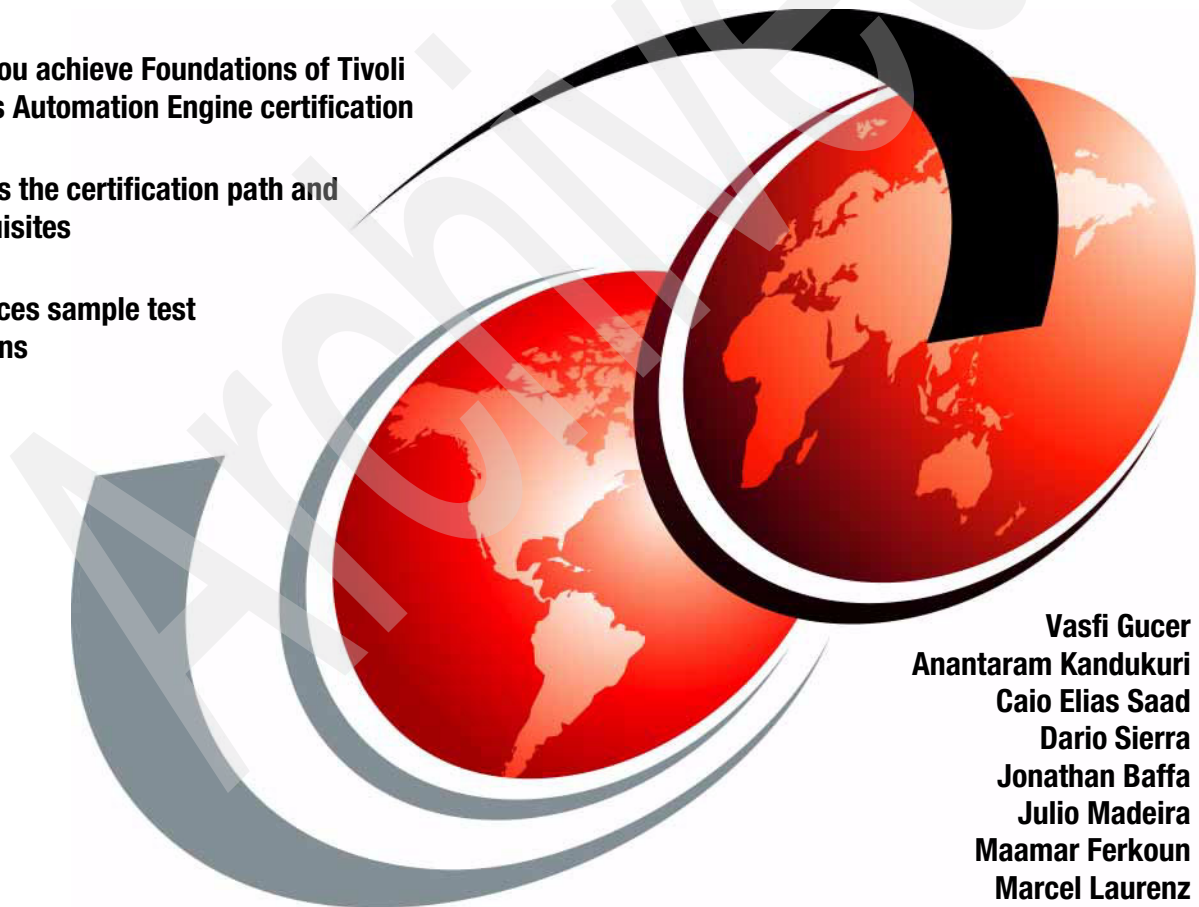


Certification Study Guide Series: Foundations of Tivoli Process Automation Engine

Helps you achieve Foundations of Tivoli
Process Automation Engine certification

Explains the certification path and
prerequisites

Introduces sample test
questions



Vasfi Gucer
Anantaram Kandukuri
Caio Elias Saad
Dario Sierra
Jonathan Baffa
Julio Madeira
Maamar Ferkoun
Marcel Laurenz



International Technical Support Organization

**Certification Study Guide Series: Foundations of
Tivoli Process Automation Engine**

July 2009

Archived

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (July 2009)

This edition applies to Foundations of Tivoli Process Automation Engine Version 7.1.

© Copyright International Business Machines Corporation 2009. All rights reserved.

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

Contents

Notices	vii
Trademarks	viii
Preface	ix
The team that wrote this book	x
Become a published author	xii
Comments welcome	xii
Chapter 1. Certification overview	1
1.1 IBM Professional Certification Program	2
1.1.1 Benefits of certification	3
1.1.2 Tivoli Software Professional Certification	4
1.2 Test 017: Foundations of Tivoli process automation engine	7
1.2.1 Receive a 15% discount when taking the test	7
1.3 Recommended resources for study	8
1.3.1 Courses	8
Chapter 2. Prerequisites and installation	9
2.1 Tivoli process automation engine overview	10
2.2 Prerequisites	12
2.3 Typical deployment environments	12
2.3.1 Simple	12
2.3.2 Custom	13
2.4 Installation example	14
2.4.1 Before you begin	14
2.4.2 Middleware installation	15
2.4.3 Solution description and assumptions	16
2.4.4 Middleware installation	17
2.4.5 Tivoli Asset Management for IT 7.1 installation	21
Chapter 3. Platform configuration	29
3.1 Working with domains	30
3.1.1 SYNONYM domains	30
3.1.2 ALN domains	30
3.1.3 NUMERIC domains	31
3.1.4 NUMERIC RANGE domains	31
3.1.5 TABLE domains	31
3.1.6 CROSSOVER domains	31
3.2 Configure the database	32

3.2.1 Creating or modifying an object	32
3.3 Organizations and sites	34
3.3.1 Working with organizations	34
3.3.2 Delete an organization	35
3.3.3 Working with sites	36
3.4 Working with locations	37
3.5 Working with the Calendars application	37
3.6 Working with Classifications application	38
3.7 Working with E-Mail Listener	41
3.8 Working with Cron tasks	42
3.9 Working with communication templates	43
3.10 Working with escalations	45
3.10.1 Maintaining the Escalation application	45
3.10.2 Escalation components	46
3.10.3 Working with escalation points	47
3.11 Working with Workflow Designer	50
3.11.1 Creating workflows	55
3.12 Workflow Administration application	56
3.12.1 Conditional Expression Manager	57
3.12.2 Conditional Expression Manager Builder	58
3.13 Platform Configuration summary	60
Chapter 4. Financial configuration	65
4.1 Introduction to Financial configuration	66
4.2 Currency codes	66
4.3 Exchange rates	67
4.4 Chart of accounts	69
4.4.1 General Ledger Account (GL Account)	69
4.4.2 Financial Periods	71
4.5 Cost management	72
Chapter 5. Security configuration	75
5.1 Security profiles	76
5.1.1 Security Groups application	76
5.1.2 Adding security groups	78
5.1.3 The Users application	91
5.1.4 Start Centers	92
5.1.5 Security group types	93
5.2 Setting up security users	93
5.2.1 Default insert site	94
5.2.2 User statuses	94
5.2.3 Managing users	95
5.3 Setting up authentication	106

5.3.1 LDAP authentication	106
5.3.2 Native authentication.	107
5.3.3 Application server authentication	107
5.4 Conditional security overview	108
5.4.1 Conditional Expression Manager	109
Chapter 6. Migration configuration	117
6.1 Integration Framework	118
6.2 Basic integration configuration	119
6.2.1 Object structures	120
6.2.2 Publish channels	121
6.2.3 Invocation channels	122
6.2.4 Enterprise services	123
6.2.5 External systems	124
6.2.6 Endpoints	124
6.2.7 Importing data	124
6.2.8 Integration Framework summary	125
6.3 Migration Manager	125
6.3.1 Overview	126
6.3.2 Migration Manager concepts and components	126
6.3.3 Migration objects and migration groups	128
6.3.4 Compiled sources	128
6.3.5 Migration Manager applications	129
6.3.6 Migration planning	132
6.3.7 Migration flow	133
6.3.8 Migration Manager summary	134
Chapter 7. Start Center configuration	135
7.1 Start Center templates	136
7.1.1 Start Center permissions	136
7.1.2 Creating a new Start Center template	137
7.1.3 Modifying a portlet	139
7.1.4 Modifying an existing Start Center template	140
7.1.5 Associating a Start Center template to a security group	141
7.2 Key Performance Indicators	142
7.2.1 Creating a Key Performance Indicator	142
7.2.2 KPI Crontask	143
Chapter 8. Work management configuration and administration	145
8.1 Work order settings	146
8.1.1 Organizations application	146
8.1.2 Start Center setup for work management	151
8.2 Setting up job plan templates	152
8.2.1 Job plan concepts	153

8.3 Work Order module	153
8.3.1 Work Order applications	154
8.3.2 Creating work orders	156
8.4 Work management capabilities	156
8.4.1 Nested job plans	156
8.4.2 Job plan template	157
8.4.3 Work management status flow control	157
Chapter 9. Reporting configuration	159
9.1 Report administration	160
9.1.1 Generating the Request pages	161
9.1.2 Importing a report	162
9.1.3 Adding a report	163
9.2 Report configuration	164
9.3 Running reports	166
9.3.1 To schedule a report and send with e-mail	169
9.3.2 To view and edit scheduled reports	171
Appendix A. Sample certification test questions	173
Questions	174
Answers	179
Related publications	181
IBM Redbooks	181
Online resources	181
How to get Redbooks	182
Help from IBM	182
Index	183

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 give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS 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.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.


Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

DB2®
Foundations™
IBM®

Lotus®
Maximo®
Redbooks®

Redbooks (logo) ®
Tivoli®
WebSphere®

The following terms are trademarks of other companies:

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.

Snapshot, and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the U.S. and other countries.

Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

J2EE, Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Active Directory, Expression, Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Preface

This IBM® Redbooks® publication is a study guide for Test 000-017: Foundations™ of Tivoli® Process Automation Engine and is aimed at individuals who want to get an IBM Professional Certification on Tivoli Process Automation Engine.

The Foundations of Tivoli Process Automation Engine certification exam, offered through the Professional Certification Program from IBM, is designed to validate the skills required of technical professionals who works in the implementation and configuration of Tivoli's process automation engine. Note that this test is a prerequisite for several other certifications, such as IBM Certified Deployment Professional - Tivoli Asset Management for IT V7.1.

This book provides a combination of theory and practical experience needed for a general understanding of the subject matter. It also provides sample questions that will help in the evaluation of personal progress and provide familiarity with the types of questions that you will encounter in the exam.

This publication does not replace practical experience, nor is it designed to be a stand-alone guide for any subject. Instead, it is an effective tool that, when combined with educational activities and experience, can be an extremely useful preparation guide for the exam.

For your convenience, we structure the chapters based on the sections of the Test 000-017: Foundations of Tivoli Process Automation Engine, such as Prerequisites and Installation, Platform Configuration and so on, so studying each chapter will help you prepare for one section of the exam.

The team that wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.



Vasfi Gucer is a Project Leader at the International Technical Support Organization, Austin Center. He has been with the ITSO since January 1999. He has more than 12 years of experience in the areas of systems management, networking hardware, and software on mainframe and distributed platforms. He has worked on various Tivoli client projects as a systems architect in the U.S. He writes extensively and teaches IBM classes worldwide on Tivoli software. Vasfi is also an IBM Certified Senior IT Specialist, PMP, and ITIL® Expert.



Anantaram Kandukuri is a Maximo® - Sr. Delivery Manager at Envision Enterprise Solutions Pvt. Ltd, Hyderabad, India. He has 12 years of production experience in process industry and more than 13 years of IT experience in software development, customization, and implementation of ERP, EAI, and J2EE™ applications. He has broad experience in Maximo Solutions, including the 5.1, 5.2, 6.2, and 7.1 versions.



Caio Elias Saad is a Software Engineer at IBM Brazil Software Laboratory, based in São Paulo, Brazil. He has over 5 years of experience in Java™ Enterprise development and over 2 years working on IBM Maximo Asset Management development. He has been involved in many Maximo Core EAM development projects for v6.x, v7.x and V8.x, as well as a huge Maximo V7.x implementations using Integration Framework and other products like Maximo for Oil and Gas, and Calibration industry solutions.



Dario Sierra is a System Management Integration coordinator at IBM Argentina. He has worked at IBM for more than 9 years. He has 8 years of experience working in Information Technology and Tivoli products, focusing on Configuration manager, TPM, and TAMIT. He holds a degree in Systems from UTN Argentina and he is ITIL certified.



Jonathan Baffa is the Director of Information Technology for SaS, a long term Maximo and IBM Business Partner. Jonathan is an IBM Certified Advanced Deployment Professional, ITIL Certified, and has over 4 years of experience with Maximo and its related products. Jonathan provides strategic direction for corporate IT and establishes best practices for hosted and non-hosted solutions as well as their technical engagements and deployments.



Julio Madeira is a Software Engineer with more than 15 years experience in the IT field, including the last 2 years at IBM. He holds the Bachelor Degree in Computer Sciences from Catholic University of Santos and also a Post-Graduate degree in IT Management from Fundação Getúlio Vargas in Brazil.



Maamar Ferkoun is a Senior Product Professional with the IBM worldwide Software Advanced Technology group. Currently based in IBM China and Hong Kong, he has over 20 years of experience in the IT industry, including 10 years with IBM. He holds a degree in computer science, an EXIN ITIL Manager, and a COBIT certification. Maamar began his career in IBM as a software field engineer engaged across the Asia Pacific region. His area of expertise covers the service management product portfolio and best practices.



Marcel Laurenz is a Senior IT Consultant and Director of LAURENZ-IT, based in northern Germany. Marcel has more than 10 years experience leading international projects and teams, specifically in area of operations and service management. He is a certified IBM Lotus®, WebSphere®, Tivoli, Microsoft®, and ITIL expert and holds a degree in Sport Science and Economy. His entrepreneurial focus is on building high performance teams.

Thanks to the following people for their contributions to this project:

Wade Wallace

International Technical Support Organization, Austin Center

Tamikia Barrow
International Technical Support Organization, Raleigh Center

Alison Chandler
International Technical Support Organization, Poughkeepsie Center

Kristin Wall Gibson, Emma Jacobs, Craig Kokay
IBM USA

Karim Badr
IBM Egypt

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:
ibm.com/redbooks
- ▶ Send your comments in an e-mail to:
redbooks@us.ibm.com
- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Archived

Certification overview

This chapter provides an overview of the skills required to become an IBM certified Advanced Technical Expert. It covers the following topics related to obtaining the certification:

- ▶ IBM Professional Certification Program
- ▶ Test 017: Foundations of Tivoli process automation engine
- ▶ Recommended resources for study

1.1 IBM Professional Certification Program

Having the right skills for the job is critical in the growing global marketplace. IBM Professional Certification, designed to validate skill and proficiency in the latest IBM solution and product technology, can help provide that competitive edge. The IBM Professional Certification Program Web site is available at:

<http://www.ibm.com/certify/index.shtml>

The IBM Professional Certification Program offers a business solution for skilled technical professionals seeking to demonstrate their expertise to the world.

In addition to demonstrating your skill and proficiency in the latest IBM technology and solutions, professional certification can help you excel at your job by giving you and your employer confidence that your skills have been tested. You can deliver higher levels of service and technical expertise than non-certified employees and move on a faster career track. Professional certification puts your career in your control.

The certification requirements are difficult but not overwhelming. Certification is a rigorous process that differentiates you from everyone else.

The mission of the IBM Professional Certification Program is to:

- ▶ Provide a reliable, valid, and fair method of assessing skills and knowledge.
- ▶ Provide IBM with a method of building and validating the skills of individuals and organizations.
- ▶ Develop a loyal community of highly skilled certified professionals who recommend, sell, service, support, and use IBM products and solutions.

The IBM Professional Certification Program has developed certification role names to guide you in your professional development. The certification role names include IBM Certified Specialist, IBM Certified Solutions/Systems Expert, and IBM Certified Advanced Technical Expert for technical professionals who sell, service, and support IBM solutions. For technical professionals in application development, the certification roles include IBM Certified Developer Associate and IBM Certified Developer. An IBM Certified Instructor certifies the professional instructor.

The IBM Professional Certification Program provides a structured pathway leading to an internationally recognized qualification. The program is designed for flexibility by enabling you to select your role, prepare for and take tests at your own pace, and, in some cases, select from a choice of elective tests best suited to your abilities and needs. Some roles also offer a shortcut by offering credit for a certification obtained in other industry certification programs.

You can be a network administrator, systems integrator, network integrator, solution architect, solution developer, value-added reseller, technical coordinator, sales representative, or educational trainer. Regardless of your role, you can start charting your course through the IBM Professional Certification Program today.

1.1.1 Benefits of certification

Certification is a tool to help objectively measure the performance of a professional on a given job at a defined skill level. Therefore, it is beneficial for individuals who want to validate their own skills and performance levels, those of their employees, or both. For optimum benefit, the certification tests must reflect the critical tasks required for a job, the skill levels of each task, and the frequency a task must be performed. IBM prides itself in designing comprehensive, documented processes that ensure that IBM certification tests remain relevant to the work environment of potential certification candidates.

In addition to assessing job skills and performance levels, professional certification can also provide such benefits as the following:

- ▶ For employees:
 - Promotes recognition as an IBM certified professional
 - Creates advantages in interviews
 - Assists in salary increases, corporate advancement, or both
 - Increases self-esteem
 - Provides continuing professional benefits
- ▶ For employers:
 - Measures the effectiveness of training
 - Reduces course redundancy and unnecessary expenses
 - Provides objective benchmarks for validating skills
 - Facilitates long-range planning
 - Helps to manage professional development
 - Aids as a hiring tool
 - Contributes to competitive advantage
 - Increases productivity
 - Increases morale and loyalty
- ▶ For IBM Business Partners and consultants:
 - Provides independent validation of technical skills
 - Creates competitive advantage and business opportunities
 - Enhances prestige of the team
 - Contributes to meeting IBM requirements for various IBM Business Partner programs

Specific benefits can vary by country (or region) and role. In general, after you become certified, you should receive the following benefits:

- ▶ Industry recognition

Certification may accelerate your career potential by validating your professional competency and increasing your ability to provide solid, capable technical support.

- ▶ Program credentials

As a certified professional, you receive through e-mail your certificate of completion and the certification mark associated with your role for use in advertisements and business literature. You can also request a hardcopy certificate, which includes a wallet-size certificate.

IBM Professional Certification acknowledges the individual as a technical professional. The certification mark is for the exclusive use of the certified individual.

- ▶ Ongoing technical vitality

IBM certified professionals are included in mailings from the IBM Professional Certification Program.

1.1.2 Tivoli Software Professional Certification

The IBM Tivoli Professional Certification program offers certification testing that sets the standard for qualified product consultants, administrators, architects, and partners.

The program also offers an internationally recognized qualification for technical professionals seeking to apply their expertise in today's complex business environment. The program is designed for those who implement, buy, sell, service, and support IBM Tivoli solutions and want to deliver higher levels of service and technical expertise.

Whether you are a Tivoli client, partner, or technical professional wanting to put your career on the fast track, you can start on the road to becoming a Tivoli Certified Professional today.

Benefits of Tivoli certification

This section describes the benefits of IBM Tivoli certification. Tivoli certification provides the following benefits:

- ▶ For the individual:

- IBM Certified certificate and use of logos on business cards

Note: Certificates are sent by e-mail. However, a paper copy of the certificate along with a laminated wallet card can also be requested by sending an e-mail to <mailto:certify@us.ibm.com>.

- Recognition of your technical skills by your peers and management
- Enhanced career opportunities
- Focus for your professional development
- ▶ For the IBM Business Partner:
 - Confidence in the skills of your employees
 - Enhanced partnership benefits from the IBM Business Partner program
 - Ability to bill your employees' services at higher rates
 - Strengthens proposals to customers
 - Deepens technical skills available to prospective customers
- ▶ For the customer:
 - Confidence in the services professionals handling your implementation
 - Ease of hiring competent employees to manage your Tivoli environment
 - Enhanced return on investment (ROI) through more thorough integration with Tivoli and third-party products
 - Ease of selecting a Tivoli Business Partner that meets your specific needs

Certification checklist

This section provides a certification checklist. Follow these steps to pursue certification:

1. Select the certification that you want to pursue.
2. Determine which test or tests are required by reading the certification role description.
3. Prepare for the test, using the following resources provided:
 - Test objectives
 - Recommended educational resources
 - Sample assessment test
 - Other reference materials
 - List of opportunities for gaining experience

Note: These resources are available from each certification description page, as well as from the test information page.

4. Register to take a test by contacting one of our worldwide testing vendors:
 - Thomson Prometric
 - Pearson Virtual University Enterprises (VUE)

Note: When providing your name and address to the testing vendor, be sure to specify your name exactly as you want it to appear on your certificate.

5. Take the test. Be sure to keep the Examination Score Report provided upon test completion as your record of taking the test.

Note: After taking a test, your test results and demographic data (including name, address, e-mail, and phone number) are sent from the testing vendor to IBM for processing (allow two to three days for transmittal and processing). After all the tests required for a certification are passed and received by IBM, your certificate is issued.

6. Repeat steps 3 through 5 until all required tests are successfully completed for the desired certification role. If you must meet additional requirements (such as an “other vendor” certification or exam), follow the instructions on the certification description page to submit these requirements to IBM.
7. After you complete your certification requirements, you are sent an e-mail asking you to accept the terms of the IBM Certification Agreement before receiving the certificate.
8. Upon acceptance of the terms of the IBM Certification Agreement, an e-mail is sent containing the following electronic deliverables:
 - A Certification certificate in PDF format, which can be printed in either color or black and white
 - A set of graphic files of the IBM Professional Certification mark associated with the certification achieved
 - Guidelines for the use of the IBM Professional Certification mark
9. To avoid unnecessary delay in receiving your certificate, ensure that your current e-mail is on file by maintaining an up-to-date profile. If you do not have an e-mail address on file, your certificate is sent through postal mail.

After you receive a certificate by e-mail, you can also contact IBM at <mailto:certify@us.ibm.com> to request that a hardcopy certificate be sent by postal mail.

Note: IBM reserves the right to change or delete any portion of the program, including the terms and conditions of the IBM Certification Agreement, at any time without notice. Some certification roles offered through the IBM Professional Certification Program require recertification.

1.2 Test 017: Foundations of Tivoli process automation engine

This section describes the process of obtaining Foundations of Tivoli process automation engine certification. We can categorize the certification process as follows:

- ▶ Job role description and target audience:
An IBM Certified Deployment Professional - Foundations of Tivoli process automation engine is a technical professional responsible for planning, installation, configuration, operations, administration, and maintenance of a Tivoli process automation engine. This individual is expected to perform these tasks with limited assistance from peers, product documentation, and support resources.
- ▶ To be certified you must select Test 017: Foundations of Tivoli process automation engine certification
 - Approximate number of questions: 51
 - Duration in minutes: 75
 - Format: Multiple choice
 - Required passing score: 70%
- ▶ Test 017 objectives:
For the most up to date objectives of the Foundations of Tivoli process automation engine certification test, refer to the following link:
<http://www-03.ibm.com/certify/tests/obj017.shtml>

1.2.1 Receive a 15% discount when taking the test

You can receive a 15% discount on the Foundations of Tivoli process automation engine certification exam if you take it at any Thomson Prometric testing center. Just remember to use the code *15T017*.

1.3 Recommended resources for study

Courses and publications are offered to help you prepare for the certification tests. The courses are recommended, but not required, before taking a certification test. If you want to purchase Web-based training courses or are unable to locate a Web-based or classroom course at the time and location you desire, contact one of our delivery management teams at:

- ▶ Americas:
<mailto:tivamedu@us.ibm.com>
- ▶ EMEA:
<mailto:tived@uk.ibm.com>
- ▶ AP:
<mailto:tivtrainingap@au1.ibm.com>

Note: Course offerings are continuously being added and updated. If you do not see the courses listed in your location, contact one of the previously listed delivery management teams.

1.3.1 Courses

Refer to the following link for a list of courses related to Tivoli process automation engine:

<http://www-03.ibm.com/certify/tests/edu017.shtml>

Prerequisites and installation

This chapter provides an overview of IBM Tivoli process automation engine and the installation steps along with its components. You should consider the scenarios, topologies, hardware, and software that must be analyzed before starting the installation.

The following topics are discussed in this chapter:

- ▶ Tivoli process automation engine overview
- ▶ Prerequisites
- ▶ Typical deployment environments
- ▶ Installation example

2.1 Tivoli process automation engine overview

The Tivoli's process automation engine provides a common foundation to the Tivoli Service Management products installer.

