for IT installation program to configure WebSphere Application Server automatically for use by Asset Management for IT.

If you choose not to have the Asset Management for IT installation program automatically configure WebSphere Application Server, you will have to configure WebSphere Application Server manually prior to the installation of Asset Management for IT. Configuration tasks include creating a profile, running WebSphere Application Server as a Windows service, copying WebSphere Application Server keystore file from the computer where WebSphere Application Server is installed to the administrative workstation, setting up JMS queues, and so on. For more information, see “Manually configuring the J2EE server” on page 127.

21. From the WebSphere Deployment Manager Configuration panel, enter values for the following fields, and then click **Next**.

WebSphere installation directory (*was_install_dir*)

Enter the directory where WebSphere Application Server is installed on the host system.

Windows

Windows :

This value might be C:\Program Files\IBM\WebSphere\AppServer.

Linux

Linux :

This value might be /opt/IBM/WebSphere/AppServer.

AIX

AIX :

This value might be /usr/IBM/WebSphere/AppServer

Solaris

Sun Solaris:

This value might be /opt/IBM/WebSphere/AppServer.

User ID

Enter the administrative user ID used to access the WebSphere Application Server server.

Default for all platforms is wasadmin.

Password

Enter the password for the administrative user ID used to access the WebSphere Application Server server.

Profile name

Enter the name of the WebSphere Application Server profile.

Default for all platforms is ctgDmgr01.

22. From the WebSphere Application Server Configuration panel, enter the following information, and then click **Next**.

Web server port

Enter the Web server port used by WebSphere Application Server. Default for all platforms is *80*.

Web server name

Enter the name of the Web server. Default for all platforms is *webserver1*.

Node name

Enter the name of the WebSphere Application Server node containing the application server. Default for all platforms is *ctgNode01*.

Cluster name

Enter the name of the WebSphere Application Server cluster containing the application server. Default for all platforms is *MAXIMOCLUSTER*. The cluster name is optional. The cluster and application server will be created if they do not exist.

Application server

Enter the name of the application server. Default for all platforms is *MXServer*.

23. From the Security panel, indicate whether application server security should be enabled automatically, and then click **Next**. If you do not want the WebSphere Application Server security, you might use Maximo security for authentication and authorization.
24. From the Integration Adapter JMS Configuration panel, enter the following information, and then click **Next**.

JMS DataSource name

A JMS server requires a DB2 data repository to be configured to maintain messages. Enter the name of the database to be used by JMS. Default is *intjmsds*.

Select whether the JMS datastore should be persisted.**Persist JMS messages**

Select this option if you want the Asset Management for IT installation program to set the JMS implementation to persist messages.

Do not persist JMS messages

Select this option if you do not want the Asset Management for IT installation program to set the JMS implementation to persist messages automatically. A database will not be used to persist messages. If you later decide that you would like to persist JMS messages, you will have to configure the JMS implementation manually.

Attention: The next several steps of Asset Management for IT installation procedure assume you do not allow Asset Management for IT installation program to configure the JMS implementation to persist messages.

25. From the WebSphere Keystore File panel, enter the location of the keystore file, and then click **Next**.

Attention: This step is only required if you selected **Do not Automate** in Step 18 on page 70.

Note: If you install Asset Management for IT on a remote computer, make sure you copied keystore file from the computer where WebSphere

Application Server is installed. The keystore name is trust.p12 and it will be kept in the *was_install_dir/profiles/your_profile/etc* directory.

26. From the SMTP Configuration panel, enter the **SMTP server** and **Administrator e-mail** . Click **Next**.

SMTP server

Enter the mail server configured to work with Asset Management for IT. This server will be used to send workflow and process notifications. This field is optional.

Administrator e-mail

Enter the e-mail address of the person assigned to the role of Asset Management for IT Administrator. This field is optional.

27. In the Run Configuration Step window, choose whether to perform configuration steps at this point, or to defer them until later, manual configuration.

The configuration values that you enter are stored in the *maximo_install_dir\applications\maximo\properties\maximo.properties* file. You can execute the configuration steps outside of the Asset Management for IT installation program by using the taskrunner utility, located in the *tamit_install_dir\scripts* directory. Simply run the taskrunner utility from the command line, and it will use the configuration values stored in the *maximo.properties* file to configure Asset Management for IT.

tamit_install_dir\scripts\taskrunner

If there is an installation failure, the taskrunner utility can be run again after the error conditions have been rectified. The taskrunner utility will resume the install at the point where the last successfully completed task was recorded in the previous attempt.

The configuration includes:

- database configuration
- application server configuration
- process managers installation

You are also prompted to mark one of these options:

Deploy application files automatically

Mark this radio button if you choose to deploy enterprise archive (EAR) files during this installation.

Deploy applications files manually later

Mark this radio button if you choose to deploy enterprise archive (EAR) files during after the installation completes. For performance reasons, you might want to deploy EAR files later manually.

28. From the Choose Shortcut Folder panel, select the type of shortcut you would like to arrange for Asset Management for IT, and then click **Next**.

In a new Program Group

Select this option and enter the name of a new program group if you would like to create Asset Management for IT shortcuts in a new program group.

In an existing Program Group

Select this option and choose the name of an existing program group to store Asset Management for IT shortcuts.

In the Start Menu

Select this option to create shortcuts for Asset Management for IT in the Start menu.

In order to use the Start Menu shortcut with Microsoft Internet Explorer, ensure that you have added the Asset Management for IT URL to the trusted sites Web content zone and disable the option of requiring server verification for all sites in the zone.

On the Desktop

Select this option to create shortcuts for Asset Management for IT on the desktop.

In the Quick Launch Bar

Do not select this option. Selecting this option does not create a shortcut in the Quick Launch bar.

Other Select this option and use the **Choose...** button to select another location to create Asset Management for IT shortcuts.

Don't create icons

Select this option if you do not want any Asset Management for IT shortcuts created.

Create Icons for All Users

Select this option if you would like Asset Management for IT desktop icons to appear on the desktop for all system users.

29. From the Input Summary panel, review the information you have provided to the Asset Management for IT installation program, and then click **Next**.
Use the **Previous** button to return to previous panels to change anything.
30. From the Pre-Installation Summary panel, review the installation information presented, and then click **Install**. The installation now begins. Progress can be monitored by viewing messages displayed above the progress bar.
31. From the Install Complete panel, click **Done**.
32. From the DB2 Database Server Configuration panel, enter the following information, and then click **Next**:

Note: The JMS data store can only be created as a DB2 database.

Host name

Enter the fully qualified host name of the server hosting the JMS data store.

Port Enter the port used to access the database server. Default for all platforms is *50005*.

Database name

Enter the name of the database serving as the JMS data store.

Default for all platforms is `maxsibdb`.

User ID

Enter the user ID used to access the database server.

Default for all platforms is the database user ID you entered when you selected your database type. If the user does not exist, it will be created for you.

Password

Enter the password for the User ID used to access the database server.

33. From the DB2 Database Server Remote Access Authorization panel, enter authorization information for the automatic configuration feature, and then click **Next**:

User ID

Enter a valid user ID that will allow the Asset Management for IT installation program to access the system that is hosting the JMS database. This user ID should have administrative rights on the computer you are accessing.

Windows **Windows :**

This user must be a member of the DB2ADMNS group.

Windows **UNIX :**

This user must be a member of the db2grp1 group.

Password

Enter the password for the user ID.

34. From the DB2 Database Instance Configuration panel, enter the following information, and then click **Next**.

Installation directory

Enter the installation directory for the DB2 server that is hosting the JMS database that contains the instance to be used with WebSphere Application Server.

Windows **Windows :**

This value might be C:\Program Files\IBM\SQLLIB.

Linux **Linux**

This value might be /opt/IBM/db2/V9.5.

Instance

Enter the JMS database instance to be used with WebSphere Application Server.

For all platforms, the default is ctginst1.

Instance administrator user ID

Enter the administrator's user ID for the JMS database instance.

Windows **Windows**

This value might be db2admin.

Linux **Linux**

This value might be ctginst1.

Instance administrator password

Enter the password for the JMS database instance administrator's user ID.

35. From the Maximo panel, enter the following configuration information, and then click **Next**.

Installation directory

Select the folder where Maximo application will be installed. C:\IBM\maximo is the default value. The path you specify must not contain spaces.

SMTP server

Enter the mail server configured to work with Asset Management for IT. This server will be used to send workflow and process notifications. This field is optional.

Workflow administrator e-mail

Enter the e-mail address of the person assigned to the role of Asset Management for IT Workflow Administrator. This address will be used for workflow notifications. This field is optional.

Administrator e-mail

Enter the e-mail address of the person assigned to the role of Asset Management for IT Administrator. This field is optional.

If you choose to not configure optional properties at this time, you can configure them in the Asset Management for IT user interface using the System Properties application. The relevant properties are:

- **mail.smtp.host**
- **mxe.workflow.admin**
- **mxe.adminEmail**

What to do next

Once the Tivoli Asset Management for IT installation program has completed installation and configuration tasks, it exits. Logs can be found at *tamit_install_dir/logs*.

Chapter 6. Installing IBM Tivoli Asset Management for IT with manual middleware configuration

You can have one or more IBM Tivoli Asset Management for IT middleware components configured automatically by the Asset Management for IT installation program. Alternatively, you can choose to manually configure one or more of the middleware servers to work with Asset Management for IT. Configure the components before you install the product.

Manually configured installations involve configuring:

- middleware components,
- the database server,
- the directory server,
- the J2EE server

to work with IBM Tivoli Asset Management for IT prior to using the Asset Management for IT installation program.

The information contained in this section provides details on how to manually configure Asset Management for IT middleware prior to running the Asset Management for IT installation program. Also included in this section is a procedure describing how to advance through the Asset Management for IT installation program to complete the Asset Management for IT deployment.

Before you begin, ensure you have addressed the following prerequisite conditions:

- You have designated a Windows-based computer that will be used to launch the Asset Management for IT installation program.
- For WebSphere Application Server Network Deployment, ensure that the Cell and all related nodes are active.

You must complete the manual configuration of each server you plan to not configure using the autoconfigure feature of the Asset Management for IT installation program before you actually install Asset Management for IT.

Ensure that all of your middleware is at the level described in “Hardware and software requirements” on page 2.

Related concepts

“Reusing existing middleware components” on page 15

You can reuse some existing middleware installations as Tivoli Asset Management for IT components. If you plan to do so, ensure that they are at the level supported by Asset Management for IT. The middleware and Asset Management for IT installation programs do not provide a mechanism for patching unsupported servers, nor do these programs provide remote prerequisite checks to ensure they are at the right level.

Manually configuring the database server

If you choose to not have the Asset Management for IT installation program automatically configure the database server, you must complete the manual configuration before you use the Asset Management for IT installation program .

- **UNIX** For DB2 on UNIX systems, ensure you have a minimum of 8 GB (binary) free of space in the DB2 database instance home directory (/home/ctginst1) in order to meet the default table space disk space requirements of the DB2 install.
- **Windows** For DB2 on Windows, ensure you have a minimum of 8 GB of free space in the DB2 installation directory.

Manually configuring DB2 9.x

For better performance, you might need to manually configure DB2 9.1 before running the Tivoli Asset Management for IT installer to set the preferable environment on different operating systems.

About this task

To configure an existing DB2 9.x server for use with Asset Management for IT, complete the following steps **prior** to launching the Asset Management for IT installation program:

1. Create system users:
 - a. Log into the system as a user that has administrative permissions on the system.
 - b. DB2 requires user accounts that are operating system user accounts. Create operating system users named ctginst1 and maximo, using user management tools available on the system.
 - c. **AIX** For AIX, use SMIT to add the users. For the ctginst1 user, assign the primary group as db2grp1 and secondary groups of staff and dasadm1. For the maximo user, it is not necessary to assign a specific group. After the user IDs have been created, log into the system using the user IDs and change the password for each account.
2. Create the DB2 instance:
 - a. Use the following command to create the DB2 instance:

Windows **Windows:**
`db2icrt -s ese -u db2admin,password -r 50005,50005 ctginst1`

Linux **Linux:**
`db2icrt -a SERVER -s ese -p 50005 -u db2fenc1 ctginst1`

AIX **AIX:**
`db2icrt -a SERVER -s ese -p 50005 -u db2fenc1 -w 64 ctginst1`

- b. Set the listening port for the instance. For example, for **Windows**
 Windows:
`db2 update dbm cfg using svcename 50005`
- c. Set instance service to start automatically. For example, for **Windows**
 Windows:
`sc config ctginst1-0 start= auto`
- d. Start the ctginst1 database instance:

Windows **Windows:**
`db2start`

UNIX **UNIX:**
`su - ctginst1`
`db2start`

3. Create a new database:
 - a. Open up the DB2 Control Center for the instance you plan to use:

Windows Windows:

- 1) Open a command window.
- 2) Type the following command:

```
set DB2INSTANCE=ctginst1
db2set DB2COMM=tcpip
```
- 3) Type the following command:

```
db2cc
```

UNIX UNIX:

- 1) Open a command window.
 - 2) Source the instance you plan to use.
 - 3) Type the following command:

```
db2cc
```
- b. From the DB2 Control Center, navigate to **All Systems** → *System hosting the database instance* → **Instances**.
 - c. Right-click the Databases folder located below the instance name, and then select **Create Database** → **With Automatic Maintenance**.
 - d. From the Specify a name for your new database panel, enter maxdb71 for both the **Database name** and **Alias** fields.
 - e. Enable the **Enable database for XML** option. This will create a Unicode database with a code set of UTF-8.
 - f. Click **Next**.
 - g. From the Specify where to store your data panel, click **Next**. Alternatively, if you don't want to use the database path as the storage path, specify a different directory. If you specify a path, the directory must already exist.
 - h. From the Select your maintenance strategy panel, select **Yes, I can specify an offline maintenance window of at least an hour when the database is inaccessible**, and then click **Next**.
 - i. From the Specify when offline automatic maintenance activities can run, provide scheduling details for offline maintenance, and then click **Next**.
 - j. From the Provide a valid SMTP server panel, enter the name of the SMTP server that is used to communicate DB2 messages concerning this database, and then click **Next**.
 - k. From the Review the actions that will take place when you click **Finish** panel, review the choices you have made, and then click **Finish**.

The database will be created.

AIX For AIX 5.3 systems, you can use the following command to create the DB2 instance.

```
db2icrt -a SERVER -s ese -p 50005 -u db2fenc1 ctginst1
```

To create the database on AIX 5.3 systems, switch the user to ctginst1, and use the following command:

```
db2 create database maxdb71 using codeset UTF-8 territory us pagesize 32 K
```

4. Configure the database.
 - a. Right-click the **maxdb71** database created in the previous step, and choose **Configure Parameters**.
 - b. From the Database Configuration panel, select the **LOGFILSIZ** value and click the button labeled with the ellipsis (...) in the **Value** column.

- c. Enter 4096, and then click **OK**.
- d. From the Database Configuration panel, select the **APP_CTL_HEAP_SZ** value and click the button labeled with the ellipsis (...) in the **Value** column.
- e. Enter 1024, and then click **OK**.
- f. From the Database Configuration panel, select the **APPLHEAPSZ** value and click the button labeled with the ellipsis (...) in the **Value** column.
- g. Enter 1024, and then click **OK**.
- h. From the Database Configuration panel, select the **LOCKLIST** value and click the button labeled with the ellipsis (...) in the **Value** column.
- i. Enter 30000, and then click **OK**.
- j. From the Database Configuration panel, select the **LOGSECOND** value and click the button labeled with the ellipsis (...) in the **Value** column.
- k. Enter 4, and then click **OK**.
- l. From the Database Configuration panel, click **OK**.
- m. Click **Close**.
- n. Restart the database by right-clicking the ctginst1 instance, clicking **Stop**, and then clicking **Start**.

Note: AIX For AIX 5.3 systems, you cannot launch the DB2 Control Center locally. The best way to configure the database on AIX 5.3 systems is to configure it remotely from a system that can run the DB2 Control Center, using the DB2 client.

5. Add users to the database.
 - a. Once the database has restarted, right-click it and select **Authorities**.
 - b. From the User tab of the Database Authorities window, click **Add User**.
 - c. From the Add User dialog, select the user maximo, and then click **OK**.
 - d. Highlight the user, maximo in the Database Authorities window, and click **Grant All**.
 - e. Click **OK**.
6. Create table space:
 - a. From the DB2 Control Center, locate and right-click the **Table Spaces** entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Create**.
 - c. Specify MAXDATA as your new table space, and then click **Next**.
 - d. Select **Regular** as the type of table space and then click **Next**.
 - e. Click **Create** to create a buffer pool for the table space.
 - f. Specify MAXBUFPOOL as your new buffer pool, and then change the **Page size** value to 32 and the **Size in 32 KB pages** value to 4096.
 - g. Ensure the Create buffer pool immediately choice is selected, and then click **OK**.
 - h. Highlight the newly created buffer pool and click **Next**.
 - i. From the Specify the extent and prefetch sizes for this table space panel, choose the **Between 200 MB and 2 GB** option, and leave **Extent size** as 32, and then click **Next**.
 - j. Define a hard drive specification by choosing **Server (SCSI)**, and then click **Next**.

k. Click **Finish**.

Note: By default, index data is stored in the data table space. If you would rather create a separate index table space, you could create one at this point.

7. Grant permissions for the table space:
 - a. From the DB2 Control Center, locate and right-click the MAXDATA Table Spaces entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Privileges**.
 - c. Click **Add User**.
 - d. Select the user `maximo`, and then click **OK**.
 - e. From the **Privileges** drop-down menu, select **Yes**, and then click **OK**.

Note: If you created a separate index table space, you will have to grant permissions for it at this time.

8. Create a schema:
 - a. From the DB2 Control Center, locate and right-click the **Schema** entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Create**.
 - c. Specify a name for your new schema, and then click **OK**. This name must be the same as was used for the Database User ID.
 - d. Right-click on the new schema name and select **Privileges**.
 - e. From the **Privileges** drop-down menus, select **Add User**, and then select the `maximo` user.
 - f. Click **OK**.
 - g. Select the `maximo` user and then click **Grant all**.
 - h. From the dialog box, select **No Grant**, and then click **OK**.
9. Create a temporary table space:
 - a. From the DB2 Control Center, locate and right-click the **Table Spaces** entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Create**.
 - c. Specify `MAXTEMP` for your new table space, and then click **Next**.
 - d. Select **System temporary** as the type of table space and then click **Next**.
 - e. Select the previously created bufferpool (`MAXBUFPOOL`), and click **Next**.
 - f. From the Specify the extent and prefetch sizes for this table space panel, choose the **Between 200 MB and 2 GB** option, and leave **Extent size** as 32, and then click **Next**.
 - g. Define a hard drive specification by choosing **Server (SCSI)**, and then click **Next**.
 - h. Specify the dropped table recovery option for the table space by enabling the Enable dropped table recovery option, and then click **Next**.
 - i. Click **Finish**.
10. Refer to the tables presented in "Hardware and software requirements" on page 2 and install the appropriate fix pack. Ensure you review and complete all of the installation and post-installation tasks contained within the fix pack

readme file. Failure to do so can potentially cause the Asset Management for IT installation to fail. Refer to the appropriate product support page for more information.

What to do next

After you have installed the fix pack, run the `dasupdt` command to update the DB2 Administration Server to the applied fix pack.

Also run the `db2iupdt` command to update the DB2 instance. Start by first stopping all processes that are running for the database instance (`ctginst1`), and then run the following command:

Windows **Windows:**
`C:\Program Files\IBM\SQLLIB\BIN\db2iupdt ctginst1`

UNIX **UNIX:**
`DB2DIR/instance/db2iupdt ctginst1`

Manually configuring DB2 8.2

This section contains instructions for manually configuring DB2 8.2 servers for use by Tivoli Asset Management for IT. Asset Management for IT supports DB2 8.2 only when manually configured.

About this task

To configure an existing DB2 8.2 server for use with Asset Management for IT, complete the following steps prior to launching the Asset Management for IT installation program:

1. Create system users:
 - a. Log into the system as a user that has administrative permissions on the system.
 - b. DB2 requires user accounts that are operating system user accounts. Create operating system users named `ctginst1` and `maximo`, using user management tools available on the system.

AIX For AIX, use SMIT to add the users. For the `ctginst1` user, assign the primary group as `db2grp1` and secondary groups of `staff` and `dasadm1`. For the `maximo` user, it is not necessary to assign a specific group. After the user IDs have been created, log into the system using the user IDs and change the password for each account.

2. Create the DB2 instance:
 - a. Use the following command to create the DB2 instance:

Windows **Windows:**
`db2icrt -s ese -u db2admin,password -r 50005,50005 ctginst1`

Linux **Linux:**
`db2icrt -a SERVER -s ese -p 50005 -u db2fenc1 ctginst1`

AIX **AIX:**
`db2icrt -a SERVER -s ese -p 50005 -u db2fenc1 -w 64 ctginst1`

- b. Set the listening port for the instance:

Windows **Windows:**
`db2 update dbm cfg using svcename 50005`

- c. Set instance service to start automatically:

Windows **Windows:**
sc config ctginst1-0 start= auto

- d. Start the ctginst1 database instance:

Windows **Windows:**
db2start

UNIX **UNIX:**
su - ctginst1
db2start

3. Create the database:

Windows **Windows:**

- a. Open a command window and type the following command:
set DB2INSTANCE=ctginst1
- b. Type db2cmd to open the DB2 Command Window.
- c. From the new instance window issue the following commands:
db2start
db2 create db maxdb71 using codeset utf-8 territory us pagesize 32 k

UNIX **UNIX:**

- a. Open a command window and type the following command:
su - ctginst1
- b. From the new instance window issue the following commands:
db2start
db2 create db maxdb71 using codeset utf-8 territory us pagesize 32 k

4. Configure the database:

- a. From the DB2 Command Window, type the following command:
db2cc
- b. From the DB2 Control Center, navigate to **All Systems** → **DB2_server** → **Instances** → **CTGINST1** → **Databases** → **MAXDB71**.
- c. Right-click the maxdb71 database and choose **Configure Parameters**.
- d. From the Database Configuration panel, select the *LOGFILSIZ* value and click the button labeled with the ellipsis (...) in the **Value** column.
- e. Enter 4096, and then click **OK**.
- f. From the Database Configuration panel, select the *APP_CTL_HEAP_SZ* value and click the button labeled with the ellipsis (...) in the **Value** column.
- g. Enter 1024, and then click **OK**.
- h. From the Database Configuration panel, select the *APPLHEAPSZ* value and click the button labeled with the ellipsis (...) in the **Value** column.
- i. Enter 1024, and then click **OK**.
- j. From the Database Configuration panel, select the *LOCKLIST* value and click the button labeled with the ellipsis (...) in the **Value** column.
- k. Enter 30000, and then click **OK**.
- l. From the Database Configuration panel, select the *LOGSECOND* value and click the button labeled with the ellipsis (...) in the **Value** column.
- m. Enter 4, and then click **OK**.

- n. From the Database Configuration panel, click **OK**.
 - o. Click **Close**.
 - p. Restart the database by right-clicking the ctginst1 instance, clicking **Stop**, and then clicking **Start**.
5. Add users to the database:
- a. Once the database has restarted, right-click it and select **Authorities**.
 - b. From the **User** tab of the Database Authorities window, click **Add User**.
 - c. From the **Add User** dialog, select the user maximo, and then click **OK**.
 - d. Highlight the user, maximo in the Database Authorities window, and click **Grant All**.
 - e. Click **OK**.
6. Create table space:
- a. From the DB2 Control Center, locate and right-click the **Table Spaces** entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Create**.
 - c. Specify MAXDATA as your new table space, and then click **Next**.
 - d. Select **Regular** as the type of table space, and then click **Next**.
 - e. Click **Create** to create a new buffer pool for the table space.
 - f. Specify MAXBUFPOOL as your new buffer pool, and then change the **Page size** value to 32 and the **Size in 32 KB** pages value to 4096.
 - g. Ensure the **Create buffer pool immediately** choice is selected, and then click **OK**.
 - h. Highlight the newly created buffer pool and click **Next**.
 - i. From the Space management panel, specify Database-managed space and click **Next**.
 - j. From the Containers panel, click **Add**.
 - k. Set the **Type** to File, **Size** to 5000 Mb, and **File name** to CTGDAT. UNIX
For UNIX, enter /home/ctginst1 as the location of the file.
 - l. Click **OK**, and then click **Next**.
 - m. From the Specify the extent and prefetch sizes for this table space panel, click **Next**.
 - n. Define a hard drive specification by choosing Server (SCSI), and then click **Next**.
 - o. Specify the dropped table recovery option for the table space by enabling the Enable dropped table recovery option, and then click **Next**.
 - p. From the Summary panel, click **Finish**.

Note: By default, index data is stored in the data table space. If you would rather create a separate index table space, you could create one at this point.

7. Create a temporary table space:
- a. From the DB2 Control Center, locate and right-click the **Table Spaces** entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Create**.
 - c. Specify MAXTEMP for your new table space, and then click **Next**.
 - d. Select **System temporary** as the type of table space and then click **Next**.
 - e. Select the previously created bufferpool (MAXBUFPOOL), and click **Next**.

- f. From the Space management panel, specify Database-managed space, and then click **Next**.
 - g. From the Containers panel, click **Add**.
 - h. Set the **Type** to File, **Size** to 3000Mb, and **File name** to CTGTMP. UNIX
For UNIX, enter /home/ctginst1 as the location of the file.
 - i. Click **OK**, and then click **Next**.
 - j. From the Specify the extent and prefetch sizes for this table space panel, click **Next**.
 - k. Define a hard drive specification by choosing **Server (SCSI)**, and then click **Next**.
 - l. From the Summary panel, click **Finish**.
8. Grant permissions for the table space:
 - a. From the DB2 Control Center, locate and right-click the MAXDATA table spaces entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Privileges**.
 - c. Click **Add User**.
 - d. Select the user maximo, and then click **OK**.
 - e. From the Privileges drop-down menu, select **Yes**, and then click **OK**.

Note: If you created a separate index table space, you will have to grant permissions for it at this time.
 9. Create a schema:
 - a. From the DB2 Control Center, locate and right-click the **Schema** entry under the DB2 database that you created for use with Asset Management for IT.
 - b. From the right-click menu, select **Create**.
 - c. Specify a name for your new schema, and then click **OK**. This name should be the same as was used for the Database User ID.
 - d. Right-click on the new schema name and select **Privileges**.
 - e. From the **Privileges** drop-down menus, select **Add User**, and then select the maximo user.
 - f. Click **OK**.
 - g. Select the maximo user and then click **Grant all**.
 - h. From the dialog box, select No Grant, and then click **OK**.
 10. Install the appropriate fix pack. Refer to the tables presented in “Hardware and software requirements” on page 2.

What to do next

If you installed a fix pack, run the dasupdt command to update the DB2 Administration Server to the applied fix pack.

After you have installed a fix pack, you will also need to run the db2iupdt command to update the DB2 instance. Start by first stopping all processes that are running for the database instance (ctginst1), and then run the following command:

Windows **Windows:**
C:\Program Files\IBM\SQLLIB\BIN\db2iupdt ctginst1

Manually configuring Oracle 11g

Use the following instructions to manually configure Oracle 11g for use with Asset Management for IT.

Before you begin

The `max_cursors` size for the Asset Management for IT database should be set to 1000 before Asset Management for IT installation.

About this task

To configure an existing Oracle 11g server for use with Asset Management for IT, complete the following steps before launching the Asset Management for IT installation program:

1. Log in as the Oracle software user. Typically this user is named `oracle`.
2. Create the database listener. The listener manages requests to connect to the database.
 - a. Open the Oracle Network Configuration Assistant application.
 - b. From the Welcome panel, select **Listener configuration**, and then click **Next**.
 - c. From the action panel, select **Add**, and then click **Next**.
 - d. Enter a name for the listener or accept the default value, and then click **Next**.
 - e. Accept the default Selected Protocols listed by clicking **Next**.
 - f. From the port panel, select **Use the standard port of 1521**, and then click **Next**.
 - g. Select **No** to indicate that you are finished configuring listeners, and then click **Next**.
 - h. From the Listener Configuration Done panel, click **Next**.
 - i. Click **Finish**.
3. Create a new database for use by Asset Management for IT.
 - a. Open the Oracle Database Configuration Assistant.
 - b. Click **Next**.
 - c. Select **Create a Database**, and then click **Next**.
 - d. Select **General Purpose or Transaction Processing**, and then click **Next**.
 - e. Enter `ctginst1` for both the Global Database Name value and the SID value, and then click **Next**.
 - f. Leave the defaults selected, and click **Next**.
 - g. Ensure **Use the Same Administrative Password for All Accounts** is selected, enter a password for Oracle users, and then click **Next**.
 - h. Ensure **File System** is selected as the storage mechanism to use for the database, and then click **Next**.
 - i. Ensure **Use Database File Locations from Template** is selected as the value to use for database file location, and then click **Next**.
 - j. Leave defaults selected for the database recovery options panel, and then click **Next**.
 - k. From the Sample Schemas panel, click **Next**.

- l. From the memory allocation panel, select **Custom**, provide the following values (measured in bytes), and then click **Next**.

Memory Management

Set this value to **Manual Shared Memory Management**.

Shared Pool

Set this value to 157286400.

Buffer Cache

Set this value to 36000000.

Java Pool

Set this value to 33554432

Large Pool

Set this value to 8388608.

PGA Size

Set this value to 37748736.

- m. From the Character Sets tab, select **Use Unicode (AL32UTF8)**,
- n. Click **All Initialization Parameters...**
- o. Click **Show Advanced Parameters**.
- p. Locate the following parameters, change them to the values indicated, and then click **Close**.

nls_length_semantics

Change this value to CHAR

open_cursors

Change this value to 1000

cursor_sharing

Set this value to SIMILAR.

- q. From the Security Settings panel, accept the defaults, and then click **Next**.
- r. From the Automatic Maintenance Tasks panel, accept the defaults, and then click **Next**.
- s. From the Initialization Parameters panel, click **Next**.
- t. From the Database Storage panel, click **Next**.
- u. From the Creation Options panel, click **Finish**.
- v. Once the database has been successfully created, click **Password Management**.
- w. Unlock the CTXSYS account by clearing the check mark in the Lock Account? column for that entry, enter a password for the account, and then click **OK**.
- x. Click **Exit** to exit the Database Configuration Assistant. The database has been successfully created.

Note: The Oracle Database Configuration Assistant executes the *oracle_install_dir/ctx/admin/defaults/drdefus.sql* script as part of the configuration of the CTXSYS user. This needs to be executed manually if the Oracle Database Configuration Assistant is not used.

4. Create a table space using the following command in SQL*Plus:

```
Create tablespace maxdata datafile
'C:\oracle\product\11.1.0\db_1\dfs\maxdata.dbf'
size 1000M autoextend on;
```

The directory specified in the example should be changed to the location where the database will reside. If the directory does not already exist, this command will fail.

5. Create a temporary table space using the following command in SQL*Plus

```
create temporary tablespace maxtemp tempfile
'C:\oracle\product\11.1.0\db_1\dfs\maxtemp.dbf'
size 1000M autoextend on maxsize unlimited;
```

The directory specified in the example should be changed to the location where the database will reside. If the directory does not already exist, this command will fail.

6. Create the maximo user and grant permissions using the following command in SQL*Plus:

```
create user maximo identified by maximo default tablespace maxdata temporary
tablespace maxtemp;
grant connect to maximo;
grant create job to maximo;
grant create trigger to maximo;
grant create session to maximo;
grant create sequence to maximo;
grant create synonym to maximo;
grant create table to maximo;
grant create view to maximo;
grant create procedure to maximo;
grant alter session to maximo;
grant execute on ctxsys.ctx_ddl to maximo;
alter user maximo quota unlimited on maxdata;
```

Manually configuring Oracle 10g

If you want to use the existing Oracle 10g server instance for Asset Management for IT, make sure you complete these steps before installing Asset Management for IT.

Before you begin

If you are using Oracle 10g Rel2, ensure the Oracle 10g Rel2 patch 3 is installed.

About this task

To configure an existing Oracle 10g Rel2 or 10g Rel1 server for use with Tivoli Asset Management for IT, complete the following steps prior to launching the Asset Management for IT installation program:

1. Log in as a user designated as a dba, such as sys or system.
2. Create a new database for use by Asset Management for IT.
 - a. Open the Oracle Database Configuration Assistant, and click **Next**.
 - b. Select **Create a Database**, and then click **Next**.
 - c. Select **General Purpose**, and then click **Next**.
 - d. Enter ctginst1 for both the **Global Database Name** value and the **SID** value, and then click **Next**.
 - e. Leave the defaults selected, and click **Next**.
 - f. Ensure **Use the Same Password for All Accounts** is selected, enter a password for Oracle users, and then click **Next**.
 - g. Ensure **File System** is selected as the storage mechanism to use for the database, and then click **Next**.

- h. Ensure **Use Database File Locations from Template** is selected as the value to use for database file location, and then click **Next**.
- i. Leave defaults selected for the database recovery options panel, and then click **Next**.
- j. From the Sample Schemas panel, click **Next**.
- k. From the **Memory** tab, select **Custom**, provide the following values (measured in bytes), and then click the **Character Sets** tab:

Shared Memory Management

Set this value to Manual.

Shared Pool

Set this value to 157286400.

Buffer Cache

Set this value to 36000000.

Java Pool

Set this value to 33554432.

Large Pool

Set this value to 8388608.

PGA Size

Set this value to 37748736.

- l. From the **Database Character Set** tab, select **Use Unicode (AL32UTF8)**,
- m. Click **All Initialization Parameters...**
- n. Click **Show Advanced Parameters**.
- o. Locate the following parameters, change them to the values indicated, and then click **Close**:

cursor_sharing

Change this value to FORCE

nls_length_semantics

Change this value to CHAR

open_cursors

Change this value to 1000

- p. From the Initialization Parameters panel, click **Next**.
 - q. From the Database Storage panel, click **Next**.
 - r. From the Creation Options panel, click **Finish**.
 - s. From the Confirmation panel, click **OK**.
 - t. Click **Exit** to exit the Database Configuration Assistant.
- The database has been successfully created.

- 3. Log into SQL *Plus using the following information:

User Name

system

Password

Password you entered in step 2f.

Host String

ctginst1

- 4. Create a table space using the following command in SQL*Plus:

```
Create table space maxdata datafile
'C:\oracle\product\10.2.0\oradata\ctginst1\maxdata.dbf'
size 1000M autoextend on;
```

The directory specified in the example should be changed to the location where the database will reside.

5. Create a temporary table space using the following command in SQL*Plus:

```
Create temporary tablespace maxtemp tempfile
'C:\oracle\product\10.2.0\oradata\ctginst1\maxtemp.dbf'
size 1000M autoextend on maxsize unlimited;
```

The directory specified in the example should be changed to the location where the database will reside.

6. Create the Maximo user and grant permissions using the following command in SQL*Plus:

```
Create user maximo identified by maximo default table space maxdata temporary
tablespace maxtemp;
grant create job to maximo;
grant create trigger to maximo;
grant create session to maximo;
grant create sequence to maximo;
grant create synonym to maximo;
grant create table to maximo;
grant create view to maximo;
grant create procedure to maximo;
grant alter session to maximo;
grant execute on ctxsys.ctx_ddl to maximo;
alter user maximo quota unlimited on maxdata;
```

Manually configuring Oracle9i Rel2

If you want to use the existing Oracle Oracle9i Rel2 server instance for Tivoli Asset Management for IT, make sure you complete these steps before installing Asset Management for IT.

Before you begin

If you are using Oracle9i Rel2, ensure Oracle 9.2.0.8 is installed.

About this task

To configure an existing Oracle Oracle9i Rel2 server for use with Asset Management for IT, complete the following steps prior to launching the Asset Management for IT installation program:

1. Create a new database for use by Asset Management for IT:
 - a. Open the Oracle Database Configuration Assistant, and click **Next**.
 - b. Select **Create a database**, and then click **Next**.
 - c. Select **General Purpose**, and then click **Next**.
 - d. Enter ctginst1 for both the **Global Database Name** value and the **SID** value, and then click **Next**.
 - e. Leave the default of **Dedicated Server Mode** selected, and click **Next**.
 - f. From the **Memory** tab, select **Custom**, enter the following values (M Bytes), and then click **Next**:

Shared Pool

Set this value to 150.

Buffer Cache

Set this value to 36.

Java Pool

Set this value to 32.

Large Pool

Set this value to 8.

PGA Size

Set this value to 36.

- g. Select the **Character Sets** tab and select **Use Unicode (AL32UTF8)** as the **Database Character Set**.
- h. Click **All Initialization Parameters**.
- i. Locate the following parameters, change them to the values indicated, and then click **Close**, and then **Next**:

nls_length_semantics

Change this value to CHAR.

open_cursors

Change this value to 1000.

- j. From the Database Storage panel, click **Next**.
- k. From the Creation Options panel, select the **Create Database** option, and click **Finish**.
- l. From the Confirmation panel, click **OK**.
- m. Once the database has been successfully created, click **Password Management**.
- n. Unlock the CTXSYS account by removing the check mark in the **Lock Account?** column for that entry, enter a password for the account, and then click **OK**.
- o. Click **Exit** to exit the Database Configuration Assistant.

The database has been successfully created.

- 2. Create a table space using the following command in SQL*Plus:

```

Create table space maxdata datafile
'C:\oracle\oradata\maxdata\maxdata.dbf'
size 1000M autoextend on;

```

The directory specified in the example should be changed to the location where the database will reside.

- 3. Create a temporary table space using the following command in SQL*Plus:

```

create temporary table space maxtemp tempfile
'C:\oracle\oradata\maxtemp\maxtemp.dbf'
size 1000M autoextend on maxsize unlimited;

```

The directory specified in the example should be changed to the location where the database will reside.

- 4. Create the Maximo user and grant permissions using the following command in SQL*Plus:

```

create user maximo identified by maximo default table space maxdata temporary
table space maxtemp;
grant connect to maximo;
grant create job to maximo;
grant create trigger to maximo;
grant create session to maximo;
grant create sequence to maximo;

```

```
grant create synonym to maximo;
grant create table to maximo;
grant create view to maximo;
grant create procedure to maximo;
grant alter session to maximo;
grant execute on ctxsys.ctx_ddl to maximo;
alter user maximo quota unlimited on maxdata;
```

Manually configuring SQL Server

Windows If you want to use the existing SQL Server instance for Tivoli Asset Management for IT, make sure you complete these steps before installing Asset Management for IT.

Before you begin

Note that because Microsoft SQL Server does not support UTF-8, Asset Management for IT does not have multilingual support when deployed with Microsoft SQL Server.

Microsoft SQL Server collation settings must be set to the following options:

- Dictionary order
- Case-insensitive
- For use with 1252 Character set

About this task

To configure an existing SQL Server 2008 for use with Asset Management for IT, complete the following steps prior to launching the Asset Management for IT installation program:

1. Configure the listener port.

If enabled, the default instance of the Microsoft SQL Server Database Engine listens on TCP port 1433. Named instances of the SQL Server Database Engine and SQL Server Compact Edition are configured for dynamic ports, which means they select an available port when the SQL Server service is started. When connecting to a named instance through a firewall, configure the Database Engine to listen on a specific port, so that the appropriate port can be opened in the firewall.

- a. Open **Programs** → **Microsoft SQL Server 2008** → **Configuration Tools** → **Microsoft SQL Server Configuration Manager**.
- b. From the Microsoft SQL Server Configuration Manager navigation pane, expand **SQL Server 2008 Network Configuration** → **Protocols for *your_instance_name*** for the instance name to be used with Asset Management for IT, and then double-click **TCP/IP**.
- c. In the TCP/IP Properties dialog box, click the **IP Addresses** tab.
- d. For each IP address listed, ensure the **TCP Dynamic Ports** field is blank. If the **TCP Dynamic Ports** field contains a value of 0, that IP address is using dynamic ports. Since Asset Management for IT requires SQL Server to listen on a static port, this field must be blank.
- e. For each IP address listed, enter 1433 for the **TCP Port** field, and click **OK**.
- f. From the SQL Server Configuration Manager navigation pane, click **SQL Server 2008 Services**.
- g. Right-click **SQL Server *instance_name*** and then click **Restart**, to stop and restart SQL Server.