Note: IBM Service Management (ISM) is a comprehensive and integrated approach for Service Management, integrating technology, information, processes, and people to deliver service excellence and operational efficiency and effectiveness for traditional enterprises, service providers, and mid-size companies.

Tivoli process automation engine provides a user interface, configuration services, workflows and the common data system needed for IBM Service Management products and other services. Tivoli process automation engine records choices you make about your ISM product and configuration parameters associated with those choices, and then installs and deploys the product based upon the information you entered.

Tivoli process automation engine, previously known as Tivoli base services, is provided with Tivoli Maximo Asset Management, Change and Configuration Manager Database (CCMDB), Tivoli Service Request Manager (SRM) and Tivoli Asset Management for IT (TAMIT).

Any product that has the Tivoli process automation engine as its foundation can be installed with any other product that has the Tivoli process automation engine. The installer will detect that the Tivoli process automation engine is already installed and just enable the additional applications and features of the product being installed.

Every product ships with a specific version of the Tivoli process automation engine. The versions must match up if you are installing more than one product.

- ▶ Tivoli Change and Configuration Management Database 7.1
Includes Tivoli process automation engine 7.1
- ▶ Tivoli Change and Configuration Management Database 7.1.1
Includes Tivoli process automation engine 7.1.1
- ▶ Tivoli Service Request Manager 7.1
Includes Tivoli process automation engine 7.1.1
- ▶ Tivoli Asset Management for IT 7.1
Includes Tivoli process automation engine 7.1.1
- ▶ Enterprise Asset Management and Maximo Asset Management 7.1
Includes Tivoli process automation engine 7.1.1

Once you have installed one of these products, you can install others on top of it. There is a different install option for each product's launchpad that you must choose, if you want to install the product on top of another. With this option, the Tivoli process automation engine will not be reinstalled. The new product's applications will be enabled, as well as the existing applications.

Now we put the Tivoli process automation engine and the Tivoli process automation engine-based products in the perspective of ISM architecture. Figure 2-1 shows the Tivoli process automation engine integrated portfolio.

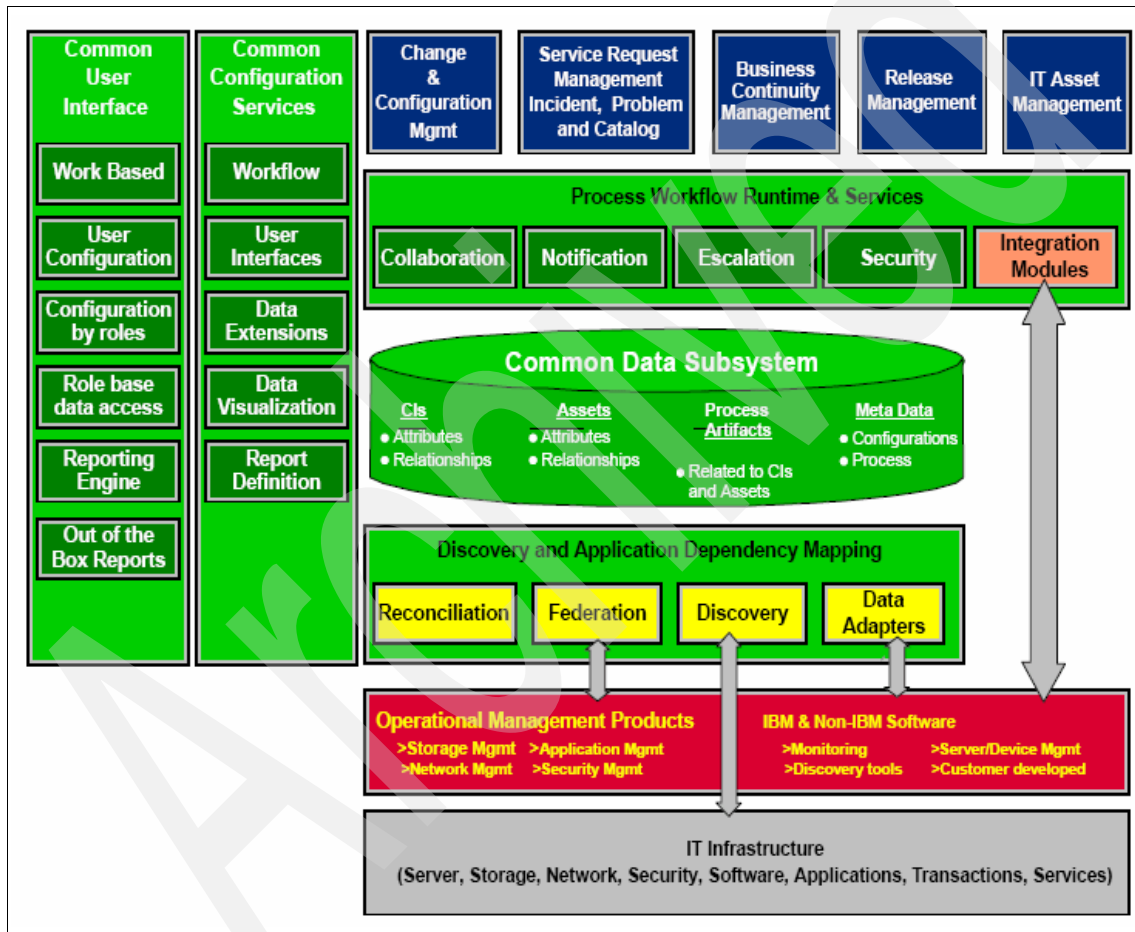


Figure 2-1 Tivoli process automation integrated portfolio

2.2 Prerequisites

Tivoli process automation engine requires multiple software servers that can be installed on separate, dedicated server machines (for best performance) or the same physical server (not recommended for production environments). The different components of the ISM solution environment, called middleware, are as follows:

- ▶ **Database:** The database serves as the repository for all configuration information (CI).
- ▶ **Application server:** Tivoli process automation engine is built using Java 2 Enterprise Edition (J2EE) technology, which requires a commercial application server, such as IBM WebSphere Application Server.
- ▶ **HTTP server:** A separate, dedicated HTTP server can be configured to work with the J2EE application server.
- ▶ **Directory server:** A directory server can be configured to work with the ISM product to maintain lists of users and groups for security purposes.
- ▶ **Administrative system:** The administrative system is not part of the middleware but is used to deploy the ISM product. After the initial deployment, the administrative system is used to make updates or changes to the deployment. This machine has to be a Windows® system.

For specific information about prerequisites of a particular ISM product, refer to the installation manual of each product.

2.3 Typical deployment environments

This section describes the two installation paths available when installing the Tivoli process automation engine.

2.3.1 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. All middleware used in conjunction with Tivoli process automation engine must be installed on the system using the Tivoli middleware installer using default values. The ISM product will be installed using default values provided by the Tivoli middleware and Tivoli process automation engine installation programs. If you intend to override default values used by the simple deployment path, you must use the custom deployment path instead.

Figure 2-2 shows a simple deployment scenario.

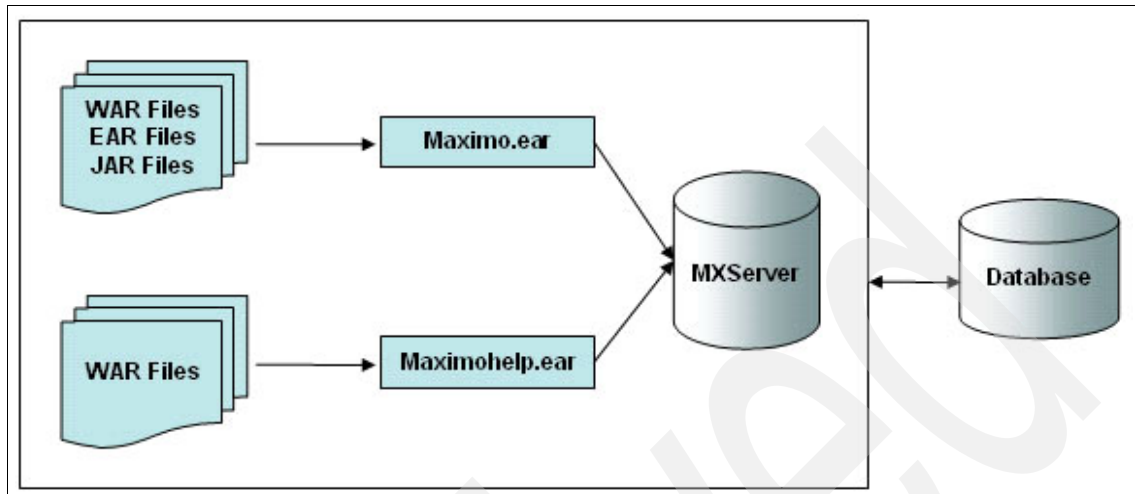


Figure 2-2 Simple deployment

2.3.2 Custom

A custom deployment typically involves deploying the ISM product across several systems, some of which probably already host middleware products that you want to use with your product 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 ISM product deployment across several systems. You can enter the name of the local host as the destination for all the product components that are to be installed using the Tivoli middleware installer and the Tivoli process automation engine.

Figure 2-3 on page 14 shows a custom deployment scenario.

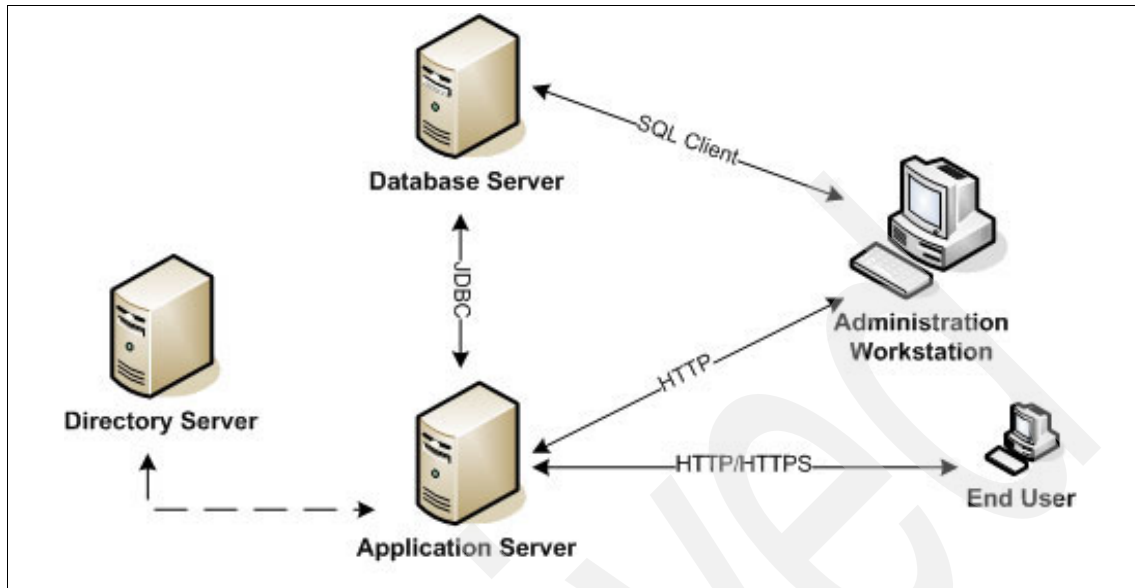


Figure 2-3 Custom deployment

The Tivoli process automation engine program can automate the configuration of middleware for use with an ISM product. For example, if you are preparing to deploy the Tivoli process automation engine and you already have your database software deployed, and you will reuse this environment, the Tivoli process automation engine installer will build the schema required.

If you choose not to have the Tivoli process automation engine automatically configure middleware, configure that piece of middleware manually prior to the execution of Tivoli process automation engine.

2.4 Installation example

In this section we discuss the installation of the prerequisite middleware and Tivoli process automation engine on a multiserver topology. Our example is based on IBM Tivoli Asset Management for IT Version 7.1

2.4.1 Before you begin

Before you install middleware or Tivoli Asset Management for IT, you must prepare your environment by, for example, disabling the firewall, deleting the

TEMP and TMP user environment variables on Windows systems, setting the limit, and so forth.

2.4.2 Middleware installation

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

- ▶ Database server
- ▶ Directory server
- ▶ J2EE server

The Tivoli middleware installer deploys software on a single machine. To deploy Tivoli Asset Management for IT middleware on multiple machines, the Tivoli middleware installer must be invoked on each machine in the topology configuration you have chosen.

If you intend to reuse existing Tivoli Asset Management for IT middleware servers, they must be configured prior to running the Tivoli Asset Management for IT installation program. You can use the Tivoli Middleware installer to configure it or you can configure it manually.

For more information about reusing middleware consult *Tivoli Asset Management for IT Release 7.1, Installation Guide / IBM WebSphere Application Server* at:

<http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itmaxam.doc/welcome.htm>

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 Tivoli middleware installer cannot subsequently deploy additional features and products onto the machine at a later time. The existing plan must first be completely undeployed through the Tivoli 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 Tivoli middleware installer process, are located in the workspace. By default, the Tivoli middleware installer workspace is defined as:

- ▶ Windows C:\ibm\tivoli\mwi\workspace
- ▶ 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 Tivoli middleware installer. Locating the workspace on a shared resource avoids the need to copy files such as the topology file manually from one machine to another. The workspace contains the items described in the following paragraphs.

Deployment plan

The deployment plan is a collection of installation steps, configuration parameters for those steps, and target machine information. It is generated through the Tivoli middleware installer and 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 about the deployment plan itself. Whenever a deployment plan is modified, which includes re-configuring 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 Tivoli 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 Tivoli Asset Management for IT middleware, this file will have to be copied to the workspace of each machine where Tivoli Asset Management for IT middleware is being deployed. The contents of this file can be used by the Tivoli Asset Management for IT installation program to populate its panels with meaningful default values. This file is saved in `<workspace>/topology.xml`.

Logs

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

2.4.3 Solution description and assumptions

Our example is based on the following software and hardware components:

- ▶ Computer 1: Windows 2003 Server EE with DB2® Enterprise Server Edition v9.5.1 and Tivoli Directory Server V6.2
- ▶ Computer 2: Windows 2003 Server EE with WebSphere Application Server v6.1.0.19 and other components

Note: In this example, this computer is a Windows computer so a separate administrative workstation is not required.

- ISM product: Tivoli Asset Management for IT 7.1

2.4.4 Middleware installation

In this section we demonstrate installation of the middleware using the default parameters. For more information refer to *Tivoli Asset Management for IT Release 7.1, Installation Guide / IBM WebSphere Application Server* at: <http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itmaxam.doc/welcome.htm>

Note: WebSphere Application Server must be installed after the directory server so that you can secure it with the Directory server.

1. Create a middleware workspace in a directory location that is accessible to all computers in the topology. This is the simplest way to share the installation data for installed middleware between each computer and the various installers you will run. In our example, we created the workspace directory in Computer 2 and mapped the network drive from Computer 1.

Note: If you do not use a shared location for the middleware workspace, a separate topology.properties will be saved for each middleware installation that you perform on each computer. You will need to manually consolidate the data into a single topology.properties file and copy the middleware workspace to a local directory on each computer in the topology as you perform installation.

2. On Computer 1, start the Launchpad and run the Middleware Installer.

3. Select the directory to create the workspace (Figure 2-4).

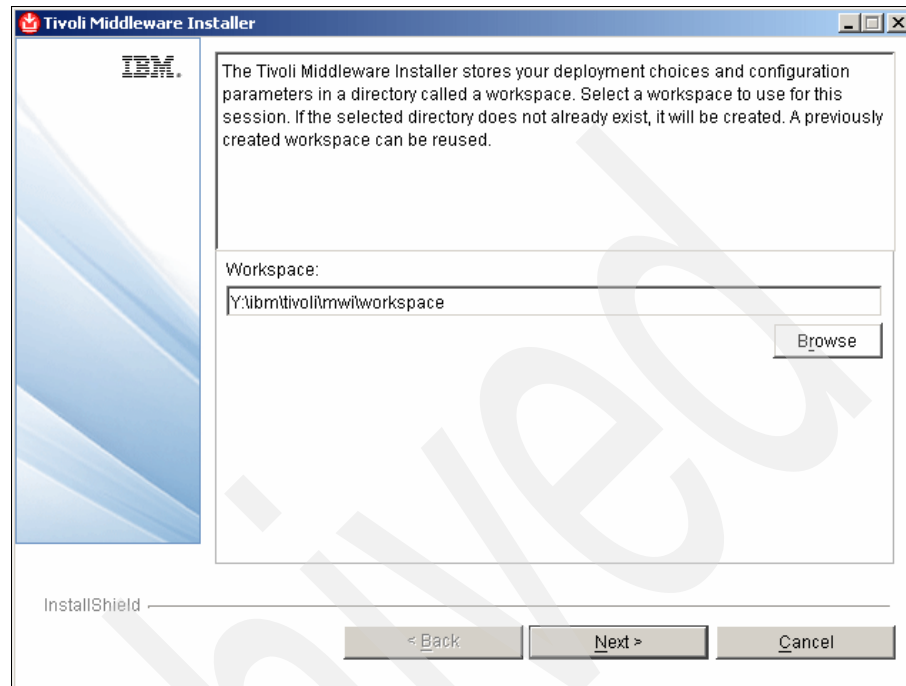


Figure 2-4 Workspace directory on Computer 2

4. Install DB2 and Tivoli Directory Server (Figure 2-5).

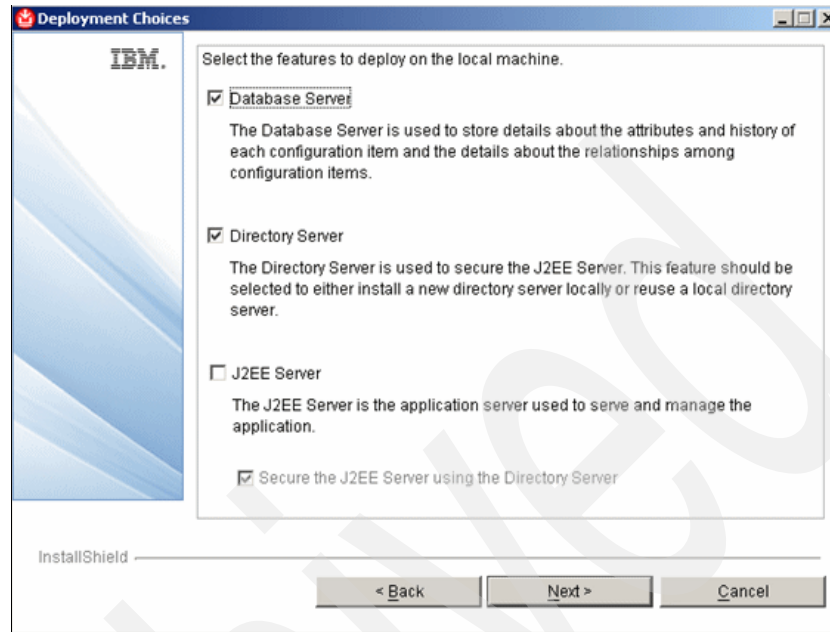


Figure 2-5 Features selection on Computer 1

Once you finish the installation, note that the workspace directory in Computer 2 has the data for the middleware installation of Computer 1, including the *topology.properties* file. See Figure 2-6.

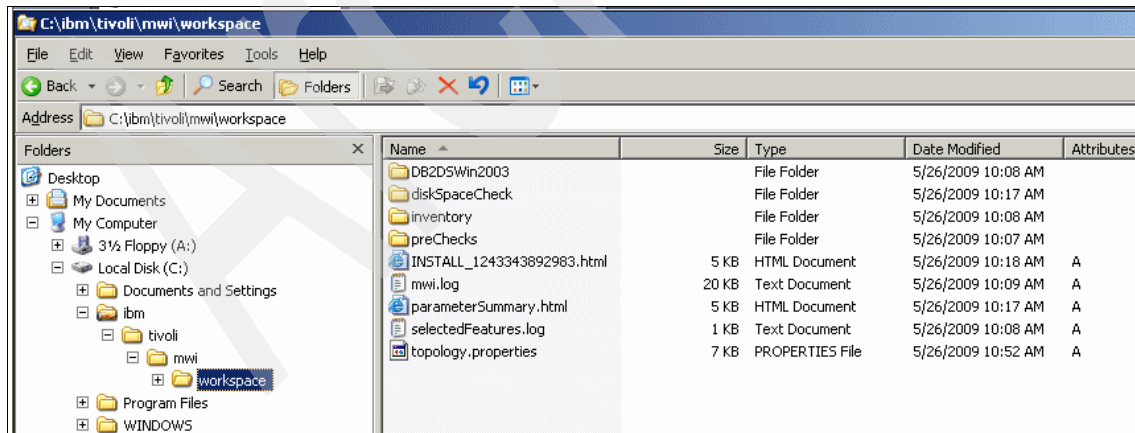


Figure 2-6 Workspace directory

5. On Computer 2, start the Launchpad and run the Middleware Installer.
6. Select the local directory to create the workspace. The installation will update the workspace including the topology.properties file. See Figure 2-7.

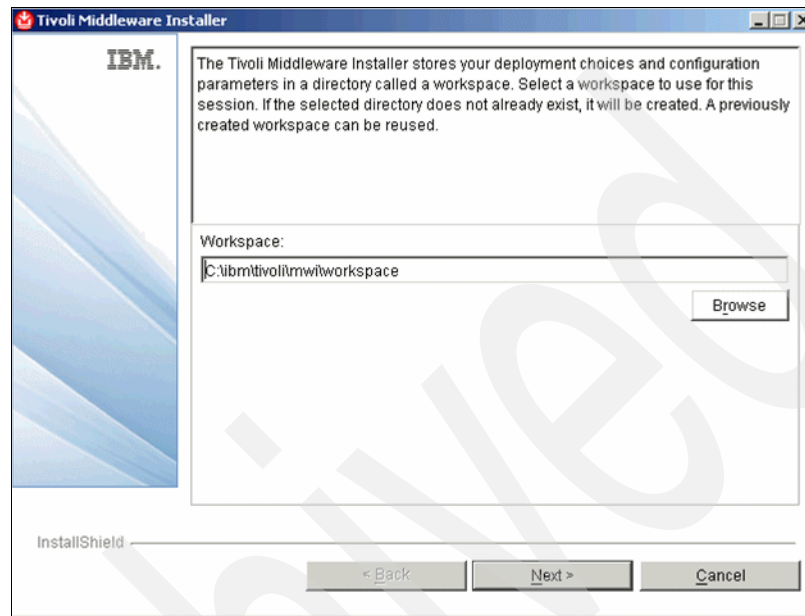


Figure 2-7 Workspace local directory on Computer 2

7. Install the WebSphere Application, as shown in Figure 2-8 on page 21.

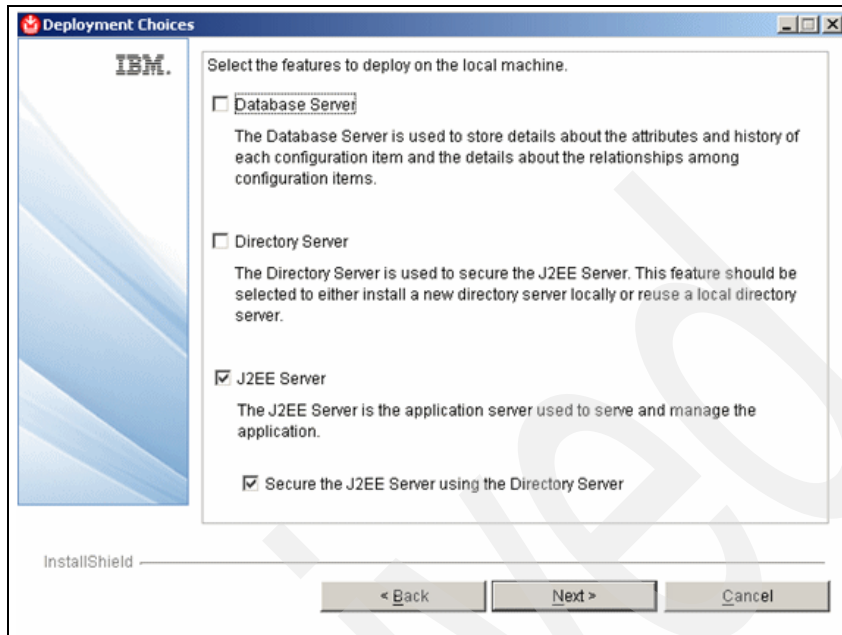


Figure 2-8 Features selection on Computer 2

2.4.5 Tivoli Asset Management for IT 7.1 installation

To install Tivoli Asset Management for IT, follow these steps:

1. Log in as Administrator on the Tivoli Asset Management for IT administrative system.
2. Launch the Tivoli Asset Management for IT installation program (Tivoli process automation engine).
3. Select a language for the installation and click **OK**.
4. From the Introduction panel, click **Next**.
5. Select the **Import Middleware Configuration Information** check box and fill out the fields, as shown in Figure 2-9 on page 22.

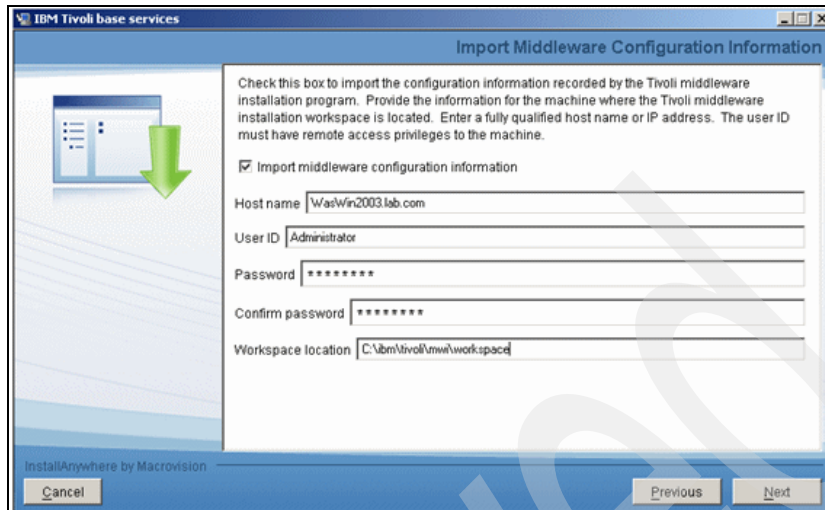


Figure 2-9 Import Middleware Configuration Information

Specify the following parameters in this panel:

- **Host name:** Enter the fully qualified host name of the system where the Tivoli middleware installer was run.
- **User ID:** Enter the User ID that was used to run the Tivoli middleware installer.
- **Password:** Enter the password of the User ID that was used to run the Tivoli middleware installer.
- **Workspace Location:** Enter the location of the topology file that contains the values entered for the Tivoli middleware installer. This file is found in the workspace that was defined during the Tivoli Asset Management for IT middleware installation task. In this example, it is:
C:\ibm\tivoli\mwi\workspace

Important: The minimum level of access required by the installer for configuring the middleware is Administrator or root.

6. Choose the Deployment Type (**Simple** or **Custom**) and click **Next**.
7. Enter installation location and click **Next**.
8. Select the Maximo database type as **DB2**.
9. Enter the Tivoli process automation engine database information as shown in Figure 2-10 on page 23.

The fields are:

- Host name
- Port
- Database name
- Instance
- Database user ID
- Database password
- Confirm password

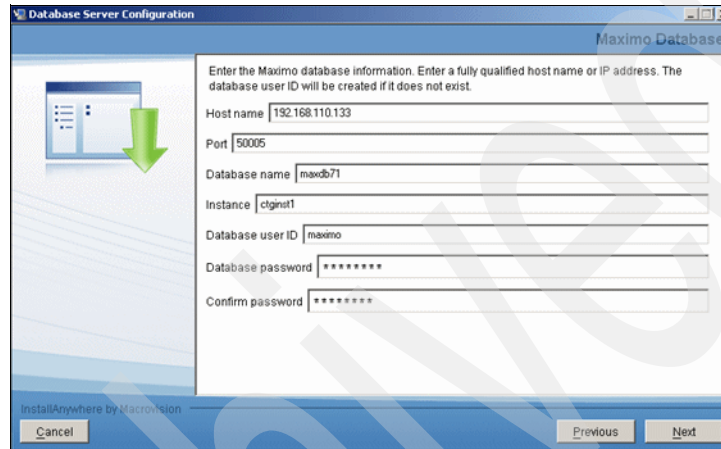


Figure 2-10 Database server configuration screen

This information will be placed in the `maximo.properties` file, which supplies database connection parameters for the Tivoli process automation engine. Tivoli process automation engine uses several other properties files to set up the system. Figure 2-11 shows an example of the `maximo.properties` file.

```
mxe.db.url=jdbc:db2://192.168.110.128:50005/maxdb71
mxe.db.driver=com.ibm.db2.jcc.DB2Driver
mxe.db.user=maximo
mxe.encrypted=true
mxe.registry.port=13400
mxe.name=MXServer
mxe.db.schemaowner=maximo

mxe.encrypted=true
```

Figure 2-11 `maximo.properties` file

In addition, you can use the `mxreportdatasources.properties` file to specify datasource information for reporting.

10. Choose to automate database creation and click **Next**.
11. Enter the following database information and click **Next**:
 - Remote access user ID
 - Password
 - Confirm password.
12. As shown in Figure 2-12, enter the following DB2 administration data and click **Next**:
 - Database software installation directory
 - Instance administrator user ID
 - Instance administrator password
 - Confirm password
 - Windows service user ID
 - Windows service password
 - Confirm password

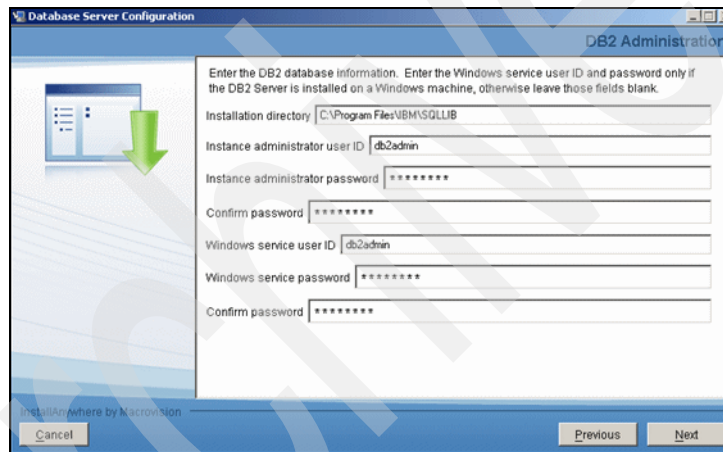


Figure 2-12 DB2 database information screen

13. In the next panel fill in the DB2 tablespace data and click **Next**.
 - Data tablespace name
 - Data tablespace size
 - Temporary tablespace name
 - Temporary tablespace size
 - Index tablespace name
 - Index tablespace size
14. Select **IBM WebSphere application server** as the J2EE Application Server.
15. Fill in the following WebSphere connectivity data and click **Next**:
 - Deployment manager host name

- Deployment manager SOAP port (8879)
16. Enter the Deployment manager operating system user ID, operating system password, confirm the password, and click **Next** (Figure 2-13).

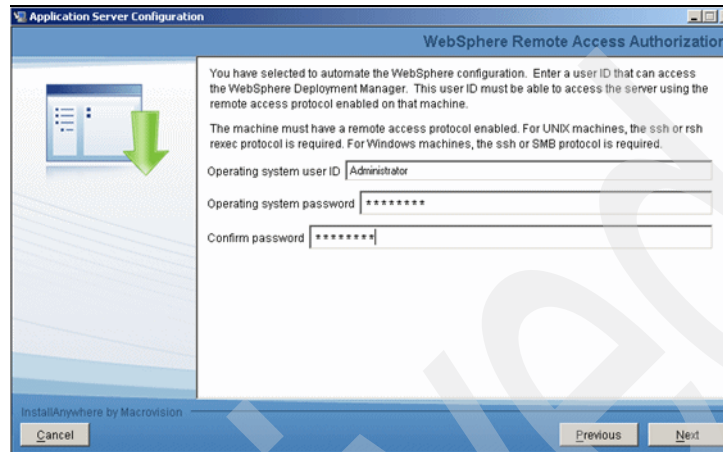


Figure 2-13 WebSphere remote access authorization screen

17. Choose to automate the creation of WebSphere configuration and click **Next**.
18. Fill in the following WebSphere administrative data (Figure 2-14) and click **Next**:
- WebSphere Application Server installation directory
 - WebSphere administrative User ID
 - WebSphere administrative user password
 - Confirm password
 - Profile name

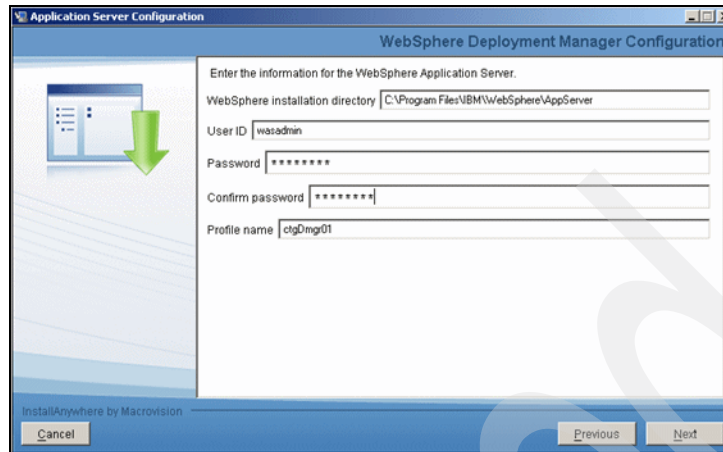


Figure 2-14 WebSphere deployment manager configuration screen

19. Fill in the WebSphere Configuration data, as shown in Figure 2-15 on page 26, and click **Next**.

- Web server port
- Web server name
- Node name
- Cluster name

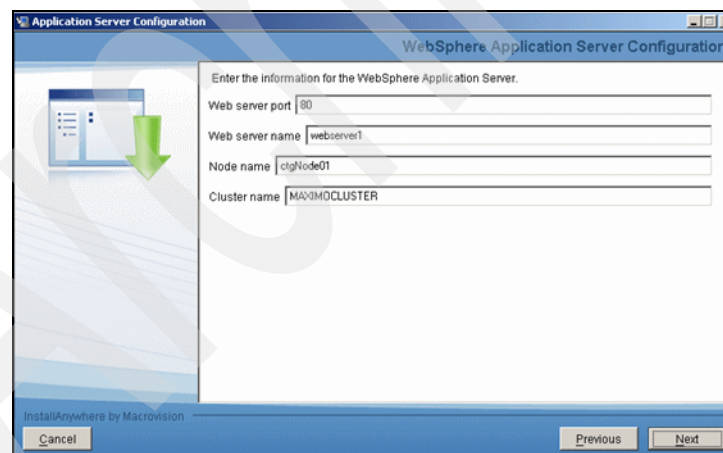


Figure 2-15 WebSphere application Server configuration screen

20. Select the **Configure J2EE application security** check box and click **Next**.

Note: This modifies the J2EE application so that authentication will be handled by an external source such as IBM Tivoli Directory Server or Microsoft Active Directory®.

21. Select whether your environment is using the IBM default schema and whether the installer should create the required users; click **Next**.
22. Enter the JMS Data Source name, choose **Do not persist JMS messages**, and click **Next**.

Note: A JMS messaging engine must be configured with a persistent data store in order to ensure that any data sent to the Tivoli process automation engine's Integration Framework for retrieval of financial data into the Tivoli process automation engine can survive restarts and failures.

23. Choose **Run Configuration Step** now and click **Next**.
24. Choose where to create the product icons and whether to create icons for all users; click **Next**.
25. Click **Next** in the Input Summary window.
26. Click **Install** in the Pre-Installation Summary window.

For information about other installation options consult *Tivoli Asset Management for IT Release 7.1, Installation Guide | IBM WebSphere Application Server*.

Platform configuration

This chapter provides details about the *Platform Configuration application*. This application collects all platform configuration options in a single place. After installing the ISM product, you have to configure various options to meet your business needs. This chapter will help you to understand the options. Besides the basic setup, you will find options to configure your database, tailor workflows to your needs, and define escalations where needed.

This chapter covers the following topics:

- ▶ Working with domains
- ▶ Configure the database
- ▶ Organizations and sites
- ▶ Working with locations
- ▶ Working with the Calendars application
- ▶ Working with Classifications application
- ▶ Working with E-Mail Listener
- ▶ Working with Cron tasks
- ▶ Working with communication templates
- ▶ Working with escalations
- ▶ Working with Workflow Designer
- ▶ Workflow Administration application
- ▶ Platform Configuration summary

3.1 Working with domains

Some fields in the system are associated with select value lists from which users choose an appropriate value. These lists of defined values are known as *domains* (sometimes referred to as value lists). The system uses many domains in its applications. Also, domains are one of the two possible ways to validate field values (the other one is Java classes). As an administrator, you use the Domains application to add, view, modify, or delete domains to fit with your business practices.

The system uses the following six kinds of domains:

- ▶ SYNONYM
- ▶ ALN
- ▶ NUMERIC
- ▶ NUMERIC RANGE
- ▶ TABLE
- ▶ CROSSOVER

3.1.1 SYNONYM domains

These are special, reserved domains in the system. You cannot add new SYNONYM domains or delete existing ones. You can add new synonym values. An example of a SYNONYM domain is work order status. The system has several values to reflect status: APPR (Approved), CAN (Canceled), CLOSE (Closed), COMP (Completed), WAPPR (Waiting on Approval), and others. Each work order status has an internal value, used by the system in its business rules, and a value that users see and choose from. You cannot add a new internal value. You can add a synonym, the value presented to the user. For example, suppose your company procedure requires two people to approve a work order. You could add synonym values for the internal WAPPR value. You could then present two different values to the user, for example, WAPPRMAN and WAPPRVP, to represent approvals at the manager and vice president level.

3.1.2 ALN domains

ALN domains are a simple list of values using one of the alphanumeric data types.

3.1.3 NUMERIC domains

Numeric domains are a simple list of values using one of the numeric data types.

3.1.4 NUMERIC RANGE domains

Numeric Range domains use one of the numeric data types, by which you specify a range rather than specific values.

You can specify the following two kinds of ranges:

- ▶ Discrete: A range with a defined interval between values, for example, a range from 0 to 10, with valid values 0, 2, 4, 6, 8, and 10. The interval in this example is 2.
- ▶ Continuous: A range within which any value that satisfies the data type is valid. For example, in a range of 1 to 6 with a decimal data type and scale of 2, values such as 1, 1.03, 2.14, 3, 4.73, 5.2, and 6 are all valid. The interval in this example is null (no value in the Interval field).

Note: You cannot create a lookup for NUMERIC RANGE domains.

3.1.5 TABLE domains

Table domains are a dynamic set of values based on the values of another object. You use the TABLE Domain dialog box to add a new domain that draws its values directly from a column in the database. This is in effect a dynamic value list because the values it draws from the database can change. It is not a list of static values that you create.

In this kind of domain you can optionally specify a group value and a key value to select an error message to display when domain validation fails.

- ▶ In the Error Message Group field, specify the group value of the error message.
- ▶ In the Error Message Key field, specify the key value of the error message.

3.1.6 CROSSOVER domains

Crossover domains are a special type of table domain in which the system brings back another value (or values) from the specified record.

3.2 Configure the database

You use the *Database Configuration application* to create or modify the objects and attributes in the database used by applications. An object is a self-contained software entity that consists of both data and functions to manipulate data. Every application is associated with an object.

When you use the Database Configuration application, you interact at the business object level. Internally, the application determines the actions to take on the tables to support the needs of business objects.

A database table stores several objects, and each object has different business rules. For example, the TICKET table defines Incident, Problem, and Ticket business objects.

3.2.1 Creating or modifying an object

Use any tab of the Database Configuration application to create or modify an object. An object can be either a view or a table. Figure 3-1 shows the object form.

The screenshot displays the 'Database Configuration' application window. The 'Object' tab is selected, showing a form for creating or modifying an object. The form is divided into three main sections: 'Details', 'View', and 'Audit'. The 'Details' section contains fields for 'Service' (CUSTAPP), 'Description' (Custom Application Service), 'Entity' (DAS), 'Class' (psdi.mbo.custapp.CustomMboSet), 'Extends Object' (CLASSIFICATIO), and 'Level' (SYSTEM). It also includes checkboxes for 'Main Object?', 'Persistent?', 'User Defined?', 'Imported?', and 'Internal?'. The 'View' section includes a 'View?' checkbox, a 'View Where' field with a dropdown menu, a 'Join to Object' field with a dropdown menu, a 'View Select' field, and an 'Automatically Select?' checkbox. The 'Audit' section includes an 'Audit Enabled?' checkbox, an 'Audit Table' field, an 'E-audit Filter' field, and an 'E-signature Filter' field.

Figure 3-1 New object screen

To create a new object, perform the following steps:

1. In the Database Configuration application, click **New Object**.

2. Type a name in the **Object** field.

The Entity field shows the value that you typed in the Object field and becomes the name of the view on the database.

3. Type a description for the new object.
4. To use Views, specify a value in the **Extends Object field**.
5. After you specify a value, the **View?** check box is selected. If the view joins two tables, type the name for the second table in the Join to Object field.
6. Complete the appropriate fields:
 - Level: Specify a value.
 - Main Object?: To make the object a main object for Workflow, select this check box.
 - Persistent?: If the object is persistent, three attributes are created: ID, description, and rowstamp (if selected). If the object is non-persistent, nothing is added for attributes, but you cannot configure the database without creating at least one attribute for the object.
 - Storage Partition: If applicable to your database, click Detail and select a storage partition for the object.
 - Optional: Provide additional details.

For more information about objects options see the System Administrator Guide.

7. Click **Save Object**.

Tip: Optionally you can also configure the Autonumbering feature in the attributes area. To set up the configuration, you have to select the **Can Number?** field and the **Autonumber** field, and you have to set the Default value to &AUTOKEY&.

Figure 3-2 Autonumbering attribute

3.3 Organizations and sites

Organizations and sites are logical divisions of a company determined by what types of operations are performed at different locations, and what data can be shared among them.

An organization is a major division of a company that contains one or more sites.

3.3.1 Working with organizations

Use the *organizations application* to set up organizations and sites to use with the system. This section provides some tips to assist you in setting up organizations.

Create an organization

Before you can create the first organization you must complete the following tasks:

- ▶ Create at least one currency code. Use the *Currency Codes application* to do this.
- ▶ Create at least one item set and one company set. Use the *Sets application* to do this.

Several data elements are required to create an organization, as shown in Figure 3-3. The steps used to create an organization follow.

The screenshot shows the 'Organizations' application interface. At the top, there's a navigation bar with 'Organizations' and a search bar. Below the navigation bar, there's a tabbed interface with 'List', 'Organization', 'Addresses', and 'Sites'. The 'Organization' tab is active. The form contains the following fields:

- Organization: A text input field with a magnifying glass icon.
- Base Currency 1: A dropdown menu with a magnifying glass icon.
- Base Currency 2: A dropdown menu with a magnifying glass icon.
- Item Set: A dropdown menu with a magnifying glass icon.
- Company Set: A dropdown menu with a magnifying glass icon.
- Default Item Status: A dropdown menu with a magnifying glass icon.
- Clearing Account: A dropdown menu with a magnifying glass icon.
- Active?: A checkbox.

Figure 3-3 New organization screen

1. In the Base Currency 1 field, enter the currency code for your base currency or click **Select Value**.

2. In the Item Set field, enter the item set you want to associate with this organization or click **Select Value**. You cannot change the item set after you save the record.
3. In the Company Set field, enter the company set you want to associate with this organization or click **Select Value**. You cannot change the company set after you save the record.
4. In the Default Item Status field, click **Select Value** and select the status you want new item master, service item, and tool records to have.

When you are creating a new organization, the **Clearing Account** and **Active?** fields are read-only until you save the record. The organization is inactive by default, the **Active?** check box is cleared and the organization cannot currently be used in the system. To activate the organization, you must edit the organization, check the **Active?** field and enter a GL account in the **Clearing Account** field.

You can also add the Autonumbering feature from the **Select Action** menu. Autonumbering is configured using the *Autonumbering attribute* described previously.

Note: You can also configure the drilldown option in the Organization application.

Edit an organization

After you create an organization, you might want to edit addresses or other information, but you cannot edit the item or company set after you save an organization record, nor can you edit **Base Currency 1** after you add a site to the organization and save the record.

3.3.2 Delete an organization

You can delete an organization only if it has no sites associated with it.

You cannot delete sites at all; therefore, you can only delete organizations that have never had sites associated with them.

More information on organizations is presented in the Asset chapter in *Certification Study Guide Series: IBM Maximo Asset Management for IT*, SG247762.

3.3.3 Working with sites

A *site* is a subdivision of an organization that can track inventory and other data separately from other sites. Certain types of information are unique to a site and not visible to other sites within the organization.

Sites belonging to the same organization must use the same currency and share the same options for work orders, assets, labor, and certain other types of data.

Use the Sites tab to add sites within an organization and to specify associated information. Sites are defined at the organization level. You can add as many sites to the same organization as needed.

After you add a new site, you cannot delete it, but you can make it inactive. If a site is inactive, users cannot access site-level records for that site.

Use the Sites tab in the Organizations application to set up the sites to use with the system. This section provides some guidelines for setting up sites.

Add a site

To add a site you only need the site name (site ID). The site name must be unique for each site across the system, not just within the organization. See Figure 3-4.

The screenshot shows the 'Organizations' application interface. The 'Sites' tab is selected. The 'Organization' dropdown is set to 'COMPANY1'. The 'Sample Company' is displayed. The 'Sites' table has columns: Site, Description, Ship to Address Code, Bill to Address Code, and Active?. Below the table, there are input fields for Site, Ship to Contact, Ship to Address Code, Bill to Contact, Bill to Address Code, Site Contact, Site Contact Group, and Active?. A 'New Row' button is at the bottom right.

Figure 3-4 Add site screen

By default, the active status for a new site follows the status for the organization—selected if the organization is active, cleared if the organization is

not active. If the check box is selected and you do not want the site to be used in the system at this time, clear the check box.

Note: To set a site to active, the organization must be active. If a site and its organization are both inactive, and you activate the organization, the site is not automatically activated. However, if you make an organization inactive, then its sites are automatically inactive.

3.4 Working with locations

The *Locations application* lets you enter and track locations for assets and organize these locations into logical hierarchical systems or network systems. Using hierarchies or systems of locations and specifying the location for assets on the asset record provides the groundwork for gathering and tracking valuable information on the history of an asset, including its performance at specific sites, as it is moved from location to location. With locations organized into systems, you can quickly find a location on the Drill down page, and identify the asset at that location.

To open the application, select **GoTo** → **Asset** → **Location** and fill in the appropriate information. Detailed information on locations is presented in the Asset chapter in *Certification Study Guide Series: IBM Maximo Asset Management for IT*, SG247762.

3.5 Working with the Calendars application

You can use the *Calendars application* to create and modify calendars associated with these system records:

- ▶ Assets
- ▶ Labor
- ▶ Locations
- ▶ Organizations
- ▶ People
- ▶ Preventive maintenance records
- ▶ Service Level Agreements
- ▶ Tools
- ▶ Work orders

Calendar records incorporate start and end dates, shift definitions, and nonworking time. Holidays are examples of non-working time. Any number of person, asset, or other records can reference a single calendar.

To open the Calendars application, select **Go To** → **Administration** → **Calendars** and fill in the appropriate information.

Calendars are an organization-level application. You create calendars for organizations. If you want site-specific calendars, you can create them with names that refer to the site, and have the site agree to just use those calendars (see Figure 3-5). You can define shifts with complex repeating patterns using the Define Pattern dialog box.

The screenshot shows the 'Calendar' application interface. At the top, there are tabs for 'List', 'Calendar', and 'Work Periods'. Below the tabs, there are input fields for 'Calendar*' (set to 'LIT'), 'LIT Department', 'Organization' (set to 'EAGLENA'), 'Start Date*' (set to '6/1/09'), and 'End Date*' (set to '6/30/09'). Below these fields is a calendar for June 2009. The calendar shows days of the week (Sunday through Saturday) and dates (1 through 30). The date '10' is highlighted in yellow. The text 'Today is: Wednesday, June 10, 2009' is visible at the top right of the calendar grid.

Figure 3-5 Calendars application

For more details about the Calendars application, refer to:
<http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itmaxam.doc/welcome.htm>

3.6 Working with Classifications application

The *Classifications application* is used to create classifications and establish an overall classification hierarchy. Classifications can help you to retrieve historical data from other applications and to create detailed information about objects that

can be classified and retrieved later. These objects include assets, locations, items, tickets, work orders, solutions, configuration items, purchasing documents, and job plans. A classification is a word, a number, or an alphanumeric. A classification can stand alone, or you can group it with other classifications for more detailed descriptions. Classifications let you store information about many objects, such as locations, assets, items, and work orders.