2. Verify that you enabled the Full-text Search setting during the installation of Microsoft SQL Server 2008. To determine if Full-text Search is installed on your existing Microsoft SQL Server database, perform the following steps:
 - a. Open SQL Query Analyzer. You can run SQL Query Analyzer from the Start menu, from inside SQL Server Enterprise Manager, or from the command prompt by executing `isqlw`.
 - b. Type the following command:


```
select FULLTEXTSERVICEPROPERTY ( 'IsFulltextInstalled' )
```

In the event that you did not install Full-text Search (the resulting value is zero), you must do so at this time. The following steps provide a general guideline describing how you can change this and other settings after having installed SQL Server.

 - a. Insert the “Microsoft SQL Server 2008” CD-ROM onto the server where you had it installed originally.
 - b. Navigate through the installation dialog boxes and from the **Setup Type** dialog box, select **Custom**.
 - c. Check the **Full-Text Search** option.
 - d. Complete remaining installation steps. You finish the installation process by choosing to restart the server.
3. Create a SQL Server Database for Maximo
 - a. Open SQL Server Enterprise Manager Studio: **Start** → **Programs** → **Microsoft SQL Server 2008** → **SQL Server Management Studio**.
 - b. Right-click the **Databases** folder from the tree view, and select **New Database**.
 - c. In the Database Properties dialog box, in the **General** tab, specify a unique database name (for example maxdb71).
 - d. For the maxdb71 **Logical Name**, change the Initial size attribute to 500 (MB), and also set the value of the **Autogrowth** field to By 1MB, unrestricted growth.
 - e. If you prefer, modify the log settings to accommodate your production environment.
 - f. Click **Add**.
4. Create the Maximo user for SQL Server:
 - a. Open SQL Server Enterprise Manager Studio: **Start** → **Programs** → **Microsoft SQL Server 2008** → **SQL Server Management Studio**.
 - b. Click **New Query**.
 - c. Select the **Tivoli Asset Management for IT database** (maxdb71) from the **Available Databases** drop-down menu.
 - d. Enter the following script to create the Maximo user.


```
sp_addlogin MAXIMO,MAXIMO
go
```
 - e. Click **Execute**.
 - f. Enter the following script to change the database owner to maximo.


```
sp_changedbowner MAXIMO
go
```
 - g. Click **Execute**.

What to do next

Note: If you add additional logical names to the database and set their file group to a value other than PRIMARY, you will have to complete the following steps after you have completed setting up the database and created the Maximo user:

1. Run the Asset Management for IT installation program and choose the **Do not run the configuration step now** option.
2. Add the following property to the `tamit_install_dir\maximo\applications\maximo\properties\maximo.properties` file:
`Database.SQL.DataFilegroupName=your_logical_name`
3. Execute the configuration steps outside of the Asset Management for IT installation program by using the taskrunner utility, located in the `tamit_install_dir\scripts` directory.

Note that these additional steps must be completed only if you have added additional logical names to the database and set their file group to a value other than PRIMARY.

Manually configuring the directory server

You must complete the manual configuration of the directory server before you use the Tivoli Asset Management for IT installation program if you choose to not have the Asset Management for IT installation program automatically configure it.

Important: When entering LDAP values for Asset Management for IT installation panel fields, entries in LDIF files, or values you enter directly into an directory instance using the directory server's own tools, be aware of the product-specific syntax rules for using special characters in an LDAP string. In most cases, special characters must be preceded by an escape character in order to make it readable by the directory server. Failing to escape special characters contained in an LDAP string used with Asset Management for IT will result in Asset Management for IT errors.

Many directory server products consider a blank space as a special character that is part of the LDAP string. Therefore, if you mistakenly enter an LDAP string that contains a blank, at the end of a field value, for example, and you do not precede the blank character with an escape character, you will encounter Asset Management for IT errors that will be difficult to troubleshoot.

Refer to the product documentation for your directory server for more information on special characters in LDAP strings.

Manually configuring IBM Tivoli Directory Server

To configure Directory Server prior to launching the Tivoli Asset Management for IT installation program, you must create a new Directory Server instance.

1. Create a user on the system and assign it to the appropriate group:

Windows **Windows:**

Create the user `idsccmdb` and make it a member of the Windows Administrators group.

UNIX **UNIX:**

Create the user `idsccmdb` and make it a member of the `root`, `db2grp1`, and `idsldap` groups. The user `idsccmdb` must have `root` assigned as its primary group.

2. If the Instance Administration Tool is not already started, ensure you are logged in as an administrator on the system, and then start the tool:

Windows

Windows:

Select **Programs** → **IBM Tivoli Directory Server 6.2** → **Instance Administration Tool**.

UNIX

UNIX:

Type in `/opt/IBM/ldap/V6.2/sbin/idsxinst` at the command line.

3. From the Instance Administration Tool, click **Create**.
4. On the Create a new directory server instance window, click **Create a new directory server instance**, and then click **Next**.
5. From the Instance details window, complete the following fields, and then click **Next**.

User name

Select **idscmdb** as the system user ID of the user who will own the directory server instance. This name will also be the name of the directory server instance.

Install location

Enter the location where the directory server instance files will be stored.

Encryption seed string

Type a string of characters that will be used as an encryption seed. This value must be a minimum of 12 characters.

Instance description

Enter a brief description of the instance.

6. From the DB2 instance details panel, enter **idscmdb** as the value for the DB2 instance name field, and then click **Next**.
7. From the TCP/IP settings for multihomed hosts panel, select **Listen on all configured IP addresses**, and then click **Next**.
8. On the TCP/IP port settings panel, complete the following fields, and then click **Next**.

Server port number

Enter 389 as the contact port for the server.

Server secure port number

Enter 636 as the secure port for the server.

Admin daemon port number

Enter 3538 as the administration daemon port.

Admin daemon secure port number

Enter 3539 as the administration daemon secure port.

9. From the Option steps panel, leave the following options selected, and then click **Next**.

Configure admin DN and password

You will configure the administrator DN and password for the directory server instance now.

Configure database

You will configure the database for the directory server instance now.

10. From the Configure administrator DN and password window panel, complete the following fields, and then click **Next**.

Administrator DN

Enter `cn=root` for the administrator distinguished name.

Administrator Password

Enter a password for the Administrator DN.

- From the Configure database panel, complete the following fields, and then click **Next**.

Database user name

Enter `idscmdb` as the database user.

Password

Enter the password for the `idscmdb` user.

Database name

Enter `idscmdb` as the database to be used with this directory instance.

- From the Database options panel, complete the following fields, and then click **Next**.

Database install location

Enter the location where you installed DB2.

Character-set option

Leave the **Create a universal DB2 database (UTF-8/UCS-2)** option selected.

- From the Verify settings panel, review the instance creation details provided, and then click **Finish** to create the `idscmdb` instance.
- Click **Close** to close the window and return to the main window of the Instance Administration Tool.
- Click **Close** to exit the Instance Administration Tool.
- Ensure the server is stopped:

Windows

Windows:

IBM Tivoli Directory Server Instance V6.2 - `idscmdb`

UNIX

UNIX:

V6.2 `ibmslapd` server daemon

- Launch the IBM Tivoli Directory Server configuration tool:

Windows

Windows:

Select **Programs** → **IBM Tivoli Directory Server 6.2** → **Instance Administration Tool**.

UNIX

UNIX:

Type in `/opt/IBM/ldap/V6.2/sbin/idsxcfg` at the command line.

- Click **Configure**.
- Select **Manage suffixes**.
- From the Manage suffixes panel, type the following suffix, and then click **Add**:
`o=IBM,c=US`

Then, click **OK**.

- Create and save an LDIF file.
Add the following DNs:
 - `ou=SWG,o=IBM,c=US`
 - `ou=users`

- ou=groups

Define the following users and groups and their positions within the ou=users and ou=groups DN's you created. These users and groups are defined in order for Virtual Member Manager to be used to secure Asset Management for IT.

Important: Before you begin this procedure, ensure you have the following users and groups created in your LDAP repository:

Table 15. Asset Management for IT required users and groups

User	Groups
wasadmin	
maxadmin	MAXADMIN (must be uppercase)
mxintadm	MAXADMIN (must be uppercase)
maxreg	

Here is an example of the default base ldif data:

```
dn: o=ibm,c=us
objectClass: top
objectClass: organization
o: IBM

dn: ou=SWG, o=ibm,c=us
ou: SWG
objectClass: top
objectClass: organizationalUnit

dn: ou=groups,ou=SWG, o=ibm,c=us
ou: groups
objectClass: top
objectClass: organizationalUnit

dn: ou=users,ou=SWG, o=ibm,c=us
ou: users
objectClass: top
objectClass: organizationalUnit

dn: cn=wasadmin,ou=users,ou=SWG, o=ibm,c=us
uid: wasadmin
userpassword: wasadmin
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: person
objectclass: top
title: WebSphere Administrator
sn: wasadmin
cn: wasadmin
```

Note: Windows If you create the LDIF file on Windows, ensure that you remove the ^M characters from the file before using.

22. From the **Directory Server Configuration Tool**, click **Import LDIF data**. Use the browse button to locate the LDIF file.
23. Click **Import**.
24. Close the **Directory Server Configuration Tool** and restart the server.

Manually configuring Microsoft Active Directory

Windows You can choose to configure a Microsoft Active Directory resource manually for better use with Tivoli Asset Management for IT.

About this task

If you choose to manually configure a Microsoft Active Directory resource for use with Asset Management for IT, complete the following steps prior to running the Asset Management for IT installation program:

1. Open the domains security policy for editing by selecting **Start** → **Administrative Tools** → **Domain Security Policy**.
2. From the Default Domain Security Settings interface, navigate to **Security Settings** → **Account Policies** → **Password Policy**.
3. For each password policy setting displayed, right-click the setting, select **Properties**, and set it to the appropriate value, as shown in the table below:

Table 16. Policy settings and their values.

Policy Setting	Value	Step
Enforce password history	Not Defined	On the properties panel, set the check box for Define this policy setting to unchecked.
Maximum password age	Not Defined	On the properties panel, set the check box to unchecked.
Minimum password age	Not Defined	On the properties panel, set the check box to unchecked.
Minimum password length	7 characters	On the properties panel set the check box Define this policy setting to checked and set the value to 7.
Password must meet complexity requirements	Disabled	On the properties panel, set the check box Define this policy setting to checked and ensure that the value Disabled is selected.
Store passwords using reversible encryption	Disabled	On the properties panel, set the check box Define this policy setting to checked and ensure that the value Disabled is selected.

4. Open a command prompt window and type `gpupdate /force`, or, alternatively, you can simply reboot the system.
5. Open the Active Directory Users and Computers user interface by selecting **Start** → **Control Panel** → **Administrative Tools** → **Active Directory Users and Computers** and then select the domain that you will be working with.
6. Edit the domain functional level of the domain by selecting **Action** → **Raise Domain Functional Level**. The Raise Domain Functional Level dialog box will appear.
7. Select **Windows Server 2003** from the Select an available domain functional level dropdown menu, and then click **Raise**. An alert dialog box will appear. Click **OK**.
8. When the domain raise task has completed, click **OK**.
9. In the Active Directory Users and Computers user interface, right-click the domain you want to work with and select **New** → **Organizational Unit**.
10. Enter a name for the new Organizational Unit (OU), for example, **SWG**, and then click **OK**.
11. Create a groups object under the SWG organizational unit:
 - a. Right-click the **SWG** OU, and select **New** → **Organizational Unit**.
 - b. Enter **Groups** as the name for the new OU then click **OK**.

12. Create a users object under the SWG organizational unit:
 - a. Right-click the **SWG OU**, and select **New → Organizational Unit**.
 - b. Enter Users as the name for the new OU then click **OK**.
13. Create the MAXADMIN group:
 - a. Right click the **Groups OU** and select **New → Group**.
 - b. From the New Object - Group dialog, enter the following values, and then click **OK**:
 - Group name**
Enter MAXADMIN as the group name.
This value **must** be capitalized.
 - Group name (pre-Windows 2000)**
Enter MAXADMINPRE2K as the pre-Windows 2000 group name.
This value must be capitalized and must be different than the name entered above for Group name.
 - Group scope**
Global
 - Group type**
Security
14. Create the MAXIMOUSERS group:
 - a. Right click the **Groups OU** and select **New → Group**.
 - b. From the New Object - Group dialog, enter the following values, and then click **OK**:
 - Group name**
Enter MAXIMOUSERS as the group name.
This value must be capitalized.
 - Group name (pre-Windows 2000)**
Enter MAXIMOUSERS as the pre-Windows 2000 group name.
This value must be capitalized.
 - Group scope**
Global
 - Group type**
Security
15. Create the wasadmin user:
 - a. Right click the **Users OU** and select **New → User**.
 - b. From the New Object - User dialog, enter the following values, and then click **Next**:
 - First name**
Enter wasadmin.
 - Initials**
Leave this field blank.
 - Last name**
Leave this field blank.
 - Full name**
Enter wasadmin.

User login name

Enter wasadmin in the first field. Leave the default value of the second field.

User login name (pre-Windows 2000)

This field will be filled with the same value (wasadmin) entered for the User login name.

- c. From the next panel, enter the following information, and then click **Next**:

Password

Enter a 7 character password for wasadmin.

User must change password at next logon

Ensure this check box is deselected.

User cannot change password

Ensure this check box is selected.

Password never expires

Ensure this check box is selected.

Account is disabled

Ensure this check box is deselected.

- d. Review the password settings in the summary panel, and click **Finish**.

16. Create the maxadmin user:

- a. Right click the **Users** OU and select **New** → **User**.
b. From the New Object - User dialog, enter the following values, and then click **Next**:

First name

Enter maxadmin.

Initials

Leave this field blank.

Last name

Leave this field blank.

Full name

Enter maxadmin.

User login name

Enter maxadmin in the first field. Leave the default value of the second field.

User login name (pre-Windows 2000)

This field will be filled with the same value (maxadmin) entered for the User login name.

- c. From the next panel, enter the following information, and then click **Next**:

Password

Enter maxadmin as the password for the maxadmin user.

User must change password at next logon

Ensure this check box is deselected.

User cannot change password

Ensure this check box is selected.

Password never expires

Ensure this check box is selected.

Account is disabled

Ensure this check box is deselected.

- d. Review the password settings in the summary panel, and click **Finish**.
17. Create the mxintadm user:
- a. Right click the **Users** OU and select **New** → **User**.
 - b. From the New Object - User dialog, enter the following values, and then click **Next**:

First name

Enter mxintadm.

Initials

Leave this field blank.

Last name

Leave this field blank.

Full name

Enter mxintadm.

User login name

Enter mxintadm in the first field. Leave the default value of the second field.

User login name (pre-Windows 2000)

This field will be filled with the same value (mxintadm) entered for the User login name.

- c. From the next panel, enter the following information, and then click **Next**:

Password

Enter a 7 character value as the password for the mxintadm user.

User must change password at next logon

Ensure this check box is deselected.

User cannot change password

Ensure this check box is selected.

Password never expires

Ensure this check box is selected.

Account is disabled

Ensure this check box is deselected.

- d. Review the password settings in the summary panel, and click **Finish**.
18. Create the maxreg user:
- a. Right click the **Users** OU and select **New** → **User**.
 - b. From the New Object - User dialog, enter the following values, and then click **Next**:

First name

Enter maxreg.

Initials

Leave this field blank.

Last name

Leave this field blank.

Full name

Enter maxreg.

User login name

Enter maxreg in the first field. Leave the default value of the second field.

User login name (pre-Windows 2000)

This field will be filled with the same value (mxintadm) entered for the User login name.

- c. From the next panel, enter the following information, and then click **Next**:

Password

Enter a 7 character value as the password for the maxreg user.

User must change password at next logon

Ensure this check box is deselected.

User cannot change password

Ensure this check box is selected.

Password never expires

Ensure this check box is selected.

Account is disabled

Ensure this check box is deselected.

- d. Review the password settings in the summary panel, and click **Finish**.

19. Add users to the MAXADMIN group:

- a. Click on the **Groups** object under the **SWG OU**.
- b. Double-click the **MAXADMIN** group listed in the **Groups** pane.
- c. From the MAXADMIN properties dialog, select the **Members** tab and then click **Add**.
- d. From the Select Users, Contacts, Computers, or Groups dialog, click **Advanced**.
- e. On the Advanced panel, click **Find Now**.
- f. From the Search results list, select the maxadmin and mxintadm users, and then click **OK**.

Ensure you are selecting the maxadmin user and not the maxadmin group from this list.

- g. Click **OK** to add the users.

20. Add users to the MAXIMOUSERS group:

- a. Click on the **Groups** object under the **SWG OU**.
- b. Double-click the **MAXIMOUSERS** group listed in the **Groups** pane.
- c. From the MAXIMOUSERS properties dialog, select the **Members** tab and then click **Add**.
- d. From the Select Users, Contacts, Computers, or Groups dialog, click **Advanced**.
- e. On the Advanced panel, click **Find Now**.
- f. From the Search results list, select the maxadmin, maxreg, and mxintadm users, and then click **OK**.

Ensure you are selecting the maxadmin user and not the maxadmin group from this list.

- g. Click **OK** to add the users.

21. You can now exit out of the Active Directory Users and Computers user interface.

What to do next

Microsoft Active Directory configuration is complete and you are now ready to install the remaining Asset Management for IT middleware and configure the J2EE server to use Active Directory.

Related concepts

“Planning for security” on page 18

Planning for security includes choosing a security option, deciding which users will work with each application in Asset Management for IT, and optionally which users can work with which configuration items.

Manually configuring the J2EE server

You must complete the manual configuration of the J2EE server before you use the Tivoli Asset Management for IT installation program if you choose to not have the Asset Management for IT installation program automatically configure it.

About this task

To configure the J2EE server prior to launching the Asset Management for IT installation program, follow these steps:

1. Manually copy the keystore file from the WebSphere Network Deployment manager host to a temporary directory on the Asset Management for IT administrative system where you are installing Asset Management for IT:
was_install_dir/profiles/ctgDmgr01/etc/trust.p12.
2. Launch the profile creation wizard.
3. Click **Next** in the Welcome dialog box.
4. Select the create a deployment manager option. Click **Next**.
5. Accept the default value or specify a **Profile name**. Click **Next**.
6. Accept the default installation location. Click **Next**.
7. Accept the default values or specify the **Node name**, **Host name**, and **Cell name**. Click **Next**.
8. Review the assigned port numbers. Click **Next**. Note the Administrative port number. You will use this context when invoking the console through a browser.
9. Select the **Run the Application Server as a Windows service** and log on as a local system account. Click **Next**.
10. Click **Next** in the Profile summary dialog box.
11. Select the **Launch the First steps** console option. Click **Finish**.
12. Click the Installation verification link.
13. After Installation Verification completes, close the output window.
14. Use the Launchpad command and click the **Profile creation** wizard to open the First Steps window (if not open already) .
15. Click **Next** in the Welcome dialog box.
16. Select **Create a custom profile**. Click **Next**.
17. Accept the default values or specify the appropriate information. Click **Next**.
18. Specify a unique Profile name and select the **Make this profile the default** check box. Click **Next**.
19. Accept the default directory path. Click **Next**.

20. Specify a unique node name and the computer name (or IP address) of the computer where you are performing this installation. Click **Next**.
21. Review the port number listings. Click **Next**.
22. Click **Next** in the Profile summary dialog box.
23. Select the **Launch the First steps console** check box. Click **Finish**.
24. Click **Exit**. If another First steps window is open, close it.

Manually configuring Virtual Member Manager on IBM WebSphere Application Server

This procedure provides task information for manually configuring Virtual Member Manager (VMM) to secure Tivoli Asset Management for IT.

Before you begin

During the installation process, the Asset Management for IT installation program provided you with the option of automatically configuring Asset Management for IT middleware. If you elected to have the Asset Management for IT installer automatically configure the middleware, then it will, among other tasks, perform Virtual Member Manager configuration for you.

If you elected to manually configure the middleware for use with Asset Management for IT, you will have to manually configure Virtual Member Manager.

Virtual Member Manager provides you with the ability to access and maintain user data in multiple repositories, and federate that data into a single virtual repository. The federated repository consists of a single named realm, which is a set of independent user repositories. Each repository might be an entire external repository or, in the case of LDAP, a subtree within that repository. The root of each repository is mapped to a base entry within the federated repository, which is a starting point within the hierarchical namespace of the virtual realm.

Note that if you intend to configure Virtual Member Manager to use SSL with a federated LDAP repository, it must be done only after a successful Asset Management for IT installation. If Virtual Member Manager is configured to use SSL with a federated LDAP repository prior to completing the Asset Management for IT installation, the installation will fail. Do not configure a Virtual Member Manager LDAP federated repository to use SSL with an LDAP directory prior to installing Asset Management for IT. Configure SSL after the Asset Management for IT installation program has completed successfully.

To add an LDAP directory to the Virtual Member Manager virtual repository, you must first add the LDAP directory to the list of repositories available for configuration for the federated repository and then add the root of baseEntries to a search base within the LDAP directory. Multiple base entries can be added with different search bases for a single LDAP directory.

The instructions provided here are for IBM Tivoli Directory Server. If you are configuring Virtual Member Manager to use Microsoft Active Directory, substitute values you used in "Reusing Microsoft Active Directory" on page 79 and "Manually configuring Microsoft Active Directory" on page 121 where appropriate in this procedure. You will also have to modify the VMMSYNC as shown in "Manually configuring the VMMSYNC cron task for Microsoft Active Directory" on page 230.

Important: Before you begin this procedure, ensure you have a wasadmin user created in your LDAP repository.

About this task

To add the Directory Server to Virtual Member Manager, complete the following steps:

1. Log in to the administrative console, then navigate to **Security** → **Secure administration, applications, and infrastructure**.
2. Locate the **User account repository** section and select **Federated repositories** from **Available realm** definition, and then click **Configure**.
3. Click **Manage repositories**, located under **Related Items**.
4. Click **Add** to create new repository definition under the current default realm.
5. Enter the following values, and then click **Apply** and the click **Save**.

Repository identifier

Enter ISMITDS.

Directory type

Select the directory type, in this example, Directory Server 6.2.

Primary host name

Enter the fully-qualified host name or IP address of the Directory Server.

Port Enter 389.

Support referrals to other LDAP servers

Set this to ignore.

Bind distinguished name

Enter cn=root.

Bind password

Enter the password for the bind distinguished name.

Login properties

Leave this value blank.

Certificate mapping

Select EXACT_DN.

6. Return to the Federated repositories page by clicking **Security** → **Secure administration, applications, and infrastructure**, selecting **Federated repositories** from the **Available realm definitions** drop-down list, and then clicking **Configure**.
7. Locate the Repositories in the realm section and click **Add Base entry to Realm**.

Note that if there is an existing file repository entry in the Repositories in the realm table, you must select it, click **Remove**, and save the change, after creating the new entry.

8. Enter the following values, and then click **Apply** and then click **Save**.

Repository

Select ISMITDS.

Distinguished name of a base entry that uniquely identifies this set of entries in the realm

ou=SWG,o=IBM,c=US

Distinguished name of a base entry in this repository

ou=SWG,o=IBM,c=US

9. From the Federated repositories configuration page, enter the following values and then click **Apply** and then click **Save**:

Realm name

Enter ISMRealm.

Primary administrative user name

Enter wasadmin. This value should be a valid user from the configured LDAP repository.

Server user identity

Select **Automatically generated server identity**.

Ignore case for authorization

Select this check box.

10. Click **Supported entity types**, and then click **PersonAccount**.
11. From the PersonAccount configuration page, enter the following values:

Entity type

Verify that the value is PersonAccount.

Base entry for the default parent

Enter ou=users,ou=SWG,o=IBM,c=US.

Relative Distinguished Name properties

Enter uid.

12. Click **OK** and then click **Save**.
13. Click **Supported entity types**, and then click **Group**.
14. From the Group configuration page, enter the following values:

Entity type

Verify that the value is Group.

Base entry for the default parent

Enter ou=groups,ou=SWG,o=IBM,c=US.

Relative Distinguished Name properties

Enter cn.

15. Click **Supported entity types**, and then click **OrgContainer**.
16. From the OrgContainer configuration page, enter or verify the following values:

Entity type

Verify that the value is **OrgContainer**.

Base entry for the default parent

Enter ou=SWG,o=IBM,c=US.

Relative Distinguished Name properties

Enter o;ou;dc;cn.

17. Click **OK** and then click **Save**.
18. Navigate to **Security** → **Secure administration, applications, and infrastructure**.
19. From the Secure administration, applications, and infrastructure configuration page, complete the following:
 - a. Enable **Enable administrative security**.
 - b. Enable **Enable application security**.

- c. Deselect **Use Java 2 security** to restrict application access to local resources.
 - d. From **Available realm definition**, select **Federated repositories**.
 - e. Click **Set as current**.
20. Click **Apply**, and then click **Save**.
 21. Restart WebSphere Application Server and the managed nodes:
 - a. `was_install_dir\profiles\ctgDmgr01\bin\stopManager.bat`
 - b. `was_install_dir\profiles\ctgAppSrv01\bin\stopNode.bat`
 - c. `was_install_dir\profiles\ctgDmgr01\bin\startManager.bat`
 - d. `was_install_dir\profiles\ctgAppSrv01\bin\startNode.bat`

Note: UNIX Substitute UNIX path and file extension values where appropriate.

What to do next

You have now successfully completed setting up Virtual Member Manager. The next step is to perform post install J2EE server tasks.

Related concepts

“Planning for security” on page 18

Planning for security includes choosing a security option, deciding which users will work with each application in Asset Management for IT, and optionally which users can work with which configuration items.

Manually configuring WebSphere Application Server Network Deployment

This section contains instructions for manually configuring an existing WebSphere Application Server Network Deployment for use by Asset Management for IT.

You need to complete the manual configuration of WebSphere Application Server Network Deployment before you use the Asset Management for IT installation program if, in the case of WebSphere Application Server Network Deployment, you choose to not have the Asset Management for IT installation program automatically configure it.

Manually configuring JMS queues

This procedure provides details on steps to configure JMS queues, which must be completed prior to deploying Tivoli Asset Management for IT EAR files.

Before you begin

During the installation process, the Asset Management for IT installation program provided you with the option of automatically configuring Asset Management for IT middleware. If you elected to have the Asset Management for IT installation program automatically configure Asset Management for IT middleware, then it will, among other tasks, create and configure JMS message queues for you. If you elected to manually configure Asset Management for IT middleware for use with Asset Management for IT, you will have to manually configure these message queues.

About this task

To configure the JMS queues, complete the following steps:

1. Start the WebSphere Application Server.
2. Launch the browser and open the WebSphere Administrative Console by typing the following URL:
`http://computer_name:port_number/ibm/console`

For example, enter a URL similar to the following:

`http://local_host:9060/ibm/console`

3. At the Welcome, please enter your information login screen, enter your User ID, then click **Log in**. This action opens the Welcome screen for the WebSphere Administrative Console.
4. Start the MXServer server by navigating to **Servers** → **Application Servers**, selecting **MXServer**, and then clicking **Start**.
5. Click **System** → **administration** → **Console preferences**.
6. Select the **Synchronize changes** with Nodes option, and then click **Apply**.
7. Click **Service Integration** → **Buses** to open the Buses dialog. A bus is a group of interconnected servers and clusters that have been added as members of the bus.
8. Click **New** to open the **Buses** → **New dialog box** where you can add a new service integration bus.
9. Enter `intjmsbus` as the name of the new bus in the **Name** field.
10. Deselect the **Bus security** check box. If you leave this box checked, `intjmsbus` inherits the Global Security setting of the cell.
11. Click **Next** → **Finish** → **Save**. Marking **Save** propagates the JMS bus setup to the cluster configuration. Confirm that build completed screen displays the following:
 - Bus name, for example, `intjmsbus`.
 - Auto-generated, unique ID (UUID), for example, `4BCAC78E15820FED`.
 - The **Secure** field is unchecked.

Adding a server to the service integration bus:

A complete, step-by-step procedure of adding a server to the service integration bus is described in this section.

About this task

Complete the following steps to add a server to the service integration bus:

1. From the WebSphere Administrative Console, click **Service Integration** → **Buses** to open the Buses dialog box.
2. Click `intjmsbus` to open the **Buses** → `intjmsbus` dialog box.
3. Under **Topology**, click **Bus members**.
4. In the **Buses** → `intjmsbus` → **Bus members** dialog box, click **Add** to open the Add a new bus member dialog box.
5. Click the **Server** drop-down arrow, and select the server name `ctgNode01:MXServer` to add to the bus, and then click **Next**.
6. Check that the **File store** radio button is selected, and then click **Next**.
7. From the Provide the message store properties panel, click **Next**.

8. Click **Finish** → **Save** → **OK**, and then select **intjmsbus**.
9. Change the value of the **High message threshold** field to a minimum value of 500,000 messages, and then click **Apply**.

If the number of messages awaiting processing exceeds the **High Message Threshold** you set, the application server will take action to limit the addition of new messages in the processing queues.

Depending on your message requirements, you might want to enter a higher message threshold value. You can determine an optimal message threshold setting by monitoring the messaging in/out queues and the impact of the message threshold setting on system performance. You might, for example, lower the threshold value if a higher value is degrading system performance.

If you decide to change the **High Message Threshold** setting after the initial configuration, you must open the Additional Properties menu in WebSphere Administrative Console and change the threshold value for each child configuration.

10. Click **Save** → **OK**.

Creating the service integration bus destination for the continuous inbound (CQINBD) queue:

The procedure in this section describes how to add a logical address for the continuous inbound bus destination queue.

About this task

To add a logical address for the continuous inbound bus destination queue (CQINBD) within the JMS bus, complete the following steps:

1. From the WebSphere Administrative Console, click **Service Integration** → **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the intjmsbus dialog box.
3. Click **Destinations** under **Destination resources** to open the **Buses** → **intjmsbus** → **Destinations** dialog box.

A bus destination, for example CQINBD, is a virtual place within a service integration bus where applications can attach and exchange messages.

4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Type CQINBD in the **Identifier** field and Continuous Queue Inbound in the **Description** field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box.

Note: You must use this value and it must contain only uppercase letters.

7. Select the **Bus Member** pull-down and choose **Node=ctgNode01:Server=MXServer** as the bus member that will store and process messages for the CQINBD bus destination queue.
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to complete the creation of the CQINBD bus destination queue.
10. Navigate to **Buses** → **intjmsbus** → **Destinations**, then click **CQINBD** to open the configuration dialog box where you must make the following changes:
 - Click **None** as the Exception destination value.
 - Change the **Maximum failed deliveries** value to 1.

This is the maximum number of times you want the system to process a failed messaging attempt before forwarding the message to the exception destination.

11. Click **Apply** → **Save** to complete the task.

Creating the service integration bus destination for the sequential inbound (SQINBD) queue:

To add a logical address for the sequential inbound bus destination queue (SQINBD) within the service integration bus, complete the steps in the section.

1. From the WebSphere Administrative Console, click **Service Integration** → **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the **Buses** → **intjmsbus** dialog box.
3. Click **Destinations** under **Destination resources** to open the **Buses** → **intjmsbus** → **Destinations** dialog box. A bus destination is a virtual place within a service integration bus where applications can attach and exchange messages.
4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Enter SQINBD in the **Identifier** field and **Sequential Queue Inbound in the Description** field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box. Note that you must use this value and it must contain only uppercase letters.
7. Select the **Bus Member** pull-down and choose **Node=ctgNode01:Server=MXServer**.
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to complete the creation of the SQINBD bus destination queue.
10. Navigate the path **Buses** → **intjmsbus** → **Destinations** , then click **SQINBD** to open the configuration dialog box where you must make the following changes:
 - Click **None** as the Exception destination value.
 - Change the **Maximum failed deliveries** value to 1. This is the maximum number of times you want the system to process a failed messaging attempt before forwarding the message to the exception destination.
11. Click **Apply**.
12. Click **Save**.

Creating the service integration bus destination for the sequential outbound (SQOUTBD) queue:

This section describes the procedure how to add a logical address for the sequential outbound bus destination queue (SQOUTBD) within the service integration bus.

About this task

To add a logical address for the sequential outbound bus destination queue (SQOUTBD) within the service integration bus, complete the following steps:

1. From the WebSphere Administrative Console, click **Service Integration** → **Buses** to open the Buses dialog box.

2. Click **intjmsbus** to open the **Buses** → **intjmsbus** dialog box.
3. Click **Destinations** under **Destination resources** to open the **Buses** → **intjmsbus** → **Destinations** dialog box. A bus destination, for example SQOUTBD, is a virtual place within a service integration bus where applications can attach and exchange messages.
4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Enter SQOUTBD in the **Identifier** field and **Sequential Queue Outbound** in the **Description** field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box.

Note: The value you type in must contain only uppercase letters.

7. Select the **Bus Member** pull-down and choose **Node=ctgNode01:Server=MXServer** as the bus member that will store and process messages for the SQOUTBD bus destination queue.
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to complete the creation of the sqinbd queue.
10. Navigate to the **Buses** → **intjmsbus** → **Destinations**, then click **SQOUTBD** to open the configuration dialog box where you must make the following changes:
 - Click **None** as the **Exception destination** value.
 - Change the **Maximum failed deliveries** value to 1. This is the maximum number of times you want the system to process a failed messaging attempt before forwarding the message to the exception destination.
11. Click **Next**, and then **Save**.

Creating the JMS connection factory:

You add a connection factory for creating connections to the associated JMS provider of point-to-point messaging queues.

About this task

To add a connection factory for creating connections to the associated JMS provider, perform the following:

1. From the WebSphere Administrative Console, click **Resources** → **JMS** → **Connection factories**.
2. From the Scope drop-down list, select **Cell=ctgCell01**, and click **New**.
3. Verify that the **Default Messaging Provider** is selected and click **OK**.
4. Enter the following information, and then click **OK**:

Name Enter intjmsconfact.

JNDI name

Enter jms/maximo/int/cf/intcf.

Bus name

Select **intjmsbus**.

5. Click **Save**.

Creating the continuous inbound (CQIN) JMS queue:

You need to create a JMS queue (CQIN) as the destination for continuous inbound point-to-point messages.

About this task

To create a JMS queue (CQIN), perform the following steps:

1. From the WebSphere Administrative Console, click **Resources** → **JMS** → **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**, and then click **New**.
3. Verify that the **Default Messaging Provider** is selected and click **OK**.
4. Enter the following information, and click **OK**.

Name Enter CQIN.

Note this value must only contain uppercase letters.

JNDI name

Enter `jms/maximo/int/queues/cqin`

Bus name

Select **intjmsbus**.

Queue name

Select **CQINBD**.

5. Click **OK**, and then **Save**.

Creating the sequential inbound (SQIN) JMS queue:

You must create a JMS queue (SQIN) as the destination for sequential inbound point-to-point messages.

About this task

To create a JMS queue, perform the following procedure:

1. From the WebSphere Administrative Console, click **Resources** → **JMS** → **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**, and click **New**.
3. Verify that the **Default Messaging Provider** is selected and click **OK**.
4. Enter the following information, and click **OK**.

Name Enter SQIN.

Note this value must only contain uppercase letters.

JNDI name

Enter `jms/maximo/int/queues/sqin`

Bus name

Select **intjmsbus**.

Queue name

Select **SQINBD**.

5. Click **OK**, and then **Save**.

Creating the sequential outbound (SQOUT) JMS queue:

You need to create a JMS queue (SQOUT) as the destination for sequential outbound point-to-point messages.

About this task

To create a SQOUT JMS queue, perform the following steps:

1. From the WebSphere Administrative Console, click **Resources** → **JMS** → **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**. Click **New**.
3. Verify that the **Default Messaging Provider** is selected and click **OK**.

Name Enter **SQOUT**.

Note: This value must only contain uppercase letters.

JNDI name

Enter `jms/maximo/int/queues/sqout`

Bus name

Select **intjmsbus**.

Queue name

Select **sqoutbd**.

4. Enter the following information, and click **OK**, and then **Save**.

Creating JMS activation specification for the continuous inbound queue (CQIN):

You need to activate the continuous inbound queue (CQIN) before it can receive messages.

About this task

Complete the following steps to activate the CQIN queue:

1. From the WebSphere Administrative Console, click **Resources** → **JMS** → **Activation Specifications**.
2. From the Scope drop-down list, select **Cell=ctgCell01**. Click **New** to complete the General Properties section for the new JMS activation specification.
3. Click **OK**.
4. Enter the following information, and then click **OK**:

Name `intjmsact`

This value is case-sensitive. This value must be lowercase.

JNDI name

`intjmsact`

Destination type

Queue

Destination JNDI name

`jms/maximo/int/queues/cqin`

Bus name

`intjmsbus`

Maximum concurrent endpoints

10

5. Click **Save**.
6. Ensure to stop all IBM-related processes and daemons.
7. Restart these processes for the update to take effect.

8. Start the bus member for the ctgNode MXServer intjmsbus if it is not started. If you cannot start ctgNode MXServer intjmsbus, restart MXServer under **Servers** → **Application servers**.

Error queues:

You can create an optional error queue that will receive redirected messages from the continuous queue (cqin) when the messages go in error.

Creating the service integration bus destination for the inbound error queue (CQINERRBD):

This section describes a step-by-step procedure how to add a logical address for the inbound error queue (CQINERRBD) queue within the JMS bus.

About this task

To add a logical address for the inbound error queue (CQINERRBD) within the JMS bus, complete the following steps:

1. From the WebSphere Administrative Console, click **Service Integration** → **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the **Buses** → **intjmsbus** dialog box.
3. Click **Destinations** under **Destination resources** to open the **Buses** → **intjmsbus** → **Destinations** dialog box.

A bus destination is a virtual place within a service integration bus where applications can attach and exchange messages.

4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Enter CQINERRBD in the **Identifier** field and Error Queue Inbound in the **Description** field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box.

Note:

You need to use this value and it must contain only uppercase letters.

7. Select the Bus Member pull-down and choose **Node=ctgNode01:Server=MXServer**.
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to complete the creation of the CQINERRBD bus destination queue.
10. Navigate to the **Buses** → **intjmsbus** → **Destinations**, then click **CQINERRBD** to open the configuration dialog box where you must make the following changes:
 - a. Click **Specify** and enter CQINERRBD as the exception destination value.
 - b. Change the Maximum failed deliveries value to 5. This is the maximum number of times you want the system to process a failed messaging attempt before forwarding the message to the exception destination.
11. Click **Apply**, and then **Save**.

Creating the error (CQINERR) JMS queue:

After creating the Error Queue Bus Destination, you create the error queue.

About this task

To create an error queue:

1. From the WebSphere Administrative Console, click **Resources** → **JMS** → **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**, and then click **New**.
3. Verify that the **Default Messaging Provider** is selected and click **OK**.
4. Enter the following information, and click **OK**.

Name Enter CQINERR.

Note this value must only contain uppercase letters.

JNDI name

Enter jms/maximo/int/queues/cqinerr

Bus name

Select **intjmsbus**.

Queue name

Select **CQINERR**.

5. Click **OK**, and then **Save**.

What to do next

For a complete message queue configuration information, see [../com.ibm.itam.doc/migrating/c_configuring_message_queues.html](http://com.ibm.itam.doc/migrating/c_configuring_message_queues.html).

Creating JMS activation specification for the inbound error queue (CQINERR):

You must activate the inbound queue (CQINERR) before it can receive messages. Follow the procedure described in this section to do so.

About this task

Complete the following steps to activate the CQINERR queue:

1. From the WebSphere Administrative Console, click **Resources** → **JMS** → **Activation Specifications**.
2. From the Scope drop-down list, select **Cell=ctgCell01**.
3. Click **New** to complete the General Properties section for the new JMS activation specification, and then click **OK**.
4. Enter the following information, and click **OK**:

Name Enter intjmsacterr.

This value must only contain lowercase letters.

JNDI name

Enter intjmsacterr.

Destination type

Enter Queue.

Destination JNDI name

jms/maximo/int/queues/cqinerr.