For example, you can assign attributes to a classification creating the attribute and specifying the data type, as shown in Figure 3-6.

The screenshot shows the 'Classifications' application interface. At the top, there's a 'List' tab and a 'Classifications' tab. Below the tabs, there's a form for editing a classification. The 'Classification' field is set to 'CONTAINER'. The 'Classification Path' is also 'CONTAINER'. The 'Parent Classification' is empty. The 'Generate Description?' checkbox is checked. The 'Container Model' field is set to 'Container Model'. The 'Organization' field is empty. The 'Site' field is empty. The 'Use Classification?' checkbox is checked. Below the form, there's a 'Use With' section with a 'Filter' button and a 'Children' section with a 'Filter' button. The 'Attributes' section shows a table with columns: Attribute, Description, Section, Domain, and Data Type. The table has one row: 'A/C', 'Air Conditioning', 'Section', 'Domain', and 'ALN'. Below the table, there's a 'Details' section for the attribute 'A/C'. The 'Attribute' field is set to 'A/C'. The 'Data Type' field is set to 'ALN'. The 'Domain' field is empty. The 'Table Attribute' field is empty. The 'Lookup Name' field is empty. The 'Section' field is empty. The 'Unit of Measure' field is empty. The 'Description Prefix' field is empty. The 'Apply Down Hierarchy?' checkbox is unchecked. The 'Inherited from' field is empty.

Figure 3-6 Classification with new attribute

The system does not provide standard classifications. However, you can apply industry standards when you create classifications.

Tip: To simplify the implementation process, base your classification structure on how you currently group things in your business.

You must group information so that you can perform statistical analysis later. For example, to determine how many customers complained about problem A versus problem B, classify problem A differently than problem B.

The Classification application allows you specify the following details:

- ▶ **Using Classifications:** Users can search classification structures and attributes with associated values when they use any object that can be classified, such as assets, items, locations, configuration items, work orders, tickets, and so on.
- ▶ **Classification Structure/Hierarchy:** The structure consists of parent-child relationships between individual nodes and is also called the Classification

Hierarchy. You build a classification structure the same way that you build a directory structure: from the top down in parent-child relationships. First, you create a parent (a classification), and then you add its children (each child is also a classification), which belong to the parent. Each child then can become a parent and have its own children. This pattern can continue indefinitely. The structure from the top-level parent to the child that you are working with is the classification path.

For example, you create a classification called IT. Under it, you create two children - hardware and software - which belong to IT. Each child is a classification. IT is the parent of the children: hardware and software. Next, you create a child under hardware: printers. Hardware is now a parent of printers, with the following classification path:

IT\HARDWARE\PRINTERS

This path shows that printers belongs to hardware, and hardware belongs to IT.

- ▶ **Associates Classifications:** You can define associations between actual configuration item classifications and authorized configuration item classifications. Defining, or mapping, these associations lets you create an authorized configuration item from a configuration item record, and lets you include the limited number of attributes that you need for configuration management and change control.
- ▶ **Separate Classification Hierarchies:** You can add objects such as assets, locations, or items in the Use With area of the Classifications tab. By indicating the objects that can be used with the classification path, you can create one classification path that you can use with multiple objects, such as assets, locations, and items. For example, you can use one hierarchy to classify an asset, but a different hierarchy to classify the repair of that asset.
- ▶ **Attributes:** You can use attributes to search for objects that can be classified, such as assets, locations, items, tickets, work orders, solutions, configuration items, purchasing documents, and job plans (for example, you can search for a blue car). Each classification node contains a list of attribute characteristics of a classification object.
- ▶ **Sections:** You can break attributes into sections. Sections are groupings of attributes. This allows the same attribute to be used multiple times in a classification.
- ▶ **Other systems:** You can integrate classification with other applications in the system. You can create classifications for activities, assets, changes, incidents, items, locations, problems, releases, service requests, solutions, work orders, configuration items, purchasing documents, and job plans (for more details see 3.1, “Working with domains” on page 30).

To open the application, **GoTo** → **Administration** → **Classifications** and fill in the appropriate information.

3.7 Working with E-Mail Listener

The *E-mail Listeners application* is used to receive and process service requests and other types of tickets through e-mail in the form of e-mail messages. Using the E-mail Listener function, you can create or update tickets, and indicate whether the status is changed or queried based on specified criteria. The E-mail Listeners application can monitor multiple e-mail accounts to retrieve messages. The application supports embedded and normal message attachments.

Note: The E-mail Listeners application cannot process encrypted or digitally signed e-mail messages. Inform users of this limitation.

The E-mail Listeners application provides the following features:

- ▶ Free form and formatted e-mails

The E-mail Listeners application can process free form e-mail and formatted e-mail, and allows you to send and store attachments. Formatted e-mail can be composed using XML tags or text typed in the form of attribute-value pairs to perform specific actions, such as changing the status of a business object or querying the business object based on criteria.

Note: A built-in workflow process that supports various types of ticket objects is shipped with the application.

- ▶ Storing attachments

The E-mail Listeners application processes attachments to e-mail messages and stores the attachments as attached documents on the application server.

- ▶ Other features

- The E-mail listener Cron task: Used to encapsulates a staging process which processes inbound e-mail through a staging table.
- Workflow Process: Used to parse e-mail information from the staging table and process it according to the subject and content of each message.
- Security: The E-mail Listeners application enables users to create, update, query, and change the status of tickets, so it is critical to ensure that only authorized users can run these functions using e-mails. For the

sender of an e-mail, the application checks security authorizations against the system's security configuration. This check establishes the ability of the sender to run each specific function. More information on Tivoli process automation engine security configuration is provided in Chapter 5, "Security configuration" on page 75.

- Communication templates: The E-mail Listeners application uses numerous communication templates to generate notifications to end users and administrators.

To open the E-mail Listeners application, select **Go To → System Configuration → Platform Configuration → E-Mail Listener**.

Fill in the appropriate information, as shown in Figure 3-7.

Figure 3-7 E-mail Listener

You can customize the E-mail Listeners application to fit your needs. For detailed information about the E-mail Listeners application, refer to the *Maximo Online Help*.

3.8 Working with Cron tasks

Use the *Cron Task Setup* application to add Cron tasks, Cron task instances, remove Cron tasks or their instances, and to modify Cron task parameters. You can also change the **Active?** status or adjust the schedule of a Cron task. The Cron tasks can be rescheduled and parameter values can be changed without stopping and restarting the server. The server performs Cron tasks a specific

number of times, following a schedule, and without user interaction. Cron tasks are behind-the-scene jobs set to run automatically and on a fixed schedule. The system contains a set of default Cron tasks (for example, LDAP Sync), but you can also create custom Cron tasks to fit your business needs. Cron tasks include activities like generating preventive maintenance work orders (see Chapter 8, “Work management configuration and administration” on page 145) and reordering inventory items on a schedule.

To open the Cron Task Setup application, select **Go To → System Configuration → Platform Configuration → Cron Task Setup**.

Fill in the appropriate information. Figure 3-8 shows the entries for a Cron task used to synchronize LDAP data between Tivoli and the IBM Tivoli Directory Server.

The screenshot displays the 'Cron Task Setup' application interface. At the top, there are tabs for 'List' and 'Cron Task'. Below these, the 'Cron Task' section shows 'LDAPSYNC' with a description 'Synchronizes Users and Groups from Director'. The 'Class' is 'psdi.security.ldap.LdapSyncCronTask' and the 'Access Level' is 'FULL'. Below this, the 'Cron Task Instances' table lists one instance, 'LDAPSYNC01', with a schedule of '5m.*.*.*.*.*', running as 'MAXADMIN', and with checkboxes for 'Active?' and 'Keep History?'. The 'Max Number of History Records' is set to 1. Below the instances table, there are 'Parameters' and 'History' tabs. The 'Parameters' tab is active, showing a table of parameters for the task. The parameters table has columns for 'Parameter', 'Value', and 'Description'. The parameters listed are: 'Credential' (LDAP credentials), 'GroupMapping' (The GROUP XML used by the LDAP task), 'Host' (LDAP connection host), 'Port' (LDAP connection port), and 'Principal' (LDAP principal).

Parameter	Value	Description
Credential		LDAP credentials.
GroupMapping	<?xml version="1.0" encoding="UTF-8" ?><IDO	The GROUP XML used by the LDAP task.
Host	myldapserverhost	LDAP connection host.
Port	389	LDAP connection port.
Principal	cn=principaluser,dc=mydomain,dc=com	LDAP principal.

Figure 3-8 Cron Task Setup

A detailed discussion about the Cron task is in the *MAXIMO Administration Guide*, available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.mam.doc_7.1/pdf/mam71_sys_admin_guide.pdf

3.9 Working with communication templates

Communication templates are available in any application that has the *Create Communication action*. Use the templates to:

- ▶ Create and manage generic communication templates that users can use to standardize frequently used e-mail communications (notifications).

- ▶ Create e-mail notifications for use with workflow and escalation processes.
- ▶ Associate file attachments or document folders to templates, for example, to receive an e-mail triggered by a workflow including a pre-defined attachment.

When communications are sent, any attachments to the template are included in the communication, either in a folder or as an individual attachment. For your convenience this can be sent to Roles, Person, or even Person Groups.

Tip: To store and track e-mail, you can enable the **Com Log Entry?** to add the e-mails to the communication log of your requests.

To create a communication template, select **Go To → System Configuration → Platform Configuration → Communication Templates** and fill in the appropriate information.

Figure 3-9 shows an example of a communication template you can use to reply to a work order by sending back the work order number.

The screenshot displays the 'Communication Template' configuration window. At the top, there are tabs for 'List', 'Communication Template' (selected), 'Recipients', and 'Attachment Folders'. The main form contains the following fields:

- Template ***: CT_A_ANSWER
- Applies To ***: WORKORDER
- Accessible From ***: ALL
- Comm Log Entry?**: ☐
- Created By**: MAXADMIN
- Date**: 6/10/09 9:50 AM

Below these fields is a section titled 'Template Details' with the following fields:

- To**: [Empty text box]
- cc**: [Empty text box]
- bcc**: [Empty text box]
- Send From ***: WO Management
- Reply To**: Service Desk
- Subject**: Work Order :WONUM
- Message**: The Ticket Number is:
Work Order :WONUM

Figure 3-9 Communication Template example

For detailed information about maintaining Communication Templates, refer to the Maximo Online Help.

3.10 Working with escalations

This section provides an overview of the *Escalation application*.

An escalation is a mechanism to monitor records. It can take actions or send notifications when a record reaches a defined escalation point. Use the Escalations application to create, view, modify, and delete escalation records. You can create an escalation for any business object. Because all applications are associated with business objects, you can create escalations for any application and you can add any related notification to the escalation configuration. For additional information, refer to the *Maximo Administration Guide*.

You can use escalations with any application. However, you are most likely to use them with the Service Desk applications, IT Asset Management applications, and workflow processes, as shown in the following examples.

- ▶ **Service Desk Management** - Service level agreements (SLAs) are contracts defined between a service provider and the recipient of the services. You can use escalations to determine how incidents, problems, and service requests are handled, and work to ensure that you remain compliant with any SLAs by solving problems in a timely manner.
- ▶ **IT Asset Management** - You can use escalations to monitor IT contracts, procurement, and inventory. For instance, by defining an escalation to alert managers 30 days in advance of a lease contract expiring, the managers can effectively manage leases and avoid penalties or costly lease extensions.
- ▶ **Workflow processes** - You can use escalations to escalate assignments before they time out in a recipient's Inbox. When you assign specific steps in a workflow process to employees, those assignments display in their Inbox. If the assignments are not completed promptly, they time-out in the recipients' Inboxes. When this happens, you can use escalations to assign the tasks to other people. This helps tasks get completed on time and helps to prevent work backlogs.

Note: You can create escalations at the site, organization, or system level.

3.10.1 Maintaining the Escalation application

To support the daily requirements of your company you can configure the Escalation application with the following procedures:

To open the Escalation application, select **Go To → System Configuration → Platform Configuration → Escalation**.

To create an escalation, fill in the required data fields, as shown in Figure 3-10.

The screenshot displays the 'Escalation' configuration page in the Tivoli Process Automation Engine. It includes a top navigation bar with 'List', 'Escalation', and 'Communication Log' tabs. The main form contains several sections: 'Escalation' details (Name: MSTRCTREFF, Applies To: MASTERVIEW, Condition: STATUS=(select value from synonymdomain where domainid = 'CONTRACTSTATUS' and maxvalue = 'WSTART')), 'Active?' checkbox, 'Site', 'Organization' (LIT), 'Schedule' (24h * 0,*****), 'Create Successful Execution Entry?' checkbox, and 'Last Run Time'. Below this is a 'Validation Results' section. The 'Escalation Points' section features a table with columns 'Escalation Point', 'Elapsed Time Attribute', 'Elapsed Time Interval', and 'Interval Unit of Measure'. The table contains one row with '1' in the first column and 'STARTDATE' in the second. An 'Actions' section follows, with a 'Select Action Group or add individual actions by clicking New Row.' prompt and an 'Action Group' dropdown set to 'MSTRCTRGRP'. Below this is another table with columns 'Action', 'Description', 'Type', and 'Sequence'. It contains one row with 'MSTRCTRAPP', 'Master contract approve action', 'CHANGESTATUS', and '1'. A 'Notifications' tab is also visible at the top of the actions section.

Figure 3-10 Escalation application

3.10.2 Escalation components

An escalation record consists of the following elements:

- **Object (Applies To field):** You create escalation records for a specific business object. The escalation engine retrieves records from the business object that meet the escalation point criteria.

Tip: Select the object for which you are trying to use the Conditional SQL Expression® Builder.

- **SQL Statement (Condition field):** An escalation record can apply to all application records, or to a specific set of records. You can create an SQL statement that specifies records to which the escalation is applied. The conditions can apply to one or more tables associated with the object. Example 3-1 shows a valid statement about the history flag.

Example 3-1 SQL - Statement

```
historyflag=0 and ticketuid in (select ownerid from slarecords where
ownertable= 'TICKET' and slanum= '1009' )
```

- **Organization or Site:** Escalations are at the System level. You can create escalations for use with a specific organization or site.

- ▶ **Schedule:** A schedule that defines how often the system checks for records that meet the criteria for the escalation. The polling interval can be seconds, minutes, hours, days, weeks, or months. You also can specify that the interval be calendar- or date-based.
- ▶ **Escalation Point:** Date- and time-based, or other condition criteria for when the actions or notifications specified on the escalation record are triggered. An escalation record can have one or more escalation points.
- ▶ **Actions:** Any actions that must be taken when a record reaches the conditions of an escalation point. Actions are defined separately for each escalation point. You can associate multiple actions for each escalation point. Use the Actions application to define actions.
- ▶ **Notifications:** Any notifications that the system must generate when a record reaches the conditions of an escalation.

You can create escalations with the following items:

- ▶ Header attributes, which identify the set of records that the escalation monitors (the global search criteria)
- ▶ Escalation points, which define thresholds that must be met before an escalation occurs
- ▶ Actions, which are events you want to occur when the escalation points are reached
- ▶ Notifications, which are e-mail messages that are sent when the escalation points are reached

In addition, the system provides numerous pre-defined escalations that can be tailored to your needs. In addition, you can use the escalation in conjunction with *Workflow application* action (APPACTION). For example, you can use the Workflow Assignment (WFASSIGNMENT object) to reject (WFREJECT), accept (WFACCEPT), or escalate (WFESCALATE) a workflow process. For more information about the Escalation configuration, refer to the *Maximo Online Help*.

3.10.3 Working with escalation points

You can define multiple escalation points, and each one can be associated with one or more actions and notifications. Activating an escalation does not trigger an escalation process.

Typical escalation points include:

- ▶ Measuring elapsed time against an attribute (time period from now to an event in the past, which can be defined with a negative value), such as how many hours an assignment has been untouched in a person's inbox

- ▶ Measuring time until lapse (time period from now to an event in the future), such as how many days until a contract expires
- ▶ A standalone condition without a time measurement, such as using the system to automatically accept or reject an assignment in a workflow process

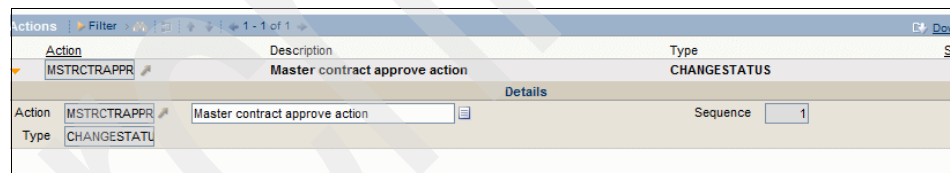
Note: The system triggers an escalation only when the escalation engine finds records that meet the criteria defined by the escalation points.

Actions and notifications

You can associate one or more actions or one or more notifications, or both, to an escalation point. You must associate at least one action or notification to an escalation before you can activate the escalation. You are not required to have both actions and notification.

Action

An action is an event you want the system to trigger when it finds records that meet the conditions defined by the escalation point, such as changing a status or an owner. When you add an action, you can select a preexisting action and assign it a sequence number (if multiples). The system defaults the description and the action type, which is based upon the record and action you chose. An example is shown in Figure 3-11. You can also go to the *Actions application* to create a new action and return it for use with your current escalation.



Action	Description	Type	Sequence
MSTRCTRAPP	Master contract approve action	CHANGESTATUS	1

Details

Action: MSTRCTRAPP
 Type: CHANGESTATUS
 Sequence: 1

Figure 3-11 Action

The system ships with a number of predefined action types, such as Set Owner, Status Change, or Create Ticket. You can create additional action types as needed.

Action groups are predefined sets of actions that are grouped together in a specific sequence. The system associates an escalation point with one or more actions through the action group. For detailed information, refer to *MAXIMO Online Help*.

Notification

A notification is an e-mail you want the system to send when it finds records that meet the conditions defined by the escalation point. Figure 3-12 shows an example of how you can configure the notification.

Template	Role/Recipient	Subject
MSTRCTREFF	PURCHAGNTM	Contract :CONTRACTNUM is now effective

Details

Template: MSTRCTREFF

Role/Recipient: PURCHAGNTM

Subject: Contract :CONTRACTNUM is now effective

Message: The effective date of contract :CONTRACTNUM has been reached and the status has been changed from W5

New Role

Figure 3-12 Notification

You can create two types of notification:

- ▶ Free-form notification: Free-form notifications require you to define only a role/recipient, subject, and message.
- ▶ Template-based notification: You can pre-define several “communications templates” (see “Working with communication templates” on page 43) to send the needed information using the Escalation application.

Tip: You can use the Roles record **Broadcast?** field to send out a notification to all people in a person group.

Deleting escalation rules

After you deactivate an escalation, you can delete the escalation point. If you do delete an escalation point, the system also deletes the links to the actions and notifications associated with the escalation point. The system will not delete the actions and notifications themselves. You must have at least one escalation point in an escalation. If you delete all escalations points, you cannot activate the escalation.

You can delete an action or notification associated with an escalation point without affecting other actions and notifications tied to it.

Validate escalation

When the system validates an escalation, it is only validating the SQL statement within the Condition field and the escalation points defined for the escalation. Validating the escalation points ensures that when the criteria that defines the escalation point is met, the escalation mechanism triggers the associated actions

and notifications. The system does not validate the actions or notifications themselves.

If there is an error in either the SQL statements in the escalation header's Condition field or in the SQL statements in the Escalation Point Condition field within an escalation point, you must expand the Validation Results table window to see information about the specific errors. If you have more than one escalation point and the validation fails, the system indicates which escalation point produced the errors by highlighting the row in red.

The validation is started by selecting **Validate** from the **Select Action** menu.

Escalation schedule

An Escalation must be scheduled to give the right notification at the right time. From the **Set Schedule** dialog box, you can choose a date or time interval (or both) and preview the first twenty occurrences of the schedule. The schedule filed in the escalation record is the schedule by which the escalation will poll for conditions. For example, depending on the available fields, a schedule can be as simple as “every 5 minutes” or as complex as “the fourth Monday of the month at 9:30 PM, every month.”

3.11 Working with Workflow Designer

Use the *Workflow Designer application* to create, view, modify, and delete Workflow process records that reflect your business processes. An active Workflow process revision defines the different paths that a record can take as it moves through the business process. The process also defines the actions and notifications that should take place at various points in the process.

To open the Workflow Designer application, select **Go To → System Configuration → Platform Configuration → Workflow Designer**.

The Workflow Designer application includes three tabs: List, Canvas, and Process. They are used as follows:

- ▶ **List:** Used to search for processes.
- ▶ **Canvas:** Provides the tools and work space to create, view, and modify Workflow processes. The Workflow canvas is a graphical view of a Workflow process. It lets you see the process elements and how they are connected, as shown in Figure 3-13 on page 51. You use the canvas to add nodes and connection lines as you construct a process and configure the properties of each process element.

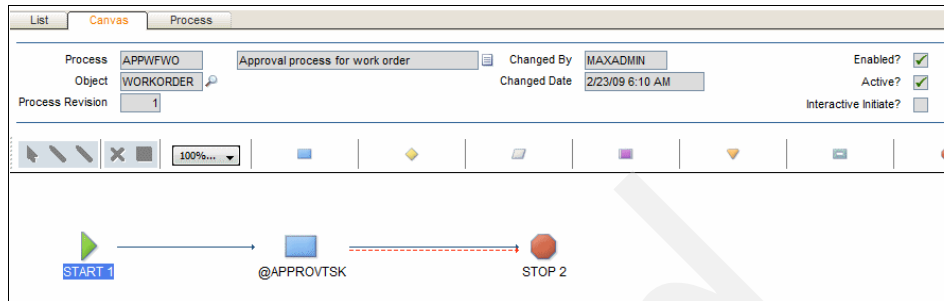


Figure 3-13 Workflow Designer - Canvas

The Canvas Tab consists of the following sections:

- Record header
- Workflow tool palette
- Workflow canvas

For details about the Workflow tool palette refer to:

http://publib.boulder.ibm.com/tividd/td/ITMax/621_mx_wkfl_imp/en_US/PDF/621_mx_wkfl_imp.pdf

- **Process:** While the Canvas tab provides a graphical view of the elements in a process, the Process tab presents the process elements in a pair of table windows. The *Process Nodes* table window displays all nodes in the process. Each row includes the node Title, Description, and Type. The row that you select in the Process Nodes table window determines the data that the system displays in the Actions table window. The *Actions* table window displays any actions associated with the connection lines exiting the selected node. Each row includes the name of the action record, the instructions to the assignee, the node to which the connection line leads, and whether the connection is positive or negative. You can click the **Edit Properties** button for any node or action to access the Properties dialog box for the node or connection line.

Process nodes

A node is a graphical element that represents a point in your business process. Workflow Designer includes different types of nodes that can represent different points in your business process, for example:

- The entry of a record into the process
- Decision points
- Points when a path branches
- Manual input from an individual or group
- Navigation of the user to a user interface element of an application

- Automated actions
- Record exit from the process

You can drag and drop nodes from the palette onto the canvas. You can add any number of nodes to a process. However, if a process exceeds 50 to 100 nodes, you might want to consider whether you can break the process down into subprocesses to simplify managing and maintaining it.

The types of process nodes are defined in the following subsections.

Start nodes

A *Start node* indicates the point when a record enters or starts a Workflow process. The tool palette does not include a Start Node tool because when you create a new process, Tivoli process automation engine places a single Start node on the canvas. Each process can have only one Start node, and you cannot delete Start nodes.

Task nodes

A *Task node* indicates when a user has two choices, for example, to approve or reject a record. Use Task nodes when your business process requires a user to evaluate the record and you want to create a task assignment that routes the record to one or more individuals. When Tivoli process automation engine encounters a Task node while routing a record through the process, it stops the process and generates one or more task assignments, based on the node properties. Individuals can receive task assignments via the Workflow Inbox portlet on their Start Center, or via e-mail. The assignee views and completes the assignment in the Complete Workflow Assignment dialog box. Use the Task node tool in the palette to place a new Task node on the canvas. A process can have one or more Task nodes, but you do not have to include Task nodes in a process.

For example, a client has a workflow requirement on new asset records. Part of this requirement is that the Contracts representatives from the Lease and Warranty groups review and validate contracts the asset may or may not be under. The asset record cannot move to the next part of the workflow process until all assignments are completed.