5. Click **OK**, and then **Save**.

Manually creating a data source for the persistence store:

If you chose to manually configure WebSphere Application Server, you will need to create a data source in order to store JMS messages in a DB2 database.

About this task

You have the option of having WebSphere Application Server use a DB2 database to store JMS messages. For more information about WebSphere Application Server message storage, including the usage of products other than DB2, refer to

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/welcome_nd.html

and

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.pmc.nd.doc/tasks/tjm0035_.html

To create a data source for the persistence store, complete the following steps:

1. Create a system user and password on the computer hosting the database server.
For example, `mxsibusr/mxsibusr`.
2. Create and configure the database:
 - a. Open DB2 Control Center.
 - b. Navigate down to the **Databases** folder listed under your system.
 - c. Right-click the **Databases** folder and select **Create Database** → **Standard**.
 - d. Create a database named `maxsibdb` using default settings.
 - e. Once the database has been created, expand the `maxsibdb` database and select **User** and **Group** objects.
 - f. Right-click **DB Users** and select **Add**.
 - g. Select `mxsibusr` from the **User** drop-down list.
 - h. Grant all authorities to the `mxsibusr` with the exception of Security administrator authority. Click **Apply**.
 - i. Verify that you can connect to the database using the `mxsibusr` user by right-clicking `maxsibdb` and selecting **Connect**.
3. Configure J2C authentication data and JDBC provider in WebSphere Application Server:
 - a. Open and login to the WebSphere Administrative Console.
 - b. Navigate to **Security** → **Secure administration, applications, and infrastructure**.
 - c. Under the **Authentication** header, click on **Java Authentication and Authorization Service** → **J2C authentication data**, and then click **New**.
 - d. Complete the following fields in the **User** identity form:
Alias `maxJaasAlias`
User ID
 `mxsibusr`
Password
 Password you created for `mxsibusr`.
Description
 SIB database user alias.

- e. Click **Apply**, and then click **Save**.
- f. Click **Scope** and then select **Cell=ctgCell01**.
- g. From the WebSphere Administrative Console navigation pane, navigate to **Resources** → **JDBC** → **JDBC Providers**, and then click **New**.
- h. Specify the following values:
 - Database type**
DB2
 - Provider type**
DB2 JDBC Driver Provider
 - Implementation type**
XA data source
 - Name** maxJdbcProvider
- i. Click **Next**.
- j. Fill in the WebSphere Application Server variable: *#{db2_jdbc_driver_path}* field with a value of *was_install_dir\ctgMX\lib*. For example, C:\Program Files\IBM\WebSphere\AppServer\ctgMX\lib.
- k. Click **Next**, **Finish**, and then **Save**.
4. Open a command prompt and copy *db2_install_dir/java/db2jcc.jar* and *db2_install_dir/java/db2jcc_license_cu.jar* to the *was_install_dir\ctgMX\lib* directory.
 - a. Go back to **Resources** → **JDBC** → **JDBC Providers** → **maxJdbcProvider**, and correct the Class path if required for both *db2jcc.jar* and *db2jcc_license_cu.jar*.
 - b. Ensure that each jar file has the full path from *#{db2_jdbc_driver_path}*.
5. Configure WebSphere Application Server:
 - a. From the WebSphere Administrative Console, navigate to **Resources** → **JDBC** → **Data sources**.
 - b. Click **Scope** and then select **Cell=ctgCell01**.
 - c. Click **New**.
 - d. Specify the following values:
 - Data source name**
intjmsds
 - JNDI name**
jdbc/intjmsds
 - e. From the Component-managed authentication alias and XA recovery authentication alias drop-down list, select **maxJaasAlias**.
 - f. Click **Next**.
 - g. Choose **Select an existing JDBC provider**, and then select **maxJdbcProvider** from the drop-down list.
 - h. Click **Next**.
 - i. Specify the following values:
 - Database name**
maxsibdb
 - Driver type**
4
 - Server name**
Specify the DB2 server host name.

Port number

Specify the DB2 port number. For example, *50005*.

- j. Ensure the **Use this data source in container managed persistence (CMP)** option is enabled, and then click **Next**.
 - k. Click **Finish**, and then click **Save**.
6. Verify the data source by selecting **intjmsds**, and then clicking **Test Connection**.

Chapter 7. Installing IBM Tivoli Asset Management for IT without middleware autoconfiguration

This procedure will instruct you on installing IBM Tivoli Asset Management for IT and choosing to not have the Asset Management for IT installation program autoconfigure the Asset Management for IT middleware servers. You might elect to not have the Asset Management for IT installation program autoconfigure the middleware if your organization has specific policies and procedures that govern how you create databases, database instances, users, and so on, within your organization.

About this task

If you intend to use DB2 on UNIX systems with Asset Management for IT, you need to add root to the DB2GRP1 group prior to starting the Asset Management for IT installer.

To install Asset Management for IT, follow these steps:

1. Log in to the Asset Management for IT administrative workstation as Administrator.
2. Launch the Asset Management for IT installation program from the Launchpad:
 - a. On the DVD titled "Tivoli Asset Management for IT V7.2", navigate to the root directory of the product disc or the downloaded installation image, and run the command: `launchpad.exe`.
 - b. In the Launchpad navigation pane, click **Install the Product**.
 - c. Click **IBM Tivoli Asset Management for IT**.
3. Select a language for the installation and click **OK**.
4. From the Introduction panel, click **Next**.
5. From the Import Middleware Configuration Information panel, specify that you want to use field values you input into the Tivoli middleware installer as default values for those same fields in the Asset Management for IT installation program.

Import Middleware Configuration Information

Select this check box if you want to allow the Asset Management for IT installer to reuse values entered in the middleware installer.

The middleware default information will not be used if you select the **Simple deployment** path.

Host name

Enter the host name of the system where the middleware installer was run.

User ID

Enter the User ID that was used to run the middleware installer.

Password

Enter the password of the User ID that was used to run the middleware installer.

Workspace Location

Enter the location of the topology file that contains the values entered

for the middleware installer. This file is found in the workspace that was defined during the Asset Management for IT middleware installation task. For example, C:\ibm\tivoli\mwi\workspace.

6. From the Choose Deployment panel, select the **Custom** deployment topology, and then click **Next**.

Simple

Select simple if you want to deploy all Asset Management for IT components on a single system. This deployment option is typically only used for demonstration, proof-of-concept, or training purposes.

Custom

Select custom if you want to deploy Asset Management for IT components across several systems. This deployment option is typically used in a production environment.

7. From the Choose Install Folder panel, specify the directory you will use to install Asset Management for IT, and then click **Next**. Fill in the **Where Would You Like to Install?** field, providing the information on the path you want to install Asset Management for IT. By default, for Windows, it is C:\IBM\SMP. The path you specify must not contain spaces.
8. From the Maximo Database Type panel, select the product that you will be using for the Maximo database, and then click **Next**.

DB2 Select this choice to use DB2 as the Maximo database.

Oracle Select this choice to use Oracle as the Maximo database.

SQL Server

Select this choice to use Microsoft SQL Server 2008 as the Maximo database.

Each database will have its own unique set of configurable parameters and values.

9. From the Maximo Database panel, enter configuration information on the database, and then click **Next**.

DB2

Host name

Enter the host name of the computer hosting DB2.

The host name must be fully qualified.

Port

Enter the port being used by DB2 instance.

The default is 50005.

Database Name

Enter the name of the database to use with Maximo.

The default database name is maxdb72. The database will be created if it does not already exist.

Instance

Enter the name of the database instance to be used with Maximo.

The default instance name is ctginst1. This instance will be created if it does not already exist, however, the user and its associated home directory must already exist on the DB2 server.

Database User ID

Enter the user ID used for Maximo to access DB2.

Default for all platforms is maximo.

This user ID will be created if it does not already exist.

This user ID cannot be the same one used as the instance administrator user ID.

Database Password

Enter the password for the user ID used to access DB2.

Oracle**Host name**

Enter the host name of the computer hosting Oracle.

The host name must be fully qualified.

Port Enter the port being used by Oracle.

The default is 1521.

Instance

Enter the name of the database instance to be used with Maximo.

The default instance name is ctginst1.

Database User ID

Enter the user ID used for Maximo to access Oracle.

Default for all platforms is maximo.

This user ID will be created if it does not already exist.

Database Password

Enter the password for the user ID used to access Oracle.

SQL Server**Host name**

Enter the host name of the computer hosting SQL Server.

The host name must be fully qualified.

Port Enter the port being used by SQL Server.

The default is 1433.

Database Name

Enter the name of the database to use with Maximo.

The default database name is maxdb71.

User ID

Enter the user ID used to access SQL Server.

Default for all platforms is maximo.

This user ID will be created if it does not already exist.

Password

Enter the password for the user ID used to access SQL Server.

After you have entered configuration information for the database that was selected, the Asset Management for IT installation program will connect to the database server to validate the information you have entered.

10. From the Automate Database Configuration panel, select **Do not automate database configuration**, and then click **Next**.

Note: This step assumes you have already created a database instance, a database, table spaces, a user, and schema for use with Asset Management for IT. Refer to “Manually configuring the database server” on page 101. If you have not manually configured the database prior to selecting Do not automate database configuration from within the Asset Management for IT installer, the installation will verify that you have not completed these pre-install tasks and you will be reminded to complete them prior to restarting the Asset Management for IT installation program.

11. Once the database validation task has completed, from the WebSphere Connectivity panel, enter host information on the WebSphere Application Server, and then click **Next**.

Host name

Enter the fully-qualified host name of the system hosting WebSphere.

Alternatively, you can provide the IP address for the system.

SOAP port

Enter the SOAP port of the WebSphere system.

The default value for this field is 8879.

12. From the Remote Access Authorization panel, enter authorization information for WebSphere configuration, and then click **Next**.

Operating system user ID

Enter a valid user ID that will allow the Asset Management for IT installation program to access the system that is hosting WebSphere.

This user ID should have administrative rights on the computer you are accessing.

Operating system password

Enter the password for the system user ID.

13. From the Automate WebSphere configuration panel, select **Do not automate WebSphere configuration**, and then click **Next**.

Note: Remember that in choosing not to have the Asset Management for IT installation program automatically configure middleware, you will have had to configure WebSphere manually **prior** to the installation of Asset Management for IT. Configuration tasks include creating a profile, running WebSphere as a Windows service, copying the WebSphere keystore file from the computer where WebSphere is installed to the administrative workstation, setting up JMS queues, and so on.

14. From the WebSphere Deployment Manager configuration panel, enter values for the following fields, and then click **Next**.

WebSphere installation directory

Enter the directory where WebSphere is installed on the host system.

Windows

Windows

On Windows, this value might be C:\Program Files\IBM\WebSphere\AppServer

Linux

Linux

On Linux, this value might be /opt/IBM/WebSphere/AppServer

AIX

AIX

On AIX, this value might be /usr/IBM/WebSphere/AppServer

Solaris

Sun Solaris

On Sun Solaris, this value might be /opt/IBM/WebSphere/AppServer

User ID

Enter the administrative user ID used to access the WebSphere server.

Default for all platforms is wasadmin.

Password

Enter the password for the administrative user ID used to access the WebSphere server.

Profile name

Enter the name of the WebSphere profile.

Default for all platforms is ctgDmgr01.

15. From the WebSphere Application Server Configuration panel, enter the following information, and then click **Next**.

Web server port

Enter the Web server port used by WebSphere.

Default for all platforms is 80.

Web server name

Enter the name of the Web server.

Default for all platforms is webserver1.

Node name

Enter the name of the WebSphere node containing the application server.

Default for all platforms is ctgNode01.

Cluster name

Enter the name of the WebSphere cluster containing the application server.

Default for all platforms is MAXIMOCLUSTER.

The cluster name is optional. The cluster and application server will be created if they do not exist.

16. From the Security panel, indicate application server security should not be enabled automatically, and then click **Next**. You'll be prompted to manually configure security.

Use the default schema.

Leave this option selected.

Selecting this option indicates that WebSphere Virtual Member Manager has been configured using the default schema supplied with Asset Management for IT with a default Virtual Member Manager base entry, ou=swg,o=IBM,c=us.

If you have elected to supply your own schema for use with Virtual Member Manager, you should deselect this option. You will be required to manually configure Virtual Member Manager to work with

your custom schema and also manually configure the Virtual Member Manager synchronization cron task (see “Synchronizing data” on page 267).

Create the required users.

Leave this option selected.

Selecting this option indicates that you wish to have Asset Management for IT default users created automatically by the Asset Management for IT installation program. You will need write access to Virtual Member Manager.

If you have elected to create users manually, you should deselect this option. Users must be created prior to advancing past the Security panel.

Here is an example of the default add on ldif data you would have to modify and import into your LDAP repository if you elected to customize the schema and create your own users manually.

```
dn: uid=maxadmin,ou=users,ou=SWG, o=ibm,c=us
userPassword: maxadmin
uid: maxadmin
objectClass: inetorgperson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: maxadmin
cn: maxadmin
```

```
dn: uid=mxintadm,ou=users,ou=SWG, o=ibm,c=us
userPassword: mxintadm
uid: mxintadm
objectClass: inetorgperson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: mxintadm
cn: mxintadm
```

```
dn: uid=maxreg,ou=users,ou=SWG, o=ibm,c=us
userPassword: maxreg
uid: maxreg
objectClass: inetorgperson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: maxreg
cn: maxreg
```

```
dn: cn=maxadmin,ou=groups,ou=SWG, o=ibm,c=us
objectClass: groupofnames
objectClass: top
member: uid=dummy
member: uid=maxadmin,ou=users,ou=SWG,o=IBM,c=US
member: uid=mxintadm,ou=users,ou=SWG,o=IBM,c=US
cn: maxadmin
```

```
dn: cn=maximousers,ou=groups,ou=SWG, o=ibm,c=us
objectClass: groupofnames
objectClass: top
member: uid=dummy
member: uid=mxintadm,ou=users,ou=SWG,o=IBM,c=US
member: uid=maxreg,ou=users,ou=SWG,o=IBM,c=US
member: uid=maxadmin,ou=users,ou=SWG,o=IBM,c=US
cn: maximousers
```


Refer to “Synchronizing data” on page 267 for synchronization tasks you will have to complete post installation if you choose to customize your schema.

17. From the Integration Adapter JMS Configuration panel, enter the following information, and then click **Next**:

JMS DataSource name

A JMS server requires a DB2 data repository to be configured to maintain messages. Enter the name of the database to be used by JMS. Default is `intjmsds`.

Select whether the JMS datastore should be persisted.

Persist JMS messages

Select this option if you want the Asset Management for IT installer to set the JMS implementation to persist messages. Refer to “Manually creating a data source for the persistence store” on page 139 for more information.

Do not persist JMS messages

Select this option if you do not want the Asset Management for IT installer to set the JMS implementation to persist messages automatically. If you later decide that you would like to persist JMS messages, you will have to configure the JMS implementation manually.

Attention: The next several steps of this Asset Management for IT installation procedure assume you are allowing the Asset Management for IT installer to configure the JMS implementation to persist messages.

18. From the DB2 Database Server Configuration panel, enter the following information, and then click **Next**.

Note: The JMS data store can only be created as a DB2 database.

Host name

Enter the fully qualified host name of the server hosting the JMS data store.

Port Enter the port used to access the database server.

Default for all platforms is `50000`.

Database name

Enter the name of the database serving as the JMS data store.

Default for all platforms is `maxsibdb`.

User ID

Enter the user ID used to access the database server.

Default for all platforms is `mxsibusr`.

Password

Enter the password for the User ID used to access the database server.

19. From the WebSphere keystore file panel, navigate to where you copied the `trust.p12` keystore, and then click **Next**.
20. From the Run Configuration Step panel, select when you would like to configure Asset Management for IT, and then click **Next**.

Run the configuration step now

Asset Management for IT will be configured when you select this option and press **Next**.

Do not run the configuration step now

You will have to configure Asset Management for IT after you have completed the Asset Management for IT installation task.

The Asset Management for IT installer is used to complete three tasks:

- gathering information on your Asset Management for IT deployment and configuration,
- copying files to your local system,
- performing configuration tasks using the values you have specified

By selecting **Do not run the configuration steps now**, you can instruct the Asset Management for IT installer to gather your configuration information and copy Asset Management for IT files to your local system now, and then allow you to run the configuration step at a later date.

The configuration values that you enter are stored in the *tamit_install_dir*\applications\maximo\properties\maximo.properties file. You can execute the configuration steps outside of the Asset Management for IT installer by using the taskrunner utility, located in the *tamit_install_dir*\scripts directory. Simply run the taskrunner utility from the command line, and it will use the configuration values stored in the maximo.properties file to configure Asset Management for IT.

```
tamit_install_dir\scripts\taskrunner
```

In the event of an installation failure, the taskrunner utility can be run again after the error conditions have been rectified. The taskrunner utility will resume the install at the point where the last successfully completed task was recorded in the previous attempt.

21. From the Choose Shortcut Folder panel, select the type of shortcut you would like to arrange for Asset Management for IT, and then click **Next**.

In a new Program Group

Select this option and enter the name of a new program group if you would like to create Asset Management for IT shortcuts in a new program group.

In an existing Program Group

Select this option and choose the name of an existing program group to store Asset Management for IT shortcuts.

In the Start Menu

Select this option to create shortcuts for Asset Management for IT in the Start menu.

In order to use the Start Menu shortcut in conjunction with Internet Explorer, ensure that you have added the Asset Management for IT URL to the trusted sites Web content zone and disable the option of requiring server verification for all sites in the zone.

On the Desktop

Select this option to create shortcuts for Asset Management for IT on the desktop.

In the Quick Launch Bar

This option should not be used. Do not select this option. Selecting this option will not create a shortcut in the Quick Launch bar.

Other Select this option and use the **Choose...** button to select another location to create Asset Management for IT shortcuts.

Don't create icons

Select this option if you do not want any Asset Management for IT shortcuts created.

Create Icons for All Users

Select this option if you would like Asset Management for IT desktop icons to appear on the desktop for all system users.

22. From the Input Summary panel, review the information you have provided to the Asset Management for IT installer, and then click **Next**.

Use the **Previous** button to return to previous panels to make any changes.

23. From the Pre-Installation Summary panel, review the installation information presented, and then click **Install**. The installation task will begin. Progress can be monitored by viewing messages displayed above the progress bar.
24. From the Install Complete panel, click **Done**.

What to do next

Once the Asset Management for IT installation program has completed installation and configuration tasks, it will exit. Logs can be found at *tamit_install_dir/logs*.

Chapter 8. Installing IBM Tivoli Asset Management for IT language pack



This procedure provides task information for installing the IBM Tivoli Asset Management for IT language pack.

If you choose to install Asset Management for IT with manual WebSphere Application Server configuration, follow the procedures described in “Installing and refreshing language support files for a package” on page 261 and “Installing language packs with Process Solution Installer” on page 155.

Related concepts

“Installing and refreshing language support files for a package” on page 261

A process solution package might define one or more language support features.

“Planning language support” on page 20

Language support refers to the languages you plan to support in the product user interface.

Installing IBM Tivoli Asset Management for IT language pack with the Launchpad

After you installed Tivoli Asset Management for IT, set the Maximo language. Tivoli Asset Management for IT installation program does not install languages, so you need to add them.

Before you begin

Because language pack installation can take several hours to complete, decide which additional languages you need prior to starting installation. Each additional language selected increases the amount of time to complete the installation. Also, do not add as an additional language the language you select as your base. This is not necessary and only increases the installation time.

Important:

- MXServer must be started prior to running the Asset Management for IT language pack installation.
- If you plan to add language support to Asset Management for IT, use the Asset Management for IT language pack installation **before** you perform post installation steps described in Chapter 17, “IBM Tivoli Asset Management for IT post installation tasks,” on page 221.

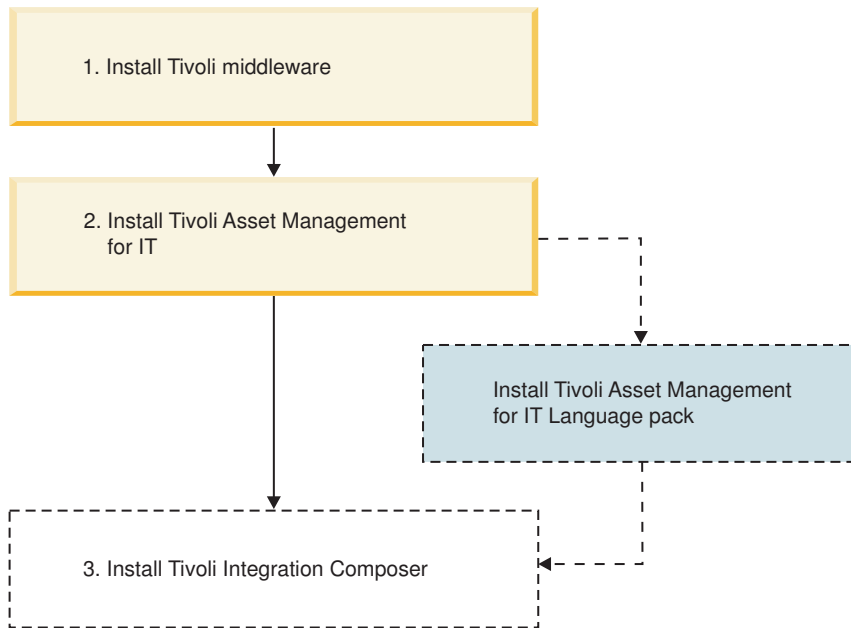


Figure 6. Asset Management for IT installation flow- Installing Asset Management for IT language pack.

About this task

To use the Asset Management for IT language pack installation program to install the Asset Management for IT language pack, complete the following steps:

1. Ensure all Asset Management for IT middleware servers and services are running. If you encounter a failure resulting from an inactive the middleware server or service, start that server or service, and then rerun the language pack installation program. The language pack installation program first uninstalls the base and additional languages installed by the process solution installation wizard from the failed installation attempt, and perform a reinstall.
2. Login as Administrator on the Asset Management for IT administrative system.
3. On the Launchpad, click the **Asset Management for IT Language Pack Installer** link under 2.
4. Select a language for the install, and then click **OK**. This choice is only for use during the installation and its selection will not affect the languages being installed.
5. From the Welcome panel, click **Next**.
6. From the Base Language panel, select a base language that is to be used with Asset Management for IT, and then click **Next**.
Attention: This is the only opportunity you can select a base language. You cannot change the base language at a later time.
7. From the Additional language selection panel, select 0 or more additional languages to be supported, and then click **Next**. You are not prevented from selecting the language you specified in the Base Language panel as an Additional Language. While no error will occur during installation, in practice, do not specify the base language as an additional language. Doing so would be redundant.
8. From the language selection summary panel, review the information and then click **Next**.
9. From the Pre-install Summary Panel, click **Install**.

Results

Even if you added additional languages through the language pack installation program, and you set the locale of your computer to a language that was installed as an additional language, you might still encounter instances in the Asset Management for IT user interface where items are displayed in the language you identified as the base language of the computer. This problem is a known limitation and does not indicate that the Asset Management for IT language pack installation failed.

In some cases, shortcut elements appearing in the Asset Management for IT user interface, for example, menu choices, only display in the base language designated or in English only.

Installing language packs with Process Solution Installer

The Process Solution Installer guides you through the installation of a process manager product (PMP) or Integration Module. Use the Process Solution Installer to refresh languages to synchronize them with Maximo languages.

Before you begin

If you have run the language pack installation, you have Maximo languages set. The next step is to refresh languages on newly created IBM Tivoli Asset Management for IT 7.2.

About this task

Note: Perform this task *after* you installed Asset Management for IT and Integration Composer. To pick up language packs for Asset Management for IT and Integration Composer, install **ITIC_PMP_7.2.0.zip** and **TAMIT_ENG_7.2.0.zip** packages *again*, after running the launchpad.

To install additional languages with Process Solution Installer, launch the Process Solution Installer and follow the instructions on the consecutive windows. In the Choose PSI Package window, you are prompted to choose PMP archive files.

By default, the packages are located in the C:/IBM/SMP/pmp directory.

To choose and install *any* PSI package, perform these steps:

1. On the Administrative workstation, launch the Process Solution Installer (PSI): Click **Start** → **Programs** → **IBM Tivoli base services** → **Process Solution Installer**.
2. Select a language for your installation, and then click **OK**.
3. On the Introduction panel, click **Next**.
4. On the Choose PSI Package panel, click **Choose** and:
 - a. Navigate to the temporary directory where you downloaded and uncompressed the fix pack.
 - b. Select a PSI archive package and click **Open**.
5. On the Package Validation Results panel, review and verify the information displayed, and then click **Next**.
6. On the Middleware Login Information panel, enter the credentials for which you are being prompted, and then click **Next**.

The contents of this panel are constructed dynamically, depending on the type of package you are installing. The package is queried to determine which middleware login credentials are necessary to complete the installation of the package.

After you enter the requested user IDs and passwords, the Process Solution Installer validates the credentials by connecting to the middleware servers using the supplied credentials.

7. After the credentials have been verified, a package options panel is displayed that details the deployment options that the package supports.

Note: When installing any of the fix pack PSI packages using PSI, the updatedb step cannot be deferred. *DO NOT* select the option to **Defer the Upgrade of the Maximo Database**.

After you specify which options will be used, the Process Solution Installer performs a system check to ensure that all system requirements necessary for the package to be installed are present. Click **Next**.

8. On the "Pre-Install Summary" panel, review and verify the information displayed, and then click **Next**. The Process Solution Installer begins installing the PSI package. A progress panel informs you of the progress of the deployment. When the installation is complete, the Package Successfully Deployed panel is displayed. Click **Next**.
9. On the Install Another Package panel, do one of the following:
 - If you want to install another PSI package, select **Install Another Package?** and click **Done**. Then repeat the preceding steps of this procedure, starting with 4 on page 155.
 - If you are finished installing PSI packages, deselect **Install Another Package?** and click **Done** to exit the Process Solution Installer.

Related concepts

"Planning language support" on page 20

Language support refers to the languages you plan to support in the product user interface.

"Process solution package installation methods" on page 232

Included within Asset Management for IT are common installation programs that provide you with the ability to manage the software lifecycle of Asset Management for IT process solutions, including functions to query, install, upgrade, and uninstall process solution packages. These common installation programs are collectively referred to as the *process solution installation programs*.

Chapter 9. Installing IBM Tivoli Asset Management for IT middleware on Linux on System z

Linux Using the native installation program for IBM Tivoli Asset Management for IT product middleware, you could install middleware manually in the order shown above if you choose to deploy Asset Management for IT in an environment where Linux on System z systems will host the Asset Management for IT middleware.

Before you begin

The Asset Management for IT product package includes installation images for the following middleware products:

- IBM DB2 9.5
- IBM Tivoli Directory Server 6.2

If you have existing DB2 and Microsoft Active Directory instances at the appropriate level in your network, you can also reuse those resources in your installation deployment.

The Directory Server uses DB2 as its data repository, while WebSphere Application Server uses the Directory Server for security.

You will need to copy the images off of the product media provided and uncompress them onto your system.

Installing and configuring DB2 on Linux on System z

Use this information to successfully install and configure DB2 on Linux on System z.

Before you begin

To install IBM DB2 on Linux on System z, certain operating system, hardware, and communications prerequisites must be met. Before you start the DB2 Setup wizard, consider the following:

- Refer to the relevant information for installing DB2 on Linux at the DB2 Enterprise Server Edition Information Center:
<http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp>
- Ensure that your system meets installation, memory, and disk requirements. Refer to the DB2 Enterprise Server Edition Information Center to ensure you meet all hardware and software prerequisites.
- You must have root authority to perform the installation.
- The DB2 product image must be available. If the DVD does not automount, mount your “Tivoli Asset Management for IT 7.2 Middleware for Linux on System z” product DVD.
- The DB2 Setup wizard is a graphical installer (Available only on Linux for x86 and Linux on AMD 64/EM64T.). You must have X windows software capable of rendering a graphical user interface for the DB2 Setup wizard to run on your

computer. Ensure that the X windows server is running. Ensure that you have properly exported your display. For example, export `DISPLAY=your_ip_address:0`.

- (DB2 Clients only) If you plan to use Kerberos Authentication, you require IBM Network Authentication Service (NAS) client version 1.4 or higher. The NAS client can be downloaded from:
`https://www6.software.ibm.com/dl/dm/dm-nas-p`
- One of the following browsers is required to view online help and to run First Steps (db2fs):
 - Mozilla 1.4 and up
 - Firefox 1.0 and up
 - Netscape 7.0 and up

The use of XML features is restricted to a database that is defined with the code set UTF-8 and has only one database partition.

About this task

The DB2 Setup wizard is used to define your installation preferences and to install your DB2 product on your system. Features include:

- A Launchpad from which you can view installation notes and release notes, and learn about IBM DB2 9.x features.
- Selecting DB2 installation type (typical, compact, or custom).
- Selecting DB2 product installation location (*db2_install_dir*).
- Setting up database partitioning options for the DB2 instance.
- Setting the user interface and product messages. The user interface and product messages are available in several languages and are installed in the languages that you choose. By installing multiple languages, you can view the interface and messages in your preferred languages.
- Setting up the DB2 Administration Server (including DAS user setup).
- Setting up Administration contact and health monitor notification.
- Setting up and configuring your instance setup and configuration (including instance user setup).
- Preparing the DB2 tools catalog.
- Creating response files.

Installation help is available from the DB2 Setup wizard installation panels to guide you through the steps. To invoke the installation help, click Help or press F1. You can click **Cancel** at any time to end the installation. Your DB2 product will be installed, by default, in the `/opt/IBM/db2/V9.5` directory.

The installation logs, `db2setup.log` and `db2setup.err` will be located, by default, in the `/tmp` directory. You can specify the location of the log files.

The `db2setup.log` file captures all DB2 installation information including errors. The `db2setup.err` file captures any error output that is returned by Java (for example, exceptions and trap information).

To install DB2 on Linux on System z, follow these steps:

1. Log in as root.

2. Create a user (recommended value is maximo with a password of maximo) on the system and assign the new user to a group with administrative authority.
3. Insert the "Tivoli Asset Management for IT 7.2 Middleware for Linux on System z" DVD in your DVD-ROM drive.
4. Change directory to linux390\DB2-ESE_9.5.0 on the DVD.
5. Copy the DB2_Enterprise_Svr_Ed_Linux_zSeries.tar file down to a local directory on your system.
6. Unpack the file:

```
tar -xvf DB2_Enterprise_Svr_Ed_Linux_zSeries.tar
```
7. Type ./db2setup to start the DB2 Setup wizard. The IBM DB2 Setup Launchpad opens. From this window, you can view installation prerequisites and the release notes, or you can proceed directly to the installation. You might want to review the installation prerequisites and release notes for late-breaking information.
8. Click **Install a Product**. The Install a Product window will display the products available for installation.
9. Launch the DB2 Enterprise Server Edition installation by clicking **Install New**. The Welcome to DB2 setup wizard panel is displayed.
10. Click **Next**. The Software License Agreement panel is displayed.
11. Review the license agreement displayed, select **Accept**, and then click **Next**. The Select the installation type panel is displayed.
12. Select **Typical: 410 - 500 MB**, and then click **Next**. The Selection installation, response file creation, or both panel is displayed.
13. Select **Install DB2 Enterprise Server Edition on this computer and save my settings in a response file**. You will need to enter a location and file name to store response file values.
14. Enter a path and file name for the response file, and then click **Next**. The Select the installation directory panel is displayed.
15. Provide the following information, and then click **Next**.

Directory (*db2_install_dir*)

Designate a directory for installing DB2.

By default, this path is /opt/IBM/db2/V9.5.

The Set user information for the DB2 Administration Server panel is displayed.

16. Provide the following information, and then click **Next**.

New user

Select **New user** to enable the fields for creating a new DB2 user.

User name

Enter a user name to associate with the DB2 administration server. The user name should consist of 1 - 8 characters.

The default is dasusr1.

The user name should have SYSADM authority so it can start and stop instances.

UID Leave **Use default UID** checked to have the installation program generate a UID for the user.

Group name

Enter a primary group for the user. If it does not already exist on the system, it will be created.

The default is dasadm1.

GID Leave **Use default GID** checked to have the installation program generate a GID for the group.

Password

Create a password for the user. The password should consist of 1 - 8 characters

Home directory

Enter a directory to use for storing information on the database instance.

The default is /home/dasusr1.

The Set up a DB2 instance panel is displayed.

17. Select **Create a DB2 instance**, and then click **Next**. The Set up partitioning options for the DB2 instance panel is displayed.
18. Select **Single partition instance**, and then click **Next**. If you wish to set up the DB2 instance across multiple partitions, refer to the installation wizard panel help by using the F1 function key. The Set user information for the DB2 instance owner panel is displayed.
19. Provide the following information, and then click **Next**.

New user

Select **New user** to enable the fields for creating a new DB2 user.

User name

Enter a user name to associate with the DB2 instance. The user name should consist of 1 - 8 characters.

The default is ctginst1.

The user name should have SYSADM authority so it can start and stop instances.

UID Leave **Use default UID** checked to have the installation program generate a UID for the user.

Group name

Enter a primary group for the user. If it does not already exist on the system, it will be created.

The default for UNIX is db2grp1.

GID Leave **Use default GID** checked to have the installation program generate a GID for the group.

Password

Create a password for the user. The password should consist of 1 - 8 characters

Home directory

Enter a directory to use as the home directory of the database instance user.

The default is /home/ctginst1.

The Set user information for the fenced user panel is displayed.

20. Provide the following information, and then click **Next**.

New user

Select **New user** to enable the fields for creating a new DB2 user.

User name

Enter a user name to assign as the fenced user. The user name should consist of 1 - 8 characters.

The default is db2fenc1.

The user name should have SYSADM authority so it can start and stop instances.

- UID** Leave **Use default UID** checked to have the installation program generate a UID for the user.

Group name

Enter a primary group for the user. If it does not already exist on the system, it will be created.

The default is db2fgrp1.

- GID** Leave **Use default GID** checked to have the installation program generate a GID for the group.

Password

Create a password for the user. The password should consist of 1 - 8 characters

Home directory

Enter a directory to use as the home directory of the fenced user.

The default is /home/db2fenc1.

The Prepare the DB2 tools catalog panel is displayed.

21. Select **Do not prepare the DB2 tools catalog**, and then click **Next**. If you wish to set up the DB2 tools catalog, refer to the installation wizard panel help for more information by using the F1 function key. The Set up notifications panel is displayed.
22. Select **Set up your DB2 server to send notifications**, provide the following information, and then click **Next**.

Notification SMTP server

Enter the name of the SMTP server that will be responsible for sending database notifications to the database administrator.

Administration contact list location

Local Select **Local** to create a contact list on the local computer.

Remote

Select **Remote** and then provide the fully qualified name of the remote DB2 server to use an existing contact list that will be used remotely.

The Specify a contact for the health monitor notification panel is displayed.

23. Select **New contact**, provide the following information, and then click **Next**.

Name

Enter the user name of the individual assigned to receive notifications related to the state of the DB2 instance

The default is ctginst1.

E-mail address

Enter the e-mail address for the contact entered in the **Name** field.

The Start copying files and create response file panel is displayed.

24. Click **Finish** to initiate the installation.
25. After successfully completing the DB2 installation, install DB2 fix pack.
 - a. Change directory to linux390\DB2-Universal_9.5_Fixpacks on the Linux on System z Middleware DVD.
 - b. Copy the v9fp2_linux390_universal_fixpack.tar.gz file down to a local directory on your system.
 - c. Uncompress the file:
`gzip -dfv v9fpx_linux390_universal_fixpack.tar.gz`
 - d. Unpack the file:
`tar -xvf v9fp2_linux390_universal_fixpack.tar`
 - e. cd to universal/disk1 then run `./installFixPack` to start the Fix Pack installation.
 - f. When prompted, enter the install location of DB2.
 - g. After the fix pack installation has concluded, stop all instances associated with this copy.
`su - db2inst1 db2stop`
 - h. Run update:
`db2_install_dir/instance/db2iupdt -e`
26. Start the DB2 instances.

Installing and configuring IBM Tivoli Directory Server on Linux on System z

Use this information to successfully install and configure IBM Tivoli Directory Server on Linux on System z

Before you begin

There are two installation paths used in the Directory Server installation program.

Typical

Use the *Typical* installation path if you want to accept default settings, install the Directory Server components that are not already installed, and create a default directory server instance. Typical installation does not allow you to select features for installation.

Custom

Use the *Custom* installation path if you want to select components for installation and create a directory server instance using the Instance Administration Tool. When you use this tool you can customize the directory server instance.

For more information on reusing an existing DB2 server for use with Directory Server, consult the Directory Server product information for conducting an Directory Server custom installation. Note that Directory Server cannot make use of a remote DB2 server as its data repository. Also, Asset Management for IT is not designed to interact with a system that has two different active copies of DB2 running at the same time, so plan accordingly when you are designing your Asset Management for IT deployment.

About this task

To install Directory Server 6.2 using the Custom installation path, follow these steps:

1. Log in as root.
2. Insert the “Tivoli Asset Management for IT Middleware for zLinux” DVD in your DVD-ROM drive.
3. Change directory to linux390 on the DVD.
4. Copy the tds6.2-linux-s390x-CD1_w_entitlement.tar file down to a local directory on your system.
5. Unpack the file:

```
tar -xvf tds6.2
-linux-s390x-CD1_w_entitlement.tar
```
6. Change to the /tdsV6.2/tds directory and then type ./install_tds.sh If you prefer, you can specify a temporary directory other than the system temporary directory. To use this option, change directories to the appropriate directory and type ./install_tds.sh -is:tempdir *directory* at a command prompt, where *directory* is the directory you want to use for temporary space. Be sure that you have at least 400 MB of free space in this directory. For example:
./install_tds.sh -is:tempdir /opt/tmp The Select Language panel is displayed.
7. Select the language you want to use during the Directory Server installation, and then click **OK**. This is the language used in the installation program, not in Directory Server. The language used in Directory Server is determined by the language pack you install. The Welcome panel is displayed.
8. Click **Next**. The License Agreement panel is displayed.
9. Read the software license agreement, select **I accept both the IBM and the non-IBM terms**, and then click **Next**.
10. Select **Custom** and then click **Next**.
11. De-select **DB2 V9.5, Embedded WebSphere Application Server, and Tivoli Directory Integrator**, and then click **Next**. You will install the products separately. The Select WebSphere Application Server panel is displayed.
12. Select **Do not specify. I will manually deploy at a later time**, and then click **Next**. The Summary panel is displayed.
13. Click **Install**. Directory Server will be installed into the /opt/IBM/ldap/V6.2 directory.
14. Click **Finish**. The Directory Server instance creation tool will now launch.
15. Create the idscmdb ITDS instance. Refer to “Manually configuring IBM Tivoli Directory Server” on page 118 for more information.
16. Start Directory Server.

```
/opt/IBM/ldap/V6.2/sbin/idsdiradm -I idscmdb
/opt/IBM/ldap/V6.2/sbin/ibmslapd -I idscmdb
```

Installing and configuring WebSphere Application Server Deployment Manager on Linux on System z

Use this information to successfully install and configure WebSphere Application Server Deployment Manager on Linux on System z.

About this task

To install WebSphere Application Server Deployment Manager, follow these steps:

1. Log in as root.
2. Insert the “Tivoli Asset Management for IT 7.2 Middleware for Linux on System z” DVD in your DVD-ROM drive.
3. Change directory to `linux390/WS-WAS_ND_6.1.0.23_Custom_ISCAE7.1` on the DVD.
4. Copy the `WAS-ND_linux390_Custom_v6.113.tar.gz` file down to a local directory on your system.
5. Uncompress the file:

```
gzip -dfv WAS-ND_linux390x_Custom_v6.123.tar.gz
```
6. Unpack the file:

```
tar -xvf WAS-ND_linux390x_Custom_v6.123.tar
```
7. Enter the `./install` command from the WebSphere Application Server directory, `/WAS`, for example, where you unpacked the tar file to start the WebSphere Application Server Setup wizard. The Welcome to the IBM WebSphere Application Server Network Deployment install wizard panel is displayed.
8. Click **Next**. The Software License Agreement panel is displayed.
9. Review the license agreement displayed, select **Accept**, and then click **Next**. The Prerequisite Check panel is displayed.
10. Confirm that your operating system is supported and that you have installed all necessary patches, and then click **Next**. The Installation Directory panel is displayed.
11. Enter the installation path for WebSphere Application Server Network Deployment, and then click **Next**. The default is `/opt/IBM/WebSphere/AppServer`. Do not use symbolic links as the destination directory. Symbolic links are not supported. Spaces are not supported in the name of the installation directory. The WebSphere Application Server Environments panel is displayed.
12. Select **None** as your environment, and then click **Next**. Selecting **None** means you will be creating the Asset Management for IT deployment cell, deployment manager profile, and the application server profile using the profile management tool.
13. Click **Yes** to indicate that you want to proceed. The Installation Summary panel is displayed.
14. Click **Next**. The Installation Results panel is displayed.
15. Click **Finish**.

Creating profiles using 64-bit WebSphere Application Server Deployment Manager for Linux on System z

Use this information to successfully create profiles using 64-bit WebSphere Application Server Deployment Manager for Linux on System z.

Before you begin

This section provides instructions for creating two profiles that will be expected by the Tivoli Asset Management for IT installation program.

To create 64-bit WebSphere Application Server Deployment Manager profiles on your Linux on System z, the following prerequisite tasks must first be completed:

Table 17. Prerequisite Tasks and their Commands

Prerequisite Task	Command
Augment the ctgDmgr01 profile.	<code>was_install_dir/bin/manageprofiles.sh -augment -templatePath was_install_dir/ profileTemplates/iscae7.1 -profileName ctgDmgr01 -serverName dmgr</code>
Restart servers after augmenting the ctgDmgr01 profile.	<code>was_install_dir/profiles/ctgDmgr01/bin/ stopManager.sh -username <username> -password password was_install_dir/profiles/ctgDmgr01/bin/ startManager.sh</code>

The 64-bit version of WebSphere Application Server Network Deployment for Linux on System z includes the *manageprofiles* command line tool which you will use to create profiles required by Asset Management for IT.

The following commands can be useful for managing profiles:

Table 18. Profile commands

Task	Command
Delete a profile	<code>was_install_dir/bin/manageprofiles.sh -delete -profileName profile_name</code>
Refresh the profile registry (for example, after deleting a profile)	<code>was_install_dir/bin/manageprofiles.sh -validateAndUpdateRegistry</code>
List existing profiles	<code>was_install_dir/bin/manageprofiles.sh -listProfiles</code>

About this task

To create profiles, follow these steps:

1. Source the `setupCmdLine.sh` script in the `bin` directory of the `was_install_dir` folder to set the WebSphere Application Server environment to the configuration instance. `was_install_dir/bin/setupCmdLine.sh`
2. Create a profile ports file for the `ctgDmgr01` profile. This file will be used by the `manageprofiles` command to set the ports that will be used by this profile. It is important that you ensure no spaces appear after any value in this file. If there is an extra space trailing any of the values, as can happen when cutting and pasting an example, WebSphere will use that space as the last character of that value. For example, you might intend the value `"WC_adminhost=9060"`, but with an extra space, that value will be `"WC_adminhost=9060<sp>"` where `<sp>` denotes a blank space.
 - a. Create a new text file named `_portdef_DMgr.props` and enter the following text:

```
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9403
WC_adminhost=9060
DCS_UNICAST_ADDRESS=9352
BOOTSTRAP_ADDRESS=9809
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9401
CELL_DISCOVERY_ADDRESS=7277
SOAP_CONNECTOR_ADDRESS=8879
```

```
ORB_LISTENER_ADDRESS=9100
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9402
WC_adminhost_secure=9043
```

- b. Place the file in the *was_install_dir* directory.
3. Create the ctgDmgr01 profile using the manageprofiles command:
was_install_dir/bin/manageprofiles.sh
-create
-templatePath *was_install_dir/profileTemplates/dmgr*
-hostName *yourfullyqualifiedhost*
-profileName ctgDmgr01
-profilePath *was_install_dir/profiles/ctgDmgr01*
-portsFile *was_install_dir/_portdef_DMGr.props*
-cellName ctgCell01
-nodeName ctgCellManager01
-enableAdminSecurity "false"
-adminUserName wasadmin
-adminPassword wasadmin
4. Start the ctgDmgr01 server:
was_install_dir/profiles/ctgDmgr01/bin/startManager.sh
5. Create a profile ports file for the ctgAppSrv01 profile. This file will be used by the manageprofiles command to set the ports that will be used by this profile.
 - a. Create a new text file named *_portdef_AppSvr.props* and enter the following text:
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9201
DCS_UNICAST_ADDRESS=9353
NODE_DISCOVERY_ADDRESS=7272
NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=5001
BOOTSTRAP_ADDRESS=2809
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9901
SOAP_CONNECTOR_ADDRESS=8878
NODE_MULTICAST_DISCOVERY_ADDRESS=5000
ORB_LISTENER_ADDRESS=9101
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9202
 - b. Place the file in the *was_install_dir* directory.
6. Create the ctgAppSrv01 profile using the manageprofiles command:
was_install_dir/bin/manageprofiles.sh
-create
-templatePath *was_install_dir/profileTemplates/managed*
-hostName *yourfullyqualifiedhost*
-profileName ctgAppSrv01
-profilePath *was_install_dir/profiles/ctgAppSrv01*
-cellName ctgNodeCell01
-nodeName ctgNode01
-portsFile *was_install_dir/_portdef_AppSvr.props*
-dmgrHost *yourfullyqualifiedhost*
-dmgrAdminUserName wasadmin
-dmgrAdminPassword wasadmin
-dmgrPort 8879
-isDefault
7. If it is not already started, start the ctgAppSrv01 node.
was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh
8. Launch firststeps.sh to verify installation:
was_install_dir/profiles/ctgDmgr01/firststeps/firststeps.sh

Installing and configuring IBM HTTP Server on Linux on System z

Use this information to successfully install and configure IBM HTTP Server on Linux on System z.

About this task

To install IBM HTTP Server, follow these steps:

1. Log in as root on the computer where you have installed WebSphere Application Server.
2. Log into the WebSphere Administrative Console and ensure the ctgDmgr01 deployment manager is running and the SOAP port is set to listen at the correct port (8879 is the default). If the deployment manager needs to be started, use the following command:
`was_install_dir/profiles/ctgDmgr01/bin/startManager.sh`
3. From a command line, launch the HTTP Server installation program:
`was_image_directory/IHS/install`
The Welcome panel is displayed.
4. Click **Next**. The License Agreement panel is displayed.
5. Accept the license agreement and click **Next** System prerequisites check panel is displayed.
6. Click **Next**.
7. Specify the install location information and click **Next**. The default is `/opt/IBM/HTTPServer`. The Port Values Assignment panel is displayed.
8. Specify the following values and then click **Next**.

HTTP Port

80

HTTP Administration Port

8008

The Setup HTTP Administration Server panel is displayed.

9. Create a User ID for the HTTP administration server authentication and click **Next**.
10. Specify the following values, and click **Next**.

Setup IBM HTTP administration server to administer IBM HTTP Server
Enabled

Create a unique user ID and group for IBM HTTP Server administration
Enabled

User ID
wasadmin

Group ihsadmin

The IBM HTTP Server Plug-in for WebSphere Application Server panel is displayed.

11. Specify the following values, and click **Next**.

Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server
Disable

In an environment where you have multiple deployment manager profiles, it is more practical to run the Web server plug-ins installation task separately by running the plug-in installation program after exiting the HTTP server installation program. However, if your WebSphere Application Server environment only contains the single deployment manager profile used for Asset Management for IT, you can leave the WebSphere Application Server plug-in option selected, which will launch the Web server plug-ins installation task when you click **Next**.

The Installation Summary panel is displayed.

12. Click **Next**.
13. Click **Finish**.
14. Install the following HTTP Server fix pack: linux390\WS-WAS_IHS_6.1.0_FP13\6.1.0-WS-IHS-LinuxS39064-FP0000013.pak

What to do next

For more information on deployment scenarios for IBM HTTP Server, refer to http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/welcome_ihs.html

Installing and configuring the WebSphere plug-in on Linux on System

z

Use this information to successfully install and configure the WebSphere Application Server plug-in on Linux on System z.

About this task

To install the WebSphere Application Server plug-in, follow these steps:

1. Log in as root on the computer where you have installed WebSphere Application Server.
2. From a command line, launch the WebSphere Application Server plug-in installation program:

```
was_image_directory/plugin/install
```

The Welcome panel is displayed.
3. Click **Next**.
The License Agreement panel is displayed.
4. Accept the license agreement and click **Next**.
5. From the system check panel, click **Next**.
6. Select **WebSphere Application Server machine (local)**, and then click **Next**.
The Web server install path panel is displayed.
7. Browse to the directory where you installed the HTTP server, and then click **Next**. By default, this directory is listed as `/opt/IBM/HTTPServer/Plugins`.
The WebSphere Application Server install path panel is displayed.
8. Browse to the directory where you installed WebSphere Application Server (`was_install_dir`), and then click **Next**. By default, this directory is listed as `/opt/IBM/WebSphere/AppServer`.
The select profile panel is displayed.

9. Select **ctgDmgr01** from the drop-down list, and then click **Next**. The Web server configuration file panel is displayed.

10. Specify the following:

Select the existing IBM HTTP Server httpd.conf file

Browse to the location of the httpd.conf file. By default, this file is located at /opt/IBM/HTTPServer/conf/httpd.conf.

Specify the Web server port

80

The Web server definition panel is displayed.

11. Specify a unique Web server definition name (webserver1, for example), and then click **Next**. The Web server plugin-cfg.xml file panel is displayed.

12. Accept the default, and click **Next**. The input summary panel is displayed.

13. Click **Next**. The installation summary panel is displayed.

14. When the installation is complete, click **Finish**.

15. Install the following WebSphere Application Server plug-in fix pack:

linux390\WS-WAS_Plugins_6.1.0_FP23\6.1.0-WS-PLG-LinuxS39064-FP0000023.pak

16. Restart deployment manager:

Stop the deployment manager

was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh

Start the deployment manager

was_install_dir/profiles/ctgDmgr01/bin/startManager.sh

17. Copy the /opt/IBM/HTTPServer/Plugins/bin/configurewebserver1.sh file to *was_install_dir*/bin/ directory.

18. Change directory to *was_install_dir*/bin and then execute the following command:

./configurewebserver1.sh

19. Start the HTTP servers:

/opt/IBM/HTTPServer/bin/adminctl start
/opt/IBM/HTTPServer/bin/apachectl start

20. Login to the WebSphere Administrative Console and ensure that webserver1 has started.

Installing and configuring Virtual Member Manager on WebSphere on Linux on System z

Use this information to successfully install and configure Virtual Member Manager on WebSphere on Linux on System z.

About this task

Virtual Member Manager (VMM) provides you with the ability to access and maintain user data in multiple repositories, and federate that data into a single virtual repository.

Refer to “Manually configuring Virtual Member Manager on IBM WebSphere Application Server” on page 128 for information on adding an IBM Tivoli Directory Server repository to Virtual Member Manager.

Chapter 10. Installing middleware on Solaris and HP-UX

Middleware versions that are not installable by the middleware installer program are installed by using graphical installation programs that are provided with each middleware product. The procedures described in this section can be used to manually install the following products on Solaris and HP-UX.

Solaris 10 SPARC and HP-UX 11i v2 64 bit

- IBM DB2 Enterprise Server Edition 9.5 with fix pack 3a
- IBM Tivoli Directory Server 6.2 fix pack 1
- WebSphere Application Server Network Deployment 6.1 with fix pack 23
- IBM HTTP Server 6.1 with fix pack 23

Operating system preparation

Some operating system default configuration settings must be change to provide an environment that can host middleware operations.

The steps needed to prepare each newly supported operating system are operating system dependent.

Perform the operating system preparation steps before installing any middleware.

Solaris 10

Some of the default kernel configuration parameters on Solaris 10 might not be sufficient to run IBM DB2 9.5.

In order to ensure your Solaris system has required kernel parameters in place, you will need to run the `db2osconf` utility after you install IBM DB2, but before you create any database objects. See <http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp> for information.

HP-UX 11i

In order for IBM DB2 9.5 to run correctly on HP-UX 11i, certain group membership requirements must be addressed following the installation of IBM DB2.

After IBM DB2 9.5 has been installed, you must ensure that the root user has been assigned as a member of the `db2iadm1` group.

Installing the components

After the operating system is configured as needed, install the middleware components.

Middleware components are installed in the following order:

1. IBM DB2
2. IBM Tivoli Directory Server
3. IBM WebSphere Network Deployment
4. IBM HTTP Server

Note: The media or Web site you use to install middleware has directory-specific locations for each supported operating system. The directory structure is `/Middleware/os/product`.

The command following displays the top level directories under the Middleware directory.

```
ls -m Middleware
```

Within each Middleware subdirectory (the `os` directory) are the installation directories for each middleware product.

```
ls Middleware/solaris
DB2_ESE_V95_SUN_SPARC,
v9.5fp3a_sun64_server,
TIV-DirectoryServer_6.2.0,
TIV-DirectoryServer_6.2.0_FP0002,
WS-ESS_6.1_GA,
WS-WAS_IHS_6.1.0_FP23,
WS-WAS_ND_6.1.0.23_Custom_ISCAE71,
WS-WAS_ND_6.1.0_Supplemental_64bit,
WS-WAS_Plugins_6.1.0_FP23,
WS-WAS_UpdateInstaller_6.1.0_FP23
```

Installing DB2

Run the `db2setup` program to install DB2.

Before you begin

Before you install DB2, review the requirements. See the DB2 information center at <http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp> for operating system-specific information.

There are a number of things you must check to ensure a successful installation. Before you start the DB2 setup wizard, consider the following:

- `db2setup` launches a wizard installer so X Window must be installed and running before you start the DB2 installer program. Export your display:
`export DISPLAY= your_ip_address:0`
- If NIS, NIS+, or similar security software is used in your environment, you must manually create the required DB2 users, before you start the DB2 setup wizard. Refer to the centralized user-management considerations topic in the DB2 information center, before you begin. See <http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/topic/com.ibm.db2.luw.qb.server.doc/doc/r0007059.html>
- In general, you can choose to defer some installation activities. For example, if you choose to not set up e-mail notifications of database events at installation time. If you want to defer specific installation activities, select that option, and configure them later.
- Some middleware products have specific requirements or conventions for account names and other settings. Override the installation defaults as shown if the defaults provided are not satisfactory. On panels that prompt for passwords, both the password and its confirmation entry must be specified before the installer can continue to the next panel.

About this task

This procedure describes how to perform a typical installation of DB2 on a single computer. If you need to install DB2 components on multiple computers, see the DB2 information center for those instructions.

Databases must contain a single partition and unicode data (UTF-8).

DB2 is installed, by default, in the `/opt/IBM/db2/V9.5` directory.

The `/opt/IBM/db2/V9.5/logs` directory contains a `db2install.history` file. This file contains the installation settings used, and errors that occurred during the installation process. The `vmrfis.history` file contains information on maintenance that has been applied to DB2, such as fix packs that have been installed.

The `db2setup.log` file captures all DB2 installation information including errors. The `db2setup.err` file captures any error output that is returned by Java (for example, exceptions and trap information). By default, both logs are created in the `/tmp` directory unless you change that location during the installation process.

1. Log in as root.
2. Copy the tar IBM DB2 Enterprise Server Edition tar file to a writable disk.

Solaris For Solaris

Copy `Middleware/solaris/DB2-ESE_9.5/DB2_ESE_V95_SUN_SPARC.tar`

HP-UX For HP-UX

Copy `hpux-ia64/DB2-ESE_9.5/DB2_ESE_V95_HP-UX_IA64.tar`

3. Change to the directory where you copied the tar file and run the following command: `tar -xvf tarFileName.tar`,
4. Extract the file `DB2_Enterp_Svr_OEM_Activation.zip` into an appropriate directory. For example, for Solaris, `solaris64/DB2-ESE_9.5/`
5. Start the installer. Type `./db2setup`.
6. From the Launchpad, select **Install a Product**.
7. Click **Install New**.
8. Accept the license agreement.
9. In general, accept all defaults, except where you must provide custom values. For example, the e-mail address of the recipient of e-mail notifications of database events defaults to `host_name@local_server_name`. This value needs to be changed to a valid e-mail address if you choose to enable SMTP notifications. This value can also be changed at a later time.
10. Leave the check boxes for the **GUI** and **UID** options selected; the system will assign them for you.
11. On the Start copying files and create response file panel, click **Finish** to initiate the installation.
12. Start the DB2 instance.
13. Register the DB2 server license:
 - a. Switch to the instance user:

```
su ctginst1
```
 - b. Use the DB2 license management tool command to apply the license:

```
db2licm -a full_path_to_the_license_file
```

The license file can be found in the appropriate folder for your operating system. For Solaris, the license file is located in solaris64/DB2-ESE_9.5/DB2_Enterp_Svr_OEM_Activation/db2/license/db2ese_o.lic.

- c. Stop and then restart the DB2 instance using the db2stop and db2start commands, respectively.

- d. Verify that the license was installed successfully:

```
db2licm -l
```

This command should result in output similar to the following:

```
Product name:          "DB2 Enterprise Server Edition"
License type:          "Restricted"
Expiry date:           "Permanent"
Product identifier:    "db2ese"
Version information:   "9.5"
```

Installing DB2 fix packs

Installing the fix pack for DB2 ensures that it is up to date with the latest fixes.

Before you begin

Stop all instances of DB2 before installing a fix pack.

1. Log in as root.
2. Run db2ilist to view all instances.
3. Become (su) the instance owner of a DB2 account.
4. Stop each instance, use db2stop *instance_name* for each instance.
1. Copy the fix pack tar file to a writeable disk.

Solaris On Solaris

Copy DB2-ESE_9.5_FP3a/v9.5fp3a_sun64_server.tar.gz

HP-UX On HP-UX

Copy DB2-ESE_9.5_FP3a/v9.5fp3a_hpipf64_server.tar.gz

2. Uncompress the file:

```
gzip -dfv fixpack_name.tar.gz
```
3. Unpack the file:

```
tar -xvf fixpack_name.tar
```
4. Change to the /server directory.
5. To start the fix pack installation, type ./installFixPack -b \$DB2DIR, where \$DB2DIR is the location of the DB2 product that you want to update, for example, /opt/IBM/db2/V9.5.
6. When prompted, enter the installation directory where you installed DB2. The default location is a version-specific directory under /opt/IBM/db2.
7. Run the update command on each instance:

```
db_install_dir/instance_name/db2iupdt -e
```
8. Run the *db_install_dir/instance_name/dasupdt* command.
9. Restart each instance that you stopped before you installed the fix pack.

Installing IBM Tivoli Directory Server

Directory Server is typically installed on a computer that is not hosting other middleware products.

1. Log in as root.

2. Copy the tar files for Directory Server to a writable disk. The files are in the TIV-DirectoryServer_6.2.0 directory.

Solaris For Solaris

Copy the C1N9LML.tar and C1N9QML.tar files from Middleware/solaris/TIV-DirectoryServer_6.2.0.

HP-UX For HP-UX

Copy the C1N9LML.tar and C1N9QML.tar files from Middleware/hpux-ia64/TIV-DirectoryServer_6.2.0

3. Unpack the files:

```
tar -xvf C1N9LML.tar
tar -xvf C1N9QML.tar
```

For HP-UX, you would unpack the C1NC0ML.tar and C1NC4ML.tar files.

4. Change to the /tdsV6.2/tds directory and then type ./install_tds.sh
If you prefer, you can specify a temporary directory other than the system temporary directory. To use this option, change directories to the appropriate directory and type the following at a command prompt:

```
./install_tds.sh -is:tempdir directory
```

where *directory* is the directory you want to use for temporary space. Be sure that you have at least 400MB of free space in this directory. For example:

```
./install_tds.sh -is:tempdir /opt/tmp
```

5. When the installation wizard starts, select a language to use for the installation process, accept the license agreement, and choose a **Custom** installation.
6. Unselect **DB2 V9.1, Embedded WebSphere Application Server, and Tivoli Directory Integrator**, and click **Next**.
You will install these products separately. The following options should be selected: **C Client, Java Client, Web Administration Tool, Proxy Server, Server**
7. From the **Select WebSphere Application Server** panel, select **Do not specify. I will manually deploy at a later time**, then click **Next**.
8. Click **Install**.
9. Click **Finish**.
The IBM Tivoli Directory Server instance creation tool launches.
10. Close the instance creation tool.
11. Create the idscmdb instance. Refer to “Manually configuring IBM Tivoli Directory Server” on page 118 for details. When creating the idscmdb user, include it as a member of the root, db2iadm1, and idslldap groups, where root is the primary group for the idscmdb user.
12. Start the directory server, type the following commands:
 - a. /opt/ibm/ldap/V6.2/sbin/idsdiradm -I idscmdb
 - b. /opt/ibm/ldap/V6.2/sbin/ibmslapd -I idscmdb

Installing WebSphere Application Server Network Deployment

WebSphere Application Server Network Deployment must be installed, and you must create two profiles that will be needed later.

1. Log in as root.

- Copy the WebSphere compressed file to a writable disk. The file is in the `WS-WAS_ND_6.1.0.23_Custom_ISCAE71` directory.

Solaris For Solaris

Copy `WS-WAS_ND_6.1.0.23_Custom_ISCAE71/WAS-ND_Solaris-Sparc-Custom_v6.1023_ISC7106.tar.gz`

HP-UX For HP-UX

Copy `WS-WAS_ND_6.1.0.23_Custom_ISCAE71/WAS-ND_HpuxIA64_Custom_v6.1023_ISC7106.tar.gz`

- Uncompress the file:
`gzip -dfv file_name.gz`
- Unpack the file:
`tar -xvf tar_file_name.tar`
- Remove the tar and gz files.
- Change to the directory where you unpacked the tar file.
- Change to the `was_install_dir` directory.
- Type `./install`
- Accept the license agreement and accept the defaults provided unless you have a specific reason to change them.
- On the Installation directory panel, accept the default installation directory. The default is `/opt/IBM/WebSphere/AppServer`. If you change the installation directory, do not use symbolic links as the destination directory and do not add space characters to the path.
- From the WebSphere Application Server Network Deployment environments panel, select **None** as your environment, and then click **Next**. Selecting **None** means you will be creating the deployment cell, deployment manager profile, and the application server profile using the profile management tool.
- Click **Yes** to indicate that you want to proceed.
- Advance to the end of the installation and click **Finish**.

Creating WebSphere Application Server Network Deployment profiles

The 64-bit version of WebSphere Application Server Network Deployment includes the `manageprofiles` command line tool which you will use to create profiles.

Before you begin

Ensure you are familiar with the character limitations for commands or the shell you are using. In some cases, you might have to enter commands in order to avoid exceeding these limitations. Refer to WebSphere Application Server Network Deployment product documentation for more information about entering lengthy commands on more than one line.

About this task

The following commands can be useful for managing profiles:

Table 19. Profile commands

Task	Command
Delete a profile	<code>was_install_dir/bin/manageprofiles.sh -delete -profileName profile name</code>

Table 19. Profile commands (continued)

Task	Command
Refresh the profile registry (for example, after deleting a profile)	<code>was_install_dir/bin/manageprofiles.sh -validateAndUpdateRegistry</code>
List existing profiles	<code>was_install_dir/bin/manageprofiles.sh -listProfiles</code>

`was_install_dir` is equal to where WebSphere Application Server Network Deployment is installed, for example, `/opt/IBM/WebSphere/AppServer/`.

1. Source the `setupCmdLine.sh` script in the `bin` directory of the `was_install_dir` folder to set the WebSphere Application Server Network Deployment environment to the configuration instance. `was_install_dir` is typically in `/opt/IBM/WebSphere/AppServer`.
`. was_install_dir/bin/setupCmdLine.sh`
2. Create a profile ports file for the `ctgDmgr01` profile. This file will be used on the `manageprofiles` command to set the ports that will be used by this profile.

Note: It is important that you ensure no spaces appear after any value in this file. If there is an extra space trailing any of the values, as can happen when cutting and pasting an example, WebSphere Application Server will use that space as the last character of that value. For example, you might intend to specify the value `WC_adminhost=9060`, but if an extra space is typed after `9060`, the value will be interpreted as `WC_adminhost=9060<sp>` (where `<sp>` represents a space character).

- a. Create a new text file named `_portdef_DMgr.props` and enter the following text:

```
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9403
WC_adminhost=9060
DCS_UNICAST_ADDRESS=9352
BOOTSTRAP_ADDRESS=9809
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9401
CELL_DISCOVERY_ADDRESS=7277
SOAP_CONNECTOR_ADDRESS=8879
ORB_LISTENER_ADDRESS=9100
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9402
WC_adminhost_secure=9043
```

- b. Place the file in the `was_install_dir` directory.

3. Create the `ctgDmgr01` profile using the `manageprofiles` command. Type the following, all on one line, with a space between each entry:

```
was_install_dir/bin/manageprofiles.sh
-create
-templatePath was_install_dir/profileTemplates/dmgr
-hostName yourfullyqualifiedhost
-profileName ctgDmgr01
-profilePath was_install_dir/profiles/ctgDmgr01
-portsFile was_install_dir/_portdef_DMgr.props
-cellName ctgCell01
-nodeName ctgCellManager01
-enableAdminSecurity "false"
```

4. Start the `ctgDmgr01` server:

```
was_install_dir/profiles/ctgDmgr01/bin/startManager.sh
```

5. Create a profile ports file for the `ctgAppSrv01` profile. This file will be used by the `manageprofiles` command to set the ports that will be used by this profile.

- a. Create a new text file named `_portdef_AppSvr.props` and enter the following text:

```
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9201
DCS_UNICAST_ADDRESS=9353
NODE_DISCOVERY_ADDRESS=7272
```

```

NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=5001
BOOTSTRAP_ADDRESS=2809
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9901
SOAP_CONNECTOR_ADDRESS=8878
NODE_MULTICAST_DISCOVERY_ADDRESS=5000
ORB_LISTENER_ADDRESS=9101
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9202

```

- b. Place the file in the *was_install_dir* directory.
6. Create the ctgAppSrv01 profile using the manageprofiles command:

```

was_install_dir/bin/manageprofiles.sh
-create
-templatePath was_install_dir/profileTemplates/managed
-hostName your_fully_qualified_host
-profileName ctgAppSrv01
-profilePath was_install_dir/profiles/ctgAppSrv01
-cellName ctgNodeCell01
-nodeName ctgNode01
-portsFile was_install_dir/portdef_AppSvr.props
-dmgrHost your_fully_qualified_host
-dmgrPort 8879
-isDefault

```
7. Start the ctgAppSrv01 node.

```

was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh

```
8. Augment the ctgDmgr01 profile:

```

was_install_dir/bin/manageprofiles.sh
-augment
-templatePath was_install_dir/profileTemplates/iscae71
-profileName ctgDmgr01
-serverName dmgr

```
9. Restart servers.

```

was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh
was_install_dir/profiles/ctgDmgr01/bin/startManager.sh
was_install_dir/profiles/ctgAppSrv01/bin/stopNode.sh
was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh

```
10. Launch firststeps.sh and select the **Installation Verification** option to confirm that your server has been properly installed and started.

```

was_install_dir/profiles/ctgDmgr01/firststeps/firststeps.sh

```

Installing the WebSphere update installer

This procedure is optional; it can be performed now or later, when you want to use the update installer to apply maintenance. During the initial installation of middleware, maintenance is not applied using the update installer.

Before you begin

Complete documentation for the update installer is at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tins_updi_install.html. Review the prerequisites before installing the update installer.

About this task

The update installer simplifies maintenance of WebSphere Application Server Network Deployment and its related components, such as the HTTP server plug-in and fix packs.

1. Copy the update installer archive file to a writable disk. The file is in the *WS-WAS_UpdateInstaller_7.0.0.3* directory.

Solaris For Solaris

Copy 7.0.0.3-WS-UPDI-SolarisSparc64.zip

HP-UX For HP-UX

Copy 7.0.0.3-WS-UPDI-HpuxIA64.zip

2. Uncompress the file. Type `unzip file_name.zip`
3. Change to the directory containing the uncompressed files and type: `./install`.
4. Accept the license agreement.
5. The default installation directory is `/usr/IBM/WebSphere/UpdateInstaller`. Change this if you need to do so; otherwise accept the default location.
6. Before you finish the installation, uncheck the option to **Launch IBM Update Installer for WebSphere software on exit**.

Installing and configuring IBM HTTP Server

This procedure provides task information for manually installing and configuring IBM HTTP Server.

1. Log on as root, on the machine where you installed WebSphere Application Server Network Deployment.
2. Log into the WebSphere Administrative Console and ensure the `ctgDmgr01` deployment manager is running and that the SOAP port is set to listen at the correct port (8879 is the default).

If the deployment manager needs to be started, use the following command:

```
was_install_dir/profiles/ctgDmgr01/bin/startManager.sh
```

3. Copy the IBM HTTP Server zip file to a writable disk.

Solaris For Solaris

Copy `Middleware/solaris/WS-WAS_ND_6.1.0_Supplemental/C943UML.tar.gz`

HP-UX For HP-UX

Copy `hpux-ia64/WS-WAS_ND_6.1.0_Supplemental\C88TNML.tar.gz`

4. Uncompress the `C943UML.tar.gz` file.
5. Extract the contents of the `C943UML.tar` file.
6. Change to the IBM HTTP Server directory and start the installation program:
`./install`
7. From the Welcome panel, click **Next**.
8. Accept the license agreement and click **Next** to display the installation root directory panel.
9. From the System prerequisites check panel, click **Next**.
10. Specify the install location, the default is `/opt/IBM/HTTPServer`, and click **Next**.
11. From the Port Values Assignment panel, specify the following values, and click **Next**.

HTTP Port

80

HTTP Administration Port

8008

12. From the HTTP Administration Server Authentication panel, specify the following values, and click **Next**.

Create a user ID for IBM HTTP administration server authentication

Enable this option by selecting this check box.

User ID

Specify wasadmin

Password

Enter the password for the wasadmin user.

13. From the Setup HTTP Administration Server panel, specify the following values, and click **Next**.

Setup IBM HTTP administration server to administer IBM HTTP Server

Enable this option by selecting this check box.

Create a unique user ID and group for IBM HTTP Server administration

Enable this option by selecting this check box.

User ID

Specify wasadmin.

Group Specify ihsadmin

14. From the IBM HTTP Server Plug-in for WebSphere Application Server panel, specify the following values, and click **Next**.

Install the IBM HTTP Server Plug-in for IBM WebSphere Application

Server Enable or clear this check box to disable this option as is appropriate for your configuration. In an environment where you have multiple deployment manager profiles, it is more practical to run the Web server plug-ins installation task separately by running the plug-in installation program after exiting the IBM HTTP Server installation program. However, if your WebSphere Application Server environment only contains a single deployment manager profile, you can leave the WebSphere Application Server plug-in option selected. When it is selected, the Web server plug-ins installation task starts when you click **Next**.

For more information about deployment scenarios for IBM HTTP Server, refer to http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/welcome_ihs.html

If you decide to install the HTTP Server Plug-in now, you must configure it. Perform the following steps to configure the plug-in.

- a. Stop and start the deployment manager:

```
was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh  
was_install_dir/profiles/ctgDmgr01/bin/startManager.sh
```
- b. Copy the `/opt/IBM/HTTPServer/Plugins/bin/configurewebserver1.sh` file to `was_install_dir/bin/`
- c. Change directory to `was_install_dir/bin` and then execute the following command:

```
./configurewebserver1.sh
```
- d. Start the HTTP servers:

```
/opt/IBM/HTTPServer/bin/adminctl start  
/opt/IBM/HTTPServer/bin/apachectl start
```
- e. Login to the WebSphere Administrative Console and ensure that `webserver1` has started.

Installing IBM HTTP server fix packs:

HTTP server fix pack 23 needs to be installed to update the base installation of the HTTP server to the latest maintenance level.

1. Copy the fix pack file to the `/opt/IBM/HTTPServer/maintenance` directory. Create this directory if it does not exist.

Solaris For Solaris

Copy `Middleware\solaris\WS-WAS_IHS_6.1.0_FP23\6.1.0-WS-IHS-SolarisSparc64-FP0000023.pak`

HP-UX For HP-UX

Copy `hpux-ia64/WS-WAS_IHS_6.1.0_FP23/6.1.0-WS-IHS-HpuxIA64-FP0000023.pak`

2. Stop the HTTP server. Type `/opt/IBM/IBMHttpServer/bin/.apachectl stop`
3. Stop WebSphere Application Server and the managed nodes using the following commands.
 - a. `was_install_dir/profiles/ctgAppSrv01/bin/stopNode.sh`
 - b. `was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh`
4. Install the fix pack. Type `/opt/IBM/WebSphere/UpdateInstaller/.update.sh`.
 - a. When the update installer wizard starts, select **IBM HTTP Server** from the **Directory name** drop down list.
 - b. Click **Next** to install the maintenance package.
 - c. Browse to the `/opt/IBM/HTTPServer` directory and select the fix pack (.pak) file from the file list; click **Open** and then click **Next** on the Maintenance Package Selection screen.
5. Start the HTTP server. Type `/opt/IBM/IBMHttpServer/bin/.apachectl start`
6. Restart WebSphere Application Server and the managed nodes:
 - a. `was_install_dir/profiles/ctgDmgr01/bin/startManager.sh`
 - b. `was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh`

Installing and configuring the WebSphere Plug-in

This procedure provides task information for manually installing and configuring WebSphere Plug-in for IBM HTTP Server. This procedure is optional if you chose to install and configure the WebSphere plug-in when you installed the IBM HTTP Server.

1. Log on as root to the machine where you have installed WebSphere.
2. Change to the directory where you previously extracted the C943UML tar file (when you installed IBM HTTP Server).

Solaris

For example, for Solaris, this path might be `solaris64/WS-WAS_ND_6.1.0_Supplemental/plugin`.

3. Change to the plugin directory.
4. From a command line, launch the WebSphere plug-in installation program.
`./install`
5. On the Welcome panel, unselect the option to learn more about the **Installation roadmap: Overview and installation scenarios**. Click **Next**.
6. Accept the license agreement and click **Next**.
7. From the plug-in selection panel, select the IBM HTTP Server V6 or 6.1 plug-in, and then click **Next**.
8. From the installation scenario panel, select **WebSphere Application Server machine (local)**, and then click **Next**.

9. Accept or change the installation directory; the default is `/opt/IBM/HTTPServer/Plugins1`. Click **Next**.
10. Specify the location where you installed the application server; the default is `/opt/IBM/WebSphere/AppServer`. Click **Next**.
11. From the Select Profile panel, select `ctgDmgr01` from the drop-down list, and then click **Next**.
12. From the Web server configuration file panel, specify the following:

Select the existing IBM HTTP Server `httpd.conf` file
Browse to the location of the `httpd.conf` file; the default is `/opt/IBM/HTTPServer/conf/httpd.conf`.

Specify the Web server port
The default is port `80`.

Clicking **Next** at this point might produce warning message that indicates that the selected IBM HTTP Server configuration file already contains plug-in entries. If you proceed, this configuration file will be updated with a new `plugin-cfg.xml` file location. You can click **OK** to proceed.
13. From the Web server definition panel, specify a unique Web server definition name; the default name (`webserver1`) is satisfactory.
14. Accept the default Web server plug-in configuration file name (`plugin-cfg.xml`) and location.
15. Click **Next** to acknowledge the manual configuration steps.
16. From the installation summary panel, click **Next**.
17. When the installation is complete, click **Finish**.
18. Stop and start the deployment manager:


```
was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh
was_install_dir/profiles/ctgDmgr01/bin/startManager.sh
```
19. Copy the `/opt/IBM/HTTPServer/Plugins/bin/configurewebserver1.sh` file to `was_install_dir/bin/`
20. Change directory to `was_install_dir/bin` and then execute the following command:


```
./configurewebserver1.sh
```
21. Start the HTTP servers:


```
/opt/IBM/HTTPServer/bin/adminctl start
/opt/IBM/HTTPServer/bin/apachectl start
```
22. Login to the WebSphere Administrative Console and ensure that `webserver1` has started.

Installing WebSphere plug-in fix packs:

The WebSphere plug-in fix pack 23 needs to be installed to update the base installation of the plug-in to the latest maintenance level.

1. Copy the fix pack file to the `/opt/IBM/WebSphere/UpdateInstaller/` maintenance directory. Create this directory if it does not exist.

Solaris

For Solaris

Copy `Middleware/solaris/WS-WAS_Plugins_6.1.0_FP23/6.1.0-WS-PLG-SolarisSparc64-FP0000023.pak`

HP-UX

For HP-UX

Copy `hpux-ia64/WS-WAS_Plugins_6.1.0_FP23/6.1.0-WS-PLG-HpuxIA64-FP0000023.pak`

2. Stop the HTTP server. Type `/opt/IBM/HTTPServer/bin/apachectl stop`
3. Stop WebSphere Application Server and the managed nodes using the following commands.
 - a. `was_install_dir/profiles/ctgAppSrv01/bin/stopNode.sh`
 - b. `was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh`
4. Install the fix pack. Type `/opt/IBM/WebSphere/UpdateInstaller/update.sh`.
 - a. When the update installer wizard starts, select **IBM HTTP Server Plugins** from the **Directory name** drop down list.
 - b. Click **Next** to install the maintenance package.
 - c. Browse to the `/opt/IBM/HTTPServer` directory and select the fix pack (.pak) file from the file list. Click **Open** and then click **Next** on the Maintenance Package Selection panel.
5. Start the HTTP server. Type `/opt/IBM/IBMHttpServer/bin/.apachectl start`
6. Restart WebSphere Application Server and the managed nodes:
 - a. `was_install_dir/profiles/ctgDmgr01/bin/startManager.sh`
 - b. `was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh`

Configuring Virtual Member Manager on WebSphere Application Server

Virtual Member Manager (VMM) provides you with the ability to access and maintain user data in multiple repositories, and federate that data into a single virtual repository.

Before you begin

Before configuring Virtual Member Manager, you might consider creating a system backup image. This would allow you to restore the system to a pre-VMM state, which would allow you to reconfigure Virtual Member Manager to use a different LDAP server if you chose to relocate your LDAP data in the future.

About this task

Refer to “Manually configuring Virtual Member Manager on IBM WebSphere Application Server” on page 128 for information about adding an IBM Tivoli Directory Server repository to Virtual Member Manager. This is a required task that must be performed.

The federated repository managed by Virtual Member Manager consists of a single named realm, which is a set of independent user repositories. Each repository might be an entire external repository or, in the case of LDAP, a subtree within that repository. The root of each repository is mapped to a base entry within the federated repository, which is a starting point within the hierarchical namespace of the virtual realm.

To add an LDAP directory to the Virtual Member Manager virtual repository, you must first add the LDAP directory to the list of repositories available for configuration for the federated repository and then add the root of baseEntries to a search base within the LDAP directory. Multiple base entries can be added with different search bases for a single LDAP directory.

Configuring the authentication service in IBM WebSphere Network Deployment

The authentication service provides the ability to “launch-in-context”. Launch-in-context provides a means for launching from an application, like Asset Management for IT, to the user interface of an external Web-based application such as Software Knowledge Base Toolkit. Both applications must use the same directory server for authentication, and the external application must have the authentication client installed. You authenticate only once, to the server hosting the client; you do not need to authenticate again to the external application when they launch-in-context to it.

1. Open a command prompt on the server that hosts in IBM WebSphere Network Deployment.
2. Change to *was_install_dir/bin*.
3. Log on to the wsadmin shell using the following command. If you did not change the wsadmin user name or password when you installed the application server, the default is wsadmin for the user and wsadmin for the password.

```
./wsadmin.sh
```

4. Verify that you do not already have authentication services deployed:

```
wsadmin>$AdminApp view authnsvc_ctges
```

If the command returns a message that indicates that the authnsvc_ctges application does not exist, authentication services have not been deployed.