You can configure this request by using a Task node and assigning it to the Leasing and Warranty roles. Configure the task to indicate that the Perform Acceptance Action is to be used when all assignments are accepted. Configure the Positive connection line coming from this Task node to indicate an instruction that Leasing and Warranty Contracts have been reviewed and this asset is under a contract. Configure the Negative connection line from this Task node to indicate that Leasing and Warranty Contracts have been reviewed and this asset is not under a contract.

Condition node

A *Condition node* indicates an evaluation of the record, based on data in the record. Use a Condition node to have Tivoli process automation engine make a true/false evaluation of the record, then direct the record based on that evaluation. When Tivoli process automation engine encounters a Condition node, it evaluates the record based on the SQL statement defined in the node properties, then routes the record to either the positive or negative connection line exiting the node. Use the Condition node tool in the palette to place a new Condition node on the canvas. A process can have one or more Condition nodes, but Condition nodes are not required in a process.

Manual Input nodes

A *Manual Input node* indicates a need for user input because there are multiple directions that a record can take in a process. Use a Manual Input node to have a person decide what should happen next. When Tivoli process automation engine encounters a Manual Input node, it displays a dialog box to the user. The Manual Input dialog box contains a menu of options for routing the record. When the assignee selects an option, Tivoli process automation engine triggers any actions or notifications associated with the option. Use the Manual Input node tool in the palette to place a new Manual Input node on the canvas. A process can have one or more Manual Input nodes, but Manual Input nodes are not required in a process.

Subprocess nodes

A *Subprocess node* indicates that a separate Workflow process is contained within a Workflow process. Use a Subprocess node to break a complicated business process down into smaller, self-contained units. For example, you might use different subprocesses for different categories of records, such as records from different Sites, or different classes of work orders. When Tivoli process automation engine encounters a Subprocess node while routing a record through a process, it routes the record into the subprocess. When the record encounters a Stop node within the subprocess, Tivoli process automation engine returns it to the main process at the same point where it left the process. Use the Subprocess node tool to place a new Subprocess node on the canvas. A process can have one or more Subprocess nodes, but Subprocesses nodes are not required in a process. A Workflow can have one or more Subprocess nodes based on the complexity of your business process and how you choose to design the process.

Wait nodes

A *Wait node* indicates that a record's progress through a process should pause until a required condition is met. Use a Wait node, for example, to create a reaction to a database event, such as a status change or a record being updated. You might use a Wait node when Tivoli process automation engine is integrated

with another system, such as an external financial system, and must exchange data with that system. When Tivoli process automation engine encounters a Wait node it pauses at the node indefinitely, until any event specified in the node properties occurs. At that point, the record resumes its progress through the process, and Tivoli process automation engine triggers any actions or notifications specified on the properties of the connection line exiting the node. Use the Wait node tool in the palette to place a new Wait node on the canvas. A process can have one or more Wait nodes, but you do not have to include Wait nodes in a process. A Wait node cannot precede a node that requires user interaction (Interaction node or Manual Input node).

Consider this example of using the Wait node: Part of a client's workflow requirement is that an asset record in a workflow process should not move to the next part in the workflow until the field **Is running?** on the asset record is updated. You can accomplish this by using a Wait node. Configure the Wait node event to: `maximo.asset.update`. After the Wait node, use a Condition node to compare the old and new values of the **Is running?** field.

Interaction nodes

An *Interaction node* provides one option for a user interaction with a record. Use Interaction nodes with Manual Input nodes to guide a user through a structured interaction with a record.

When an Interaction node is encountered while routing a record through a process, the result depends on how the node is configured. You can configure an Interaction node in the following ways:

- ▶ Specify that the record be displayed in the specified application.
- ▶ Specify that a certain application tab display.
- ▶ Specify that an action is triggered from the application's toolbar or Select Action menu.
- ▶ Specify that a process is triggered. For example, trigger another workflow process.

In addition, a message dialog box can display, containing instructions to the user. For example, if a user has forgotten to fill in a field required for subsequent processing, a message dialog box can be displayed.

You can use the Interaction Node tool in the palette to place a new Interaction node on the canvas. A process can have one or more Interaction nodes, but you do not have to include Interaction nodes in a process. A Manual Input node usually precedes an Interaction node. If an Interaction node leads to an application not related to the object specified on the process record, a Stop node should follow the Interaction node.

Stop nodes

A *Stop node* marks the end of a Workflow process, that is, the point where a record leaves control of the process. When you create a new process, Tivoli process automation engine places a single Stop node on the canvas. You can place additional Stop nodes on the canvas by using the Stop node tool in the palette. Use a Stop node to have a record exit the process. If you are creating a subprocess, use a Stop node when you want the record to return to the main process. When Tivoli process automation engine encounters a Stop node while routing a record through the process, the record exits the process. Each process must have at least one Stop node; a process can have multiple Stop nodes.

Connection lines

Every node in a process must be connected to at least one other node, and all nodes except Start and Stop nodes must be connected to two other nodes. You can draw two types of connections between nodes:

Positive connections

Use the Connect nodes tool to draw a positive line between nodes. A solid black line on the canvas represents a positive connection. A positive connection indicates a positive outcome, for example, that an action was performed, a record was approved, or that a record meets the condition specified by the node.

Negative connections

Use the Negative connection tool to draw a negative line between nodes. A dashed red line on the canvas represents a negative connection. A negative connection indicates a negative outcome, for example, that a record was cancelled, a record was rejected, or a record does not meet the condition specified by the node.

Note: Connection lines can cause an action to be performed. It can also notify (e-mail) someone.

For a detailed discussion about the different properties and connection lines for each node in the Workflow Designer, refer to *Maximo online help* or to:

http://publib.boulder.ibm.com/tividd/td/ITMax/621_mx_wkfl_imp/en_US/PDF/621_mx_wkfl_imp.pdf

3.11.1 Creating workflows

You create a workflow process by inserting nodes and connection lines on a Workflow canvas. Each Workflow process includes start and stop nodes. Start and stop nodes do not carry user-defined information. The other nodes carry

user-defined actions. Use the Workflow Designer tools to place, connect, and configure the nodes and lines.

For example, consider that your business requires the blocking of status changes when a work order record is in workflow, unlocking at a certain point to perform a status change to APPR, and then relocking when the status change occurs. To configure this example in the Workflow Designer, implement the following steps:

1. In the Actions application, create an Action Group for the work order object with the following members in the following order: OKSTATUS, Work Order Approval action, NOSTATUS.
2. On the workflow connector line where the status block is to begin use a NOSTATUS action.
3. To unlock the status change block prior to the next status change, on a connector line use the Action Group.
4. Each node except the Start node must have at least one line entering it.
5. Each node except a Stop node must have at least one line exiting it.

You should configure more examples to become completely familiar with the Workflow Designer. Detailed documentation about creating Workflows is found in the *IBM Maximo Workflow Implementation Guide*. Refer to:

http://publib.boulder.ibm.com/tividd/td/ITMax/621_mx_wkfl_imp/en_US/PDF/621_mx_wkfl_imp.pdf

3.12 Workflow Administration application

In addition to the Workflow Designer, you use the *Workflow Administration* application to view and manage active instances of Workflow processes. The Workflow Administration application contains a single table window, which contains a row for each active instance of workflow (Figure 3-14). A single record can show up multiple times if it is controlled by multiple workflow instances. You can see which version of a revised process was used to create each instance, the person ID of the individual who routed each record into Workflow, and the date and time that the process was initiated. The *recordkey* (for example, work order number or PO number) is displayed with the Site ID in the Owner Description field.

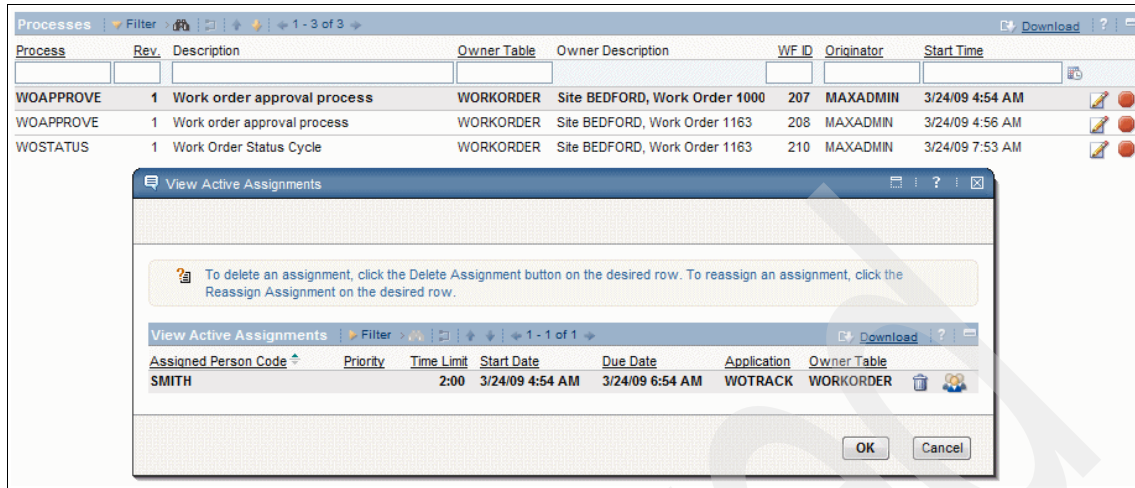


Figure 3-14 Workflow Administration

You use the Processes table window to view, modify, and stop active process instances. When a record leaves the control of Workflow, the system removes the entry from the Processes table window. You can use the Workflow Administration application to perform the following tasks:

- ▶ View Workflow assignments
- ▶ Reassign Workflow assignments
- ▶ Delete Workflow assignments
- ▶ Stop active processes, removing the record from the control of the processes

3.12.1 Conditional Expression Manager

Use the *Conditional Expression Manager* application to create and maintain a library of conditions. These conditions can contain expressions and class files. These files will be stored in the directory structure, and must be in a folder under the root of the product installation. In other applications, such as Application Designer and Security Groups, you select from predefined conditions to set up conditional behavior. The Conditional Expression Manager belongs to the Administration Section, but effectively belongs to the overall platform configuration.

To open the Conditional Expression Manager application, select **Go To → Administration → Conditional Expression Manager**.

You can add new conditions by adding **New Row** and filling in the appropriate information. The Conditional Expression Manager application contains one table

window only, which displays the list of conditions. Use the table window to add, view, modify, or delete conditions.

When the expression evaluates to true, conditions let you configure access to fields, tabs, and other user interface controls within applications. For example, you can set the following types of conditional access:

- ▶ Give read-only access to information displayed in a field.
- ▶ Give read-write access to information displayed in a field.
- ▶ Give a user group read-only access to a specific field or action in an application.
- ▶ Give all members of a user group read-write access to a specific application.
- ▶ Do not display a field or tab in an application to certain users.

You can also set access to application options, controls, or data elements. Examples include:

- ▶ Grant access to application options in the Select Action menu for a security group.
- ▶ Configure any property in a control for a group, such as making a control hidden, masked, read-only, or required.
- ▶ Configure other properties, such as color, label, and application link, to differ according to group and different conditions.
- ▶ Show or hide a data attribute globally or for a security group.

The system uses a syntax like Structured Query Language (SQL). However, the syntax of this system uses additional variables. For easier evaluation of your expression, you can use the Conditional Expression Manager Builder.

3.12.2 Conditional Expression Manager Builder

The expression syntax of this system uses a colon (:) to define a variable. The system uses this syntax to avoid ambiguity when you create expressions that relate to the current record (business object) or to a specific record. For example, you can have subselect in the expression, such as:

```
exists (select 1 from workorder where wonum=:wonum)
```

The first *wonum* is the *wonum attribute* on the workorder object. At run time, the system replaces the second *wonum* with the value of the “wonum” attribute for the current business object.

Detailed information about the Syntax is provided in *Maximo online help*.

Figure 3-15 on page 59 shows the options of the Conditional Expression Manager and the validation results.

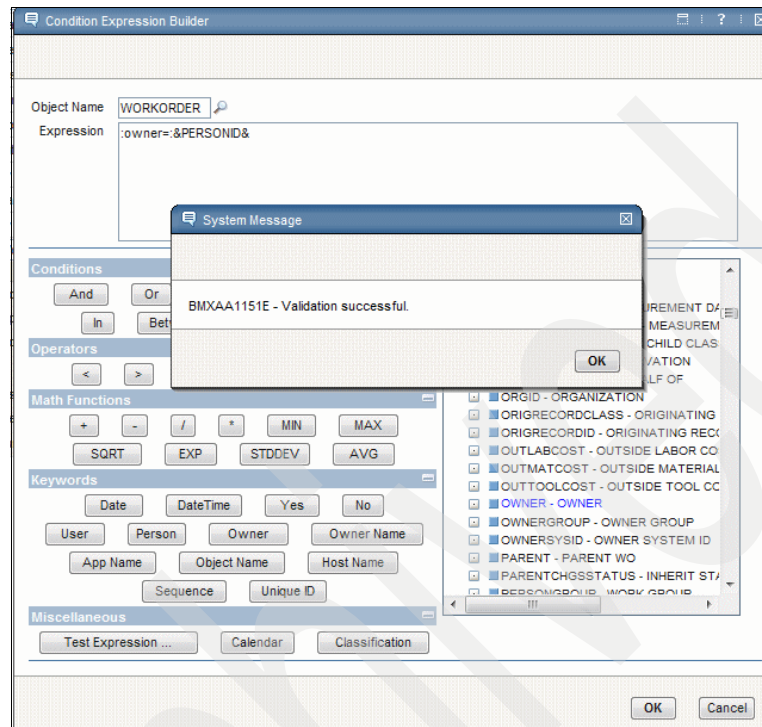


Figure 3-15 Conditional Expression Manager

Expressions that are not correct will not be validated and an error message will be shown.

Use the Condition Expression Manager and test the following expression using the **WORKORDER** object:

&owner&.jobplan.priority>&owner&.priority.

The result is the error message shown in Figure 3-16.

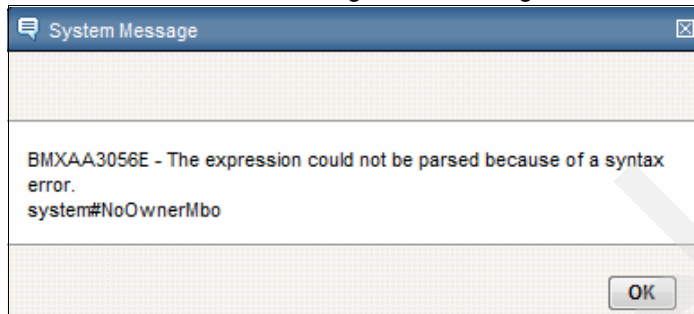


Figure 3-16 Error Message (Conditional Expression Manager)

3.13 Platform Configuration summary

This section uses simple bullet lists to summarize the options available to customize and configure the applications that are part of the Platform Configuration module.

To open the various applications within the Platform Configuration module, select **Go To → System Configuration → Platform Configuration**, as shown in Figure 3-17.

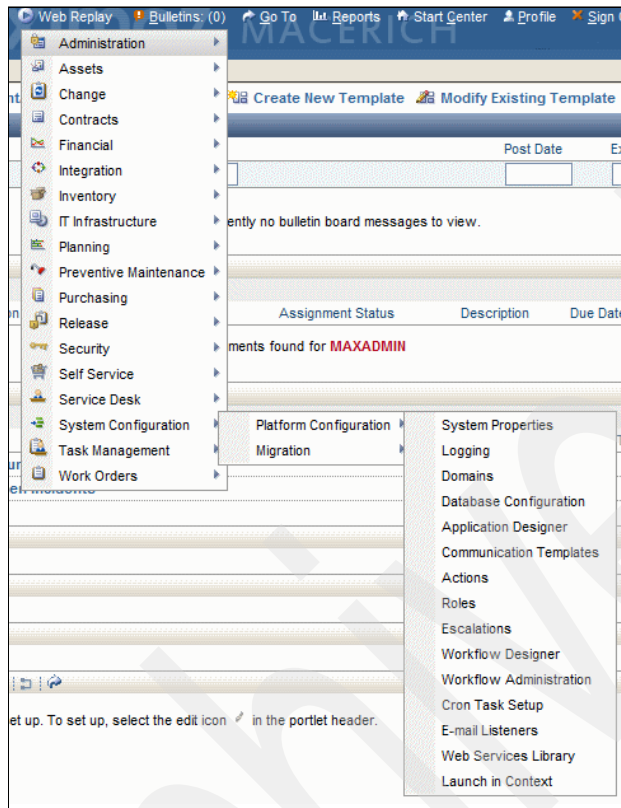


Figure 3-17 Platform Configuration Options

Platform Configuration

- ▶ **Actions**
Manage the administrative functions of creating actions and action groups within escalations.
- ▶ **Roles**
Manage roles within Tivoli Maximo Asset Management.
- ▶ **Communication templates**
 - Create and manage generic communication templates that users can leverage to standardize.
 - Frequently used e-mail communications (also known as notifications)
- ▶ **Database Configuration**
Create or modify the objects and attributes used by Tivoli Maximo Asset Management applications.

- ▶ **Application Designer**
Create new applications (clones and custom applications) or tailor the pages of existing applications.
- ▶ **Escalations**
Automatically monitor critical processes across your enterprise. The primary goal of Escalation Management is to ensure that critical tasks, such as those defined in service-level agreements (SLAs), are completed on time.
- ▶ **Cron Task Setup**
Cron tasks are behind-the-scene jobs set to run automatically and on a fixed schedule.
- ▶ **Domains**
Maintain lists of defined values that appear in drop-down lists (sometimes referred to as value lists).
- ▶ **Logging**
Manage log settings and configure log files.
- ▶ **System Properties**
Manage system properties and their values used by various product components.
- ▶ **Web Services**
Create, modify, and delete Web services. You also can generate schema and Web Service Description Language (WSDL) files for any Web service that you deploy. External applications can use Web services to query or to send transactions to the Integration Framework.
- ▶ **Workflow Administrator**
View and modify assignments within the workflow, escalation, and service-level agreement processes.
- ▶ **Workflow Designer**
Use this graphical application to create a series of decision paths for records to flow through, called workflow process.
- ▶ **E-mail Listener**
Receive and process incoming e-mail messages. This application can monitor multiple e-mail accounts to retrieve messages, and it supports embedded and normal message attachments.
- ▶ **Launch in Context**
Create and manage launch entries that open, in the same or a different browser session, an application that is external to the system.
- ▶ **Object Structures**
Create, view, modify, and manage the processing logic of an object structure. An object structure is the common data layer that the Integration Framework uses for all outbound and inbound application data processing. An object

structure consists of one or more sub-records that develops their XML content from a particular object.

In addition to the platform configuration, you will find the migration part under the System Configuration. To open the Migration application, select **Go To** → **System Configuration** → **Migration**, as shown in Figure 3-18.

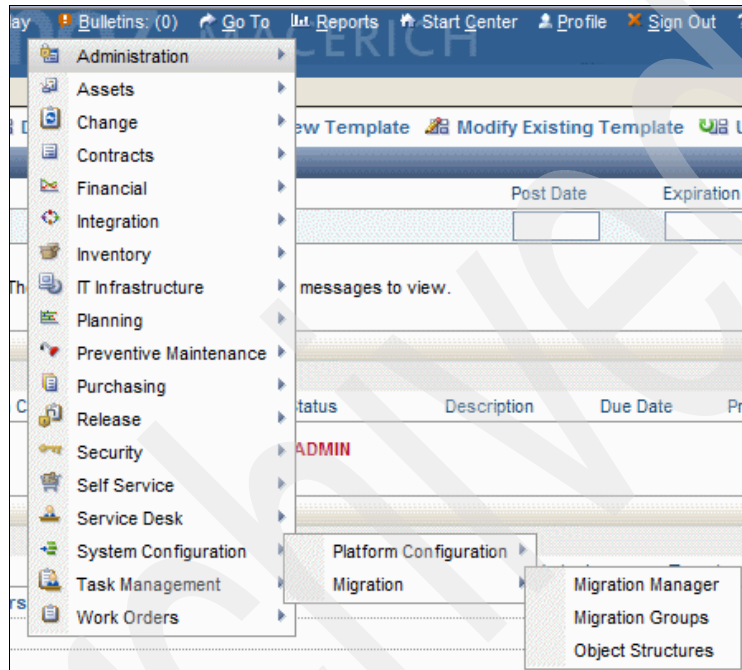


Figure 3-18 Migration Application

- ▶ **Migration Manager**
Define, create, distribute, and deploy packages. Packages are used to transfer and deploy the many configuration changes possible with the Tivoli Maximo Asset Management configuration tool set from one environment to another (that is, from a development environment, to a test environment, to a production environment).
- ▶ **Migration Groups**
Create groups of configuration objects and link related (dependent) groups to the objects that you create. You group configuration objects to ensure that all related configuration data is collected from source environments and distributed to target environments.

Financial configuration

This chapter introduces Financial configuration and its applications, such as Chart of Accounts, Currency Codes, Exchange Rates, and Cost Management.

The following topics are covered in this chapter:

- ▶ Introduction to Financial configuration
- ▶ Currency codes
- ▶ Exchange rates
- ▶ Chart of accounts
- ▶ Cost management

4.1 Introduction to Financial configuration

All *Financial Configuration applications* can be accessed using the Go To menu from the Start Center screen, as shown in Figure 4-1.

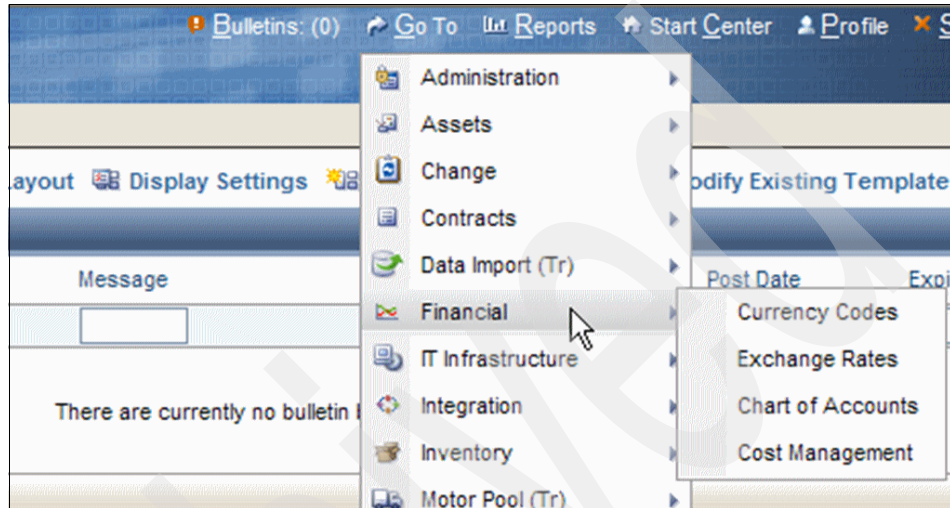


Figure 4-1 Financial Configuration

In this chapter, we will cover the functionality of the Financial configuration applications.

4.2 Currency codes

The *Currency Codes application* is responsible for creating and maintaining the list of possible currencies that are used in Maximo. To launch this application, click **Go To** → **Financial** → **Currency Codes**.

The Currency Codes application is accessed through the List Tab plus the **Select Action** menu. To create a new currency, just click the **New Row** button, as shown in Figure 4-2 on page 67, and fill in the following fields:

- ▶ **Currency:** The currency name, like USD for US Dollar.
- ▶ **Description:** The currency name, like US Dollar.
- ▶ **Active?:** This checkbox will make the currency active to be used for other applications.

Once you have created all the required currency codes, these codes will be available for use in all applications.

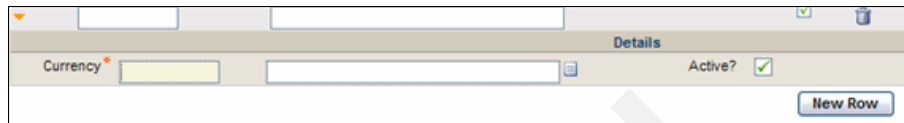
The image shows a software interface for creating a currency code. It features a 'Details' header, a 'Currency' input field with a red asterisk, an 'Active?' checkbox that is checked, and a 'New Row' button at the bottom right.

Figure 4-2 Creating a currency code

The currency codes are considered at the System level. This means that you can use the same currency code through different organizations, so you do not need to create a set of currency codes for each organization. This is important because the Currency Codes application is a very simple application, but it is the basis for all other financial applications.

Note: To use the Currency Code and any other Financial Configuration applications, you must have Organizations already configured.

4.3 Exchange rates

The *Exchange Rates application* is used to set up exchange rates to convert currencies. It is mostly used when dealing with different country sites and different currencies.