5. Open a new window and copy the *Middleware/operating_system/WS-ESS_6.1_GA/IBMESSAuthnSvc.ear* file to a local drive.
6. Return to the wsadmin shell window and deploy the *IBMESSAuthnSvc.ear* using the following command. All characters should be typed as shown.

```
wsadmin>$AdminApp install file_path/IBMESSAuthnSvc.ear  
"-usedefaultbindings -deployws -appname authnsvc_ctges"
```

As an example, *file_path* could equate to */opt/IBM/image/ESS/*.

7. Save the configuration:

```
wsadmin>$AdminConfig save
```
8. Exit the wsadmin shell by typing *exit*.
9. Stop WebSphere Application Server and the managed nodes using the following commands.
 - a. *was_install_dir/profiles/ctgAppSrv01/bin/stopNode.sh*
 - b. *was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh*
10. Copy the *Middleware/operating_system/WS-ESS_6.1_GA/com.ibm.security.ess.server_config.6.1.0.jar* file to the *was_install_dir/plugins* directory.

This file is located in the *operating_system\WS-ESS_6.1_GA* directory on the middleware DVD.
11. Restart WebSphere Application Server and the managed nodes:
 - a. *was_install_dir/profiles/ctgDmgr01/bin/startManager.sh*
 - b. *was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh*
12. Change to *was_install_dir/bin*.
13. Type *./wsadmin.sh* to log in to the wsadmin shell.
14. Configure the service, type the following at the wsadmin prompt:

```
$AdminTask configureESS.
```

15. Type the following wsadmin command to verify that the service is configured:
`$AdminTask isESSConfigured`. If true is returned, the service is configured.
16. Create an Lightweight Third Party Authentication (LTPA) key, which is required to support single sign on, by typing the following command. The password that you specify is the LTPA key password. Record it in a secure place. If the key password is lost, you must create a new key. Ensure all clients that connect to the service use the export key file that you create in step 19.

```
wsadmin>$AdminTask createESSLTPAKeys "-password password"
```

Note: If the key password is every lost, you will need to create a new key. Ensure all clients connecting to the service use the new export key file you generate.

17. Synchronize the configuration.

```
wsadmin>$AdminConfig save
wsadmin>set dmgr [$AdminControl completeObjectName type=DeploymentManager,*]
wsadmin>$AdminControl invoke $dmgr syncActiveNodes true
wsadmin>quit
```

18. Stop and restart WebSphere Application Server and the managed nodes:

- a. `was_install_dir/profiles/ctgAppSrv01/bin/stopNode.sh`
- b. `was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh`
- c. `was_install_dir/profiles/ctgDmgr01/bin/startManager.sh`
- d. `was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh`

19. Export the newly created key:

```
# wsadmin
wsadmin>$AdminTask exportESSLTPAKeys "-pathname file_path"
```

For example,

```
wsadmin>$AdminTask exportESSLTPAKeys "-pathname /root/avenESSLTPAKeyFile.exported"
```

Chapter 11. Starting IBM Tivoli Asset Management for IT middleware on Windows

Windows This procedure describes how to start middleware on Windows, should you need to restart any middleware services.

About this task

To properly start middleware products on Windows, perform the following steps:

1. Log in as a user with Administrative permissions.
2. Start servers by executing the following scripts in the order in which they are listed:

Start ctginst1

- a. Click **Start**, and select **Run**.
- b. Type `services.msc`, and click **OK**.
- c. Select **DB2 - DB2COPY1 - CTGINST1-0**, and click **Start the service**.

Alternatively, you can use the `db2start` command from a command line to start CTGINST1.

Start ITDS Admin Daemon

- a. Click **Start**, and select **Run**.
- b. Type `services.msc`, and click **OK**.
- c. Select **IBM Tivoli Directory Admin Daemon V6.2 - idscmdb**, and click **Start the service**.

Alternatively, you can use the following command from the command line to start the ITDS admin daemon:

```
idsdiradm -I idscmdb
```

Start the ITDS instance:

- a. Click **Start**, and select **Run**.
- b. Type `services.msc`, and click **OK**.
- c. Select **IBM Tivoli Directory Server Instance V6.2 - idscmdb**, and click **Start the service**.

Alternatively, you can use the following command from the command line to start the ITDS instance:

```
idsslapd -I idscmdb
```

Important: The Directory Server instance must remain as a manual startup type. It must be started manually in order to synchronize correctly with the database in the context of Asset Management for IT.

Start HTTP Server and webserver1

- a. Click **Start** and select **Run**
- b. Type `services.msc`, and click **OK**.
- c. Select **IBM HTTP Server 6.1**, and click **Start the service**.

Alternatively, you can type `apache` from the command line to start the HTTP Server .

Start Domain Manager

was_install_dir\profiles\ctgDmgr01\bin\startManager.bat

Start Node

was_install_dir\profiles\ctgAppSvr01\bin\startNode.bat

Start MXServer

was_install_dir\profiles\ctgAppSrv01\bin\startServer.bat MXServer

Chapter 12. Starting IBM Tivoli Asset Management for IT middleware on UNIX

UNIX This procedure describes how to start middleware on Linux and UNIX platforms, should you need to restart any middleware services.

About this task

To properly start middleware products on Linux and UNIX systems, perform the following steps:

1. Log in as root.
2. Start servers by executing the following scripts in the order in which they are listed:

Start ctginst1 instance

```
su - ctginst1 -c db2start
```

Start ITDS Admin Daemon

```
itds_install_dir/sbin/idsdiradm -I idscmdb
```

Start ITDS server daemon: ibmslapd

```
itds_install_dir/sbin/ibmslapd -I idscmdb
```

Start HTTP Server

Linux

Linux:

```
/opt/IBM/HTTPServer/bin/apachectl start
```

AIX

AIX:

```
/usr/IBM/HTTPServer/bin/apachectl start
```

Solaris

Sun Solaris:

```
/opt/IBM/HTTPServer/bin/apachectl start
```

Start Deployment Manager

```
was_install_dir/profiles/ctgDmgr01/bin/startManager.sh
```

Start Node

```
was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh
```

Start webserver1

```
was_install_dir/profiles/ctgAppSrv01/bin/startServer.sh  
webserver1 -username user_name -password password
```

Start MXServer

```
was_install_dir/profiles/ctgAppSrv01/bin/startServer.sh MXServer  
-username user_name -password password
```

Chapter 13. Uninstalling IBM Tivoli Asset Management for IT middleware

Uninstalling middleware consists of running the Tivoli middleware installer and using it to undeploy the previously deployed deployment plan.

Before you begin

Note: You need to use the middleware installer to uninstall any IBM Tivoli Asset Management for IT middleware installed by the middleware installer. The middleware installer creates a registry when installing Asset Management for IT middleware. If you use the native middleware uninstall programs, this registry will be out of sync with what is deployed. This will cause errors if you then try to reinstall the middleware using the middleware installer. At points during the uninstall process, the middleware installer uninstall progress bar might appear to pause. This is normal behavior. In most cases, the middleware installer uninstall progress bar will resume shortly after pausing. If you suspect your uninstall process has experienced an error, refer to the middleware installer log files.

About this task

To uninstall the J2EE server, ensure the directory server (IBM Tivoli Directory Server or Microsoft Active Directory) is active. Do not uninstall the directory server until the J2EE server has been uninstalled.

To undeploy Asset Management for IT middleware, complete the following steps:

1. Login as Administrator on Windows and root on Linux, AIX and Sun Solaris.
2. Launch the middleware installer from the Launchpad.
 - a. Start the Launchpad: On the DVD titled "Tivoli Asset Management for IT 7.2", navigate to the root directory of the product disc or the downloaded installation image, and run the command: `launchpad.[exe|sh]`, depending on the operating system.
 - b. In the launchpad navigation pane, click **Install the Product**.
 - c. Click the middleware link under **1. Install the middleware**.
3. Select a language for the installation and click **OK**.
4. From the Welcome panel, click **Next**. The middleware installer license agreement window is displayed.
5. Read the license information and select **I accept both the IBM and the non-IBM terms** if you agree with the terms. Click **Next**.
6. From the Choose Workspace panel, specify the workspace directory containing the currently deployed plan, and then click **Next**. The default location for the workspace will be the last workspace location specified. The default location for the workspace is `c:\ibm\tivoli\mwi\workspace`.
7. From the Select Operation panel, select **Undeploy the plan**, and then click **Next**.
8. From the undeployment preview panel, click **Next** to undeploy the plan.
9. From the successful undeployment panel, click **Next** to select a new operation, such as redeploying components, or click **Cancel** to exit the middleware installer.

Chapter 14. IBM WebSphere Application Server management

IBM provides comprehensive information on running and administering IBM WebSphere Application Server.

Go to the WebSphere Application Server Information Center to read more.

Starting the MXServer application server from the command line

After you created an application server named MXServer during installation (either manually or automatically), you can start it to get it into operational mode.

About this task

To start the MXServer application , complete the following steps:

1. Start the Deployment Manager:

UNIX

```
UNIX: was_install_dir/AppServer/profiles/ctgDmgr01/bin/startManager.sh
```

Windows

Windows:

```
was_install_dir\profiles\ctgDmgr01\bin\startManager.bat
```

2. Start the Node:

UNIX

```
UNIX: was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh
```

Windows

Windows:

```
was_install_dir\profiles\ctgAppSrv01\bin\startNode.bat
```

3. Start the Web server:

UNIX

```
UNIX: was_install_dir/profiles/ctgAppSrv01/bin/startServer.sh  
webserver1 -username username-password password
```

Windows

Windows:

```
was_install_dir\profiles\ctgAppSrv01\bin\startServer.bat  
webserver1 -username username-password password
```

4. Start the application server:

UNIX

```
UNIX: was_install_dir/profiles/ctgAppSrv01/bin/startServer.sh MXServer  
-username username-password password
```

Windows

Windows:

```
was_install_dir/profiles/ctgAppSrv01/bin/startServer.bat MXServer  
-username username-password password
```

Starting the MXServer application server from the administrative console

An application server named MXServer is created during Asset Management for IT deployment, either manually, or automatically by the Asset Management for IT installation program.

About this task

To start the MXServer application server from the administrative console, complete the following steps:

1. Before you start the administrative console, verify that the following server processes are running. If necessary, use the commands shown from a command prompt in order to start them.

Table 20. WebSphere Application Server processes.

Server	Go To
HTTP Server	<p>Windows</p> <p>Windows:</p> <pre>http_server_install_dir\bin\apache -k start http_server_install_dir\bin\apache -k stop</pre> <p>UNIX</p> <p>UNIX: <code>http_server_install_dir/bin/apachectl start</code> <code>http_server_install_dir/bin/apachectl stop</code></p>
Deployment Manager	<p>Windows</p> <p>Windows:</p> <pre>was_install_dir/profiles/ctgDmgr01/bin/startManager.bat was_install_dir/profiles/ctgDmgr01/bin/stopManager.bat</pre> <p>UNIX</p> <p>UNIX: <code>was_install_dir/profiles/ctgDmgr01/bin/startManager.sh</code> <code>was_install_dir/profiles/ctgDmgr01/bin/stopManager.sh</code></p>
Node Agent	<p>Windows</p> <p>Windows:</p> <pre>was_install_dir/profiles/ctgAppSrv01/bin/startNode.bat was_install_dir/profiles/ctgAppSrv01/bin/stopNode.bat</pre> <p>UNIX</p> <p>UNIX: <code>was_install_dir/profiles/ctgAppSrv01/bin/startNode.sh</code> <code>was_install_dir/profiles/ctgAppSrv01/bin/stopNode.sh</code></p>

Table 20. WebSphere Application Server processes. (continued)

Server	Go To
IBM Tivoli Directory Server Instance	<p>Windows</p> <p>Windows:</p> <ol style="list-style-type: none"> 1. Click Start, and select Run. 2. Type <code>services.msc</code>, and click OK. 3. Select IBM Tivoli Directory Server Instance V6.2 - idscmdb, and click Start the service. <p>UNIX</p> <p>UNIX: <code>/ldap/V6.2/sbin/ibmslapd -I idscmdb</code></p>
Directory Server Database	<p>Windows</p> <p>Windows:</p> <ol style="list-style-type: none"> 1. Click Start, and select Run. 2. Type <code>services.msc</code>, and click OK. 3. Select DB2 - DB2COPY1 - CTGINST1-0, and click Start the service. <p>UNIX</p> <p>UNIX: <code>su - idscmdb -c db2start</code></p>

2. To start the administrative console, open a browser window and enter the following URL:

`http://computer_name:9060/ibm/console`

Where *computer_name* is the host name of the WebSphere Application Server and *9060* is the default port number for the Administrative Console.

3. Enter an administrative user ID and password to log in, if one is required.
4. From the administrative console navigation pane, click **Servers** → **Application Servers**.
5. Select the check box next to **MXServer**, the name of the WebSphere Application Server.
6. Click **Start**. Notice that the icon in the Status column changes to running. Under WebSphere Application Server, click **Stop**, which will cause the icon in the Status column to change to stopped.

Securing WebSphere Administrative Console

You can secure the Administrative Console so that only authenticated users can use it. Virtual Member Manager must have been configured on the WebSphere server prior to securing the console.

Before you begin

Once you have enabled Virtual Member Manager for WebSphere security, you perform several steps to secure the console. First you identify users (or groups) that are defined in the active user registry. After you decide which users you want to access the console, you can determine their level of access by assigning roles. The roles determine the administrative actions that a user can perform. After enabling security, a user must enter a valid administrator user ID and password to access the console.

About this task

You can use the Administrative Group Roles page to give groups specific authority to administer application servers through the administrative console. Simply click **Security** → **Secure administration, applications, and infrastructure** → **Administrative Group Roles** to view the available administrative group roles.

Table 21. Administrative Group Roles and their descriptions.

Admin Role	Description
Administrator	Has operator permissions, configurator permissions, and the permission that is required to access sensitive data.
Operator	Has monitor permissions and can change the runtime state. For example, the operator can start or stop services.
Configurator	Has monitor permissions and can change the application server configuration.
Monitor	Has the least permissions. This role primarily confines the user to viewing the application server configuration and current state.
Deployer	Users granted this role can perform both configuration actions and runtime operations on applications.
adminsecuritymanager	Fine-grained administrative security is available using wsadmin only. However, you can assign users and groups to the adminsecuritymanager role on the cell level through wsadmin scripts and the administrative console. Using the adminsecuritymanager role, you can assign users and groups to the administrative user roles and administrative group roles. However, an administrator cannot assign users and groups to the administrative user roles and administrative group roles including the adminsecuritymanager role.
iscadmins	Has administrator privileges for managing users and groups from within the administrative console only.

Note: To manage users and groups, click **Users and Groups** in the console navigation tree and then click either **Manage Users** or **Manage Groups**.

Complete the following steps to map users and groups to security roles:

1. Select **Applications** → **Enterprise applications** → *application_name*.
2. Under **Detail** properties, click **Security role to user/group mapping**.
3. Select the role and click either **Look up users** or **Look up groups**.

Different roles can have different security authorizations. Mapping users or groups to a role authorizes those users or groups to access applications defined by the role. Users and groups are associated with roles defined in an application when the application is installed or configured. Use the **Search pattern** field to display users in the **Available** list. Click >> to add users from the **Available** list to the **Selected** list.

4. Restart all the application servers.

Related concepts

“Planning for security” on page 18

Planning for security includes choosing a security option, deciding which users will work with each application in Asset Management for IT, and optionally which users can work with which configuration items.

Configuring the WebSphere Application Server to run as a Windows service

Windows If you plan to install a Tivoli Asset Management for IT instance on Windows with WebSphere Application Server, you might want to run the WebSphere Application Server as a Windows service.

About this task

To configure the WebSphere Application Server to run as a Windows service, complete the following steps:

1. Start the WebSphere Administrative Console by opening a browser window and entering the following URL:

```
http://computer_name:9060/ibm/console
```

2. Enter an administrative user ID and password.
3. Click **Servers** → **Application Servers** in the navigation pane.
4. In the Application Servers pane, select **MXServer** and click **Start**. This action creates a server log folder used by the WASService command.
5. Select **MXServer**, and click **Stop**.
6. Open a command prompt window.
7. Navigate to the bin folder where you installed the Maximo application server. For example:

```
C:\Program Files\IBM\WebSphere\AppServer\bin
```

8. Run the WASService command with the following parameters:

serverName

Maximo application server name, MXServer.

profilePath

The profile directory of the server, for example,

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\ctgAppSrv01
```

wasHome

Home folder for MXServer, for example,

```
C:\Program Files\IBM\WebSphere\AppServer\profiles
```

logRoot

Folder location of MXServer log file, for example,

```
C:\Program Files\IBM\WebSphere\AppServer\logs\manageprofiles\ctgAppSrv01
```

logFile

Log file name for MXServer (startServer.log)

restart

Restarts the existing service automatically if the service fails when set to true.

9. Enter the WASService command using the following syntax:

```
WASService add MXServer serverName MXServer
profilePath C:\Program Files\IBM\WebSphere\AppServer\profiles\
ctgAppSrv01wasHome <D:>\IBM\WebSphere\AppServer
logRoot C:\Program Files\IBM\WebSphere\AppServer\logs\manageprofiles\
ctgAppSrv01
logFile C:\Program Files\IBM\WebSphere\AppServer\logs\manageprofiles\
ctgAppSrv01\startServer.log restart true
```

10. Press Enter after you type the WASService command. A confirmation message is displayed.
11. Open a Services window and double-click **MXServer**. Then perform the following actions:
 - a. Change the **Startup** type field value to **Automatic**.
 - b. Click **Start** to start the service.
 - c. Click **OK**.

Configuring the WebSphere node agent to run as a Windows service

Windows A node agent is a server running on every host computer in the deployed network. It performs administrative functions.

About this task

To configure the WebSphere node agent to run as a Windows service, complete the following steps:

1. Start the WebSphere 6.1 Administrative Console by opening a browser window and entering the following URL:
`http://computer_name:9060/ibm/console`
2. Enter an administrative user ID and password.
3. Click **System Administration** in the navigation pane.
4. In the System Administration pane, select the name of the Node Agent (for example, **nodeagent**), and click **Start**.
5. Before you run the WASService command, select **nodeagent** in the Administration pane, and click **Stop**.
6. Open a command prompt window.
7. Navigate to the bin folder where you installed the Node Agent. For example:
`C:\Program Files\IBM\WebSphere\AppServer\bin`
8. Run the WASService command with the following parameters:

serverName

name of node agent, for example, nodeAgent

profilePath

the profile directory of the server, for example,

`C:\Program Files\IBM\WebSphere\AppServer\profiles\ctgAppSrv01`

wasHome

home folder for MXServer, for example,

`C:\Program Files\IBM\WebSphere\AppServer\profiles`

logRoot

folder location of node agent log file, for example,

`C:\Program Files\IBM\WebSphere\AppServer\logs\manageprofiles\ctgAppSrv01`

logFile

log file name for node agent (startServer.log)

restart restarts the existing service automatically if the service fails when set to true.

9. Enter the WASService command using the following syntax:
`WASService add NodeAgent serverName nodeagent profilePath
C:\Program Files\IBM\WebSphere\AppServer\profiles\ctgAppSrv01
wasHome <D:>\IBM\WebSphere\AppServer
logRoot <D:>\IBM\WebSphere\AppServer\logs\nodeagent
logFile <D:>\IBM\WebSphere\AppServer\logs\nodeagent\
startServer.log restart true`
10. Press Enter after you type the WASService command, and you will see a confirmation message.
11. Open a Services window and double-click the Node Agent service, for example, **nodeAgent**. Then perform the following actions:
 - a. Change the **Startup type** field value to Automatic.

- b. Click **Start** to start the service.
- c. Click **OK**.

Creating a WebSphere Application Server Network Deployment cluster

This section contains information about creating a WebSphere Application Server Network Deployment cluster.

About this task

You might want to manually create WebSphere Application Server Network Deployment cluster to host Asset Management for IT. There are two approaches; using a default or existing application server template, or creating the cluster using an existing application server as the first cluster member (see Figure 2 on page 8).

When creating a cluster, you have a few options for determining the first member. The template you choose is replicated and used for all other members of the cluster.

1. Log in to the WebSphere Application Server Network Deployment administrative console.
2. From the WebSphere Application Server Network Deployment administrative console navigation pane, select **Servers** → **Clusters**
3. Click **New**.
4. From the Enter basic cluster information page, enter a new Cluster name for the new member, and then click **Next**.
5. From the Create first cluster member page, enter a name for the new member and select the first member node from the **Select node** drop-down menu.
6. If you want to create all cluster members based upon the application server created when Asset Management for IT was installed, select **MXServer** from the **Create the member using an application server template** drop-down menu. In this case, the fields for member name and node name is disabled and set to values for MXServer. Otherwise, you can select default from the **Create the member using an application server template** drop-down menu, which creates cluster members based upon the default application server template. In this case, you need to manually install the Asset Management for IT applications.
7. Click **Next**.
8. From the Create additional cluster members page, you can add additional cluster members by typing a new member name and selecting the node for the member. Click **Next** when finished.
9. On the summary panel, click **Finish**.

Related concepts

“Tivoli Asset Management for IT deployment topologies” on page 7

A typical deployment lifecycle usually begins with a single-server topology that would move through phases of demonstration, functional proof-of-concept, and testing integration within the existing environment. It then gradually moves towards a pilot multi-server environment before finally implementing a production deployment within the enterprise.

Chapter 15. IBM WebSphere Portal Server overview

An existing IBM WebSphere Portal Server system can be configured to work with your IBM WebSphere Application Server deployment after it has been successfully installed.

You can access Asset Management for IT applications through the WebSphere Portal Server interface transparently, centralizing Asset Management for IT application access alongside other service-oriented applications used by your organization.

WebSphere Portal Server needs to be hosted on a system other than the system hosting the Asset Management for IT J2EE server. WebSphere Portal Server must be configured to use a version of WebSphere that it supports.

Tivoli Asset Management for IT deployed on WebSphere Portal Server

After Tivoli Asset Management for IT has been completely deployed, the user interface for any Asset Management for IT application can be accessed through a portlet hosted on an existing WebSphere Portal Server instance.

Before you begin

The following EAR files are deployed by the Asset Management for IT installation and the process solution installation programs and are candidates for being modified, rebuilt, and redeployed:

Table 22. Asset Management for IT EAR and WAR files

EAR File	Description	Location
maximo.ear	This EAR file contains the maximo.war file which includes Asset Management for IT base tasks.	<i>tamit_install_dir</i> \maximo\deployment\default
maximohelp.ear	This EAR file contains the maximohelp.war file which is for Asset Management for IT Help	<i>tamit_install_dir</i> \maximo\deployment\default

About this task

To create a page with a portlet for a Asset Management for IT application you wish to access through WebSphere Portal Server, ensure you have a working and active Asset Management for IT deployment, and then complete the following steps:

1. From the Asset Management for IT administrative workstation, open a Web browser and access the WebSphere Portal Server Administration tool:
`http://host_name:port_number/wps/portal`
2. Log in as the WebSphere Portal Server administrator.
3. From the WebSphere Portal Server welcome page, click **Administration**, found at the bottom of the user interface.
4. From the WebSphere Portal Administration page, click **Web Modules**, found under the Portlet Management heading of the navigation pane.

5. From the Manage Web Modules page, you see a table listing all of the web modules that have been installed on the server. Click **Install** to install a new module.
6. From the Select War File page, using the **Browse** button, locate the Asset Management for IT WAR file you intend to deploy. WAR files will be located on the Asset Management for IT Administrative system. Once you have located the intended WAR file, click **Next**. In this example, we are deploying the WAR file maximo.war.
7. From the WAR file content summary page, review the WAR file contents, and then click **Finish**.
 - If the deployment is successful, you will be returned to the Manage Web Modules page. A message will be displayed confirming that the WAR file was correctly deployed.
 - For each WAR file you deploy, you will need to edit its maximointegration.properties file. This file is found in the deployment directory created after the deployment of each WAR, under the WEB-INF directory.
8. Open the appropriate maximointegration.properties file in a text editor, and edit the following properties:

maximo_host_name

Ensure this value is the same as the host name used to access the Maximo servlet on WebSphere Application Server.

maximo_port

Ensure this value is the same as the port used to access the Maximo servlet on WebSphere Application Server.

maximo_url_protocol

This value defaults to http, but you should change it to https in order to access a secure environment.

The process of editing the maximointegration.properties file will have to be repeated for every WAR file you deploy in WebSphere Portal Server.

The next step is to create a new page and place a portlet for the Asset Management for IT application on a new portal page.

9. Click **Administration**, found at the bottom of the user interface.
10. Click **Manage Pages**, found under the **Portal User Interface** heading of the navigation pane.
11. From the Manage Pages page, click the **Context Root** entry found in the My Pages table.
12. Click **New Label**.
13. Enter **Tivoli Asset Management for IT 7.2** in the **Title** field of the Page Properties window, and then click **OK**.
14. From the **Pages in Context Root** table of the Manage Pages page, click **Tivoli Asset Management for IT7.2**.
15. Click **New Page**.
16. In the Title field of the Page Properties window, enter a title that identifies the Asset Management for IT application, for example, Change for the Change application, and then click **OK**.
17. Click the **Edit Page Layout** icon located to the right of the new entry in the Pages in **Tivoli Asset Management for IT 7.2** table.
18. From the Edit Layout page, click **Add Portlets**.

19. Use the search feature of this page to locate the appropriate portlet, select it in the table, and then click **OK**.
20. From the Edit Layout page, click **Done**.

What to do next

You can now launch the portlet from the WebSphere Portal Server Launch menu.

Chapter 16. Installing IBM Tivoli Integration Composer



After you successfully installed IBM Tivoli Asset Management for IT components, install optionally IBM Tivoli Integration Composer, an integration tool that imports information technology (IT) data into the Maximo database.

Asset Management for IT installations should use the Asset Management for IT Launchpad as an interface for installing Integration Composer, unless you have a 64-bit operating system.

When you install Integration Composer and Asset Management for IT from the launchpad, the Asset Management for IT installer automatically updates the Integration Composer database tables in the Integration Composer repository for you.

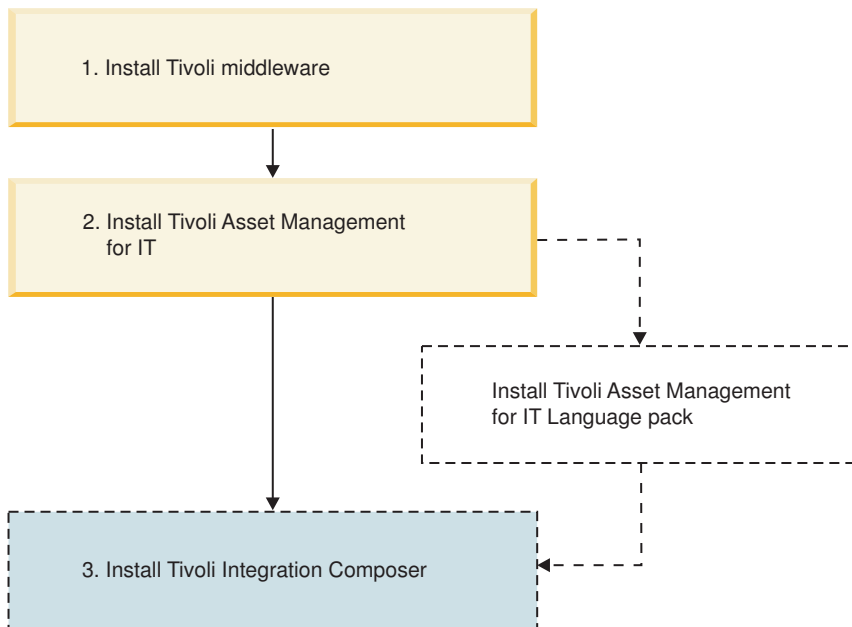


Figure 7. Asset Management for IT installation flow last step - Installing Integration Composer.

IBM Tivoli Integration Composer overview

This section introduces you to IBM Tivoli Integration Composer. Integration Composer is the IBM Tivoli application for transforming and importing inventory data about deployed hardware and software. This inventory data is imported from a discovery or system management tool database into the Maximo database tables for deployed assets or configuration items.

With Integration Composer, an enterprise can aggregate data collected by external discovery tools and integrate it into the Maximo database, creating a central repository for enterprise IT asset management, reporting, and decision support. The Maximo database is the repository used by

- IBM Tivoli Asset Management for IT,
- IBM Tivoli Service Request Manager,
- IBM Tivoli Change and Configuration Management Database

To collect the data about deployed assets or configuration items, a discovery tool scans computers, network devices, and network printers deployed in an enterprise and records information about the hardware and software it finds there. Integration Composer uses an integration adapter to transform the data collected by the discovery tool and move it from the discovery tool database into the Maximo database. For more about creating your own integration adapter, see the book *IBM Tivoli Integration Composer Administrator Guide*.)

You can view imported data from various applications on your system. The data is also used to generate reports.

Note: Integration Composer is used to import hardware and software inventory data from a discovery tool database into the Deployed Asset, Actual CI, or (for the purposes of asset initialization) Asset tables in the Maximo database. The import or export of data into or out of other tables within the Maximo database is accomplished using a different tool, the integration framework. Refer to the related book, *IBM Tivoli Asset Management for IT 7.2 Integration Guide*, for more on this subject.

Integration Composer backward compatibility

Several different Tivoli products and product combinations can use Integration Composer 7.2 to import data. Although Integration Composer 7.2 is backward compatible with these products, integration adapters and their associated data schemas and mappings might not be.

Table 23 shows the products or product combinations that can use Integration Composer 7.2, where to install it from, and what integration adapters to use.

Note: If you install Asset Management for IT 7.2 or other products that include it, you should install Integration Composer 7.2 from the Asset Management for IT 7.2 launchpad or as described (in subsequent topics) for 64-bit operating systems. *Everyone else* should install Integration Composer 7.2 from the IBM Software Support Web site.

Table 23. Product compatibility with Integration Composer 7.2 and integration adapters

Product or product combination	Install Integration Composer 7.2 from:	Use any of these compatible integration adapters from Tivoli:
Asset Management for IT 7.2	Asset Management for IT 7.2 Launchpad (or as described in "Installing IBM Tivoli Integration Composer on 64-bit Windows operating systems" on page 211 or "Installing Tivoli Integration Composer on UNIX operating systems" on page 213)	The integration adapters included with Asset Management for IT 7.2
Asset Management for IT 7.1, running on Base Services 7.1.1.4 or 7.1.1.5	IBM Tivoli Asset Management for IT Support site	The optional integration adapters made available for Asset Management for IT 7.1

Table 23. Product compatibility with Integration Composer 7.2 and integration adapters (continued)

Product or product combination	Install Integration Composer 7.2 from:	Use any of these compatible integration adapters from Tivoli:
Tivoli Service Request Manager 7.1.x, running on Base Services 7.1.1.4 or 7.1.1.5	IBM Tivoli Asset Management for IT Support site	The optional integration adapters made available for Tivoli Service Request Manager 7.1.x
Tivoli Change and Configuration Management Database 7.1	IBM Tivoli Asset Management for IT Support site	The integration adapters included with Tivoli Change and Configuration Management Database 7.1.
Tivoli Service Request Manager 7.1.x and Asset Management for IT 7.2	Asset Management for IT 7.2 Launchpad (or as described in "Installing IBM Tivoli Integration Composer on 64-bit Windows operating systems" on page 211 or "Installing Tivoli Integration Composer on UNIX operating systems" on page 213)	The integration adapters included with Asset Management for IT 7.2
Tivoli Change and Configuration Management Database 7.1 and Asset Management for IT 7.2	Asset Management for IT 7.2 Launchpad (or as described in "Installing IBM Tivoli Integration Composer on 64-bit Windows operating systems" on page 211 or "Installing Tivoli Integration Composer on UNIX operating systems" on page 213)	The integration adapters included with Tivoli Change and Configuration Management Database 7.1.

Hardware and software requirements

This section describes the products and versions supported by Integration Composer, plus the hardware and software requirements for the corequisite applications.

The hardware and software requirements for Integration Composer and its corequisites are as follows:

Integration Composer

Integration Composer 7.2 has the following minimum requirements:

- 3 GB memory
- 70 MB disk space
- IBM Java Software Development Kit 5.0 Service Release 5

Asset Management for IT,

Either IBM Tivoli Asset Management for IT 7.2, IBM Tivoli Asset Management for IT 7.1, IBM Tivoli Service Request Manager 7.1.x, or IBM Tivoli Change and Configuration Management Database 7.1 is required.

Service Request Manager, or

Change and Configuration Management Database Change and Configuration Management Database

Integration Composer server	<p>A dedicated server is required for running the Integration Composer application and Java components. Integration Composer can run on any of the following operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows 2003 Server with Service Pack 2 • IBM AIX 5L 5.3, AIX Technology Level 5300-06 • Red Hat Enterprise Linux 4 (Intel) • SUSE SLES 9 (z/OS®) • Sun Solaris 9 or 10 (SPARC processor-based systems)
Database servers	<p>The customer is responsible for the database servers, which contain and manage one or more source databases and a target (Maximo) database.</p> <p>The following databases are supported:</p> <ul style="list-style-type: none"> • IBM DB2 Version 9.5.1 for Linux, UNIX, and Windows • IBM DB2 Universal Database 9.1 with Fix Pack 2 • IBM DB2 Universal Database 8.2 with Fix Pack 14 • Oracle Database 11g Release 1 • Oracle Database 10g Release 2 • Oracle Database 10g Release 1 • Oracle Database 9i Release 2 • Microsoft SQL Server 2008 • Microsoft SQL Server 2005 <p>See the appropriate database documentation for the database server hardware requirements.</p>
Web browser	<p>To display its help information, Integration Composer requires a Web browser.</p>

Installation prerequisites

Before installing, you must have the IBM Java SDK prerequisite for Integration Composer on your system, and any software that adversely affects the InstallAnywhere installation program must be removed.

IBM Java SDK 5.0 Service Release 5 for the appropriate operating system is an installation prerequisite that must be present on the Integration Composer computer. The IBM Java SDK is provided on the IBM Tivoli Asset Management for IT Support site.

UNIX In addition, on UNIX based operating systems, be sure the PATH environment variable includes the location of the Java Virtual Machine (for example, Java50).

Because the following software can adversely affect InstallAnywhere—the installation program used by Integration Composer—disable the following programs before attempting to install Integration Composer:

- Antivirus software, such as Norton Antivirus or Symantec Client Firewall
- Dell OpenManage

- Search software, such as pcAnywhere

Use of these software programs affects the ability of InstallAnywhere to install programs; however, the problem is not specific to Integration Composer.

Before beginning your installation, make sure you have on hand the information on the *target* (Maximo) database described in “Installing IBM Tivoli Integration Composer on 64-bit Windows operating systems” on page 211.

Performing the Tivoli Integration Composer installation

Asset Management for IT installations that want to use Integration Composer must install it from the launchpad—unless you have a 64-bit operating system.

Results

When the installation completes successfully, you can access Integration Composer as follows:

Windows: From the **Start** menu, or by entering the command: `startFusion.bat`

UNIX: By entering the command: `./startFusion.sh`

Installing Tivoli Integration Composer on 32-bit Windows using the launchpad

Windows For Asset Management for IT installations using 32-bit Windows operating systems, the recommended way to install Integration Composer is from the launchpad.

Before you begin

If you have a 64-bit operating system, follow the instructions in “Installing IBM Tivoli Integration Composer on 64-bit Windows operating systems” on page 211 or “Installing Tivoli Integration Composer on UNIX operating systems” on page 213.

Installing Integration Composer 7.2, as described in this section, will upgrade the previous version of Integration Composer. You do not need to remove the previous version first. When upgrading, you might not be required to perform every step in this section; the installation program will bypass any unnecessary steps. To avoid losing any of your current data, back up your Integration Composer `data\dataschema` and `data\mappings` directories before installing.

Make sure you have up to 70 MB of free space for the installation directory.

About this task

To install Integration Composer with the Launchpad, complete the steps that follow.

1. Insert the Launchpad DVD into the server where you will install Integration Composer, and, from the Launchpad, launch the Integration Composer installation program by clicking the link under **3. Install Tivoli Integration Composer**.

Note: If you do not have the prerequisite IBM Java SDK 5.0 Service Release 5 currently installed on the Integration Composer server, an error window displays and the installation ends.

2. In the IBM Tivoli Integration Composer window, select your language from the drop-down list at the bottom and click **OK**.
3. In the Introduction window, review the information and click **Next**.
4. In the Choose IBM SDK Location window, type the directory where IBM Java SDK 5.0 Service Release 5 is located, or click **Choose** to browse and select the directory. Then click **Next**.
5. In the Choose Install Folder window, accept the default location or type a file path to specify the directory where you want to install Integration Composer. (Alternatively, you can click **Choose** to browse and select the location you want.) Then click **Next**.
6. In the Database Type window, select your Maximo database type (the Maximo database is where the Integration Composer repository will be installed) and click **Next**. **IBM DB2** is the default.

The Database Login Information window is displayed.

7. On the Database Login Information window, type login specifications for the database and click **Next**.

The Database Login Information window is where you define the parameters for connecting to the Maximo database. The fields displayed in this window vary slightly, depending on the type of database you chose in the previous step. The following table defines the fields that the installation program displays for the supported databases.

Table 24. Login specifications for the Maximo database

Field	Description
Database Server Name	Name of the server on which the Maximo database resides
Port Number	Port number of the server on which the Maximo database resides
Database Name (SID) or Database Name	For Oracle databases, this is the session identifier (SID) for the database; that is, the database instance For SQL Server or IBM databases, this is simply the name of the database
Database Username	Valid user name for signing in to the Maximo database
Database/Schema Owner	Database or schema owner

Tip: Make note of the values that you specified here. Later, when you launch Integration Composer, use the values entered in these fields to define connection parameters for the Maximo database.

8. On the Update Software Instances window, select one of the following options and click **Next**:

Yes, disable software updates

If you select this option, when Integration Composer imports data into the Maximo database, Integration Composer inserts or deletes software records but does not update software records. This option is preferred.

No, don't disable software updates

If you select this option, when Integration Composer imports data into the Maximo database, Integration Composer updates existing software records.

In the **Software Class Name** field, it is recommended to accept the default value **Software**. The Software Class name is used to identify the class that you do not want to update based on the choice above. In the Deployed Assets target schema, the name is Software.

9. On the Preinstallation Summary window, review the installation details and click **Next**.
10. On the Begin Installing window, click **Install** to begin installing Integration Composer. The Installing Integration Composer progress window displays during installation.
When installing is finished, the Installation Complete window is displayed.
11. In the Installation Complete window, click **Done**.

Installing IBM Tivoli Integration Composer on 64-bit Windows operating systems

Windows Use the procedure described here to install Tivoli Integration Composer on a 64-bit Windows computer without using the launchpad. Instead, you perform this installation from the command line.

Before you begin

Installing Integration Composer 7.2, as described in this section, will upgrade the previous version of Integration Composer. You do not need to remove the previous version first. When upgrading, you might not be required to perform every step in this section; the installation program will bypass any unnecessary steps. To avoid losing any of your current data, back up your Integration Composer data\dataschema and data\mappings directories before installing.

Make sure you have 70 MB of free space for the installation directory.

About this task

The Integration Composer files are located on the Tivoli Asset Management for IT 7.2 DVD in the \Installs\ITIC directory. Choose the setup.exe command from the DVD layout to start the installation process.

To install Integration Composer on a Windows 64-bit operating system, complete the steps that follow.

1. Run the setup command to begin your installation. Due to an installer problem with InstallAnywhere, 64-bit operating system users must specify the location of the IBM Java SDK in their setup command. From the DOS prompt, enter:

```
setup.exe LAX_VM "C:\Program Files\IBM\Java50\jre\bin\java.exe"
```

Note: If you do not have the prerequisite IBM Java SDK 5.0 Service Release 5 currently installed on the Integration Composer server, a LaunchAnywhere Error window displays and the installation ends. The error states: Windows error 3 occurred while loading the Java VM. To correct the problem, install

IBM Java SDK5.0 Service Release 5 on your operating system and run the setup command again. The IBM Java SDK was provided with Integration Composer 7.1.x.

2. On the IBM Tivoli Integration Composer window, select your language from the drop-down list at the bottom and click **OK**. The Integration Composer user interface is mirrored when you select either of the Arabic or Hebrew bi-directional languages from the drop down list.
3. On the Introduction window, review the information and click **Next**.
4. On the Choose IBM SDK Location window, type the directory where IBM Java SDK 5.0 Service Release 5 is located, or click **Choose** to browse and select the directory. Then click **Next**.
5. On the Choose Install Folder window, accept the default location or type a file path to specify the directory where you want to install Integration Composer. (Alternatively, you can click **Choose** to browse and select the location you want.) Then click **Next**.
6. On the Database Type window, select your Maximo database type (the Maximo database is where the Integration Composer repository will be installed) and click **Next**. IBM DB2 is the default database type. The Database Login Information window is displayed.

This Database Login Information window is where you define the parameters for connecting to the Maximo database. The fields displayed in this window vary slightly, depending on the type of database you chose in the previous step.

The following table defines the fields that the installation program displays for the supported databases.

Table 25. Login specifications for the target (Maximo) database

Field	Description
Database Server Name	Name of the server on which the target database resides
Port Number	Port number of the server on which the target database resides
Database Name (SID)	For Oracle databases, this is the session identifier (SID) for the database; that is, the database instance or
Database Name	For Microsoft SQL Server or IBM databases, this is simply the name of the database
Database Username	Valid user name for signing in to the target database
Database/Schema Owner	Database or schema owner

7. On the Database Login Information window, type login specifications for the database and click **Next**.

Tip: Make note of the values that you specified here. Later, when you launch Integration Composer, use the values entered in these fields to define connection parameters for the target data source.

8. On the Update Software Instances window, select one of the following options and click **Next**:
 - **Yes, disable software updates**

If you select this option, when Integration Composer imports data into the target database, Integration Composer inserts or deletes software records but does not update software records. This option is preferred.

- **No, don't disable software updates**

If you select this option, when Integration Composer imports data into the target database, Integration Composer updates existing software records.

9. On the Preinstallation Summary window, review the installation details and click **Next**.
10. On the Begin Installing window, click **Install** to begin installing Integration Composer. The Installing IBM Tivoli Integration Composer progress window displays during installation.

Note: If necessary, you can click **Cancel** to end the installation.

When installing is finished, the Installation Complete window is displayed.

11. On the Installation Complete window, click **Done**.

Installing Tivoli Integration Composer on UNIX operating systems

UNIX Use the procedure described here to install Tivoli Integration Composer on an UNIX computer without using the Launchpad. Instead, you perform this installing from the command line.

Before you begin

Installing Integration Composer 7.2, as described in this section, will upgrade the previous version of Integration Composer. You do not need to remove the previous version first. When upgrading, you might not be required to perform every step in this section; the installation program will bypass any unnecessary steps. To avoid losing any of your current data, back up your Integration Composer data\dataschema and data\mappings directories before installing.

Make sure you have up to 70 MB of free space for the installation directory.

About this task

The Integration Composer files are located on the "Tivoli Asset Management for IT 7.2" DVD in the \Installs\ITIC directory. Depending on the operating system, choose the setup.[bin|exe] command from the DVD layout to start the installation process:

```
setup.bin  
setup.exe
```

To install Integration Composer on a UNIX-based operating system, complete the following steps:

1. Sign on to the server as an administrator (for example, as root).
2. Save the binary Integration Composer installation file, setup.bin, on the server where you intend to install Integration Composer.
3. Make sure IBM Java SDK is in your system path.

To add IBM Java SDK to the path, enter the following commands (where *SDK_location* is the path for your IBM Java SDK; for example, /opt/java1.5/bin):

```
JAVA_HOME=SDK_location
export JAVA_HOME
PATH=$JAVA_HOME:$PATH
export PATH
```

4. Navigate to the location where you saved the setup.bin file.
5. Enter the following command to make the binary installation file executable:
chmod +x setup.bin
6. Run the Integration Composer installation program either as an X Window application or in console mode, as follows:
 - To run the installation program as an X Window application, enter the following command at the shell prompt:
sh ./setup.bin
 - To run the installation program in console mode, enter the following command at the shell prompt:
sh ./setup.bin -i console

In console mode, you are prompted to enter information line by line. The information you enter and the sequence in which you enter it are similar to the X Window process.

Note: If you do not have the prerequisite IBM Java SDK 5.0 Service Release 5 currently installed on the Integration Composer server, a LaunchAnywhere Error window displays and the installation ends. The error states: Windows error 3 occurred while loading the Java VM. To correct the problem, install IBM Java SDK 5.0 Service Release 5 on your operating system and run setup.bin again. The IBM Java SDK was provided with Integration Composer 7.1.1.

The instructions that follow describe the remaining installation steps using console mode.

7. In the Choose Locale step, type the number of your locale from the list of locales and press Enter.
8. In the Introduction step, review the Introduction information and press Enter.
9. In the Select Install Type step, indicate whether you want to perform a new installation or upgrade Integration Composer from the previous release. Either type the number of your selection and press **Enter**, or just press **Enter** to accept the default (**New Install**).
10. [Upgrades only.] If you selected the **Upgrade** option in the previous step, type the location (absolute path) where Integration Composer is currently installed and press **Enter**. Or just press **Enter** to accept the default (/Integration_Composer).
11. [New installations only.] In the Choose Install Folder step, specify where you want to install Integration Composer by doing one of the following:
 - Accept the default location and press **Enter**.
 - Type a different file path for the location and press **Enter**; then type y to confirm the new location, and press **Enter** again.
12. [New installations only.] In the IBM SDK Location step, specify the file path where IBM Java SDK 5.0 Service Release 5 is installed by doing one of the following:
 - Accept the default location and press **Enter**.
 - Type a different file path for the location and press **Enter**.
13. [New installations only.] In the Database Type step, indicate your Maximo database type (the Maximo database is where the Integration Composer

repository will be installed) by typing the associated number; then press Enter. The Database Login Information step is displayed.

This Database Login Information step is where you define the parameters for connecting to the Maximo database. The fields displayed in this step vary slightly, depending on the type of database you chose in the previous step.

The following table defines the fields that the installation program displays for the supported databases.

Field	Description
Database Server Name	Name of the server on which the target database resides
Port Number	Port number of the server on which the target database resides
Database Name (SID) or Database Name	For Oracle databases, this is the session identifier (SID) for the database; that is, the database instance For SQL Server or databases provided by IBM, this is simply the name of the database
Database Username	Valid user name for signing in to the target database
Database/Schema Owner	Database or schema owner

14. In the Database Login Information step, type each login specification for the database, one at a time, pressing **Enter** after each entry to advance to the next specification.

Tip: Make note of the values that you specified here. Later, when you launch Integration Composer, use the values entered in these fields to define connection parameters for the target data source.

15. In the Update Software Instances step, type a number to select one of the following options, and press **Enter**:
 - **Yes, disable software updates**
If you select this option, when Integration Composer imports data into the target database, Integration Composer inserts or deletes software records but does not update software records. This option is preferred for performance reasons.
 - **No, don't disable software updates**
If you select this option, when Integration Composer imports data into the target database, Integration Composer updates existing software records.
16. In the Software Class Name step, accept the default and press Enter.
17. In the Choose Internet Browser File step, accept the default browser, Netscape (only the Netscape browser is supported on UNIX-based operating systems); then press Enter.
18. In the Preinstallation Summary step, review the installation details and press Enter to begin installing Integration Composer. The Installing progress bar displays during installation.
When installation is complete, the Installation Complete step is displayed.
19. In the Installation Complete step, press Enter. The installation is done and you are returned to the UNIX command prompt.

Confirming the installation

This section explains how to verify that your new Integration Composer installation is working properly.

About this task

To determine if Integration Composer is installed correctly, complete the following steps:

1. Open the Integration Composer application by doing one of the following things:

Windows

From the Windows **Start** menu, select **Start** → **Programs** → **IBM Tivoli** → **Integration Composer** → **IBM Tivoli Integration Composer**

or

from the command line, enter the command: `startFusion.bat`

UNIX

Enter the command: `./startFusion.sh`.

2. Sign in to the Integration Composer application using the database (or schema owner) username and password that you supplied during the installation.
3. From the **Help** menu in the Integration Composer main window, select **About**.
4. On the About Integration Composer window, check that the number in the **Version** field is 7.2. If this number is displayed, Integration Composer 7.2 was successfully installed.

Post-installation tasks

This section provides instructions for verifying that Integration Composer is configured correctly.

Verifying the settings in the Integration Composer `fusion.properties` file

The `fusion.properties` file is the properties file for Integration Composer. Among other things, these properties specify Maximo and Integration Composer database-related properties and application properties. This verification task is to ensure that, after you have installed Integration Composer, critical property settings in the `fusion.properties` file are correct.

Before you begin

The Integration Composer `fusion.properties` file is located as follows:

`itic_install_dir\data\properties\fusion.properties`

About this task

To review the critical settings in your `fusion.properties` file:

1. Locate the Integration Composer `fusion.properties` file in your Integration Composer installation directory, `itic_install_dir..`

- In the IBM Tivoli Maximo Database-Related Properties section, verify that the database schema owner, JDBC driver specification, and JDBC URL specification are correct. Use the following table as a guide:

Property	Description	Value
mxe.db.schemaowner	Database schema owner	Enter the appropriate schema for your database; for example, dbo.
mxe.db.driver	JDBC driver specification	This varies depending on the database, for example: IBM DB2 com.ibm.db2.jcc.DB2Driver Oracle JDBC Thin driver: oracle.jdbc.driver.OracleDriver i-net Opta driver (SqlServer): com.inet.tds.TdsDriver
mxe.db.url	JDBC database URL	This varies depending on the database, for example: IBM DB2 jdbc:db2://host_name:host_port/database_name Oracle JDBC Thin driver: jdbc:oracle:thin:@host_name:host_port:host_SID i-net Opta driver (SqlServer 7.0 or higher): jdbc:inetdae7:host_name:host_port?database=database_name
mxe.db.user	Database user login name	

- UNIX** In the IBM Tivoli Integration Composer (ITIC) Application Properties section, users of UNIX-based operating systems should check that the **mxe.fusion.browser** property specifies netscape. For UNIX, Netscape is the *only* supported Web browser for Integration Composer:
mxe.fusion.browser=netscape

Note: **Windows** For Windows operating systems, the browser always defaults to Microsoft Windows Explorer.

Changing the memory allocation in the startFusion file (optional)

The *startFusion* file, named startFusion.bat in Windows operating systems or startFusion.sh in UNIX-based operating systems, is the startup file for the Integration Composer graphical user interface. This verification task is to ensure that, after you have installed Integration Composer, the memory allocation in the startFusion file is correct.

Before you begin

This task is optional. You need to perform it only if the Integration Composer graphical user interface does not start as described in “Confirming the installation” on page 216.

About this task

The Integration Composer startFusion file is located in the Windows and UNIX installation directories, as follows:

Windows	<code>itic_install_dir\bin\startFusion.bat</code>
UNIX	<code>itic_install_dir/bin/startfusion.sh</code>

When you install Integration Composer, the installation program assigns 1536 megabytes as the default amount of virtual RAM to allocate to the application. But, for example, if your server only has 1GB of physical memory, the 1536M setting will not work for you.

Procedure

If the Integration Composer graphical user interface does not start, check the memory setting for the start javaw.exe command in the startFusion file, and decrease memory as necessary.

Example

For example, change `-Xmx1536M` to `-Xmx1024M`.

Changing the memory allocation in the commandLine file (optional)

The *commandLine* file, named `commandLine.bat` in Windows operating systems or `commandLine.sh` in UNIX-based operating systems, is the startup file for the Integration Composer command line interface. This verification task is to ensure that, after you have installed Integration Composer, the memory allocation in the `commandLine` file is correct.

Before you begin

This task is optional. You need to perform it only if the Integration Composer command line interface does not start.

About this task

The Integration Composer `commandLine` file is located in the Windows and UNIX-based installation directories, as follows:

Windows	<code>itic_install_dir\bin\commandLine.bat</code>
UNIX	<code>itic_install_dir/bin/commandLine.sh</code>

When you install Integration Composer, the installation program assigns 1536 megabytes as the default amount of virtual RAM to allocate to the application. But, for example, if your server only has 1GB of physical memory, the 1536M setting will not work for you.

Procedure

If the Integration Composer command line interface does not start, check the memory setting for the java command in the `commandLine` file, and decrease memory as necessary.

Example

For example, change `-Xmx1536M` to `-Xmx1024M`.

Uninstalling Integration Composer

This section provides instructions for removing Integration Composer from Microsoft Windows and UNIX-based operating systems.

Uninstalling Integration Composer on Windows operating systems

1. In Microsoft Windows Explorer, go to the uninstall folder, *installation_dir*\Uninstall_Integration_Composer, where Integration Composer 7.2 was installed.
2. In the uninstall folder, double-click the uninstall file, `Uninstall_Integration_Composer.exe`. The Integration Composer utility for uninstalling the application displays the Uninstall IBM Tivoli Integration Composer window.
3. Click **Uninstall**. The Uninstall IBM Tivoli Integration Composer progress window is displayed as the uninstall utility removes the application.

Note: If necessary, you can click **Cancel** to stop the uninstallation.

When the removal of Integration Composer is finished, the Uninstall Complete window is displayed.

4. Click **Done**. The removal of Integration Composer is completed.
5. *Optional.* When the utility removes Integration Composer, one or more files sometimes remain in the installation directory. (For example, these files might be files that someone manually put into the directory, such as mapping files or schema files that the user imported, or they might be log files that Integration Composer created.) You can delete these files manually.

Uninstalling on UNIX operating systems

1. Go to the uninstall folder, *installation_dir*\Uninstall_Integration_Composer, where Integration Composer 7.1.1 was installed.
2. In the uninstall folder, do one of the following options:
 - If you installed the Integration Composer using the X Window application, type:

```
sh ./Uninstall_IBM_Tivoli_Integration_Composer
```
 - If you installed the Integration Composer using console mode, type

```
sh ./Uninstall_IBM_Tivoli_Integration_Composer -i console
```

The instructions that follow describe the remaining uninstallation steps using console mode.

3. Press **Enter** to initiate the command from the previous step. The Uninstalling progress bar is displayed as the uninstall utility removes the application.
When the removal of Integration Composer is finished, you are returned to the command prompt.
4. [Optional.] After the utility removes Integration Composer, one or more files sometimes remain in the installation directory. (For example, these files might

be files that someone manually put into the directory, such as mapping files or schema files that the user imported, or they might be log files that Integration Composer created.) You can delete these files manually.

Chapter 17. IBM Tivoli Asset Management for IT post installation tasks

There are some post installation tasks that must be completed following a successful Asset Management for IT deployment.

1. Provide values to Software Knowledge Base Toolkit cron task in Asset Management for IT user interface and load the software catalog from Software Knowledge Base Toolkit.
2. Provide values to Asset Discovery for z/OS cron task in Asset Management for IT user interface and load the software catalog from Asset Discovery for z/OS.
3. Load the Software Knowledge Base Toolkit catalog from Software Knowledge Base Toolkit into Asset Discovery for Distributed.
4. Define the launch-in-context to Software Knowledge Base Toolkit from Asset Management for IT user interface
5. Define the launch-in-context to Software Knowledge Base Toolkit from Asset Discovery for Distributed user interface
6. Define the Data sources/Mappings for Asset Discovery for Distributed in Integration Composer and import discovered data from Asset Discovery for Distributed
7. Define the Data sources/Mappings for Asset Discovery for z/OS in Integration Composer and import discovered data from Asset Discovery for z/OS.

The tasks include the following areas:

- “Initial data configuration” on page 223
- Chapter 8, “Installing IBM Tivoli Asset Management for IT language pack,” on page 153

Related tasks

“Performing post installation tasks for the J2EE server”

During the installation process, the Tivoli Asset Management for IT installation program provided you with the option of automatically configuring Asset Management for IT middleware. Use this procedure to perform post installation steps for the J2EE server.

Performing post installation tasks for the J2EE server

During the installation process, the Tivoli Asset Management for IT installation program provided you with the option of automatically configuring Asset Management for IT middleware. Use this procedure to perform post installation steps for the J2EE server.

About this task

- If you elected to have the Asset Management for IT installer automatically configure the middleware, then it will, among other tasks, perform J2EE server configuration for you.
 - If you elected to manually configure middleware for use with Asset Management for IT, you will have to manually configure the J2EE server.
1. Invoke a browser window and open the administrative console by typing in the browser address bar:
`http://computer_name:9060/admin.`

This URL address depicts the default port number (9060) and context (admin) for the administrative console. Enter a user name to log in.

Note: The browser will be redirected to a secure port (9043).

2. Create the MXServer application server. This step is only necessary if you did not install WebSphere Application Server using the middleware installer.
 - a. Expand the Servers link and click **Application servers**.
 - b. Click **New**.
 - c. Type MXServer and click **Next**.
 - d. Accept all default settings and click **Next**.
 - e. Accept default settings and click **Next**.
 - f. Click **Finish**.
 - g. Click **Preferences**.
 - h. Check the **Synchronize changes with Nodes** check box, and then click **Apply**.
 - i. Click **Save**.
 - j. Click **OK**.
3. Edit JVM Memory Settings for the application server:
 - a. From the **Servers** link in the tree view click **Application servers**.
 - b. Click **MXServer** in the main window.
 - c. From the **Server Infrastructure** group, expand the **Java and Process Management** link.
 - d. Click **Process Definition**.
 - e. Click **Java Virtual Machine**.
 - f. Scroll down and type 512 for **Initial Heap Size** and 1024 for **Maximum Heap Size** and click **OK**.
 - g. Click **Save** in the messages box.
4. Edit JVM Memory Settings for the deployment manager:
 - a. From the **System administration** link in the tree view click **Deployment manager**.
 - b. From the **Server Infrastructure** group, expand the **Java and Process Management** link.
 - c. Click **Process Definition**.
 - d. Click **Java Virtual Machine**.
 - e. Scroll down and type 512 for **Initial Heap Size** and 1024 for **Maximum Heap Size** and click **OK**.
 - f. Click **Save** in the messages box.
5. Start the application server:
 - a. From the **Servers** link in the tree view click **Application servers**.
 - b. Select the check box beside **MXServer**.
 - c. Click **Start**.
6. Identify the HTTP Transfer Port Numbers:
 - a. Expand **Servers** → **Application servers**, and click **MXServer** from the main window.
 - b. Open the **Web Container Settings** and click **Web container transport chains**. Note the default port number as it appears with WC_defaulthost (9080).

- c. Click **Save**.
7. Create the virtual host:
 - a. Expand the Environment link from the tree view.
 - b. Click **Virtual Hosts**.
 - c. Click **New**.
 - d. In the **General Properties** section, type `maximo_host` in the **Name** box.
 - e. Click **Apply**.
 - f. Click **Save**.
 - g. From the Virtual Hosts window, click `maximo_host`.
 - h. Click the **Host Aliases** link.
 - i. Click **New**.
 - j. Type * (asterisk) for Host Name and type the HTTP port number (by default 80).
 - k. Click **OK**.
 - l. Click **New**.
 - m. Type * (asterisk) for Host Name and type 9061 for the port number.
 - n. Click **OK**.
 - o. Click **New**.
 - p. Type * (asterisk) for Host Name and type 9443 for the port number.
 - q. Click **OK**.
 - r. Click **New**.
 - s. Type * (asterisk) for Host Name and type 9080 for the port number.
 - t. Click **OK**.
 - u. Click **New**.
 - v. Type * (asterisk) for Host Name and type 9044 for the port number.
 - w. Click **OK**.
 - x. From the navigational breadcrumb trail, click `maximo_host`.
 - y. Click **Apply** and then click **OK**.

Related concepts

Chapter 17, "IBM Tivoli Asset Management for IT post installation tasks," on page 221

There are some post installation tasks that must be completed following a successful Asset Management for IT deployment.

Initial data configuration

Once you have successfully installed and configured Asset Management for IT components, there are several data configuration tasks you must complete prior to using Asset Management for IT.

Signing in using a default user ID

User management is managed through the application server or the directory server you have configured to use with Asset Management for IT. When first installed, Asset Management for IT contains the following default user IDs, which are members of the specified security groups described in this section.

Before you begin

When first installed, Asset Management for IT contains the following default user IDs, which are members of the specified security group:

Important: Before you begin this procedure, ensure you have the following users and groups created:

Table 26. Asset Management for IT users and groups

User	Groups
wasadmin	
maxadmin (maxadminusr for Microsoft Active Directory)	maxadmin
mxintadm	maxadmin
maxreg	

The default password for each user ID is the same as the User Name (for example, maxadmin is both the user name and default password).

Note: User names and passwords are case sensitive. The default user names and passwords are lowercase.

About this task

To sign in, complete the following steps:

1. Open a browser window.
2. Navigate to the Asset Management for IT log in URL, for example:

`http://host_name:port_number/maximo.`

3. Enter the user name maxadmin (lower case).
4. Enter the password maxadmin (lower case), and click Enter. The software displays an empty start center.

Related concepts

“Planning for security” on page 18

Planning for security includes choosing a security option, deciding which users will work with each application in Asset Management for IT, and optionally which users can work with which configuration items.

Configuring SMTP

If you did not configure SMTP parameters during installation, you will have to configure them through the product console.

Before you begin

This task **must** be completed before you begin the tasks described in “Applying changes to the database” on page 226.

About this task

To configure SMTP for Asset Management for IT, complete the following steps.

1. Login to the console as maxadmin.

2. Navigate to **Go To** → **System Configuration** → **Platform Configuration** → **System Properties**
3. Using the Filter feature, search for the **mail.smtp.host** Property Name.
4. Expand the **mail.smtp.host** property and set the Global Value attribute to your SMTP host.
5. Select the **mail.smtp.host** record checkbox.
6. Click the Live Refresh icon in the toolbar.
7. From the Live Refresh dialog, click **OK**.
8. Using the Filter feature, search for the **mxe.adminEmail** Property Name.
9. Expand the **mxe.adminEmail** property and set the Global Value attribute to your e-mail address.
10. Select the **mxe.adminEmail** record checkbox.
11. Click the Live Refresh icon in the toolbar.
12. From the Live Refresh dialog, click **OK**.

Create currency codes

You need to define a currency code for an organization.

About this task

To define a currency code for an organization, complete the following steps:

1. Open the Currency Code application for Users by selecting **Go to** → **Financial** → **Currency Code**.
2. Click **New Row**.
3. Enter a currency name. For example, USD.
4. Click **Save**.

Create item and company sets

You need to define item and company sets for an organization.

About this task

To define item and company sets for an organization, complete the following steps:

1. Open the Sets application for Users by selecting **Goto** → **Administration** → **Sets**.
2. Click **New Row**.
3. Enter a company set name. For example, IT Comps.
4. Enter ITEM in the **Type** field.
5. Click **New Row**.
6. Enter an item set name. For example, IT Items.
7. Enter COMPANY in the **Type** field.
8. Click **Save**.

Create an organization

Define at least one organization for Asset Management for IT.

About this task

To define an organization, complete the following steps:

1. Open the Organizations application by selecting **Goto >Administration >Organizations**
2. Click the **New Organization** icon in the toolbar.
3. Enter an organization name in the **Organization** field. For example, ENGLENA.
4. Enter the base currency you defined in the **Base Currency 1** field. For example, USD.
5. Enter the item set you defined in the **Item Set** field. For example, IT Items.
6. Enter the company set you defined in the **Company Set** field. For example, IT Comps.
7. Enter the default item status of PENDING in the **Default Item Status** field.
8. Click **Sites** tab.
9. Click **New Row**.
10. Enter a site name in the **Site** field. For example, B901.
11. Click **Save**.

Create a general ledger account component

You need to create a general ledger account component for Asset Management for IT.

About this task

To create a general ledger account component, complete the following steps:

1. Open the Database Configuration application by selecting **Goto → System Configuration → Platform Configuration → Database Configuration**.
2. Select **GL Account Configuration** from the **Select Action** drop-down menu.
3. Click **New Row**.
4. Enter a component name in the **Component** field. For example, MYCOMPONENT.
5. Enter a numerical length for the component. For example, 5.
6. Enter a type for the component. For example, ALN.
7. Click **OK**.

Applying changes to the database

When you create a general ledger account component, it must be applied to the Maximo database.

About this task

To apply configuration changes to the Maximo database, complete the following steps.

1. Login to the Maximo console as maxadmin.
2. Navigate to **Go To → System Configuration → Platform Configuration → Database Configuration**. Every object that must be updated in the Maximo database will display a status of To Be Added.
3. On the Select Action drop-down list, select **Manage Admin Mode**.
4. Click **Turn Admin Mode ON**, and then click **OK** when prompted. This task will take several minutes to complete. You can use the **Refresh Status** button to view progress.

5. Once Admin Mode has been successfully enabled, select **Apply Configuration Changes**, which will apply the changes to the Maximo database. To Be Changed should not appear in the status column for objects listed.
6. Turn Admin Mode OFF.
 - a. Navigate to **Go To → System Configuration → Platform Configuration → Database Configuration**.
 - b. From the Select Action drop-down list, select **Manage Admin Mode**.
 - c. Click **Turn Admin Mode OFF**, and then click **OK** when prompted. Failing to turn off Admin Mode within the application will cause cron tasks to fail.

Create a general ledger account

You need to create a general ledger account for Asset Management for IT.

About this task

To create a general ledger account, complete the following steps:

1. Open the Chart of Accounts application by selecting **Goto → Financials → Chart of Accounts**.
2. Click the name of your organization to select it. For example, click **ENGLENA**.
3. Select **GL Component Maintenance** from the **Select Action** drop-down menu.
4. Click **New Row**.
5. Add a GL Component value and then click **OK**. For example, 1234.
6. Click **New Row**.
7. Select your General Ledger Account.
8. Click **Save**.
9. Open the Organizations application by selecting **Goto → Administration → Organizations**.
10. Click the organization name you created. For example, ENGLENA.
11. From the **Clearing Account** field, select the General Ledger Account you just created.
12. Select **Active**.
13. Click **Save**.

Update General Ledger Component Type Authorization

You need to update the general ledger component type authorization for Asset Management for IT

About this task

To authorize a Security Group to change a general ledge component type, complete the following steps:

1. Open the Security Groups application by selecting **Go To → Security → Security Groups**.
2. Select the Group that will be provided authorization (for example, PMSCOA).
3. Click the **GL Components** tab.
4. Click the **Authorized** checkbox for each GL Component.
5. Click **Save**

Create default insert site

You need to create a default insert site for Asset Management for IT.

About this task

To create a default insert site, complete the following steps:

1. Open the Users application by selecting **Goto** → **Security** → **Users**.
2. Search for maxadmin and then select it to open the record for maxadmin.
3. Enter the site you created earlier (“Create an organization” on page 225) in the **Default Insert Site** field. For example, B901.
4. Enter the site you created earlier in the **Storeroom Site for Self Service Requisitions** field. For example, B901.
5. Click **Save**.
6. Open the WebSphere Administrative Console and restart the MXServer application server.

Results

If you encounter an error message that indicates that the record is being updated by another user, log out as MAXADMIN and then log back in.

Create a Work Type

After you installed Asset Management for IT, you might need to optionally create a Work Type.

About this task

To create a Work Type:

1. Open the Organizations application by selecting **Go to** → **Administration** → **Organizations**.
2. Search for the organization you created, for example, ENGLENA.
3. Click the name of the organization to open the record for that organization.
4. Select **Work Order Options** → **Work Type** from the **Select Action** drop-down menu.
5. Click **New Row**.

What to do next

Depending on your product deployment configuration, select the Work Type of your choice from a drop-down list.

Specify a top-level class for IT assets and software

To distinguish IT assets from other types of assets, specify a top-level class for IT assets. Any asset that belongs to the hierarchy of the top-level IT asset class is an IT asset. Also, define a top-level class for software.

Before you begin

Before you can specify top-level classifications for IT assets and software, you must create a classification structure for IT assets and software in the Classifications application.

About this task

The class structure ID that is displayed in the System Settings window is a value stored in the database. If the classifications structure changes such that the top-level IT asset class no longer exists at the same place in the hierarchy, the **IT Asset Class Structure ID** field will remain populated, but the **IT Asset Top-Level Class** field will be blank or show the wrong class. Consequently, if changes are made to the database, and the classification is moved within the classification structure, or deleted and re-added, you must repeat this procedure to update the class structure ID.

The steps required to specify a top-level classification for IT assets and software follow.

1. On the navigation bar in Asset Management for IT, click **Go To** → **Administration** → **Organizations**.
2. From the Select Action menu in the Organizations application, select **System Settings**.
3. To specify the top-level IT asset, complete the following steps:
 - a. In the IT Options section in the Systems Settings window, in the **IT Asset Top-Level Class** field, click the Detail Menu and select **Classify**. If necessary, you can select **Clear Classification** to clear the value displayed and then click **Classify**.
 - b. In the Classify window, select the top-level asset class for IT assets by clicking the blue square to the left of the classification name. The application closes the Classify dialog box and populates the **IT Asset Top-Level Class** field.
4. To specify the top-level software classification, complete the following steps:
 - a. In the IT Options section in the Systems Settings window, in the **IT Software Top-Level Class** field, click the Detail Menu and select **Classify**.
 - b. In the Classify window, select the top-level asset class for IT assets by clicking the blue square to the left of the classification name. The application closes the Classify dialog box and populates the **IT Software Top-Level Class** field.
5. Click **OK** to save the settings and close the dialog box.

Create a classification structure for IT assets

Before you can implement IT asset management, you must define a classification structure for IT assets.

About this task

Asset Management for IT provides a Classifications application that lets administrators set up a nested, hierarchical structure in which to classify information on a company's assets. This structure lets you group assets with similar or common characteristics into categories or classes. You can use the classification to retrieve instances of assets that belong to the class. For example, you can specify that the class computers has the following subclasses: notebooks, servers, desktops. If you want to analyze or review data about all notebooks in your enterprise, you can search for all assets classified as notebooks and retrieve instances of notebooks.

Best practices content for creating classifications is provided in the Open Process Automation Library.

The steps for creating classifications follow.

1. On the navigation bar in Asset Management for IT, click **Go To** → **Administration** → **Classifications**.
2. In the Classifications application, create classifications as needed. For instructions about creating classifications and other information related to classifications, see the integrated online help for the Classifications application in the Asset Management for IT user interface.

What to do next

After you create an IT asset classification structure, specify the top-level IT asset classification and the top-level software classification in the Organizations application.

Signing out and signing in

When you change a security group that your user ID is a member of, sign out and sign in again in order to see the changes.

Example

For example, even though you have granted the MAXADMIN group permission to create start center templates, the actions are not visible until you sign in again.

1. Sign out as MAXADMIN.
2. Sign in as MAXADMIN.

Manually configuring the VMMSYNC cron task for Microsoft Active Directory

This topic details how to manually configure the VMMSYNC cron task for Microsoft Active Directory after you installed Asset Management for IT

About this task

VMMSYNC is the cron task that schedules the synchronization between Asset Management for IT and the directory server and is configured using the Maximo console user interface . This procedure is required if you use Microsoft Active Directory as your directory server. For more general information on configuring the VMMSYNC cron task, refer to “Synchronizing data” on page 267.

The steps below detail how to reconfigure the VMMSYNC cron task for use with Microsoft Active Directory.

To modify the VMMSYNC cron task for Microsoft Active Directory, complete the following steps:

1. Open a Web browser and point to `http://host_name/maximo`.
2. Log into Asset Management for IT using the maxadmin user ID.
3. From the Asset Management for IT interface, navigate to **Go To** → **System Configuration** → **Platform Configuration** → **Cron Task Setup**.
4. Type VMM in the **Cron Task** field, and press Enter.
5. Locate the **VMMSYNC** cron task, and click it.
6. Configure the following values:

Active?

Enable the **Active?** option by selecting the check box.

Credential

Password for wasadmin in LDAP

GroupMapping

Edit the **basedn** entry of the XML file and customize it to use the organizational unit *ou* and domain name *dc* values you defined for your organization when setting up Asset Management for IT middleware.

For example,

```
<basedn>ou=Groups,ou=SWG,dc=itsm,dc=com</basedn>
```

GroupSearchAttribute

cn

Principal

cn=wasadmin,ou=Users,ou=SWG,dc=itsm,dc=com

SynchAdapter

psdi.security.vmm.DefaultVMMSyncAdapter

SynchClass

psdi.security.vmm.VMMSynchronizer

UserMapping

Edit the **basedn** entry of the XML file and customize it to use the organizational unit *ou* and domain name *dc* values you defined for your organization when setting up Asset Management for IT middleware.

```
<basedn>ou=Users,ou=SWG,dc=itsm,dc=com</basedn>
```

UserSearchAttribute

uid

You will have to click the arrow located in the header of the Cron Task Parameters table to view all parameters.

7. Click the **Save** icon.

Results

The updated parameters will be used at the next scheduled synchronization.

Tuning DB2

This section details how to tune DB2 after you have completed installation.

About this task

Asset Management for IT provides scripts that can be used to tune DB2. The use of these scripts is strictly optional and contain configuration parameters that might not be ideal for all environments. However, you can modify these scripts to suit your particular configuration and workload. Before modifying these scripts, you should make a backup copy of the original script.

The following database configuration parameters will be set:

- DFT_QUERYOPT 2
- LOCKLIST 15000 DEFERRED
- MAXLOCKS 60
- PCKCACHESZ 12600

- DBHEAP 2000
- CATALOGCACHE_SZ 800
- LOGBUFSZ 256
- UTIL_HEAP_SZ 10000
- APP_CTL_HEAP_SZ 16384 DEFERRED
- STMTHEAP 16384
- APPLHEAPSZ 2048
- STAT_HEAP_SZ 8196
- CHNGPGS_THRESH 40
- MAXFILOP 200
- LOGFILSIZ 2048 DEFERRED
- LOGPRIMARY 10
- LOGSECOND 15 DEFERRED

The following database manager configuration parameters will also be set:

- PRIV_MEM_THRESH 32767
- NUMDB 2

The DB2 tuning scripts are found in the *tamit_install_dir/scripts/database* directory, and must be run by a user with database administration authority.

Windows

Windows