To use the Exchange Rates application, select **Go To → Financial → Exchange Rates**.

The application will show all valid Organizations, as shown in Figure 4-3 on page 68, and all already existing exchange rates. To create a new exchange rate, simply click the **New Row** button.

Exchange Rates

Select Action [v] [icon] [icon]

Organizations Filter [icon] [icon] [icon] 1 - 5 of 9

Organization	Description
GDCBVT2	
EAGLENA	EAGLE Inc. North America
EAGLESA	Eagle South America, Inc.
EAGLEUK	European Headquarters of Eagle, Inc.
ISTR1	

Exchange Rates for EAGLENA Filter [icon] [icon] [icon] 1 - 10 of 38

Convert from Currency	Convert to Currency
AUD [icon]	USD [icon]
AUD [icon]	USD [icon]
BOLIVAR [icon]	USD [icon]
BOLIVAR [icon]	USD [icon]
BOLIVAR [icon]	USD [icon]

Figure 4-3 Exchange Rates main screen

A Detail section is displayed, in which you can create the required exchange rate. Make the appropriate entries in the following fields:

- ▶ **Convert from Currency:** Type here the currency that must be converted, for example, EUR for Euros.
- ▶ **Convert to Currency:** Type here the currency to which you want to convert, for example USD, if you want to convert Euros to US Dollars.
- ▶ **Exchange Rate:** Specify the conversion rate between the two currencies.
- ▶ **Active Date:** Specify the date when this exchange rate was activated.
- ▶ **Expiration Date:** Specify the last date that this exchange rate can be used by the system.
- ▶ **Memo:** Use this field as needed for administrator's notes regarding this operation.

Since the Exchange Rates application is an organization-level application, you must create separate exchange rates for each organization that will need to use this function. They can share the same currency, but the exchange rate value can be different for each organization.

4.4 Chart of accounts

The *Chart of Account application* has two main sub-applications: General Ledger Account (also known as the GL Account) and Financial Periods. The General Ledger Account is responsible for accounting in the organization. The Financial Periods sub-application defines, from the financial point-of-view, when the fiscal year begins and ends.

Note: The Chart of Account application is very important because the GL Account is used for all other applications, so you need to plan very well how to implement a good set of GL accounting components to avoid major changes in the future.

4.4.1 General Ledger Account (GL Account)

The GL Account is used by all other financial applications. You can use Chart of Accounts to perform the following actions:

- ▶ Create GL (General Ledger) account codes and components
- ▶ Define Financial Periods
- ▶ Create default GL Accounts

You first need to specify the format of the account codes that will use the GL Account, then go to **Configuration** action in the *Database Configuration application* to configure the GL Account. The GL Account format includes the number and length of components and delimiters.

You define tax codes, rates, and dates using **Purchasing Options → Tax Options** in the *Organizations application*.

General Ledger account codes typically include components (segments) separated by delimiters, for example, 6210-300-000

To start using the GL Account application and Chart of Accounts:

1. From the **Go To** menu select **System Configuration → Platform Configuration → Database configuration**.
2. In the Database Configuration application, click **Select Action → GL Account Configuration** as shown in Figure 4-4 on page 70.

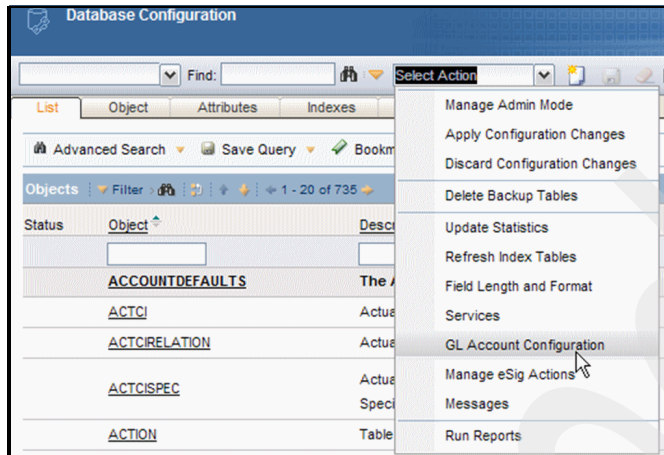


Figure 4-4 Setting up GL Account Configuration.

3. This option will allow you to create the main configuration of the GL Account. In this example we are using the format *NNNN-NNN-NNN*, with the segments related to a structure like *WORKTYPE-OBJECTTYPE-OBJECT*, but we could change this structure, as shown in Figure 4-5.

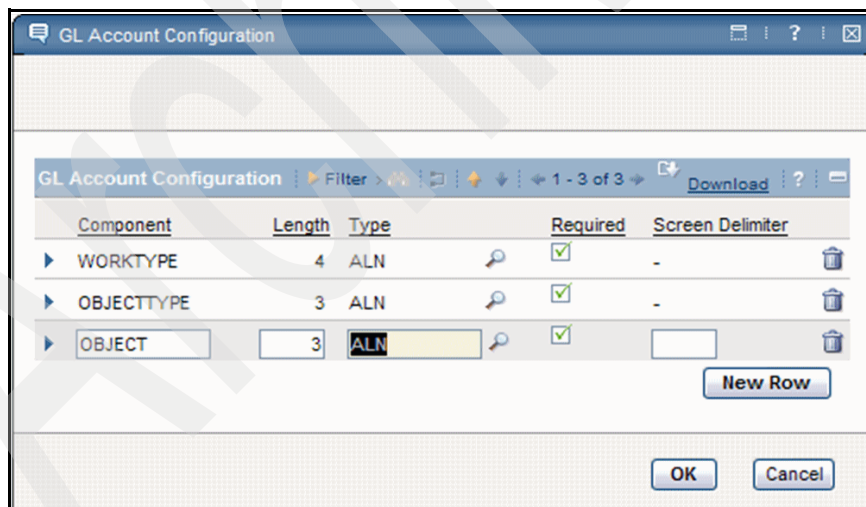


Figure 4-5 GL Account Configuration

4. Once you have specified the fields, Length, Type, and the Screen Delimiter for each of the components (Worktype, Objecttype, and Object), move to the

Organizations application and set the *Clearing Account* by clicking the **Select Value** button, as shown in Figure 4-6.

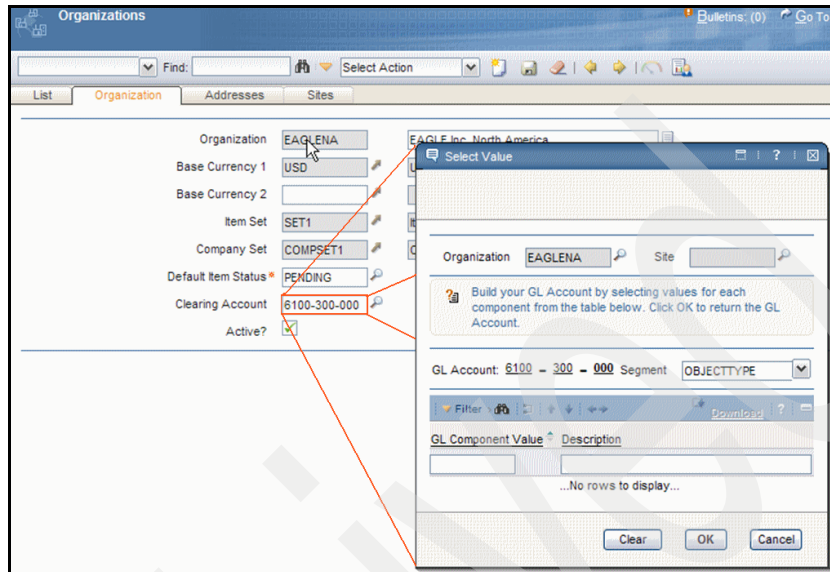


Figure 4-6 Adding a GL Account into an Organization

Important: GL Accounting is defined at the Organization level and shared by the children sites and its location (address). It is good practice to create another organization when you need to specify different sets of GL Accounts, for example, for each site or location.

4.4.2 Financial Periods

Financial Periods is the application that deals with the business year from an accounting point of view. In this application, you specify when the fiscal year is planned to start and end.

You must define at least one financial period. The system adds a financial period stamp to all transactions when you generate them. The transactions must occur during an open, valid financial period. The requirements of the accounting system you use determine the format of the period.

To specify a valid financial period, select **Go To** → **Financial** → **Chart of Accounts** → **Select Action** → **Financial Periods**.

Create financial periods by providing the following information:

- ▶ **Period:** The name of the financial period that you are creating. Specify something useful and meaningful to you.
- ▶ **From:** The date when your financial period begins.
- ▶ **To:** The end date for the financial period.
- ▶ **Accounting Close Date:** The planned date to close the financial period.
- ▶ **Actual Close Date:** The real date when the financial period was closed.
- ▶ **Closed by:** The user name of the person who actually closed the financial period, as shown in Figure 4-7.

Organization: EAGLEUK European Headquarters of Eagle, Inc.

Financial Periods: 1 - 8 of 36

Period	From	To	Accounting Close Date	Actual Close Date	Closed By
200612	02/12/06 00:00	02/01/07 00:00			
200611	02/11/06 01:00	02/12/06 00:00			
200610	02/10/06 00:00	02/11/06 01:00			
200609	02/09/06 00:00	02/10/06 00:00			
200608	02/08/06 00:00	02/09/06 00:00			
200607	02/07/06 00:00	02/08/06 00:00			
200606	02/06/06 00:00	02/07/06 00:00			
200605	02/05/06 00:00	02/06/06 00:00			

Details

Period: 200612

From: 02/12/06 00:00

To: 02/01/07 00:00

Accounting Close Date:

Actual Close Date:

Closed By:

New Row

OK Cancel

Figure 4-7 Financial Period main screen

4.5 Cost management

Cost Management is the application that manages and generates project cost information, tracks financial resources that are required to complete a project, and manages budgets more effectively.

To access the Cost Management application, select **Go To** → **Financial** → **Cost Management**.

The application is displayed in its List Tab. The main fields are as shown in Figure 4-8.

Task	Description	Type	Budget	Budget Line	Parent Task	Value
...No rows to display...						

Figure 4-8 Main fields of the Cost Management. application

The most important fields are **Project**, **Budget**, **Value**, and **Parent Project**. These fields are used to specify enough information to track a project's budget effectively and keep track of the cost of each required task.

To create a relationship between a task and the budget's cost, you need to create a separate cost line per each task by clicking **New Row**, as shown in Figure 4-9.

Task	Description	Type	Budget	Budget Line	Parent Task	Value
...No rows to display...						

Figure 4-9 Cost Line per each Task

The application itself is quite small, but very important, when you have to specify the line items and costs by project. This information can be used internally for integration with other applications.

Security configuration

Security configuration is used to define the access level for Users and Groups. It is important to plan your security strategy carefully before you implement the security configuration. This chapter will guide you through the needed steps.

The Security system is used for:

- ▶ Authentication - to validate the users credentials against the system
- ▶ Access - to give access to various resources based on the identity of the user

The *Security Groups application* defines all groups and their privileges.

This chapter has the following sections:

- ▶ Security profiles
- ▶ Setting up security users
- ▶ Setting up authentication
- ▶ Conditional security overview

5.1 Security profiles

The *Security Group application* works together with the *Users application*. While the Security Group defines the authorization, the users inherit the authorizations of the groups to which they belong, thereby creating their security profile.

A user's security privileges control the user's access to modules, applications, menu options, and data. All security access is based on security groups. A user name is associated with one or more security groups, and can have different levels of access to the applications and actions.

The Security Groups application is the building block for the security infrastructure. You configure security groups, either independent or non-independent, to provide narrow access or broad access to applications, sites, labor, and other settings, such as general ledger components and approval limits and tolerances.

The security group to which a user belongs controls the user's level of access and privileges within the system. The system generates a user's security profile from all the groups in which the user is a member, using business rules to determine how the various security groups combine to build a virtual security profile. The security profile is like a fingerprint. It uniquely defines a user's access rights and privileges.

5.1.1 Security Groups application

Security privileges are set up by group. You use the *Security Groups application* to create groups, then you specify group privileges and restrictions for applications and options, as well as other settings.

- ▶ You assign users to groups in the Security Groups application.
- ▶ You assign groups to users in the Users application.

The combination of groups to which a user belongs determines an individual user's security privileges. You can view a user's security privileges graphically on the Security Profile tab in the Users application.

When you first implement the system, the Security Groups application has four groups:

- ▶ DEFLTREG - Allows a user to change his or her password if it expires. It contains no other rights. When you insert a new Users record, the system places the user in this default group, though you can specify a different group to be the default using the Security Controls dialog box.

- ▶ **MAXADMIN** - Provides enough access to the system to add users and groups.
- ▶ **MAXREG** - A group that allows users to self register. You can use MAXREG to initiate a workflow process by which the system alerts an administrator to assign new users to the appropriate security groups.
- ▶ **EVERYONE** - Used for global settings that apply to all users in the system.

You must create additional groups, with different sets of rights, to be able to assign users different sets of privileges.

If you want new user security profiles to start with more rights, you can modify the DEFLTREG group to include them.

Note: Using LDAP (Lightweight Directory Access Protocol) with the system entails special consideration. Consult the *System Administrator's Guide* (<http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itmaxam.doc/welcome.htm>) for information on integrating the system with LDAP.

The Security Groups application contains tabs with the following purposes:

- ▶ **List:** Search for group records.
- ▶ **Group:** Add a new group, specify its Start Center, and specify whether or not the group rights are independent of other groups.
- ▶ **Sites:** Specify which sites a group has access to in a multi-site implementation.
- ▶ **Applications:** Specify which applications and options a group has rights to.
- ▶ **Storerooms:** Specify which storerooms a group has access to.
- ▶ **Labor:** Specify which labor records a group can view.
- ▶ **GL Components:** Specify which GL components a group can change.
- ▶ **Limits and Tolerances:** Specify various purchasing, requisitioning, and contract limits and invoice, tax, and service tolerances.
- ▶ **Data Restrictions:** Restrict access to certain data fields and certain functions in applications.
- ▶ **Users:** Assign users to groups and view existing group membership.

Important: If your implementation uses an application server to authenticate with a directory, you will not use the system to perform some functions. Instead, these functions will be performed in the directory and synchronized into the system. These functions might include:

- ▶ Adding users (including self-registration)
- ▶ Adding security groups
- ▶ Associating users with security groups
- ▶ Managing passwords

Note that prior to moving to production the building blocks of your migration will be:

- ▶ Organization
- ▶ Users
- ▶ Assets

5.1.2 Adding security groups

Proceed as follows to create a new security group:

1. From the **Go To** menu select **Security** → **Security Groups**.

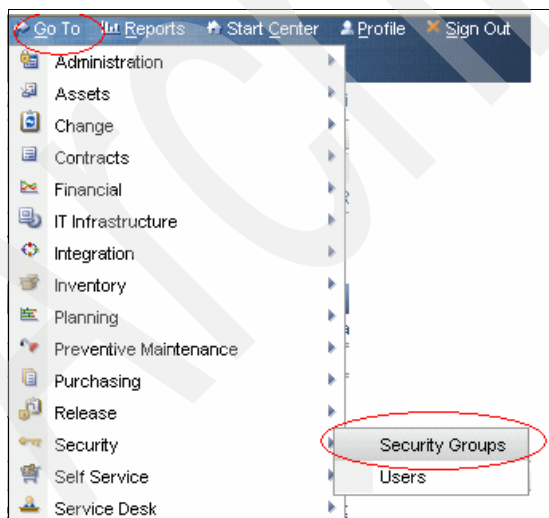
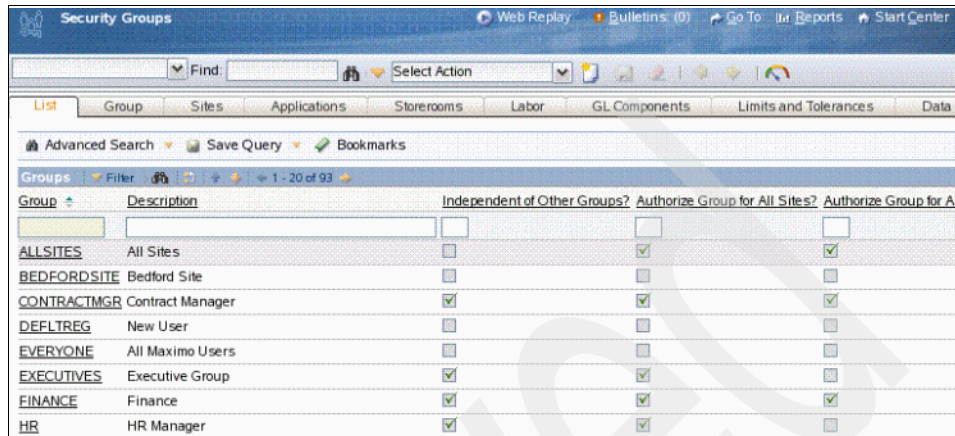


Figure 5-1 Security Groups

- The existing security groups are displayed in the Security Groups window, as shown in Figure 5-2.

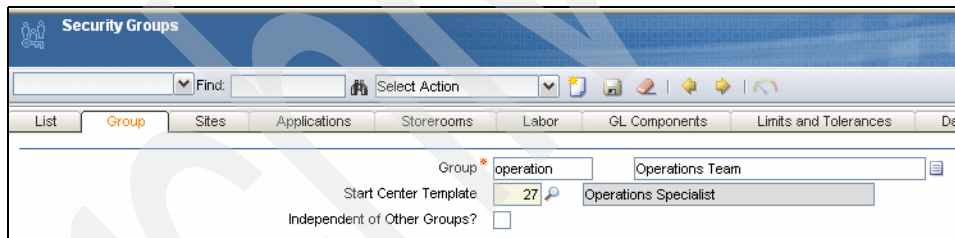


The screenshot shows the 'Security Groups' window with a list of groups. The 'List' tab is selected. The table below represents the data shown in the window.

Group	Description	Independent of Other Groups?	Authorize Group for All Sites?	Authorize Group for All Applications?
ALLSITES	All Sites	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
BEDFORDSITE	Bedford Site	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CONTRACTMGR	Contract Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEFLTREG	New User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EVERYONE	All Maximo Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EXECUTIVES	Executive Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FINANCE	Finance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HR	HR Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 5-2 Security Groups list

- Click the **New Group** icon. The system displays the Group tab (Figure 5-3).



The screenshot shows the 'Security Groups' window with the 'Group' tab selected. The form below represents the data entered in the window.

Group	operation	Operations Team
Start Center Template	27	Operations Specialist
Independent of Other Groups?	<input type="checkbox"/>	

Figure 5-3 Creating a new Security Group

- In the **Group** field, enter a name for the group.
You might name a group after a site, for example, HAMBURG, or for some functional unit, such as OPERATIONS, MAINTENANCE, and so forth.
- Add a description in the **Group Description** field. To enter additional information type in your description.
- In the **Start Center Template** field, enter the name of the Start Center you want the system to display when a user in the group logs in.
- Click the **Select Value** icon to select from a list (see Figure 5-4 on page 80).

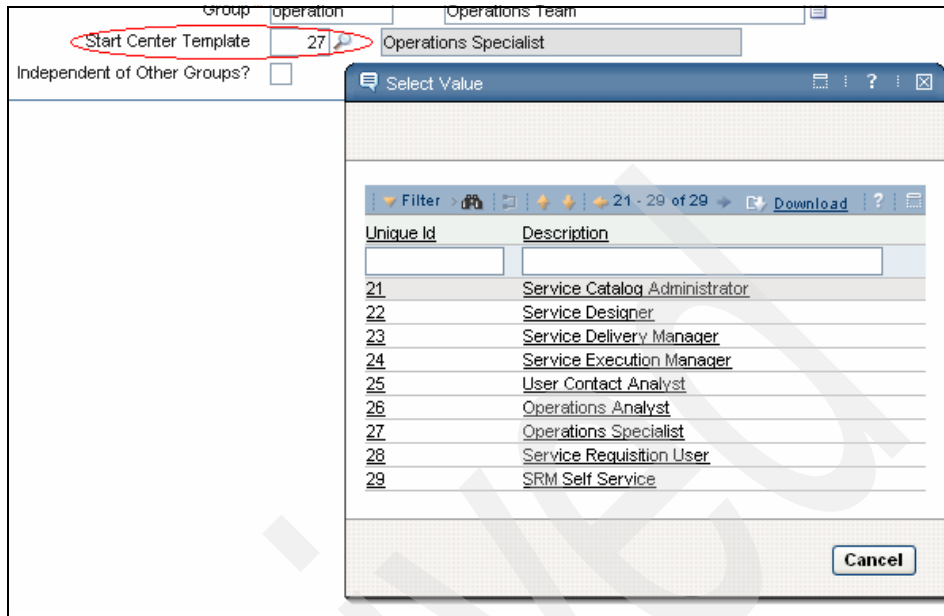


Figure 5-4 Start Center template selection

By default, the system merges rights when groups that include different sites are combined.

- If you do not want rights combined, select the **Independent of Other Groups?** check box, as shown in Figure 5-5.

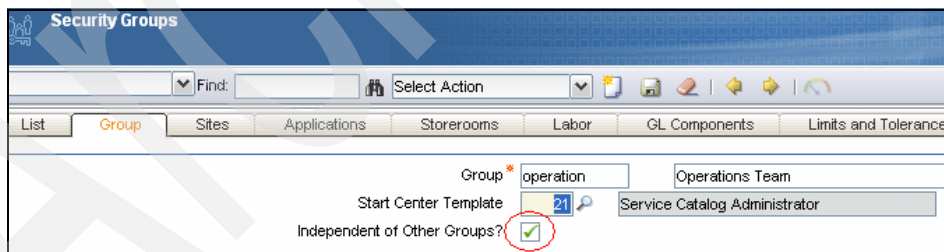


Figure 5-5 Independent of Other Groups selection

Assign sites to a security group

Now that your security group is created, you can assign sites to this group, as follows:

- Click the **Sites** tab (Figure 5-6 on page 81).

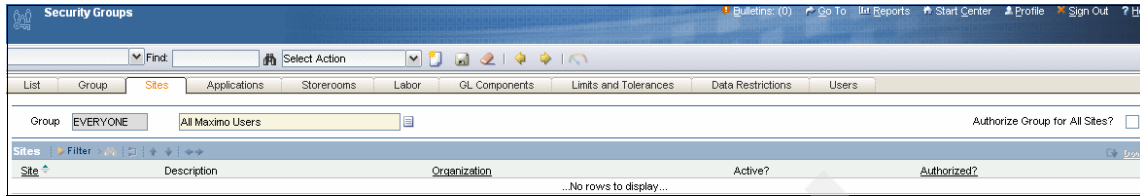


Figure 5-6 Sites tab

You use the Sites tab in the Security Groups application to assign site access privileges to a group.

2. On the List tab, select the group for which you want to assign site access.
3. Click the **Sites** tab.
4. Specify sites.
 - a. If you want the group to have access to all sites, select the **Authorize Group for All Sites?** check box.
5. Click **Save Group**.

Note: If you select this check box, you cannot add individual rows in the Sites table window.

Notes:

- You can only add sites that you have access to.
- You can only add inactive sites to a group if your user record is authorized for inactive sites.
- There is no limit to the number of security groups you can create.

Adding applications to a security group

You can add applications to a security group in the following way:

1. On the List tab, select the group for which you want to grant privileges.
2. Click the **Applications** tab. See Figure 5-7 on page 82.