```
db2tuning.cmd [ dbName [ dbInstance ] ]
```

UNIX

UNIX

```
db2tuning.sh [ dbName [ dbInstance ] ]
```

If the *dbName* is not provided, it will default to MAXDB71.

If the *dbInstance* is not provided it will default to ctginst1. If a database instance other than the default is needed, the *dbName* must also be provided.

Process solution package installation methods

Included within Asset Management for IT are common installation programs that provide you with the ability to manage the software lifecycle of Asset Management for IT process solutions, including functions to query, install, upgrade, and uninstall process solution packages. These common installation programs are collectively referred to as the *process solution installation programs*.

Asset Management for IT provides a flexible approach for incremental deployment of service management functionality using separately packaged process solutions. Process solutions can be partitioned into Process Manager Products and Integration Modules.

Process solution packages can be installed and deployed using two mechanisms:

Process Solution Installation Wizard

The process solution installation wizard provides you with a user interface for installing process solution packages.

Process Solution Command Line Interface

The process solution command line interface allows you to install process solution packages from a command line.

Note that Asset Management for IT must have been completely deployed, including post-installation steps, before the installation and deployment of additional process managers.

Related tasks

“Installing language packs with Process Solution Installer” on page 155
The Process Solution Installer guides you through the installation of a process manager product (PMP) or Integration Module. Use the Process Solution Installer to refresh languages to synchronize them with Maximo languages.

Software life cycle operations

Process solutions are versioned software components. The Process Solution Installation programs support a variety of software life cycle operations that might be applied against process solutions.

The following software life cycle operations are available:

Base Install

This operation installs and deploys a new process solution into your IBM Tivoli Asset Management for IT environment.

Add Feature and Modify Feature

These operations allow specific features within a package to be added or removed after the package has been installed.

Incremental Update or Upgrade

Once installed, a process solution might be updated in several ways. An **Incremental Update** or **Upgrade** operation modifies the existing installed process solution and changes its version. Often a process solution fix pack will be applied using the **Incremental Update** operation.

Apply Fix

Another operation that can be used to update an installed process solution is the **Apply Fix** operation. This operation is used to install individual interim fixes or patches to a currently installed process solution.

Back off, Undo, Undo Fix

Some **Incremental Updates** or **Fixes** are designed to be able to be removed or *backed off*. The **Undo** operation is used to remove the effects of an Incremental Update operation and return the process solution to its previous version and state. The **Undo Fix** operation removes a currently installed interim fix from a process solution.

Uninstall

The **Uninstall** operation removes a currently installed process solution.

Process solution packages

A *process solution package* is a self-contained archive file of installation artifacts and deployment logic that can be deployed using the process solution installation programs.

Installation artifacts are the files and content that are installed into your Asset Management for IT environment to enable the services management functionality of the Process Manager Product or Integration Module. For example, a Process Manager Product will provide J2EE application content and database content.

The deployment logic consists of the actions that are carried out in order to deploy the process solution into the Asset Management for IT environment. Typically,

these actions include building and deploying J2EE applications, running database scripts that load the process solution content into the database, and adding users and groups for security. Additionally, optional sample data can be installed.

The Asset Management for IT product provides process solution packages for the Configuration Management and Change Management Process Manager Products. These packages are automatically installed when Asset Management for IT is installed.

Package types

Closely related to the concept of the software life cycle operation is software package type.

The Process Solution Installation programs are able to process the following package types:

Base Install Package

It is required to install a new process solution using the Base Install operation.

Incremental Update Package

It is required when performing an Upgrade operation.

Fix Package

It is required when applying an interim fix to a process solution.

Full Update Package

It can be used in two separate operations. It might be used to perform a Base Install operation if no instance of the process solution is currently installed or it might be used to perform an Upgrade operation on a currently installed process solution.

Aggregation package

It consist of multiple Process Solution Installation installable packages that can be deployed as one package in a single process solution installation client CLI or user interface session.

The process solution installation programs ensure that the appropriate package type is processed for any given operation.

The Process Solution Command Line Interface will issue appropriate messages when an inappropriate package type is specified for a life cycle operation. For example, a message would be issued if a Fix Package was specified for a Base Install operation. You can use the showavail action of the Process Solution Command Line Interface to determine the package type associated with a process solution installable package.

The Process Solution Installation Wizard will determine the operation to employ based on the type of the package and the current state of the installed components. For example, if you select to deploy a Full Update Package, the Process Solution Installation Wizard will perform an Upgrade operation if a suitable base version of the process solution is already installed and a Base Install operation if no suitable base version is detected. When using the Process Solution Installation Wizard, you can view the package type for the package you selected on the Package Validation Results panel.

The following table highlights the supported operations with their required package types:

Table 27. Operations and package types

Operation	Package Type
Base Install	Base Install Package or Full Update Package
Incremental Update/Fix Pack	Incremental Update Package or Full Update Package
Apply Interim Fix	Fix Package

Aggregation packages

A process solution package might be composed from other process solution packages. This technique allows construction of single offering-level packages that might be deployed using a single session with the process solution installation programs. Such a package is referred to as a process solution aggregate package. The sub-packages that are bundled within a process solution aggregate package are referred to as child packages.

Process solution aggregate packages are deployed using the same mechanisms used to deploy non-aggregate packages. All actions defined within the process solution command line interface may be applied to a process solution aggregate package. Similarly, the process solution installation wizard can be used to base install, upgrade, and apply fixes to a process solution aggregate package.

Process solution aggregate packages support the same package types (Base Install, Full Update, Incremental Update, and Fix) and the same life cycle operations as non-aggregate packages.

Process solution aggregate packages often expose their child packages as selectable features of the aggregate. This permits you to selectively deploy only the pieces of the aggregate that you prefer.

A process solution aggregate has a version, unique identifier, and display name information just like a non-aggregate package. When you use the *showinstalled* action of the process solution command line interface, the output includes information on the installed parent aggregate package and any of the child packages within that parent aggregate package that have also been installed.

Determining which process solution installation program to use

The process solution installation programs provided each have unique benefits and both should be used in the appropriate scenario.

You should consider the following facts when deciding which process solution installation program to use.

- The Process Solution Installation Wizard provides a user experience typical of most software installation programs. You select the process solution package to install and provide additional installation options from wizard panels. The Process Solution Installation wizard is an attended installation.
- The Process Solution Command Line Interface provides a simple command line syntax for specifying the life cycle operation to perform and the package against which the operation is performed. You enter the Process Solution Command Line Interface command and messages and command output are displayed to the command line as the command is processed.

- All functions and operations are available in the Process Solution Command Line Interface program. Only a subset of those functions is supported in the Process Solution Installation Wizard. Generally, you should use the Process Solution Installation Wizard if it supports the operation you need to perform.
- The Process Solution Installation Command Line Interface is useful where you require an unattended or silent installation. The Process Solution Installation Command Line Interface will pass return codes detailing the success of the command back to the operating system. This makes the Process Solution Installation Command Line Interface suitable for use in a higher-level deployment automation package or script.

Supported operations for the process solution installation programs

There are multiple operations and functions that are supported by the Process Solution Installation Wizard and Process Solution Command Line Interface.

The following table highlights the operations and functions that are supported by the Process Solution Installation Wizard and Process Solution Command Line Interface.

Table 28. Process solution operations

Operation	Supported by Command Line Interface	Supported by Installation Wizard
List Installed Packages	Yes	No
List Available Packages	Yes	No
Base Install	Yes	Yes
Incremental Update/Fix Pack	Yes	Yes
Full Update	Yes	Yes
Undo Incremental Update/Fix Pack	Yes	No
Uninstall	Yes	No
Apply Interim Fix	Yes	Yes
Undo Interim Fix	Yes	No
List Installed Fixes for a Package	Yes	No
Refresh language support	Yes	No
Load Language Support Files	Yes	Yes
Add Features	Yes	Yes
Remove Features	Yes	Yes
Show Available Features	Yes	Yes

Note: The process solution installation programs allow an uninstall action to be initiated against a package. However, **not all packages support the uninstall action**. In particular the packages distributed and installed with Asset Management for IT do not support the uninstall action. This includes the Common, Configuration Management, and Change Management. If an uninstall action is initiated against a package that does not support this action, a message detailing this condition is displayed. If you want to restore your environment to the state before the installation of the Asset Management for IT process managers, you must backup your affected middleware servers **before** running the Asset Management for IT installation program.

Before using the process solution installation programs

Review the following prerequisite information before using process solution installation programs.

When you perform a deployment operation using the process solution installation programs, you are running actions that modify the configuration and content of your J2EE, database, and directory middleware servers. The following steps should be reviewed before invoking the process solution installation programs.

Have Middleware Login Information Available

The process solution installation programs require access to middleware servers in order to automate the deployment of the process solution package. You will need to know the administrative user IDs and passwords for the impacted middleware servers. The actual middleware servers whose login information is required will depend on the process solution package being installed. The process solution installation programs ensure that any required login information is specified before continuing with the deployment operation.

Backup Middleware Servers and Administrative Workstation

You should create backups for impacted J2EE, database, and directory servers before you deploy a process solution package using the process solution installation programs.

Ensure Middleware Servers Are Started

Start any impacted middleware servers before running the process solution installation programs. Before the actions associated with a package are executed, the process solution installation programs will attempt to connect to the middleware servers using the middleware login information that you specify. If the targeted middleware servers are not started or if connections to the middleware servers cannot be established with the specified middleware login information, then the process solution installation programs will display error messages and not continue on with the deployment actions.

Managing process solution deployment from the IBM Tivoli Asset Management for IT administrative workstation

Process solution deployment is managed from the Asset Management for IT administrative workstation.

Process solution installation programs are installed on the Asset Management for IT administrative workstation (see Figure 1 on page 1), when the Asset Management for IT is installed. In addition to invoking process solution installation programs from the Asset Management for IT administrative workstation, you must also have access to any process solution packages from the Asset Management for IT administrative workstation.

The Asset Management for IT administrative workstation provides a deployment hub from which the process solution packages are deployed. In order to automate deployment, the process solution installation programs will connect to either local or remote middleware servers from the Asset Management for IT administrative workstation.

Typical deployment operation

Process solution deployment is integrated tightly with Asset Management for IT deployment.

Process solutions use the Asset Management for IT deployment model. In this model, as process solution packages are deployed, database content and metadata in the package is loaded into the Maximo database and the Maximo core J2EE applications are redeployed with Java code provided in the process solution package. This effectively merges the functionality of the process solution package into the Maximo database and Maximo J2EE application.

High level deployment steps are:

1. Files in the process solution package are unpacked onto the Maximo installation directory on the Asset Management for IT administrative workstation. The Maximo installation directory contain the Maximo content for the process solution being deployed as well as any other currently installed Asset Management for IT process solutions or Maximo applications and industry solutions.
2. J2EE applications are rebuilt on the Asset Management for IT administrative workstation to contain the functionality of the process solution package. This functionality includes Java classes, report definitions, and other artifacts.
3. The process solution installation programs will deploy the update J2EE applications to the J2EE application server. This server can be local or remote to the Asset Management for IT administrative workstation.
4. Database content scripts associated with the package being installed are processed on the Asset Management for IT administrative workstation. This results in updates to the database.

Important: When you deploy process solution packages, the updates are made to the J2EE and database servers, which include redeploying the Asset Management for IT application. Deployment should be scheduled for a time when a brief interruption of service can be tolerated, such as during a scheduled maintenance period.

Selectable features

This section contains information on managing selectable content using features.

A process solution package might define one or more features that represent user-selectable, optional content. Examples of typical features include national language support and samples. Process solution installation methods support operations on features, including capabilities for querying, adding, and removing features.

Feature support in a process solution package is optional. Features are also package-specific. The process solution installation methods examine the process solution install package and ensure that only features defined within the package are able to be manipulated.

Attributes of a Feature

Associated with every feature are the following attributes:

- *Feature Identifier* represents a non-localized name by which the feature is uniquely identified within its package. When using the process solution command line interface, the Feature Identifier is used to specify the feature to add or remove.
- *Feature Display Name* is a localized label for the feature.
- *Parent Identifier* identifies the parent feature associated with a feature. A feature with no parent is termed a top level feature.

- *Install State* indicates whether the feature is installed.
- *Required Attribute* indicates whether the feature is a required feature. A required feature is a feature that must be installed if its parent feature is installed and may not be installed if its parent feature is not installed. A top level feature that is required is always installed.

Operations Associated with Features

Both the process solution command line interface and process solution installation wizard provide functionality for managing features associated with a process install package. This section describes those capabilities.

Installing Features during a Base Install

If a process solution package defines features, you can select the features to installation during the base installation of the package.

Installing Features Using the Wizard

For the process solution installation wizard, a Feature Selection Panel is displayed after license acceptance processing if the package being deployed supports features. The Feature Selection Panel displays a tree where the nodes in the tree are features and the tree nesting represents parent feature and child feature relationships. Each node has a check box that indicates the selection state of the feature. You select a feature to be installed by selecting the check box for the feature.

Installing Features Using the Command Line Interface

For the process solution command line interface, the **-addfeatlist** parameter on the **install** action allows you to specify the features to be installed during the base installation of the package. The value specified for this parameter is a colon separated list of Feature Identifiers representing the features to install.

Adding Features

After the base installation of a package, you can incrementally add features if there exists at least one feature not already installed for that package.

Adding Features Using the Wizard

When using the process solution installation wizard, if the package is already installed but has at least one feature not already installed, you can elect to install additional features after the Package Validation Panel is displayed.

Note that the Deployment Engine does not support both incremental feature add and removal in the same deployment operation. If the state of the installed features on a package is such that features can be both added or removed, then the Add or Remove Features Panel is displayed that allows you to select whether you want to add or remove features from the package.

If you select to install additional features from the Add or Remove Features Panel, the Feature Selection Panel is again displayed with the currently installed features checked and disabled. You may not uninstall currently installed features in this mode, but you may select additional features for installation.

Adding Features Using the Command Line Interface

For the process solution command line interface, a new **modfeatures** action allows you to install features to an already installed process solution package. The parameters on this action

are similar to the **install** action. You specify the path of the process solution package and required middleware userids and passwords. The **-addfeatlist** parameter on the **modfeatures** action allows you to specify the features to be added. The value specified for this parameter is a colon separated list of Feature Identifiers representing the features to be installed.

Removing Features

After the base installation of a package, you can incrementally remove or uninstall features if there exists at least one feature already installed for that package.

Feature Uninstall is Optional

Support for uninstall of features is optional. A process solution package that supports incremental feature installation might not support uninstall of its features. If the process solution package does not support uninstall of its features, then the process solution installation programs do not permit you to uninstall features on the package. The process solution installation wizard will not allow you to initiate feature uninstall operations against the package. The process solution command line interface will issue messages if uninstall operations are attempted against a package that does not support feature uninstall.

Removing Features Using the Wizard

When using the process solution installation wizard, if the package is already installed and has at least one feature already installed, you can elect to uninstall features after the Package Validation Panel is displayed.

As described above, if the state of the installed features on a package is such that features can be both added or removed, then the Add or Remove Features Panel is displayed that allows you to select whether you want to add or remove features from the package.

If you select to uninstall currently installed features from the Add or Remove Features Panel, the Feature Selection Panel is again displayed with the currently installed features checked. You may not install new features in this mode, but you may deselect currently installed features to trigger the uninstall operation against those features.

Removing Features Using the Command Line Interface

For the process solution command line interface, the **modfeatures** action described above also allows you to uninstall features that are already installed on a currently installed process solution package. The **-delfeatlist** parameter on the **modfeatures** action allows you to specify the features to be uninstalled. The value specified for this parameter is a colon separated list of Feature Identifiers representing the features to be uninstalled.

Showing Feature Information for a Package

The process solution installation programs allow you to display information on the supported and installed features for a process solution package.

Showing Feature Information Using the Wizard

The Feature Selection Panel of the process solution installation wizard displays the feature tree of a process solution package. This

panel depicts the parent-child relationships between the features and also displays whether the features are currently installed.

Showing Feature Information Using the Command Line Interface

For the process solution command line interface, the **showfeatures** action allows you to display information on the features associated with a process solution package. Input to the action is the path to the process solution package. The output lists the feature attributes for the features defined for the package.

Feature Selection Processing Rules and Behavior

When using the process solution installation programs to manage the features, the actual collection of features to install or uninstall are derived using a combination of the input selections/deselections you specify and a set of feature selection rules. For example, you may select a single feature for installation, but, due to feature selection rule processing, additional features may also be installed.

When you install or uninstall features, the process solution installation programs enforce these feature selection rules to ensure that the derived set of feature selections are valid and meet all the feature selection rules.

This section highlights the feature selection rules that are enforced by the process solution installation programs.

Summary of Feature Selection Rules

1. Features can be arranged in a Parent-Child tree structure. Child features cannot be installed unless their parent feature is installed.
2. A feature can be marked as required which indicates that the feature must be installed if its parent is installed. A top level feature that is marked required is always installed.
3. Features that are marked required can never be selected/deselected explicitly by you. The selection state of a required feature is always derived from the selection state of their parent feature.
4. A feature can have real content (files/actions) or can be a nesting feature which acts as a parent feature for other child features.
5. A Nesting Feature may not be installed unless at least one of its child features (with content) is also installed. This violation is detected during Feature Selection Validation. Message CTGIN0200E is issued when this rule is violated.
6. Special *select-if-selected* rules can be coded into the package to assert prerequisite dependencies between features. These are specific to a particular package. For example, select-if-selected rules can be defined in a package that ensures that Feature A is installed if Features B or C are installed.

Feature Selection Processing

1. When a child feature is selected, all its ancestor features (Parent, Grandparent, and so on) are selected as well.
2. When a parent feature is selected, any of its required child features are automatically selected.
3. When a feature is selected, that feature's select-if-selected rules are evaluated and any dependent features are automatically selected.
4. The above rules are applied against all features in the tree until there are no more features to select.

Feature Deselection Processing

1. When a parent feature is deselected, all its descendant features (Child features, Grandchild features, and so on) are deselected as well.
2. When a feature is deselected, all select-if-selected rules targeting that feature are evaluated and any dependent features are deselected.
3. The above rules are applied against all features in the tree until there are no more features to deselect.

Feature Selection Validation

The process solution installation programs enforce feature selection rules by performing a feature selection validation process. This is the process of deriving the complete set of features that are to be processed and determining if the user input violates any rules. If any feature rule violations are detected, then the operation to install or uninstall features is not carried out by the process solution installation programs.

Feature Validation Using the Wizard

When you use the process solution installation wizard, most rules are dynamically enforced as selections/deselections are made against the feature tree on the Feature Selection Panel. For example, when you select a child feature, all of its ancestor features are automatically selected.

Additional rules are validated when you have finished making your selections and attempt to move to the next panel. If any violations of the rules are detected, messages describing the violations are displayed on the Feature Selection Panel and you must correct your input before proceeding.

Feature Validation Using the Command Line Interface

For the process solution command line interface, the same feature selection rules are enforced and the complete set of features to install or uninstall is derived using those rules.

For example, if you specify only a child feature in your **-addfeatlist** parameter, the PSI CLI will add all ancestor features to the list that are actually installed. Similarly, if you specify a parent Feature on the **-delfeatlist** parameter, then any installed child features under that parent feature will also be uninstalled.

Additionally, the process solution command line interface will also perform additional checks against the features you specify. These checks include:

1. Ensuring that any feature identifier specified is a valid identifier for the package.
2. Ensuring that features specified using the **-addfeatlist** parameter are not already installed for the package.
3. Ensuring that features specified using the **-delfeatlist** parameter are already installed for the package.

Deferring J2EE and database related configuration

The process solution installation programs allow you to defer the automated redeployment of the Maximo J2EE applications and the automated update of the Maximo database with content from the process solution package being deployed. There are several reasons for why you might want to elect to skip this automation:

- Your organization may have policies that prohibit remote access and update of the J2EE application, database, or directory servers from the Asset Management for IT administrative workstation.
- You may not have the authority to perform administrative functions against the targeted middleware servers.
- Your organization may have existing procedures in place for how applications get deployed to middleware servers.

Using the Installation Wizard

When using the Process Solution Installation wizard, you can defer J2EE and database related configuration steps by selecting the *Defer the Regeneration and Redeployment of the Maximo J2EE Applications* and the *Defer the Update of the Maximo Database* check boxes on the Package Installation Options panel.

Using the Command Line Interface

When using the Process Solution Command Line Interface, you can defer J2EE and Database related configuration steps by specifying the `-skipj2eecfg` and `-skipdbcfg` command line flags.

Even if none of the scenarios above apply to you, you may still want to defer the automatic J2EE deployment if you are installing multiple process solution packages in sequence. The regeneration and redeployment of the Maximo J2EE applications is processing intensive and time consuming. When deploying a series of process solution packages, you can improve overall deployment time by only performing the regeneration and redeployment of the Maximo J2EE applications after all process solutions have been unpacked to the Maximo administrative workstation.

For example, if you are installing Process Manager Products A, B, and C as part of your deployment scenario, you would elect to skip the regeneration/redeployment of the Maximo J2EE applications when deploying Process Manager Products A and B. When deploying Process Manager Product C, you would specify the options to perform the redeployment of the Maximo J2EE applications.

Bear in mind that should you choose to not automate the update of the Maximo database, you should not use the process solution installation program with the `-loadsampdata` option because you will be unable to load sample data

You should always defer the configuration of the J2EE and database together. Never defer one and not the other.

If you defer configuration of the J2EE server, but allow the database to be configured, then the Maximo database is updated with the content of the process solution package, but the J2EE applications are not regenerated and redeployed with the content of that process solution package. You will be able to navigate to the application associated with the process solution package in the user interface, but if you attempt to create records with those applications, you will get an error messages. The applications contained in the installed package will remain unusable until the Maximo J2EE applications are regenerated and redeployed. Similarly, if you defer the configuration of the database, but allow the J2EE server to be configured, the Maximo J2EE applications are regenerated and redeployed with the content of the process solution package, but the Maximo database is not updated with the content of that process solution package. The applications associated with the process solution package will appear under the list of applications displayed from **Help** → **System** in the user interface, but will not appear in the list of

selectable applications. The applications contained in the installed package will remain unusable until the database configuration task is completed.

If you need to manually rebuild and redeploy the Maximo EAR file, refer to the System Administrator Guide for instructions.

Manually completing deployment

This procedure provides task information for manually deploying the process solution package after you elected to defer J2EE and database related configuration in the process solution installation program.

About this task

When you elect to defer automated configuration, you are responsible for manually invoking the configuration operations required to complete the deployment of the process solution package. Until the manual configuration steps are completed, the process solution package is in an incomplete and unusable state.

The following procedure assumes you have run the process solution installation program and deferred the J2EE and database configuration during package deployment.

To manually deploy the process solution package, complete the following steps:

1. Log in to the Integrated Solutions Console, navigate to **Servers** → **Application Servers**, and stop the MXServer server.
2. Update the Maximo database:

```
maximo_install_dir\tools\maximo\updatedb -s1
```
3. Rebuild the maximo.ear and maximohelp.ear files.

```
maximo_install_dir\deployment\buildmaximoear  
maximo_install_dir\deployment\buildhelpear
```
4. Uninstall the MAXIMO and MAXIMOHELP applications from within WebSphere Application Server.
5. Reinstall the MAXIMO and MAXIMOHELP applications within WebSphere Application Server.
6. Restart the MXServer.

Pre-deployment system check

Before the actions associated with a software life cycle operation are initiated, the process solution installation programs perform a system check activity. Associated with each process solution package are a set of requirements that must be satisfied before the deployment operation is carried out. The system check is a process that analyzes the requirements to determine that all requirements have been satisfied before continuing on with the deployment operation.

The actual requirements are specific to each process solution package. Requirements include disk space and memory consumption checks for the package and dependency checks between a process solution package and other process solution packages. When unsatisfied requirements are detected during the system check, the process solution installation programs display messages that describe the failed requirements. Before trying the deployment operation again, you will need to update your environment such that all requirements associated with the process solution package are satisfied.

Bypassing Unsatisfied Requirements

Under certain circumstances, you may find it necessary to bypass the system check processing and carry out a deployment operation even if one or more requirements associated with the process solution package are not satisfied. For example, a process solution package may have embedded an incorrectly specified disk space check which would prohibit the package from being installed on a system that has adequate free disk space required by the package.

Both process solution installation programs provide a mechanism that allow you to bypass failed requirements and continue with the deployment operation.

Using the Installation Wizard

When using the Process Solution Installation Wizard, a System Check Failed panel is displayed that displays messages for any failed requirements. From this panel, you can bypass the system check failures by selecting the check box entitled Ignore System Check Failures. When you select this check box, the Process Solution Installation Wizard continues with the deployment of the process solution package.

Using the Command Line Interface

When using the Process Solution Command Line Interface, you can bypass unsatisfied system check requirements by specifying the **-force** command line flag.

Package requirements represent criteria put in place to ensure a successful deployment. While it is not generally recommended to bypass any requirements, the process solution installation programs permit the following types of requirements to be bypassed:

- Capacity and consumption checks, for example, disk space and memory requirements for a package.
- Prerequisite, corequisite, and exerequisite relationships defined for a root package. For example, Package B might require that Package A be installed before Package B can be installed. You can force processing of the install operation for Package B even if Package A is not currently installed.
- Property checks defined for the package, for example, a check of the type of operating system on which the install is being performed.
- Any custom checks defined for the package.

Note: Prerequisite, corequisite, and exerequisite dependencies defined between fix packages cannot be overridden.

System check progress messages

During the processing of the system check, the IBM Autonomic Computing Deployment Engine will publish events detailing the progress of the system check. The process solution installation programs receive the events and convert them into localized messages with identifier CTGIN0146I which are displayed to the user. The messages include the label for the check being performed, the number of completed checks, and the total number of checks that are to be performed.

Note that the IBM Autonomic Computing Deployment Engine is not able to compute the total number of checks to be carried out before any checks are processed. As a result of this, the counter associated with the total number of checks to be performed may increase during system check

processing. For example, the following set of messages might be issued during the system check processing. Note that the counter associated with the total number of checks is not fixed, but recalculated and increased during system check processing.

```
CTGIN0146I: Completed system check for check "1" of "2". Check display name:
"Check_Common_PMP_Installed".
CTGIN0146I: Completed system check for check "2" of "3". Check display name:
"Check_LTA_WAR_Package_Installed".
CTGIN0146I: Completed system check for check "3" of "4". Check display name:
"Check_Foundation_PM_Package_Installed".
CTGIN0146I: Completed system check for check "4" of "4". Check display name:
"MaximoDiskSpaceCheck".
```

Installing process managers using the Process Solution Installation wizard

To install a process solution package into your Asset Management for IT instance, you might use the Process Solution Installer wizard.

About this task

Complete the following steps to install a process solution package into Asset Management for IT using the Process Solution Installation wizard:

1. Launch the Process Solution Installer by navigating to the *tamit_install_dir\bin* directory of your Asset Management for IT installation, and executing *solutionInstallerGUI.bat*. As with the Process Solution Installation Command Line Interface Client, the Process Solution Installation Install Anywhere installation program executes on the administrative workstation. The launch script is deployed and configured by the Asset Management for IT installation program. No post-installation configuration is required. Invoke *solutionInstallerGUI.bat* and the wizard is launched.

Alternatively, if you elected to create program shortcuts during the Asset Management for IT install, a link to the Process Solution Installation program user interface might be available from the Start menu, a desktop icon, or a quick launch bar.

2. Select a language for your installation, and then click **OK**.
3. From the Introduction panel, click **Next**.
4. From the Choose PSI Package panel, click **Choose** and navigate to the package file you want to deploy, select it, and then click **Open**. The PSI package selected can be a base install, incremental update, full update, or fix package. Once a package has been selected and you click **Next**, the Process Solution Installation program performs a series of validation checks to verify that the package you selected is valid. The system is checked to ensure that the package has not already been deployed, or, if the package is intended as an upgrade, the system is checked to ensure the base package has already been installed.
5. From the Package Validation Results panel, review and verify the information displayed, and then click **Next**.
6. If this is the first time you have installed this process manager, the process solution installation program license agreement window is displayed. Read the license information and select **I accept the terms in the license agreement** if you agree with the terms. Click **Next**. If you are incrementally adding or removing features from a previously installed process manager, you will encounter an Add or Remove Features? panel where you will declare whether

you are adding or removing features from the process manager, followed by another panel where you will select which specific features you are adding or removing.

7. If this is the first time you have installed this process manager and it has selectable features, you will be prompted by the Feature Selection panel to select or de-select features you would like to install or uninstall from the previously deployed package.
8. From the Middleware Login Information panel, enter the credentials for which you are being prompted, and then click **Next**. The contents of this panel are constructed dynamically, depending on the type of package you are installing. The package is queried to determine what middleware login credentials are necessary to complete the installation of the package.
Once you have entered the requested user IDs and passwords, the Process Solution Installation wizard will validate the credentials by connecting to the middleware servers using the supplied credentials.
9. After the credentials have been verified, a package options panel is displayed that details the deployment options that the package supports. If the Process Solution Installation installable package supports the Overwrite Customer Modified Data during Update option, you can select it from this page. After you specify which options will be used, the process solution installation program will perform a system check to ensure that all system requirements necessary for the package to be installed are present. Click **Next** to advance.
10. From the Pre-Install Summary panel, review and verify the information displayed, and then click **Next**. At this point, the process solution installation program begins the package installation process. A progress panel will inform you of the deployment progress of the installation.
11. When the installation has completed successfully, from the Package Successfully Deployed panel, click **Next**. If there is a package failure, a message will be displayed for the step that failed. If this was a Feature Add, or Removal, a message will display indicating the feature was added or removed successfully.
12. From the Install Another Package panel, select **Install Another Package?** and click **Done**, to install another package. Otherwise, ensure that **Install Another Package?** is deselected and click **Done** to exit the Process Solution Installation wizard.

Results

You might see an installation progress bar displayed briefly after you click **Done**. The Process Solution Installation wizard is actually terminating and no installation activities are being performed. The deployment of the Process Solution Package you were installing has already completed and the progress bar can be safely ignored.

Related concepts

“Planning language support” on page 20

Language support refers to the languages you plan to support in the product user interface.

Process solution installation client command-line interface

The process solution installation client command line interface (CLI) enables you to query, install, upgrade, and uninstall process solution packages, which can consist of process modules and integration modules.

Invoking the process solution installation client CLI

A launch script is provided for starting the Process Solution Command Line Interface. The script is named `solutionInstaller.bat` and is deployed and configured in the `tamit_install_dir\bin` directory. The Process Solution Command Line Interface executes on the Asset Management for IT administrative workstation. The launch script is deployed and configured by the Asset Management for IT installation program. No post-installation configuration is required. Invoke `solutionInstaller.bat` with the preferred command string and the action is performed.

During processing of the command, the Process Solution Command Line Interface will write messages to the standard output of the command window from which the command was launched.

General syntax:

Refer here for the general syntax of invoking the solution installation program.

The syntax for invoking `solutionInstaller` is:

```
solutionInstaller.bat parameter-clause-1 parameter-clause-2 ... parameter-clause-n
```

- Each *parameter-clause* consists of either *-parameterName parameterValue* or *-parameterName*.
- *-parameterName parameterValue* is used for parameters that require a parameter value.
- *-parameterName* is used for parameters that represent switches or flags which do not require a parameter value.
- *parameterName* represents the name of one of the supported parameters.
- *parameterNames* are always prefaced with a dash.
- *parameterValue* represents the value associated with a particular parameter name.
- *parameterValues* that contained embedded spaces should be enclosed in double-quotes

Perform action:

The solution installation program uses an action parameter when interfacing with packages.

A special parameter, **-action**, must be specified on each invocation of **solutionInstaller**. This parameter specifies the action or software life cycle operation to be performed. Based on the value specified for this parameter, additional parameters may need to be specified. For example, when *-action showinstall* is specified, the type parameter must also be provided. The following table identifies the supported actions that may be specified for the Process Solution Command Line Interface.

Table 29. Process solution command line interface actions

Operation	Value of -action Parameter
List Installed Packages	showinstalled
List Available Packages	showavail
Base Install	install
Incremental Update/Fix Pack	upgrade
Undo Incremental Update/Fix Pack	undo
Uninstall	uninstall
Apply Interim Fix	applyfix

Table 29. Process solution command line interface actions (continued)

Operation	Value of -action Parameter
Undo Interim Fix	undofix
List Installed Fixes for a Package	showfixes
Refresh Language Support Files for a Package	refreshlangs
Add or Remove Features	modfeatures
Show Available Features	showfeatures

Summary of supported parameters:

This section contains a summary of parameters supported by the command-line interface.

The collection of supported parameters for the Process Solution Command Line Interface are described in the following table.

Table 30. Process solution command line interface supported parameters

Parameter Name	Description
-action	Specify the function or software life cycle operation to perform.
-addfeatlist	Specifies the list of features to be installed. A feature is identified by its un-translated English Feature Identifier. Multiple features in the list are separated by a colon character. If any of the Feature Identifiers includes a space, then the entire value for this parameter should be enclosed in double-quotes.
-dbpwd	Specifies the password of the database user ID that is used to access the Maximo database.
-dbuser	Specifies the database user ID that is used to access the Maximo database.
-delfeatlist	Specifies the list of features to be deleted. A feature is identified by its un-translated English Feature Identifier. Multiple features in the list are separated by a colon character. If any of the Feature Identifiers includes a space, then the entire value for this parameter should be enclosed in double-quotes.
-fixid	Specifies the unique identifier of an interim fix/patch that you want processed.
-force	Specifies whether to continue on with a deployment operation even if there are one or more unsatisfied requirements associated with the package being processed.
-license	Specifies if you want to automatically accept the license agreement or be prompted for the acceptance or rejection of the license agreement by using one of the following values: accept or prompt.
-loadlanguages	Specifies whether options Language Support files for the package should be loaded into the Maximo Database
-loadsampdata	Specifies whether to load sample or demonstration data associated with the package being processed.
-maxpwd	Specifies the password of the Asset Management for IT administrative user that is used to access the Asset Management for IT application.

Table 30. Process solution command line interface supported parameters (continued)

Parameter Name	Description
-maxuser	Specifies the Asset Management for IT administrative user ID that is used to access the Maximo console.
-pkgpath	Specifies the file path of a process solution package. Paths that have embedded spaces should be enclosed in double quotes.
-pkguuid	Specifies the unique identifier of the process solution package that you want processed.
-pkgver	Specifies the version of the process solution package that you want processed.
-skipdbcfg	Specifies whether to defer the update of the Maximo database during package deployment.
-skipj2eecfg	Specifies whether to defer the regeneration and redeployment of the Maximo J2EE Applications during package deployment.
-type	Specify one of the following types of solution element package to be returned when the showavail or showinstalled actions are invoked. Valid values are processmodule, integrationmodule, or all.
-waspwd	Specifies the WebSphere Application Server administrator password (<i>was_admin_password</i>).
-wasrxapwd	Specifies the password for the user ID under which remote access to the WebSphere Deployment Manager system is performed.
-wasrxuser	Specifies the user ID under which remote access to the WebSphere Deployment Manager system is performed.
-wasuser	Specifies the WebSphere Application Server administrator user ID (<i>was_admin_user_id</i>).

Process solution command line interface reference

Refer to the following sections for process solution command line interface reference information.

Several of the command line interface actions reference a syntax element named [*<middleware login information>*].

The syntax for the middleware login element is:

```
[ -wasuser was_user -waspwd was_password ]
[ -dbuser userid -dbpwd password ]
[ -maxuser userid -maxpwd password ]
[ -wasrxuser userid -wasrxapwd password ].
```

The descriptions of the various parameters are described in “Summary of supported parameters” on page 249. The actual user IDs and passwords that are required depend on the package being processed. For example, a package that only deploys content to the Maximo database would only require the -dbuser and -dbpwd parameters.

showinstalled action - list installed packages:

Description of the action used to display the list of installed packages.

Action

showinstalled

Purpose

List information on the currently installed process solution packages.

Syntax

```
solutionInstaller  
  -action showinstalled  
  -type {processmodule|integrationmodule|all}
```

Description

The showinstalled action displays a list of the currently installed process solution packages that have been installed into the Asset Management for IT. Information about each installed package is written to the command prompt.

The following columns of information are displayed for each installed package:

- *Name* identifies the display name of the installed package.
- *Version* identifies the version-release-modification level of the installed package.
- *Solution Type* identifies whether the installed package is a Process Manager Product or a System Integration Module.
- *Package Type* identifies whether the installed package is a Base Install, Incremental Update, or Full Update package.
- *Unique Identifier* identifies the 32 character hexadecimal value that uniquely identifies the package.

Preconditions

None

Sample Usage

The following example will display information on all the currently installed Process Manager Products.

```
solutionInstaller -action showinstalled -type processmodule
```

showavail action - list available packages:

Description of the action used to display the list of available packages.

Action

showavail

Purpose

List information on process solution package archive files residing in the Asset Management for IT Install Tree.

Syntax

```
solutionInstaller  
  -action showavail  
  -type {processmodule|integrationmodule|all}
```

Description

The showavail action displays information on the process solution package archive files that are located under the Asset Management for IT Install Tree. This command will examine the process solution package archive files that are located in the `thetamit_install_dir\pmp` directory. When the

showavail action is initiated, the process solution installation service will query this directory and display information on each process solution package archive file in the directory.

The following columns of information are displayed for each package:

- *Name* identifies the display name of the process solution package.
- *Version/Fix Name* identifies the version-release-modification level of the process solution package for a Base Install, Incremental Update, or Full Update package and the fix identifier for a Fix Package.
- *Solution Type* identifies whether the process solution package is for a Process Manager Product or a System Integration Module. Package Type identifies whether the process solution package is a Base Install, Incremental Update, Fix, or Full Update package.
- *Package Path* identifies the file path of the process solution package archive file whose information is displayed.

Note: A process solution package archive does not need to reside in this directory in order to be processed by the Process Solution Command Line Interface action. Any process solution package archive file that is accessible from the Asset Management for IT administrative workstation may be identified as the parameter value for the `-pkgpath` parameter.

Preconditions

None

Sample Usage

The following example will display information on all the Integration Module process solution package archive files that are located under the `tamit_install_dir\installableApps\solutions` directory.

```
solutionInstaller -action showavail -type integrationmodule
```

install action - install a package:

Description of the action used to install packages.

Action

install

Purpose

Perform a Base Install of a process solution package not already installed.

Syntax

```
solutionInstaller  
-action install  
-pkgpath <path-to-base-install-package-file>  
[<middleware login information>]  
[-license <accept|prompt>]  
[-skipj2eecfg] [-skipdbcfg] [-loadlanguages] [-loadsampdata] [-force]
```

Description

The install action is used to install a process solution package into Asset Management for IT. When installing a package, the file name of the process solution package archive file to be installed is specified using the **-pkgpath** parameter.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package archive file you specify is a valid Base Install package.

- The package is not already be installed. You can check this by using the showinstalled action.
- All additional requirements associated with the package specified are satisfied.

Sample Usage

The following example will perform a Base Install of the Process Manager Product whose process solution package is located C:\Config_PMP_7.1.zip file. Access to both the Maximo database and to the WebSphere Application Server are performed using the specified userids and passwords. The license agreement associated with package is displayed for confirmation. Sample data associated with the Process Manager Product is loaded into the Maximo database.

```
solutionInstaller
  -action install
  -pkgpath C:\Config_PMP_7.1.zip
  -wasuser <userid>b -waspwd <password>
  -dbuser <userid> -dbpwd <password>
  -license prompt -loadsampdata
```

upgrade action - incrementally update a package:

Description of the action used to update packages.

Action

upgrade

Purpose

Perform an incremental update of a currently installed process solution package.

Syntax

```
solutionInstaller
  -action upgrade
  -pkgpath <path-to-update-package-file>
  [<middleware login information>]
  [-license <accept|prompt>]
  [-skipj2eecfg] [-skipdbcfg] [-loadlanguages] [-loadsampdata] [-force]
  [-overwrite]
```

Description

The upgrade action is used to upgrade a currently installed process solution package. During the upgrade process, the process solution installation service will check to ensure that a currently installed instance suitable to be upgraded has already been installed. When upgrading a package, you must specify the file name of the process solution package file containing the upgraded artifacts.

There are two types of upgrade packages supported:

Incremental update package

An incremental update package requires that an existing instance of the process solution package that is being upgraded is already installed.

Full update package

A full update package can be used to upgrade an existing instance, or it can be used to install a new instance using the -action install command.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package archive file you specify is a valid Incremental Update or Full Update package.
- An instance of the process solution package that is eligible to be upgraded is already installed.
- All additional requirements associated with the package specified are satisfied.

Sample Usage

The following example will perform an incremental update of an already installed process solution package. The update package is located in the C:\Config_PMP_Upgrade_7.1.1.zip file. Access to both the Maximo database and to the WebSphere Application Server are performed using the specified user IDs and passwords. The license agreement associated with package is accepted without prompting for user confirmation.

```
solutionInstaller
  -action upgrade
  -pkgpath C:\Config_PMP_Upgrade_7.1.1.zip
  -wasuser <userid> -waspwd <password>
  -dbuser <userid> -dbpwd <password>
  -license accept
```

undo action - undo an update to a package:

Description of the action used to undo an update to a package.

Action

undo

Purpose

Remove the changes made to process solution package during a previous incremental update.

Syntax

```
solutionInstaller
  -action undo
  -pkguuid <unique-id-of-package> -pkgver <package-version>
  [<middleware login information>]
  [-force]
```

Description

The undo action is used to remove the changes that were made by a previously initiated incremental update. This action restores the process solution package to its previous state. During the undo process, the process solution installation service will check to ensure that the specified version of the package is an incremental update version and that the incremental update can be undone.

When undoing an incremental update, the user must specify the unique identifier and version of the incremental update that is to be undone. Note that a particular incremental update package may not support the undo action. If an undo action is initiated for such a package, the process solution installation client will display a message.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package identified by the unique-id and version that you specify is currently installed and represents an Incremental Update Package.
- The Incremental Update that you are attempting to undo supports the Undo action.

- All additional requirements associated with the package specified are satisfied.

Sample Usage

The following example will undo a previously made incremental update to the process solution package with the specified unique identifier at version 1.1.1. Access to both the Maximo Ddatabase and to the WebSphere Application Server are performed using the specified user IDs and passwords.

```
solutionInstaller
  -action undo
  -pkguid DC2894C667CE48ABAC25214A7FED16D5 -pkgver 1.1.1
  -wasuser <userid> -waspwd <password>
  -dbuser <userid> -dbpwd <password>
```

uninstall action - uninstall a package:

Description of the action used to uninstall installed packages.

Action

uninstall

Purpose

Uninstall a currently installed process solution package.

Syntax

```
solutionInstaller
  -action uninstall
  -pkguid <unique-id-of-package>
  [<middleware login information>]
  [-force]
```

Description

The uninstall action is used to uninstall a currently installed process solution package. When uninstalling a package, the user will specify the unique identifier of the process solution package to uninstall. The unique identifier is displayed when the showinstalled action is run.

Not all process solution packages support the ability to be uninstalled. For example, the uninstall action is not supported for the process solution packages distributed and installed as part of Asset Management for IT. If the package does not support full uninstall, messages are displayed during the uninstall action.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package identified by the unique-id that you specify is currently installed.
- The process solution package supports partial or full uninstallation.
- All additional requirements associated with the package specified are satisfied.

Sample Usage

The following example will uninstall the process solution package with the specified unique identifier. Access to both the Maximo database and to the WebSphere Application Server are performed using the specified user IDs and passwords.

```
solutionInstaller
  -action undo
  -pkguuid DC2894C667CE48ABAC25214A7FED16D5
  -wasuser <userid>b -waspwd <password>
  -dbuser <userid> -dbpwd <password>
```

applyfix action - apply interim fix to a package:

Description of the action used to apply interim fixes to a package.

Action

```
applyfix
```

Purpose

Apply an Interim Fix package to a currently installed process solution package.

Syntax

```
solutionInstaller
  -action applyfix
  -pkgpath <path-to-fix-package-file>
  [<middleware login information>]
  [-license <accept|prompt>]
  [-skipj2eecfg] [-skipdbcfg] [-skipdbcfg] [-loadsampdata] [-force]
  [-overwrite]
```

Description

The applyfix action is used to apply patches or interim fixes to a currently installed process solution package. During the upgrade process, the process solution installation service will check to ensure that a currently installed instance suitable to be patched has already been installed. When applying a fix to a package, you must specify the file name of the process solution package file containing the artifacts associated with the fix. This package file is referred to as an Interim Fix Package.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package archive file you specify is a valid Interim Fix package.
- An instance of the process solution package that is eligible to be patched by the Interim Fix package is already installed.
- All additional requirements associated with the package specified are satisfied.

Sample Usage

The following example will apply an Interim Fix package to a currently installed process solution package. The Interim Fix package is located in the C:\Config_PMP_Fix_PTF0010.zip file. Access to both the Maximo database and to the WebSphere Application Server are performed using the specified user IDs and passwords. The license agreement associated with package is accepted without prompting for user confirmation.

```
solutionInstaller
  -action applyfix
  -pkgpath C:\Config_PMP_Fix_PTF0010.zip
  -wasuser <userid> -waspwd <password>
  -dbuser <userid> -dbpwd <password>
  -license accept
```

undofix action - undo an interim fix from a package:

Description of the action used to undo an interim fix from a package.

Action

undo

Purpose

Remove a previously applied Interim Fix from a process solution package.

Syntax

```
solutionInstaller
  -action undo
  -pkguid <unique-id-of-package> -fixid <fix-identifier>
  [<middleware login information>]
  [-force]
```

Description

The undofix action is used to remove a previously applied fix package. Each Interim Fix package has a fix identifier that uniquely identifies the Interim Fix within a process solution package. You specify this fix identifier (as well as the unique identifier of the base package) when you invoke the undofix action. During the undofix process, the process solution installation service will check to ensure that the specified fix is already applied.

Note that a particular Interim Fix package may not support the undofix action. If an undofix action is initiated for such a package, the process solution installation client will display a message.

You can determine the set of Interim Fixes already applied to a process solution package using the showfixes action of the Process Solution Command Line Interface.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package identified by the unique-id is currently installed.
- The Interim Fix identified by the fix identifier is already applied to the process solution package.
- The Interim Fix that you are attempting to undo supports the undofix action.
- All additional requirements associated with the package specified are satisfied.

Sample Usage

The following example will undo a previously applied Interim Fix with fix identifier PTF00001 from the process solution package with the specified unique identifier. Access to both the Maximo Database and to the WebSphere Application Server are performed using the specified userids and passwords.

```
solutionInstaller
  -action undofix
  -pkguid DC2894C667CE48ABAC25214A7FED16D5
  -fixid PTF00001
  -wasuser <userid>b -waspwd <password>
  -dbuser <userid> -dbpwd <password>
```

showfixes action - list installed fixes for a package:

Description of the action used to list installed fixes for a package.

Action

showfixes

Purpose

List information on the Interim Fixes that have been applied to a currently installed process solution package.

Syntax

```
solutionInstaller
  -action showfixes
  -pkguid <unique-id-of-package>
  -pkgver <package-version>
```

Description

The showfixes action displays a list of the currently installed Interim Fixes that have been previously applied to a currently installed process solution package. Information on each installed fix is written to the command prompt. When you use this action, you specify the unique identifier and version of the currently installed process solution package for which the collection of Interim Fixes is to be displayed.

The following columns of information are displayed for each applied fix:

- *Name* identifies the unique identifier for the Interim Fix.
- *Fix Type* identifies the type of the Interim Fix.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package identified by the unique-id and version that you specify is currently installed.

Sample Usage

The following example will list the currently applied Interim Fixes for the process solution package having the specified unique identifier and version.

```
solutionInstaller
  -action showfixes
  -pkguid 1480586C22E24D6A8754265DC38AEBDD
  -pkgver 1.1.0
```

refreshlangs action - refresh languages for a package:

Description of the action used to refresh languages for a package.

Action

```
refreshlangs
```

Purpose

Install or refresh the language support files for a package that is already installed.

Syntax

```
solutionInstaller
  -action refreshlangs
  -pkgpath <path-to-base-install-package-file>
  [<middleware login information>]
  [-license <accept|prompt>]
  [-skipj2eecfg] [-skipdbcfg] [-force]
```

Description

The refreshlangs action is used to either install or refresh the language support files associated with a package that is already installed. The action will unpack the language support files contained within the package, write those language support files to the Asset Management for IT administrative workstation, and then load the language support files into the Maximo database.

This action can be used even if language support files were not originally installed using the `-loadlanguages` flag when the base install for the package was performed using the `-action install` command.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package archive file you specify is a valid base install package.
- The package was previously installed. You can check this by using the `showinstalled` action.
- The package supports user-selectable deployment of language support files.
- All additional requirements associated with the package specified are satisfied.

Sample Usage

The following example will refresh the language support files contained within the Process Manager Product whose process solution package is located `C:\Config_PMP_7.1.zip` file. Access to the Maximo database is performed using the specified `userid` and `password`.

```
solutionInstaller
  -action refreshlangs
  -pkgpath C:\Config_PMP_7.1.zip
  -dbuser <userid> -dbpwd <password>
  -license accept
```

showfeatures action - show features of a solution package:

Description of the action used to show features of a solution package.

Action

`showfeatures`

Purpose

List information about installed and available features associated with a process solution package.

Syntax

```
solutionInstaller
  -action showfeatures
  -pkgpath path_to_base_install_package_file
```

Description

The `showfeatures` action displays a list of information about the supported and currently installed features for a process solution package. Information about each feature is written to the command prompt.

This action can be used against any process solution package, even if that process solution package has not already been installed.

- Use this command against a currently installed process solution package to determine the features that are currently installed for the package and to determine the available features (not yet installed) that might be added.
- Use this command against a process solution package not already installed to determine the available features that might be specified on the `-addfeatlist` parameter of the `-action install` CLI action.

When you use this action, you specify the package path of a process solution package for which the feature information is to be displayed. The command output includes an indication of whether the package is installed.

The following columns of information are displayed for each feature:

Feature ID	Identifies the unique identifier for feature
Display Name	Identifies the localized display name for the feature
Parent ID	Lists the parent of this feature , if applicable
Is Installed?	Identifies whether the feature is currently installed
Is Required?	Indicates whether this is a required feature for installation

Preconditions

Before using this action, you will need to ensure that:

- The process solution package identified by the packagepath is a valid process solution package archive file.

Sample Usage

The following example will list information about the features associated with the process solution package having the specified package path.

```
solutionInstaller
  -action showfeatures
  -pkgpath C:\Config_PMP_7.1.zip
```

modfeatures action - modify existing features of a deployed package:

Description of the action used to modify existing features of a deployed package.

Action

modfeatures

Purpose

Modify features of a currently installed process solution package.

Syntax

```
solutionInstaller
  -action modfeatures
  -pkgpath path_to_base_install_package_file
  [-addfeatlist FeatA:FeatB:}:Featn]
  [-delfeatlist FeatA:FeatB:}:Featn]
  [middleware_login_information]
  [-skipj2ecfg] [-skipdbcfg] [-force]
```

Description

The modfeatures action is used to modify the installed features for a currently installed process solution package. When modifying features, the file name of the process solution package archive file containing the features to be modified is specified using the **-pkgpath** parameter. To add new features not already installed, you use the **-addfeatlist** parameter. To remove currently installed features, you use the parameter. You may not both add and remove features with one invocation. One and exactly one of either the or the **-delfeatlist** parameters must be provided when this command is invoked.

Preconditions

Before using this action, you will need to ensure that:

- The process solution package archive file you specify is a valid Base Install package.
- The package is already installed. You can check this by using the `showinstalled` action.
- Any features specified with the are valid for the specified package and are not already deployed.
- Any features specified with the are valid for the specified package and are already installed.
- All additional requirements associated with the features being specified are satisfied.
- The exact feature name is known. This can be obtained by using the action

Sample Usage

The following example will add the features with identifiers **Samples** and **DBSupport**. The process solution package being modified is located `C:\Config_PMP_7.2.zip` file. Access to both the Maximo database and to the WebSphere Application Server are performed using the specified user IDs and passwords.

```
solutionInstaller
  -action modfeatures
  -pkgpath C:\Config_PMP_7.2.zip
  -wasuser was_user b -waspwd was_password
  -dbuser db_user -dbpwd db_password
  -addfeatlist Samples:DBSupport
```

Installing and refreshing language support files for a package

A process solution package might define one or more language support features.

When a language support feature for a process solution package is installed using the process solution installation programs, XLIFF files associated with all support languages are unpacked onto the Asset Management for IT administrative workstation. The Maximo Translation Data Toolkit `-PMPUPDATE` is invoked. This utility imports the XLIFF files associated with the process manager into the Maximo database, based on the base language and any other selected languages that have been installed into Maximo.

If you intend to install language support for Asset Management for IT process managers for the first time, refer to Chapter 8, “Installing IBM Tivoli Asset Management for IT language pack,” on page 153. If you intend to refresh language support files for the Asset Management for IT process managers, or you have installed another process manager, use the instructions provided in this section.

There are two models for how the process solution package can expose its language support.

- A package can define a single language support feature with a special feature identifier. The Process Solution Installation programs provide some built-in special mechanisms for deploying language support for packages using this model.
- A package can define multiple language support features. The selectable feature support in the Process Solution Installation programs are used for deploying language support for packages using this model.

Related tasks

Chapter 8, “Installing IBM Tivoli Asset Management for IT language pack,” on page 153

Deployment for packages with a single special language support feature

Packages can be deployed with a single special language support.

About this task

Many process solution packages define a single language support feature with a feature identifier of LANG_SUPT_FEATURE. For these packages, the Process Solution Command Line Interface allow this special language support feature to be deployed during a base install using the `-loadlanguages` parameter. The language support for this special feature can also be installed after a base install or refreshed using the `refreshlangs` action of the Process Solution Command Line Interface.

Installing language support files at base install

When you initially perform a base install of a package with the special language support feature, you can elect to also install the language support files for the package.

Using the Installation Wizard

When using the Process Solution Installation wizard to perform a base install of a package, the Feature Selection Panel will display the language support feature in the set of available features for the package. When you select this check box, the Process Solution Installation wizard will unpack the language support files associated with the package and then invoke the Maximo Translation Data Toolkit `-PMPUPDATE` function.

Using the Command Line Interface

When using the Process Solution Command Line Interface, you can install the language support files for the package by specifying the `-loadlanguages` command line flag when you perform a base install of a package using the `-action install` subcommand.

Installing or refreshing language support after base install

After the package has been initially installed, you can install or refresh the language support files for the package. The Process Solution Command Line Interface provides a `-action refreshlangs` subcommand for this purpose. This action is only supported for packages that are already installed. The action can be used even if the language support files were not installed when the package was originally installed. In both scenarios, the language support files for the package are unpacked and copied to the Asset Management for IT administrative workstation and the Maximo Translation Data Toolkit `-PMPUPDATE` function.

Note: The function to install or refresh language support files is only available using the Process Solution Command Line Interface. The function is not available using the Process Solution Installation wizard.

Deployment for packages with multiple language support features

Packages can be deployed with a multiple language support.

About this task

A process solution package that supports a variety of selectable features may also have multiple language support features.

Installing language support files at base install

The language support features for packages that define multiple language support can be deployed during a base install of the package or may be added after the base install using the new selectable feature support in the Process Solution Installation Wizard and Process Solution Command Line Interface. For these types of packages, the language support features are managed just like other selectable features defined for the package.

Installing or refreshing language support after base install

When the refreshlangs action of the Process Solution Command Line Interface is invoked for a package with multiple language support features, only currently installed language support features for the package are refreshed. This is accomplished by re-execution of the deployment actions associated with all currently installed language support feature.

The refreshlangs action when invoked on a package with multiple language support features, will never install those language support features. The refresh processing is only performed against currently installed language support features. Note that this behavior differs from the refreshlangs behavior when applied against a package defining the special LANG_SUPT_FEATURE identifier. In that scenario, the special language support feature would be installed if it is not currently installed or refreshed if it is installed.

Related concepts

“Planning language support” on page 20

Language support refers to the languages you plan to support in the product user interface.

Process Solution Installation logs

If you experience any problems or encounter any error messages during the use of the process solution installation program, refer to these log files.

Log files are kept in the following locations:

Table 31. Process solution installation logs

Log type	Description	Location
Package log	<p>These are log files containing the StdOut/StdErr output of external commands launched by the package as it is processed by the Deployment Engine. These log files are typically vital to the proper debugging of package issues.</p> <p>In general, logs will have two parts, a ".out" and ".err" file, both with the same pre-extension file name. .out files contain the contents of the Standard Output stream as output by the external command. .err files contain the contents of the Standard Error stream. It is normal for one to be blank, provided there was no error output (or there was ONLY error output).</p> <p>Note that you might discover numerous (10-20) package log files generated for any particular package installed.</p>	<p><i>tamit_install_dir</i>\solutions\logs\<i>package_name</i>\</p> <p>For instance, if PSI encounters an error in the Config Management package, and Asset Management for IT is installed to C:\IBM\SMP, then the logs for the Config Package would be found in: C:\IBM\SMP\solutions\logs\Config_PMP\.</p>
Asset Management for IT log	<p>These are logs kept by the Process Solution Installation subsystem.</p>	<p><i>tamit_install_dir</i>\logs\CTGInstallMessageXX.log <i>tamit_install_dir</i>\logs\CTGInstallTraceXX.log</p> <p>XX is a two digit number such as 00. These logs contain the trace output of the PSI subsystem.</p> <p>Note: You might encounter messages similar to the following in the MAXIMO_DEPLOY_ERR.err file found in the <i>tamit_install_dir</i>\solutions\logs directory for a process manager once it has been installed:</p> <ul style="list-style-type: none"> • *sys-package-mgr*: processing new jar, 'C:\IBM\SMP\lib\icl.jar' • *sys-package-mgr*: processing new jar, 'C:\IBM\SMP\lib\CTGInstallCommon.jar' • *sys-package-mgr*: processing new jar, 'C:\IBM\SMP\lib\CTGInstallResources.jar' <p>Although these messages appear in an error log file, they are informational only, and do not represent deployment errors. These messages can be safely ignored.</p>

Table 31. Process solution installation logs (continued)

Log type	Description	Location
Solution Install/Deployment Engine Logs	<p>These are logs kept by the IBM Solution installation program/Deployment engine run time. Process Solution Installation utilizes the IBM technology as the means to installation and keep track of installed packages. This run time has its own logging system.</p> <p>Note: After an installation these logs will contain sensitive credentials. It is strongly recommended that these logs be removed after a successful installation.</p>	<p>C:\Program Files\IBM\Common\acsi\logs\<i>user_name</i>\de_msg.log</p> <p>C:\Program Files\IBM\Common\acsi\logs\<i>user_name</i>\de_trace.log</p> <p>So for instance, if you installed under the user name Administrator, the logs would be found under: C:\Program Files\IBM\Common\acsi\logs\Administrator\de_msg.log</p>
WebSphere Application Server Logs	<p>These are logs kept of connections, exceptions, and other failures experienced by the WebSphere Application Server in its day-to-day running. These logs are often helpful in the diagnosis of errors in particular EAR files or other back-end operations, such as database connections.</p>	<p><i>was_install_dir</i>\profiles\<i>profile</i>\logs\AboutThisProfile.txt</p> <p><i>was_install_dir</i>\profiles\<i>profile</i>\logs\<i>server_name</i>\startServer.log</p> <p><i>was_install_dir</i>\profiles\<i>profile</i>\logs\<i>server_name</i>\stopServer.log</p> <p><i>was_install_dir</i>\profiles\<i>profile</i>\logs\<i>server_name</i>\SystemErr.log</p> <p><i>was_install_dir</i>\profiles\<i>profile</i>\logs\<i>server_name</i>\SystemOut.log</p> <p>So for instance, if your WebSphere Application Server was installed in "C:\IBM\WebSphere\AppServer\", your profile name was "AppSrv01", and your server name was "server1", you would provide the following logs: C:\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\AboutThisProfile.txt</p>
Maximo Logs	<p>There are also a few logs kept by Maximo itself. These are useful in tracking the progress, success, and failure of a few back-end commands provided by Maximo.</p>	<p><i>tamit_install_dir</i>\maximo\tools\maximo\log\updatedb\<i>time_stamp</i>.log</p> <p>So if your Maximo installation location was C:\IBM\SMP\Maximo, and the package executed the UpdateDB command on April 19th at approximately 5:06:07PM, the logging information would be written to the file: C:\IBM\SMP\Maximo\tools\maximo\log\updatedb20070419170607.log</p>

Table 31. Process solution installation logs (continued)

Log type	Description	Location
WebSphere Application Server Thin Client Logs	The WebSphere Application Server thin client is the mechanism by which the process manager packages communicate with the WebSphere Application Server. If this automated deployment should happen to fail, the exact actions the Thin Client took and the associated responses from the WebSphere Application Server are stored in logs.	<p><i>tamit_install_dir</i>\wasclient\logs\CTGIN_wsadmin.traceout</p> <p><i>tamit_install_dir</i>\wasclient\logs\wsadmin.traceout</p> <p><i>tamit_install_dir</i>\wasclient\logs\wsadmin.valout</p> <p>So if your Asset Management for IT installation location were C:\IBM\SMP, the following log files would contain the Thin WAS Client tracing information:</p> <p>C:\IBM\SMP\wasclient\logs\CTGIN_wsadmin.traceout</p> <p>C:\IBM\SMP\wasclient\logs\wsadmin.traceout</p> <p>C:\IBM\SMP\wasclient\logs\wsadmin.valout</p>

It is a good practice to rename existing logs before attempting a package install. It is useful to have a log comprised of only the information related to the success or failure of current package installation to facilitate problem determination.

Post product installation process manager tasks

If you have chosen to not automate the configuration of your IBM WebSphere Application Server server during the IBM Tivoli Asset Management for IT installation process, there are several post-installation tasks that must be performed for the product's process managers.

Ensure that you have run the configuration step portion of the Asset Management for IT installation either by performing it during installation, or outside the Asset Management for IT installation program by using the taskrunner utility. The product installation program still invokes the process solution installer and deploys the product's PSI packages, however, the WebSphere Application Server Network Deployment-related actions in those packages will not be performed and must be completed manually.

Post product installation process manager tasks include manually configuring Asset Management for IT PSI packages and manually building and deploying the product EAR file.

If you have chosen to not let the installation program automatically configure WebSphere Application Server Network Deployment, refer to the release notes located at the following URL for instructions on completing post product installation tasks for PSI packages. <http://www.ibm.com/support/search.wss?q=tamit72relnotes>

Before working with BIRT reports

Prior to running any reports, you need to set up manually the `mxe.report.birt.tempfolder` in JVM system Properties in BIRT report engine.

Before you begin

The `mxe.report.birt.tempfolder` property specifies location of temporary folder on the reporting server for BIRT.

About this task

To configure BIRT, set up JVM System Properties `mxe.report.birt.tempfolder`.

1. Log in to Integrated Solutions Console.
2. Go to **Servers** → **Application servers**.
3. From the right panel, click on the server name where you have deployed maximo.
4. Go to **Process Definition** under **Server Infrastructure**.
5. Click **Java Virtual Machine** under **Additional Properties**.
6. Add `-Dmxe.report.birt.tempfolder=c:\tempReport\BIRT-TEMP` to **Generic JVM Argument**, and then click **Save**.
7. Restart the server.

Generating xml request pages in Asset Management for IT

Perform this task after you installed Asset Management for IT and before you run request pages. This procedure needs to be performed for every language that is enabled on your system.

Before you begin

When multiple languages are enabled in Maximo, request pages have to be generated in each of the enabled languages.

1. Log in as a maxadmin user.
2. From the Start menu, go to **Administrator** → **Reporting** → **Report Administration**
3. Review all rows in the list view then in the bottom right corner click on **Generate Request Page** button. Wait a couple of minutes for the process to complete.

Related concepts

“Planning language support” on page 20

Language support refers to the languages you plan to support in the product user interface.

Synchronizing data

The scheduled synchronization of data that occurs between LDAP repositories and Asset Management for IT is governed by the federated repositories managed by Virtual Member Manager in WebSphere, and the Asset Management for IT Virtual Member Manager cron task.

About this task

For specific information on configuring the VMMSYNC cron task for Microsoft Active Directory, refer to “Manually configuring the VMMSYNC cron task for Microsoft Active Directory” on page 230.

To configure the synchronization schedule between LDAP repositories and Asset Management for IT, complete the following steps:

1. Open a Web browser and point to
`http://host_name:9081/maximo`
2. Log into Asset Management for IT using the maxadmin user ID.
3. From the Asset Management for IT interface, navigate to **Go To → System Configuration → Platform Configuration → Cron Task Setup**.
4. Type VMM in the **Cron Task** field, and hit Enter.
5. Locate the VMMSYNC cron task, and click it.
6. Ensure the following values are used for each field:

Principal

`cn=wasadmin,ou=users,ou=SWG,o=IBM,c=US`

This is the user required by the CronTask application to connect to the local Virtual Member Manager service. This value can be any WebSphere administrative user that has authorization to connect to the local Virtual Member Manager service.

Credential

This should be the password used for the Principal account. In this case, enter the password for wasadmin.

GroupSearchAttribute

This value is the LDAP group object attribute used to search for groups under the configured directory sub-tree.

`cn`

UserSearchAttribute

This value is the LDAP user object attribute used to search for users under configured directory sub-tree.

`Uid`

SynchAdapter

This value is the Java class that writes LDAP data to the database.

`psdi.security.vmm.DefaultVMMSyncAdapter`

SynchClass

This value is the Java class that connects to the Virtual Member Manager local service to search for required objects.

`psdi.security.vmm.VMMSynchronizer`

Group Mapping

This field contains XML mapping files that map LDAP object attributes to database repository table columns. Change the following object entries:

Basedn

This defines the LDAP sub-tree under which the Virtual Member Manager cron task will search for group objects.

`ou=groups,ou=SWG,o=IBM,c=US`

Filter

This is the Virtual Member Manager object class that the service uses to search for group objects in LDAP.

`Group`

User Mapping

This field contains XML mapping files that map LDAP object attributes to database repository table columns. Change the following object entries:

Basedn

This defines the LDAP sub-tree under which the Virtual Member Manager cron task will search for user objects.

`ou=users,ou=SWG,o=IBM,c=US`

Filter This is the Virtual Member Manager object class that the service uses to search for user objects in LDAP.

`PersonAccount`

7. Set the task to active.

What to do next

By default, the cron task will perform its task every 5 minutes. Make changes to the Schedule field of the cron task if you want to change the interval.

Chapter 18. Uninstalling IBM Tivoli Asset Management for IT

The procedures and instructions provided here are based upon a scenario in which the IBM Tivoli Asset Management for IT installation program has experienced an error or failure.

Before you begin

Asset Management for IT uninstallation is a comprehensive procedure and does not support partial removal of individual components or process managers, including those deployed by other products. If you have deployed a product that includes process managers before you deployed Asset Management for IT, and you want to uninstall Asset Management for IT, be advised that you will also be removing the process managers deployed with the other product.

Note that you will only run the Asset Management for IT uninstallation program once. If there are errors, messages are generated that indicate conditions that you must resolve manually before attempting a reinstall. This also includes manually removing files from the administrative workstation.

Asset Management for IT can only be uninstalled using the Asset Management for IT uninstallation program as directed. Do not use other methods to attempt to uninstall Asset Management for IT, such as using the **Add/Remove Programs** panel.

About this task

The uninstall procedure you follow depends on the type of Asset Management for IT deployment you are uninstalling. For uninstallation purposes, Asset Management for IT deployments will fall into one of the following categories:

Fully-automated configuration

In this scenario, you selected the option to allow the Asset Management for IT installation program to automatically configure middleware during deployment.

Manual configuration

In this scenario, you selected the option to manually configure middleware. You did not allow the Asset Management for IT installation program to automatically configure middleware during deployment.

What to do next

After the Asset Management for IT uninstall process is complete, you can reinstall Asset Management for IT by restarting the Asset Management for IT installation program.

Uninstalling an automatically configured IBM Tivoli Asset Management for IT

Use the information provided in this section to uninstall a Asset Management for IT deployment that was deployed using the automatic middleware configuration options.

Running the IBM Tivoli Asset Management for IT uninstall program for automatically configured middleware

Running the Asset Management for IT uninstall program will revert the administrative system and middleware servers back to a state where you can rerun the Asset Management for IT installation program.

Before you begin

Ensure all applicable services are running and all middleware servers are accessible.

The Asset Management for IT uninstall program must be able to access the database used with Asset Management for IT to fetch installation properties and configuration data. If the Asset Management for IT uninstall program cannot access the database because it is unavailable, corrupt, or otherwise inaccessible, then the Asset Management for IT uninstall program will remove files from the administrative workstation and inform you that some manual recovery might be required before another Asset Management for IT installation can be successful.

About this task

If you have not changed passwords that were used for the initial installation, you do not have to enter values for password fields in the uninstall program.

To run the Asset Management for IT uninstall program:

1. Open a command prompt and issue the following command:
`tamit_install_dir_uninstall\uninstall.exe`
2. From the Application Server Information panel, enter the following information and then click **Next**.

Remote user ID

Enter a user ID in order to access the system hosting the application server. The remote user ID must be able to access the server using the remote access protocol enabled on that system.

Remote password

Enter a password for the remote user ID.

User ID

Enter the password for the application server administrator.

Password

Enter the password for the application server administrator user ID.

3. From the database administration panel, for DB2, enter the following information and then click **Next**.

Remote user ID

Enter a user ID in order to access the system hosting the database. The remote user ID must be able to access the server using the remote access protocol enabled on that system.

Remote password

Enter a password for the remote user ID.

Instance administrator user ID

Enter the database instance administrator user ID that you input during the installation.

Instance administrator password

Enter the password for the database instance administrator user ID.

For Oracle databases, you can supply the credentials for the Administrator user ID and the Oracle software owner ID. For Microsoft SQL Server databases, you can supply the SQL Server administrator user ID and password.

4. Review the components that are listed in the uninstall summary panel, and then click **Uninstall**.
5. After the uninstall process has completed, specify whether or not you want to restart the computer now or later, and click **Done** to exit the program.
6. Check to ensure the uninstall program removed the Asset Management for IT installation directory (*tamit_install_dir*), for example, `c:\ibm\smf`. If the Asset Management for IT installation failed early in the process, the Asset Management for IT uninstall program might not remove the Asset Management for IT installation directory. If this directory still exists after you have completed the uninstall process, you will have to remove it manually before you proceed to the reinstallation process.
7. Using Windows services, stop **IBM ADE Service**.
8. To delete the service, use the following command: `sc delete acsisrv`.
9. Go to **Program Files** → **IBM** → **Common** and delete the `asci` folder.
10. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsisrv` and remove the registry keys if any exist.
11. Restart the computer.

Uninstalling a manually configured IBM Tivoli Asset Management for IT

Uninstalling a manually configured Asset Management for IT deployment consists of running the Asset Management for IT uninstallation program, and then manually dropping and recreating the database you intend to use with the reinstall process.

Running the IBM Tivoli Asset Management for IT uninstall program for a manually configured deployment

Running the Asset Management for IT uninstall program will revert the administrative system and middleware servers back to a state where you can rerun the Asset Management for IT installation program.

Before you begin

Ensure all applicable services are running and all middleware servers are accessible.

The Asset Management for IT uninstall program must be able to access the database used with Asset Management for IT to fetch installation properties and configuration data. If the Asset Management for IT uninstall program cannot access the database because it is unavailable, corrupt, or otherwise inaccessible, then the Asset Management for IT uninstall program will remove files from the administrative workstation and inform you that some manual recovery might be required before another Asset Management for IT installation can be successful.

If you have not changed passwords that were used for the initial installation, you do not have to enter values for password fields in the uninstall program.

About this task

To run the Asset Management for IT uninstall program:

1. Open a command prompt and issue the following command:
`tamit_install_dir\uninstall\uninstall.exe`
2. From the Introduction panel, read the introductory information and then click **Next**.
3. From the application server information panel, enter the following information and then click **Next**.

User ID

Enter the password for the application server administrator.

Password

Enter the password for the application server administrator user ID.

4. Review the components that are listed in the uninstall summary panel, and then click **Uninstall**.
5. After the uninstall process has completed, click **Done** to exit the program.
6. Check to ensure the uninstall program removed the Asset Management for IT installation directory, for example, `c:\ibm\smp`. If the Asset Management for IT installation failed early in the process, the Asset Management for IT uninstall program might not remove the Asset Management for IT installation directory. If this directory still exists after you have completed the uninstall process, you will have to remove it manually before you proceed to the reinstallation process.
7. After the uninstall process has completed, specify whether or not you want to restart the computer now or later, and click **Done** to exit the program.
8. Using Windows services, stop **IBM ADE Service**.
9. To delete the service, use the following command: `sc delete acsisrv`.
10. Go to **Program Files** → **IBM** → **Common** and delete the `ascii` folder.
11. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsisrv` and remove the registry keys if any exist.
12. Restart the computer.

What to do next

You can now proceed with recovery of your manually configured database.

IBM Tivoli Asset Management for IT database configuration recovery

Database objects that you created before running the Asset Management for IT installation program must be deleted after a failed installation before you can rerun the Asset Management for IT installation program again.

Before you begin

Before rerunning the Asset Management for IT installation program, you must drop the Asset Management for IT database and recreate it.

Restoring the DB2 database server

In order to rerun the IBM Tivoli Asset Management for IT installation program, you must first restore the DB2 database server to the same state as before Asset Management for IT was installed.

Before you begin

Ensure that the MXServer application server on WebSphere Application Server is stopped before dropping the database.

About this task

Restoring the DB2 database server to the same state as before Asset Management for IT was installed, requires you to drop the Asset Management for IT database that you manually created and then recreate it before rerunning the Asset Management for IT installation program.

To restore the Asset Management for IT database, complete the following steps:

1. Log on to the system hosting the DB2 server.
2. Start a DB2 command session or run `db2cmd` from the command prompt.
3. First list and then force all applications connected to the database to close using the following commands:

- a. To list applications, type this command:

```
db2 list applications
```

You might see output like the following sample output:

```
Auth Id Application Appl. Application Id DB # of
Name Handle Name Agents
-----
CTGINST1 db2taskd 507 *LOCAL.DB2.071113150237      MAXDB71 1
CTGINST1 db2stmm 506 *LOCAL.DB2.071113150236      MAXDB71 1
CTGINST1 db2bp 504 *LOCAL.ctginst1.071113150234      MAXDB71 1
```

- b. If any connections exist, close the connect application using a command like the following sample command:

```
db2 force application '( 507,506,504 )'
```

4. Drop the Asset Management for IT database (MAXDB71, by default):

```
db2 drop database MAXDB71
```

5. Manually recreate the MAXDB71 database.

Restoring the Oracle database

In order to rerun the IBM Tivoli Asset Management for IT installation program, you must first restore the Oracle database server to the same state as before Asset Management for IT was installed.

Before you begin

Ensure that the MXServer application server on WebSphere Application Server Network Deployment is stopped before deleting the database.

About this task

Restoring the Oracle database server to the same state as before Asset Management for IT was installed, requires to drop the Asset Management for IT database that you manually created, and then recreate it before rerunning the Asset Management for IT installation program.

To restore the Asset Management for IT database, complete the following steps:

1. Log in to the Oracle database server as the Oracle software owner.

2. Log in to the Oracle instance using SQLPlus as a DBA user: Note that the Oracle SID for a clean install is ctginst1. If you are using an existing Oracle instance with Asset Management for IT, use the Oracle SID associated with the existing instance.

Linux

UNIX:

- a. Set the environment variable from the command line:

```
ORACLE_SID=your_SID
export ORACLE_SID
```

- b. Invoke SQLPlus from the command line:

```
sqlplus /nolog
```

- c. Log in to SQLPlus as a DBA user:

```
connect sys/sys_password as sysdba
```

Windows

Windows:

- a. Set the environment variable from the command line:

```
ORACLE_SID=your_SID
```

- b. Invoke SQLPlus from the command line:

```
sqlplus /nolog
```

- c. Log in to SQLPlus as a DBA user:

```
connect sys/sys_password as sysdba
```

3. Delete the Asset Management for IT database user (maximo, by default) using an SQL command like the following sample command:

```
drop user maximo cascade;
```

Do not disconnect from the database. If you receive an error when issuing this command that you cannot drop a currently connected user, issue the following SQL commands and then try the SQL drop command again:

```
shutdown immediate;
startup;
```

4. Manually recreate the database. Refer to “Manually configuring Oracle 10g” on page 112 or “Manually configuring Oracle9i Rel2” on page 114 for more information.

Restoring the Microsoft SQL Server database

In order to rerun IBM Tivoli Asset Management for IT installation program, you must first restore the Microsoft SQL Server database server to the same state as before Asset Management for IT was installed.

Before you begin

Ensure that the MXServer application server on WebSphere Application Server Network Deployment is stopped before deleting the database.

About this task

Restoring the Microsoft SQL Server database server to the same state as before Asset Management for IT was installed, requires you to drop the Asset Management for IT database that you manually created and then recreate it before rerunning the Asset Management for IT installation program.

To restore the Asset Management for IT database, complete the following steps:

1. Open the Microsoft SQL Server Management Studio.

2. Log into the instance of Microsoft SQL Server that is used by Asset Management for IT install using the sa user ID, and then click **Connect**.
3. To delete the database, expand the instance tree down to the databases category, right-click the database name you created during installation (MAXDB71 for example), and then click **Delete**.
4. In the Delete Object window, select **Delete backup and restore history information for databases** and **Close existing connections**, and then click **OK**.
5. Manually recreate the MAXDB71 database. Refer to Manually configuring SQL Server for more information.

Troubleshooting the product uninstallation program

Use the information contained in this section to troubleshoot errors encountered when using the product uninstallation program.

Error CTG00001 when performing an uninstall

In certain instances, while performing a product uninstall from the administrative system, you might encounter error CTG00001 The uninstall was unsuccessful. You will need to manually uninstall the Maximo product.

About this task

Click **OK** on the error message dialog box to finish the automated uninstall process.

To complete the uninstall, you will need:

1. Manually delete installation directories located under C:\IBM\SMP\maximo.
2. Verify registry entries for the product and base services product are removed.

What to do next

Registry entries can be found under HKEY_LOCAL_MACHINE/SOFTWARE/IBM/Tivoli Base Services and under the of the ISM family product, for example, Asset Management for IT.

Uninstalling IBM Tivoli Asset Management for IT silently

In order to uninstall Asset Management for IT silently, you must have a valid response file to use with the uninstallation program.

Before you begin

Note: If the Asset Management for IT deployment included Oracle configuration, the response file must be edited to remove extraneous backslashes. Refer to “Silent middleware installation program options” on page 54 for more information.

1. Open the response file in a text editor and ensure the **INSTALLER_UI** property is set to **INSTALLER_UI=silent**.
2. Copy the response file to the target system.
3. Run the Asset Management for IT uninstall program in silent mode by opening a console window on the administrative workstation and using the following command:

```
tamit_install_dir_uninstall\uninstall.exe -f response_file_path
```

Include the whole path name while specifying the response file.

4. After the Asset Management for IT uninstall program completes, you can reinstall Asset Management for IT by restarting the Asset Management for IT installation program. After a successful installation, the server you are installing from, the administrative system will prompt you to reboot the system.
5. Check to ensure that the uninstall program removed the Asset Management for IT installation directory, for example, `c:\ibm\smp`. If the Asset Management for IT installation failed early in the process, the Asset Management for IT uninstall program might not remove the Asset Management for IT installation directory. If this directory still exists after you have completed the uninstall process, you will have to remove it manually before you proceed to the reinstallation process.

Uninstalling the maximo.ear file

After you uninstalled IBM Tivoli Asset Management for IT application, make sure you removed the maximo.ear file. This section describes how to manually remove the file.

1. Launch the browser and open the WebSphere Administrative Console by typing the following URL: `http://computer_name:port_number/ibm/console`. For example, `http://local_host:9060/ibm/console`.
2. At the Welcome, enter your information login screen, enter your **User ID** and **Password**, then click **Log in**. This action opens the Welcome screen for the WebSphere Administrative Console.
3. In the window navigation, expand **Applications**, and click on **Enterprise Applications**.
4. Select the checkbox corresponding to **MAXIMO**.
5. Click the **Uninstall** button.
6. Click **Save**.

What to do next

Verify that the application has been removed by previewing the **Application Status**.

Notices

This information was developed for products and services offered in the U.S.A.

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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

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 PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some 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 are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM 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 use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 79758 U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines 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 on the Web at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Index

Special characters

-showfeatures 261
-addfeatlist 260, 261
-delfeatlist 260, 261

A

access collection 18
action
 install 248
 showavail 248
 showinstalled 248
 undo 248
 uninstall 248
 upgrade 248
AIX file size 27

C

configuration
 Asset Management for IT 1
configuring
 Oracle 78
configuring JMS queues
 JMS connection factory 135
confirming the Integration Composer
 installation 216
CQIN JMS queue 136, 137
CQINERRBD 138
creating JMS activation specification
 queues 137

D

data source
 manually creating 140
Database server
 manual configuration 102
DB2 157
 manual configuration, 8.2 106
 manual configuration, 9.1 102
DB2 database server
 restoring 275
DB2 fix packs
 installation 174
deleting user environment variables 24
deployment plan
 invoking 37
deployment topology
 multi-server 7
 single-server 7
Directory Server
 reusing 79

E

error CQINERR JMS queue 139

error CTG00001
 Asset Management for IT
 uninstallation 277
error queues 138

F

firewall
 disabling 24

G

general ledger account 227
group 51

H

hardware and software requirements,
 Integration Composer 207

I

IBM DB2
 reusing 78
IBM HTTP Server 167
IBM Tivoli Asset Management for IT
 uninstallation 271
 troubleshooting 277
IBM Tivoli Directory Server 51, 162
inbound error queue 138
inbound error queue CQINERR 139
installation 33, 157
 Asset Management for IT 60, 84
 on Linux on System z 157
DB2 fix pack 174
Launchpad 29
middleware installer logs 47
middleware installer workspace 36
on 32-bit Windows 33
overview 33
paths 56, 81
post installation tasks 221, 223, 224,
 225, 226, 227, 228, 230
roadmap 33
Tivoli Asset Management for IT 56,
 81
WebSphere plug-ins 182
Installation
 post installation tasks 228
installation prerequisites, Integration
 Composer 208
installer workspace 36
installing
 language pack 153
 prerequisite software products 38
 silently 52
 WebSphere Application Server
 Network Deployment 175

Integration Composer installation
 prerequisites 208
Integration Composer installation,
 confirming 216
Integration Composer overview 206
Integration Composer requirements,
 hardware and software 207
Integration Composer, uninstalling 219
integration framework
 configuring JMS queues 131, 133,
 134, 136
 CQINBD queue 133
 creating SQOUT JMS queues 137
 Integration Composer 206
ITDS 162

J

JMS activation specification
 inbound error queue CQINERR 139

L

language enablement 267
language pack
 overview 153
launch-in-context 221
ledger account 226
Linux on System z
 creating profiles 164
 installing 157, 162, 167, 168, 169

M

maximo.ear
 uninstallation 278
media
 installation 23
Microsoft Active Directory
 reusing 79
Microsoft SQL Server
 restoring 276
middleware 33, 36, 38, 157
 installer logs 47
 installing 33
 planning 8
 reusing 15, 77
 starting on UNIX 189
 starting on Windows 187
 uninstalling 191
middleware configuration
 manual 101
MXServer
 starting
 from the administrative
 console 194
 from the command line 193

O

Oracle
 manual configuration, 10g 112
 manual configuration, 9i 114
 reusing 78
Oracle database
 restoring 275
organization 225
overview, Integration Composer 206

P

packages 233
password policy
 system 21
planning
 Asset Management for IT 16
 middleware 8
 Tivoli Asset Management for IT 7
plug-in 168
post installation tasks
 error queues 138
post-installation tasks 216
 top-level class for IT
 assets 228
 software 228
preparation
 IBM Tivoli Asset Management for IT
 installation 23
preparing to install
 middleware 27
prerequisite 38
prerequisites
 procedures 24, 25, 26
Prerequisites
 procedures 25
process ID 35
process solution
 deployment 237
process solution installation
 packages 233
Process Solution Installation
 logs 264
process solution installation client 248
Process Solution Installer
 installing 155
 language packs 155
 language packs
 installing 155
 PMP 155

R

response file
 options 54
restoring
 DB2 database server 275
 Oracle database 275
role 18

S

security
 planning 18
security group 18

security groups 230
service integration bus
 adding a server 132
shared memory 26
silent
 installation 52, 54
 uninstallation 277
solutionInstaller script
 solutionInstaller.bat 248
 solutionInstaller.sh 248
SQIN JMS queue 136
SQINBD queue 134
SQL Server
 manual configuration 116
 SQL Server 116
SQOUTBD queue 134
startFusion file
 memory allocation 217
system password policy settings 21

T

Tivoli Asset Management for IT
 deployment 7
Tivoli Asset Management for IT
 middleware
 UNIX systems 27
Tivoli Integration Composer
 installing
 with Process Solution
 Installationpackage 213
 with PSI package 211
 UNIX systems 213
 Windows 64-bit systems 211
troubleshooting middleware installer
 invalid DB2 password 50

U

ulimit
 setting 25
uninstallation
 IBM Tivoli Asset Management for
 IT 277
uninstalling
 IBM Tivoli Asset Management for IT
 manually deployed 273
uninstalling Integration Composer 219
uninstalling Integration Composer on
 Unix-based operating systems 219
uninstalling Integration Composer on
 Windows operating systems 219
user 51

V

Virtual Member Manager 169
VMM 169

W

WAS 164
WebSphere
 compressed file 175

WebSphere (*continued*)
 plug-ins
 installation 182
 Portal Server deployment 201
 Portal Server overview 201
WebSphere Application Server 164
WebSphere Application Server
 Deployment Manager 164
WebSphere plug-in 168
work type 228

X

xml request pages 267

Z

zLinux
 installing 164



Printed in USA