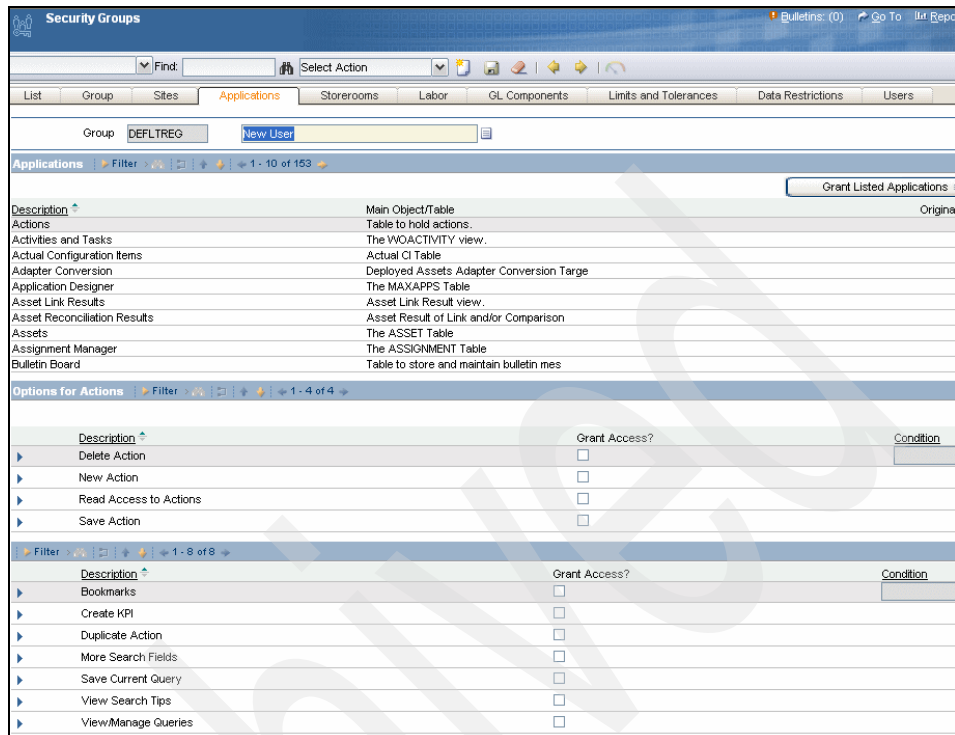


Figure 5-7 Applications tab

3. In the Applications table window, select the application. To narrow your search, use the **Filter**. The Options table window displays the options for the selected application.
4. In the Applications table window, select the appropriate options using the **Grant Listed Applications** button to grant privileges to all listed applications, or use the **Revoke Listed Applications** button to remove privileges. The privilege levels are:
 - **Read**: Users can only view records.
 - **Insert**: Users can insert new records.
 - **Save**: Users can save changes to records.
 - **Delete**: Users can delete records.
 - **All Above**: Grants or revokes **Read**, **Insert**, **Save**, and **Delete** permissions for all listed applications.

Note: You can filter the list of applications in the Applications table window, which will cause any of the changes you make using the Grant or Revoke Listed Applications buttons to affect only the applications that appear in the table window.

The Options table window displays the options, including menu items and the read, insert, save, and delete options for the application you have selected.

5. If you want to set options for a different application, select that application in the Applications table window.

In the Options table window select the check boxes for the options you want to grant access to, or clear the check boxes to remove privileges. If you want to select all check boxes, click **Grant Listed Options for This Application**.

Note: The **Grant Listed Options** button is not a toggle, so be sure you want to select all check boxes before using it. To revoke all application options in the options table window at once, you can simply revoke *Read* access from the application.

Adding storerooms to security groups

You use the Storerooms tab in the Security Groups application to authorize a group to make transactions with storerooms.

Note: In some applications, users can view storerooms even though they are not authorized for transactions.

To authorize a group's access to storerooms:

1. On the List tab, select the group for which you want to authorize storeroom transactions.
2. Click the **Storerooms** tab (Figure 5-8 on page 84).

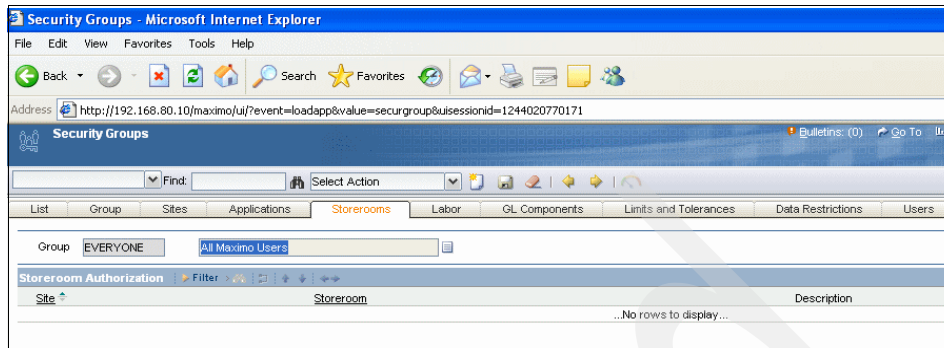


Figure 5-8 The Storeroom tab

3. Specify storerooms.

- a. If you want the group to have access to all storerooms, select the **Authorize Group for All Storerooms?** check box.

Note: If you select this check box, you cannot enter individual storerooms in the Storeroom Authorization table window.

- b. If you want the group to have access to individual storerooms:
 - i. Click **New Row** in the Storeroom Authorization table window. The Row Details open.
 - ii. In the **Site** field, enter a value or click **Select Value**. The Select Value dialog box lists all sites for all organizations.
 - iii. In the **Storeroom** field, enter a value or click **Detail Menu** to select an option and retrieve a value. If you access the Select Value dialog box, it shows only the storerooms for the site you specified in the **Site** field.
 - iv. Click **Close Details**.

4. Click **Save Group**.

5. Click the **Labor** tab (Figure 5-9 on page 85).

Note: You can only add storerooms that your user ID allows you to access.

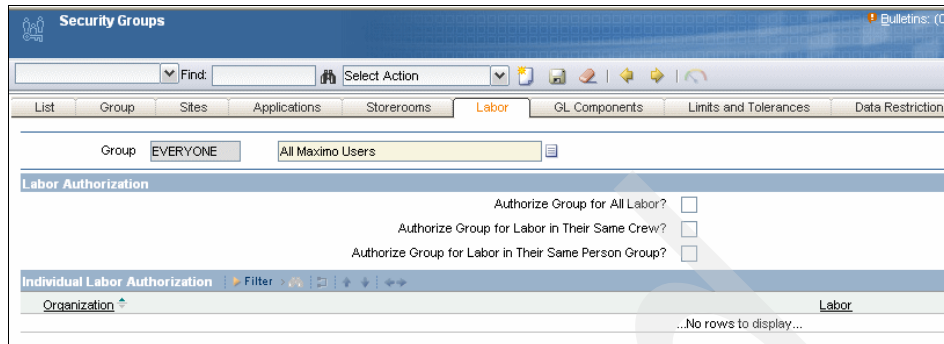


Figure 5-9 The Labor tab

Assigning GL components to security groups

To authorize GL Component access to a security group perform the following:

1. On the List tab, select the group for which you want to grant GL Component access.
2. Click the **GL Components** tab (Figure 5-10).

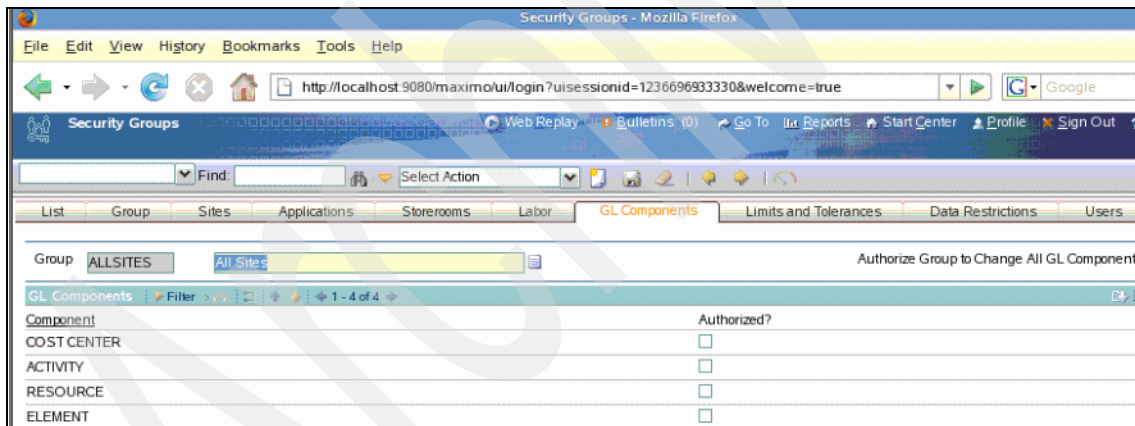


Figure 5-10 The GL Components tab

You use the GL Components tab in the Security Groups application to authorize which GL components a group can insert and edit in a GL account field.

3. If you want the group to be able to access all GL components, select the **Authorize Group to Change All GL Component Types?** check box. If you select this check box, the check boxes in the GL Components table window are no longer editable.

4. If you want to grant privileges to access individual GL components:
 - a. If selected, clear the **Authorize Group to Change All GL Component Types?** check box.
 - b. In the GL Components table window, select the appropriate **Authorized?** check box or boxes.
5. Click **Save Group**.

Adding limits and tolerances to security groups

Use the **Limits and Tolerances** tab in the Security Groups application (Figure 5-11) to set approval limits for purchase requests, purchase orders, material requisitions, invoices, and contracts; and to specify for the group how much invoices, taxes, and services can deviate from an initial agreement.

The screenshot shows the 'Security Groups' application interface. The 'Limits and Tolerances' tab is active. The 'Organizations' table is empty. The 'Details' section shows fields for Organization, Description, and Base Currency 1. The 'Limits' section includes fields for PR Limit, PO Limit, MR Limit, Invoice Limit, and Contract Limit. The 'Tolerances' section includes three tables: Invoice Tolerance, Tax Tolerance, and Service Tolerance, each with fields for Upper and Lower Amount and Percent.

Figure 5-11 Limits and Tolerances

To set purchasing limits and tolerances:

1. On the List tab, select the group for which you want to set limits and tolerances.
2. Click the **Limits and Tolerances** tab.
3. Click **New Row** to create a new record, or select an organization from the **Organizations** table window to edit limits and tolerances for an existing organization.
4. In the **Organization** field of the new row, enter the name of an organization or click **Detail Menu** to select an option and retrieve a value.

Note: The Base Currency field, which is read-only, shows **Base Currency 1** for each organization. You must use this currency in setting limits.

Values in these fields default to 0 when you create a new record. A value of 0 means that the group has a limit of 0 in that field, while an empty (null) field means the group has unlimited approval permissions in that field.

- In the Invoice Tolerance section, set as needed the upper and lower tolerances by amount, percent, or both.
- In the Tax Tolerance section, set as needed the upper and lower tolerances by amount, percent, or both.
- In the Service Tolerance section, set as needed the upper and lower tolerances by amount, percent, or both.

5. Click **Save Group**.

Applying data restrictions to security groups

Use the **Data Restrictions** tab in the Security Groups application to set restrictions on what records a group can access within the larger set specified by the privileges you grant on the Applications tab.

You can specify which records the members of a group can access. You do not use this feature to restrict access to applications and menus, or to prevent a user from entering data; you control those privileges from the Applications tab.

Object and attribute restrictions can be made conditionally using conditions created in the Conditional Expression Manager.

For example, you might want to restrict a maintenance group so that they only have access to their own personal information or to the labor in their same craft, no matter what application they are using to access the information.

The data restriction types are:

- ▶ **Object Restrictions:** Apply to an object, such as a database table or view.
- ▶ **Attribute Restrictions:** Apply to one database field.
- ▶ **Collection Restrictions:** Apply to collections of assets, locations, and configuration items.

You can set restrictions on which records a group can access. You use an SQL-style expression or a class file to define and apply these restrictions.

To set data restrictions:

1. On the List tab of the Security Groups application, select the group for which you want to set restrictions.
2. On the Data Restrictions tab, select a tab to set restrictions on either objects or the attributes.

Note: Three types of Global Data Restrictions can be applied to security groups:

- ▶ Hidden
- ▶ Qualified
- ▶ Read Only

In the table window below the tabs, click **New Row** to open the row details (Figure 5-12).

The screenshot shows the 'Security Groups' application interface. At the top, there's a navigation bar with tabs: List, Group, Sites, Applications, Storerooms, Labor, GL Components, Limits and Tolerances, Data Restrictions (selected), and Users. Below the navigation bar is a 'Find' field and a 'Select Action' dropdown. The 'Data Restrictions' tab is active, showing three sub-tabs: Object Restrictions, Attribute Restrictions, and Collection Restrictions. The 'Object Restrictions' section is expanded, displaying a table with columns: Object, Application, Type, and Condition. Below the table is a 'Details' section with fields for Object, Application, Type, Reevaluate? (checked), Condition, Condition Class, and Expression. A 'New Row' button is located at the bottom right of the details section.

Figure 5-12 Data Restrictions

3. In the **Object** field, specify the table or view on which to set the restriction. In the Attribute Restrictions tab, you can also specify the attribute that you want to restrict.
4. In the **Application** field, select the application to apply the restriction to. Leave it blank for the restriction to apply to all applications that use the object or attribute.
5. In the **Type** field, select the type of restriction.
6. Select the **Reevaluate?** check box if you want the system to reevaluate the restriction condition when the user moves to another field by pressing the Tab key. If you do not select this check box, the restriction conditions are evaluated after you save the changes to a field.

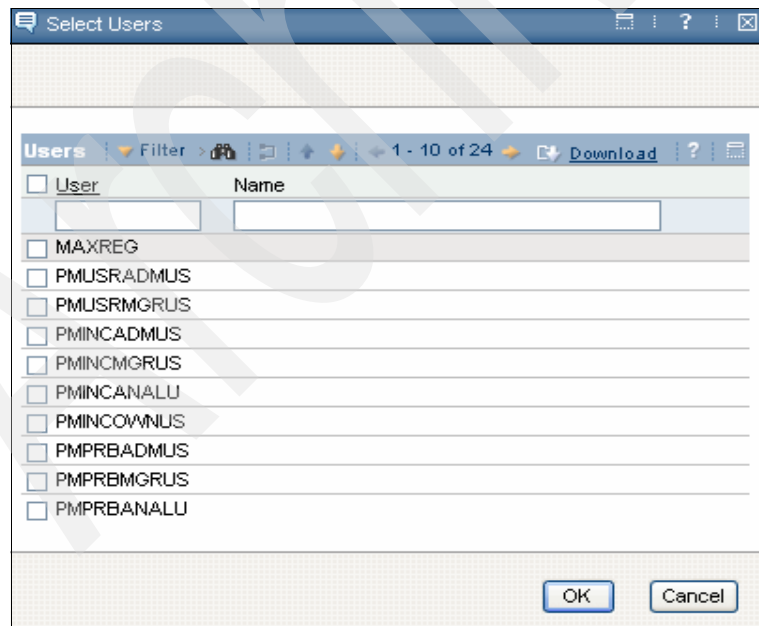
7. In the **Condition** field, click **Detail Menu** and choose either **Select Value** to pick from a list of existing expressions, or **Go To Conditional Expression Manager** to manage your existing expressions or create a new conditional expression. For more information on building conditional expressions, see Conditional Expression Manager online help.
8. Click **New Row** to add more restrictions on the group, or click **Save Group** to apply your changes

Adding users to a security group

The *Users application* works in combination with the security groups when defining security. Once the users are created, you combine them into security groups where their security privileges are associated. There is no limit on the number of user members in a group.

To add a user to a group:

1. On the List tab, select the group to which you want to add a user.
2. Click the Users tab.
3. In the Users table window, click **New Row**. The Row Details pane opens.
4. In the **User** field, enter the user ID or click **Select Users** to select an option and retrieve a user ID (Figure 5-13).



The screenshot shows a window titled "Select Users". Inside, there is a table with two columns: "User" and "Name". The "User" column contains a list of user IDs, each preceded by a checkbox. The "Name" column is empty. The user IDs listed are: MAXREG, PMUSRADMUS, PMUSRMGRUS, PMINCADMUS, PMINCMGRUS, PMINCANALU, PMINCOWNUS, PMPRBADMUS, PMPRBMGRUS, and PMPRBANALU. At the bottom right of the window are "OK" and "Cancel" buttons.

User	Name
<input type="checkbox"/> MAXREG	
<input type="checkbox"/> PMUSRADMUS	
<input type="checkbox"/> PMUSRMGRUS	
<input type="checkbox"/> PMINCADMUS	
<input type="checkbox"/> PMINCMGRUS	
<input type="checkbox"/> PMINCANALU	
<input type="checkbox"/> PMINCOWNUS	
<input type="checkbox"/> PMPRBADMUS	
<input type="checkbox"/> PMPRBMGRUS	
<input type="checkbox"/> PMPRBANALU	

Figure 5-13 Select Users pane

- Click the **Users** tab as shown in Figure 5-14. The system enters the associated user information in the other fields.

The screenshot shows the 'Security Groups' application interface. At the top, there's a navigation bar with 'Security Groups' and links for 'Bulletins (0)', 'Go To', 'Reports', 'Start Center', 'Profile', and 'Sign Out'. Below this is a tabbed interface with tabs for 'List', 'Group', 'Sites', 'Applications', 'Storerooms', 'Labor', 'GL Components', 'Limits and Tolerances', 'Data Restrictions', and 'Users'. The 'Users' tab is active. Below the tabs, there's a search bar and a 'New User' button. A table lists users, with 'MAXADMIN' selected. To the right of the table, a 'Details' panel shows fields for 'First Name', 'Last Name', and 'Type'. The 'First Name' field contains 'maxadmin', the 'Last Name' field contains 'maxadmin', and the 'Type' field contains 'TYPE 1'. At the bottom right, there's a 'Select Users' button.

Figure 5-14 Adding users to security groups

- Click **New Row** again to add another user, or click **Close Details**.
- Click **Save Group**.

Tips:

- ▶ To add a user to a group, you must be authorized to reassign users to that group. You do this using the **Authorize Group Reassignment** action in the Select Action menu. If you have created a new group, the system automatically authorizes you to reassign users to the group.
- ▶ If implementation uses an application server to authenticate with a directory, you can associate users with groups in the directory or the system, depending on your system settings.
- ▶ When you create a group, the system automatically authorizes you to add users to the group. Users can be added from the Users tab of the Security Groups application, or from the Users application.
- ▶ If implementation uses an application server to authenticate with a directory, groups can be created in the directory and synchronized into the system.

You now have a new group with no defined privileges or restrictions. Use the other tabs and the Select Action menu to define the security for the group.

5.1.3 The Users application

Use the *Users application* to add users and to manage their security privileges. You can perform these tasks in the Users application:

- ▶ Manage user status.
- ▶ Manage user sessions.
- ▶ View user security profile.
- ▶ Specify various user defaults, such as default insert site, default storeroom, default language, and default General Ledger accounts for purchasing. (The default purchasing account is the General Ledger account that will be used for Desktop Requisitions, but not for all purchasing.)
- ▶ Grant users the right to access inactive sites.
- ▶ Specify which users can access a screen reader to assist in interacting with the system.
- ▶ Set system-wide security controls and new user default groups.
- ▶ Change passwords (if you are using an external directory, this functionality is not available).
- ▶ Create database users (if you are using an external directory, this functionality is not available).

The Users application and the Security Groups application work together. You use the Security Groups application to define security groups, then assign users to one or more groups to create security profiles which control authorizations.

Note: A user record requires a person record.

In addition to granting rights to individual users, you can add, delete, and replace group privileges for multiple users at one time. You can also manage user status for multiple users. The Users application also allows you to grant a user database access.

The Users application contains these tabs:

List: To search for user records.

User: To add, view, modify, or delete user records, including specifying several default settings.

Groups: To specify and view the security groups to which a user belongs.

Security Profile: To view a user's security privileges to Sites, applications, and options.

A user record can have one of the following statuses:

- ▶ **ACTIVE** - Default status for new records. A user record must be ACTIVE to be able to sign in to the system.
- ▶ **BLOCKED** - When a user is blocked, he or she cannot log in to the system.
- ▶ **DELETED** - User names cannot be reused.

Note: For auditing purposes, most information for a deleted user is removed; however, the user ID is retained.

- ▶ **INACTIVE** - When a user is inactive, he or she cannot log in to the system.
- ▶ **NEWREG** - Default status for user records created by self-registration. This status is used to identify user records to route into a Workflow process.

Note: If you do chose to use self-registration for user records, a new user can register without having any existence. A record with a status NEWREG has a workflow, SELFREG, that notifies the user that the request is being reviewed.

5.1.4 Start Centers

To set up the Start Center, administrators must have access to the *Start Center customization application* within signature security.

Start Centers are assigned to security groups. Therefore, the first time a user logs in to the system, the user sees a Start Center based on a template for the security group.

If a user belongs to more than one security group, the user might see tabs at the top of the page, where each tab is a Start Center page for a different security group.

Note: For more information on Start Centers refer to Chapter 7, "Start Center configuration" on page 135.

You assign or change the Start Center for a group from the group's record in the Security Groups application.

To assign or change the Start Center:

1. From the List tab in the Security Groups application, select the group whose Start Center you want to assign or change.

The system displays the Group tab.

2. In the **Start Center Template** field, enter the Start Center or click **Select Value** to make a selection.
3. Click **Save Group**.

5.1.5 Security group types

There are two types of security groups: independent and non-independent. When a security group is created, there is an *Independent of Other Groups?* option, which lets you specify if a group is independent or non-independent. If you do not specify a group as independent, the access rights and grants in this group are combined with access rights and grants in other groups that are also not independent.

These two types of security groups provide flexibility when you build the security infrastructure for your organization. Simple organizations might use one or two security groups; however, larger organizations with many users and a complex infrastructure might want to build some security groups that reflect varying levels of application and storeroom access and approval limits.

5.2 Setting up security users

A user record must be associated with a person record. There are two ways the user-person association can be made:

- ▶ You can associate an existing person with a user.
- ▶ If there is no existing person, use the Users application to insert a new person ID.

Either method results in the person ID and user being associated. See Figure 5-15 on page 94.

The screenshot displays the 'Users' application window. At the top, there's a navigation bar with 'Users' and a search bar. Below it, tabs for 'List', 'User', 'Groups', and 'Security Profile' are visible. The 'User' tab is active, showing details for user 'MAAMAR'. The status is 'ACTIVE' and the type is 'PRIMARY'. The 'Login Information' section shows 'User Name' as 'maamar' with a 'Set Password' button. The 'Personal' section includes fields for 'Person' (MAAMAR), 'Status' (ACTIVE), 'First Name' (maamar), 'Last Name' (ferkoun), 'Supervisor' (rich osbrink), 'Display Name' (maamar ferkoun), 'Primary Phone', 'Primary E-mail', 'Workflow Delegate', 'Memo', 'Address', 'City' (Hong Kong), 'State/Province', 'ZIP/Postal Code', and 'Country' (China). The 'User Settings' section has a table for 'Default Insert Site' with columns for 'Site' and 'Use Default Insert Site as a Display Filter?'. The 'Purchasing' section shows 'Filter' and 'Organization' fields. At the bottom, it says 'GL Account' and '...No rows to display...'.

Figure 5-15 Users application

5.2.1 Default insert site

When a user creates a site-level record, the Site field defaults to the value that is specified in the Default Insert field in the user record. When a user creates an organization-level record, the Organization field for that record defaults to the organization of the site that is specified in the Default Insert field in the record. To set the default:

- ▶ Use the Set Security Profile action.
- ▶ Specify the default insert site on a user record.

In addition, a user can use the **My Profile** action to set their own default insert site.

Note: A default insert site is not required. However, as a best practice, assign a default.

5.2.2 User statuses

A user record can have one of the following statuses:

- ▶ **ACTIVE:** Default status for new records. A user record must be ACTIVE to log in to the system.

- ▶ **BLOCKED:** User cannot log in to the system. An administrator can choose to block a user. If login tracking is enabled and the user types their user name or password incorrectly too many times, the system can also block a user.
- ▶ **DELETED:** User names cannot be reused. If you delete a user record, the user ID is retained in the database.
- ▶ **INACTIVE:** When a user is inactive, the user cannot log in to the system. Inactive user records do not appear in select value lists. A user record with a status of INACTIVE cannot be associated with new records.
- ▶ **NEWREG:** Default status for user records created by self-registration. This status is used to identify user records to route into a Workflow process.

Note: When you add a user, their default status is ACTIVE.

5.2.3 Managing users

When you insert new users, they are added to a default security group called DEFLTREG. You can set up and configure the DEFLTREG group with limited authorizations and privileges out of the box.

The User Name field, which defaults to the new user ID you typed when you created a user, is the login name the user uses when logging into the system. The user ID must be unique for all user records in the system. However, you can change the user name, which is case sensitive, to an employee number or e-mail address.

The Security Profile tab shows the user's security profile after the system has combined all of the user's security groups. Sorted by site, the security profile is an expandable tree structure presentation of the user's virtual profile.

For an overview of the functions available in the Users application see 5.1.3, "The Users application" on page 91. In this section we provide additional details for using these functions.

Adding a new user

A user record contains the user ID and password. You create records for users in the Users application. User records cannot be created without a corresponding person record. You create person records either in the People application or in the Personal section in the User application.

Note: As a best practice, create *person records* before you create user records. You create person records in the People application. When you create a user record, the application checks for a corresponding person record by trying to match a user ID with a person ID. For example, if you create a user record for JSmith, the system checks for a corresponding person ID, JSmith, in the person table. If a corresponding person record is not found, the application notifies you.

Perform the following to add a user:

1. On the toolbar, click the **New User** icon.
2. If the **User** field is empty, type a user identifier. This identifier must be unique within the database. The application checks to see if there is a corresponding person record that matches the user ID.

Note: If you use autonumbering, the User field is populated.

3. If no matching person ID is found, select one of the following options:
 - To have the software create a person record from the information recorded in the Personal section of the user record, click **Yes**.
 - To select an existing person record, click **No**, and specify the value in the **Person** field.
 - To create a person record manually, click **No**; in the **Person** field click **Select Value** then **Go to People**.

Note: You could have a User ID that you want to associate with a different person ID. For example, an employee marries and changes their last name, and last name is used as their person ID. You use the Change Person action to change the association between the user ID and the person ID.

You cannot associate a person ID that is already a user with a second user ID.

4. In the **Type** field, click **Select Value** and select the license type.

Note: The system has user types 1 through 10. In the USERTYPE domain, update the descriptions to reflect the types of users in the license. The appropriate type must be associated with each user ID to ensure license compliance. These values can be modified in the DOMAINS option under **System Configuration → Platform Configuration**.

SYNONYM Domain

Domain: USERTYPE
Domain Type: SYNONYM
Length: 30

Internal Value	Value	Description	Default?	Organization
▶ TYPE 1	TYPE 1	TYPE 1	<input checked="" type="checkbox"/>	
▶ TYPE 10	TYPE 10	TYPE 10	<input checked="" type="checkbox"/>	
▶ TYPE 2	TYPE 2	TYPE 2	<input checked="" type="checkbox"/>	
▶ TYPE 3	TYPE 3	TYPE 3	<input checked="" type="checkbox"/>	
▶ TYPE 4	TYPE 4	TYPE 4	<input checked="" type="checkbox"/>	
▶ TYPE 5	TYPE 5	TYPE 5	<input checked="" type="checkbox"/>	
▶ TYPE 6	TYPE 6	TYPE 6	<input checked="" type="checkbox"/>	
▶ TYPE 7	TYPE 7	TYPE 7	<input checked="" type="checkbox"/>	
▶ TYPE 8	TYPE 8	TYPE 8	<input checked="" type="checkbox"/>	
▶ TYPE 9	TYPE 9	TYPE 9	<input checked="" type="checkbox"/>	

Figure 5-16 Synonym Domain

5. The **User Name** field defaults to the ID name in the **User** field, but you can type a different value. The user types a user name to access the system.
6. Click **Set Password**. The Set Password dialog box opens.
 - a. Select one of these options:
 - To generate a random password, click **Generate Password**.
 - To specify a particular password, type the password in the **Password** field and re-type it in the **Confirm Password** field.
 - b. To send an e-mail message to the user containing their password, select the **E-Mail Password to User?** check box. To be able to send an e-mail to a user, e-mail must be enabled and the user must have an e-mail address in their person record.

Note: The **E-Mail Password to User?** option is selected and read-only when the **Always E-mail Generated Passwords to Users (Never Display on Screen)** option in the Security Controls dialog box is selected.

The **E-Mail Password to User?** option is editable when the **Allow Generated Passwords to Be Displayed on Screen** option in the Security Controls dialog box is selected.

- c. If you do not want to force the user to change their password when they initially sign in, clear the **Password Should Expire After First Login?** check box. This check box is selected by default.
 - d. Click **OK** to close the Set Password dialog box.
- 7. If appropriate, enter additional personal data about the user in the Personal section. The system uses this information to create a user record.
 - 8. If appropriate, specify default settings for the user in the User Settings section.

Note: As a best practice, assign a default insert site. Without a default insert site, many applications will not function. For example, you will not be able to insert purchase orders or labor records in an application that is defined on the site level.

- 9. If appropriate, you can type one or more General Ledger accounts as a default purchasing account.
- 10. Click **Save User**. The application assigns the user to the default security group.

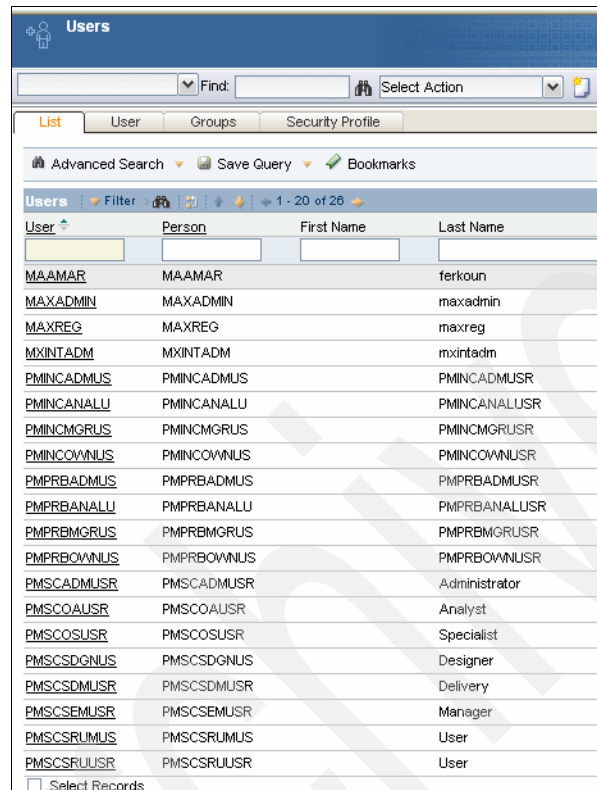
Note: A new user has no security authorizations until you assign them to security groups.

Assigning a user to a security group

Note: You can only add security groups that you have been authorized to manage. Use the **Authorize Group Reassignment** action to grant someone the ability to assign users to security groups. Depending on your security structure, an administrator authorizes you or you can authorize yourself.

To assign a user to a security group proceed as follows:

1. In the Users application, display the record that you want to assign to groups (Figure 5-17).



The screenshot shows the 'Users' application window. At the top, there is a search bar with a 'Find:' label and a 'Select Action' dropdown. Below this are tabs for 'List', 'User', 'Groups', and 'Security Profile'. The 'List' tab is active, displaying a table of users. The table has columns for 'User', 'Person', 'First Name', and 'Last Name'. The first row is highlighted in yellow. Below the table, there is a 'Select Records' checkbox.

User	Person	First Name	Last Name
MAAMAR	MAAMAR		ferkoun
MAXADMIN	MAXADMIN		maxadmin
MAXREG	MAXREG		maxreg
MXINTADM	MXINTADM		mxintadm
PMINCADMUS	PMINCADMUS		PMINCADMUSR
PMINCANALU	PMINCANALU		PMINCANALUSR
PMINCMGRUS	PMINCMGRUS		PMINCMGRUSR
PMINCOVNUS	PMINCOVNUS		PMINCOVNUSR
PMPRBADMUS	PMPRBADMUS		PMPRBADMUSR
PMPRBANALU	PMPRBANALU		PMPRBANALUSR
PMPRBMGRUS	PMPRBMGRUS		PMPRBMGRUSR
PMPRBOWNUS	PMPRBOWNUS		PMPRBOWNUSR
PMSCADMUSR	PMSCADMUSR		Administrator
PMSCOAUSR	PMSCOAUSR		Analyst
PMSCOSUSR	PMSCOSUSR		Specialist
PMSCSDGNUS	PMSCSDGNUS		Designer
PMSCSDMUSR	PMSCSDMUSR		Delivery
PMSCSEMUSR	PMSCSEMUSR		Manager
PMSCSRUMUS	PMSCSRUMUS		User
PMSCSRUUSR	PMSCSRUUSR		User

Figure 5-17 Users list

2. Click the **Groups** tab.
3. In the Groups table window, click **New Row**.
4. In the **Group** field, type a group or click **Select Groups** to select an option and retrieve a group (Figure 5-18 on page 100).

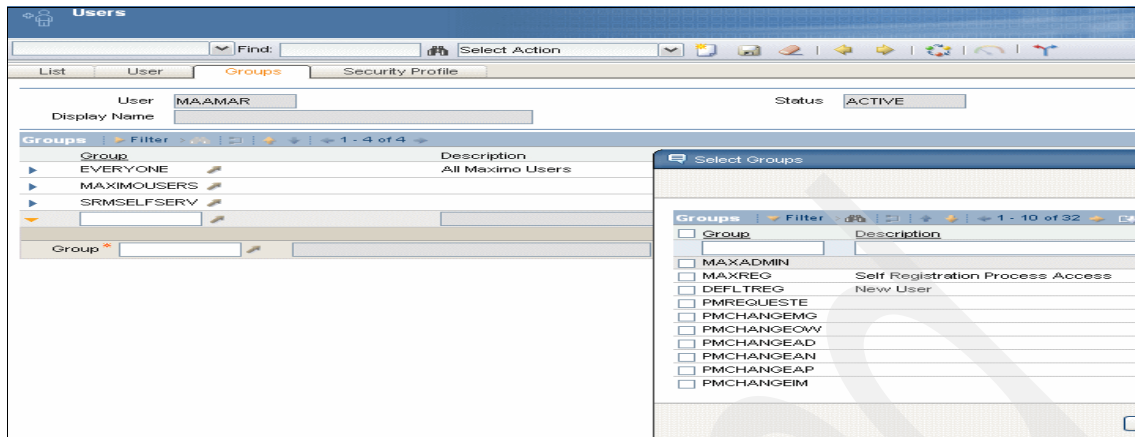


Figure 5-18 Assignment to security groups

5. Repeat steps 3 and 4 as necessary to enter more groups.
6. Click **Save User**.

Security profile tab

Use the **Security Profile** tab to access a read-only view of the user's combined security profile. The authorization of the user is presented in an expandable tree view. If the node has a plus sign (+), you can expand the node to view specific authorizations. The security profile reflects the highest level of rights as a result of the combination of all security groups to which the user belongs.

The first level of the tree contains two different types of nodes or branches, as shown in Figure 5-19 on page 101.

- ▶ **System level applications:** The System level node contains System level applications. You can expand each application to view the actions that the user has been authorized to use.
- ▶ **Sites:** These nodes contain authorizations that correspond to the tabs in the Security Groups application: Applications, Approval Limits, GL Components, Labor, Restrictions, Storerooms, and Tolerances. You can expand each authorization to view the details of the user's security authorization.

When you add or modify the groups to which a user belongs, you must save the record before you can see the modifications on the **Security Profile** tab.

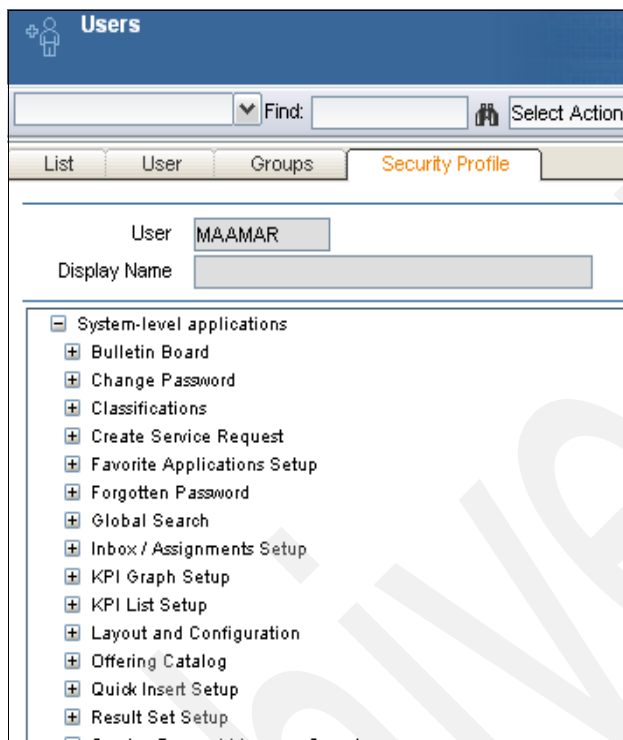


Figure 5-19 Security Profile tab

Set security profiles

To set security profiles for a user proceed as follows:

1. In the Users application, display the user whose profile you want to set.
2. From the Select Action menu, select **Set Security Profile**. See Figure 5-20 on page 102.

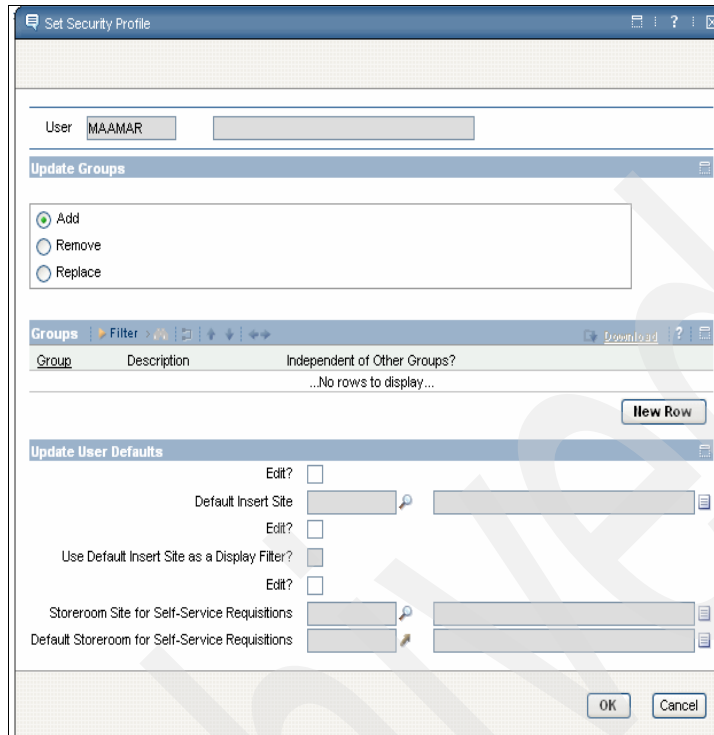


Figure 5-20 Set Security Profile

3. In the Update Groups section in the Set Security Profile dialog box, select one of these options in the **Group** field:
 - a. **Add**: Adds the groups to the profiles of the selected user. If the groups to be added exist in the selected user's profile, the record is not updated.
 - b. **Remove**: Removes the groups from the profiles of the selected user. If a selected user's profile does not include the groups to be removed, the record is not updated.
 - c. **Replace**: Replaces all groups in the profiles of selected user with the groups you specify here. All of the user's groups are removed and replaced with the specified groups.
4. In the Groups table window, click **New Row**.
5. In the **Group** field, type a group or specify a value. See Figure 5-21 on page 103.

The screenshot shows the 'Set Security Profile' window. At the top, the 'User' field contains 'MAAMAR'. Below it is the 'Update Groups' section with three radio buttons: 'Add' (selected), 'Remove', and 'Replace'. A table titled 'Groups' follows, with columns 'Group', 'Description', and 'Independent of Other Groups?'. It contains one row for 'PMSADM' where the last column is checked. Below the table is a 'Details' section for the selected group. At the bottom is the 'Update User Defaults' section with several 'Edit?' checkboxes and text input fields for 'Default Insert Site', 'Storeroom Site for Self-Service Requisitions', and 'Default Storeroom for Self-Service Requisitions'. 'OK' and 'Cancel' buttons are at the very bottom.

Figure 5-21 Set Security Profile options

The **Independent of Other Groups?** check box is read-only. You set this value in the Security Groups application.

6. If necessary, click **New Row** again to specify additional groups.
7. In the Update User Defaults section, select the **Edit?** check box above a field to make the field editable. Type new defaults as needed.
8. Click **OK**.

Modify security profiles

To modify security profiles for multiple users:

1. In the **List** tab, query for the records whose profile you want to change.
2. At the bottom of the Users table window, select the **Select Records** check box.
3. Select the check boxes for the user records whose profile you want to change, as shown in Figure 5-22 on page 104.

	User	Person
<input type="checkbox"/>	MAAMAR	MAAMAR
<input type="checkbox"/>	MAXADMIN	MAXADMIN
<input type="checkbox"/>	MAXREG	MAXREG
<input type="checkbox"/>	MXINTADM	MXINTADM
<input type="checkbox"/>	PMINCADMUS	PMINCADMUS
<input type="checkbox"/>	PMINCANALU	PMINCANALU
<input type="checkbox"/>	PMINCMGRUS	PMINCMGRUS
<input type="checkbox"/>	PMINCOVNUS	PMINCOVNUS
<input type="checkbox"/>	PMPRBADMUS	PMPRBADMUS
<input type="checkbox"/>	PMPRBANALU	PMPRBANALU
<input type="checkbox"/>	PMPRBMGRUS	PMPRBMGRUS
<input type="checkbox"/>	PMPRBOVNUS	PMPRBOVNUS
<input type="checkbox"/>	PMSCADMUSR	PMSCADMUSR
<input type="checkbox"/>	PMSCOAUSR	PMSCOAUSR
<input type="checkbox"/>	PMSCOSUSR	PMSCOSUSR
<input type="checkbox"/>	PMSCSDGNUS	PMSCSDGNUS
<input type="checkbox"/>	PMSCSDMUSR	PMSCSDMUSR
<input type="checkbox"/>	PMSCSEMUSR	PMSCSEMUSR
<input type="checkbox"/>	PMSCSRUMUS	PMSCSRUMUS
<input type="checkbox"/>	PMSCSRUUSR	PMSCSRUUSR

Figure 5-22 Records selection

4. From the Select Action menu, select **Set Security Profile**. In the Set Security Profile dialog box, the **Records Being Updated** field displays the number of selected users.
5. In the Update Groups section, in the **Group** field, select one of the following options:
 - a. **Add**: Adds the groups to the profiles of the selected users. If the groups to be added exist in the selected user's profile, the record is not updated.
 - b. **Remove**: Removes the groups from the profiles of the selected users. If a selected user's profile does not include the groups to be removed, the record is not updated.
 - c. **Replace**: Replaces all groups in the profiles of selected users with the groups you specify here. All of the user's groups are removed and replaced with the specified groups.
6. In the Groups table window, click **New Row**.
7. In the Group field, type a group or click **Detail Menu** to specify a value.

8. The **Independent of Other Groups?** check box is read-only. You set this value in the Security Groups application.
9. If necessary, click **New Row** again to specify additional groups.
10. In the Update User Defaults section, select the **Edit?** check box above a field to make the field editable. Type new defaults as needed.
11. Click **OK** to display the number of records that have been updated.

Security Controls action

Use the **Security Controls** action to specify the following defaults for new user records:

- ▶ Default security group for new users: New users are automatically assigned to a security group, which defines their security permissions until they are assigned to additional groups. The default group is DEFLTREG. The permissions for this group are limited to access to the Start Center and permission for the user to change their own password.
- ▶ Default status for new user records: The default status is NEWREG. This status allows you to search for new user records, or to route them into a Workflow process.
- ▶ Group for all users: The default security group for global permissions is EVERYONE. When you select **Group for All Users** in Security Controls, the user is added to EVERYONE.
- ▶ Electronic signature dialog: When you select **Display User ID in the Electronic Signature Dialog?** in Security Controls, the system displays the user ID in the dialog box, and prompts the user to enter their password.

You can access the **Security Controls** action from either the Security Groups or the Users applications.

To set new user defaults:

1. From the Select Action menu, select **Security Controls**. The Security Controls dialog box opens.
2. In the User Defaults section, specify the following defaults:
 - In the **Default Group for New Users** field, enter the name of the group or click **Detail Menu** to select an option and retrieve a group.
 - In the **Initial Self-Registered User Status** field, enter a user status or click **Select Value**.
 - In the **Group for All Users** field, enter the group for global permissions (the default is EVERYONE) or click **Detail Menu** to select an option and retrieve a group.

- Select the **Display User ID in the Electronic Signature Dialog?** check box to display the user ID in the dialog box when the system prompts users to enter their password.

Note: If you implement electronic signatures, you must enable Login Tracking.

3. Click **OK**.

Note: If implementation uses an application server to authenticate with an external directory (via LDAP), you cannot use the system to perform some functions. These functions include:

- ▶ Self registration: This function is not supported in conjunction with an external directory.
- ▶ Setting or changing passwords and password hints: All password-related functions are managed by the directory.

5.3 Setting up authentication

Tivoli process automation engine can use two different types of authentication: LDAP (Lightweight Directory Access Protocol) and native authentication.

5.3.1 LDAP authentication

You can authenticate users against LDAP using Microsoft Active Directory. If your organization has Virtual Member Management (VMM) in place, consider using it to perform your authentication.

When you configure the application server to authenticate against an Active Directory, you create and manage users in the LDAP directory server. The VMM cron task updates the Maximo database when users, groups, and group membership are changed in the directory server. When users and groups are deleted from the Active Directory, they are not deleted from the Maximo database because these records might be needed for auditing purposes.

You can also configure the system to populate person, user, and group information from the external directory. The system currently supports synchronization of information from Microsoft Active Directory.

Synchronization with other directories is possible, but is not supported as a standard feature and might require programming to configure.

5.3.2 Native authentication

You can use the native authentication provided with the system to authenticate users and verify their identity and security authorizations.

A user types a login ID and password in the Welcome page. The security functions validate whether the user ID and password exist in the database. The user is granted access to applications, actions, and data based on the security groups with which their user ID is associated.

In addition, when the security services load at system startup, they perform the following actions:

- ▶ Verify if Login ID is blocked or inactive
- ▶ Authenticate Login ID and update password history (if configured)
- ▶ Establish the user's default insert Site, Organization, and Person ID
- ▶ Establish the user's language, locale, time zone, and Start Center ID
- ▶ Route any Workflow assignments to the user's inbox (if Workflow processes are enabled)

The following procedure is the most common way to authenticate application access:

1. At the Web client login screen, users type a login ID (in the User Name field) and password.
2. Security services validate users' credentials against the Maximo database. This validation uses Java encryption to check the user in the Maximo schema/database.
3. The system checks users' security profiles. Based on the authorizations that they contain, the system grants users access to the applications.

5.3.3 Application server authentication

You can use application server security with an external authentication mechanism such as LDAP to authenticate users. LDAP is a set of protocols to access information directories.

The system uses application server security with an external authentication mechanism. System installation enables WebSphere Application Server security by default.

Depending on the product offering, application server security might be enabled by default.

The system is built using J2EE technology, which requires a commercial application server. The system uses WebSphere Application Server or WebLogic Server.

5.4 Conditional security overview

You can configure the system to meet different user requirements. The system provides a function that enhances the user interface and gives access to data based on user groups, by evaluating of one or more conditions.

In the system, you can use data restrictions to limit access to the data, to hide entire records, or to make them read-only. You can also create data restrictions at the attribute level and make them hidden or read-only when required. Because these data restrictions exist at the data level, they apply to any user interface element or application that uses an object or attribute.

The following information can help you determine the best place to create the restrictions:

- ▶ Data restrictions always take precedence over application configurations in the Application Designer application. For example, if an attribute has a data restriction that makes it read-only, the Application Designer application can never make that attribute editable. The hierarchy is:
 - Database configuration
 - Data restriction
 - Application Designer application
- ▶ Configurations that you create with data restrictions apply everywhere an attribute is used, while Application Designer configurations does not. For example, consider that you want to restrict access to a field that appears in the header section of multiple tabs. If you put a data restriction on the attribute, all of the fields inherit the restriction. If you configure the same restriction in the Application Designer application, apply the same configuration to each field on each tab.
- ▶ Configurations using Application Designer are always for one application. Configurations that use data restrictions can apply either to all applications that use the object/attribute or to one specific application.

5.4.1 Conditional Expression Manager

The system has a *condition library*. Within this library, a user can define conditions, either as expressions or as custom class files that you can use to drive application behavior. You can use conditions within the library for conditional option access, data restrictions, and conditional user interface. The expressions for these conditions use a syntax that is like SQL, but that uses bind variables for reusability.

Note: Conditional User Interface allows customers/administrators to change the information required within a given application based on conditions within the record set. Based on the type of asset, for example, additional fields can become required. Another example might include removing fields from the screen based on nearly any asset attribute or condition.

The *Conditional Expression Manager application* facilitates the management of these conditions. You can use the Conditional Expression Manager application to define conditions used in data restrictions and elsewhere in the system. Using this application, you can create and maintain a library of conditions.

When an expression evaluates to true, conditions let you configure access to fields, tabs, and other user interface controls within applications. For example, you can set the following types of conditional access:

- ▶ Give read-only access to information displayed in a field.
- ▶ Give read-write access to information displayed in a field.
- ▶ Give a user group read-only access to a specific field in an application.
- ▶ Give all members of a user group read-write access to a specific application.
- ▶ Do not display a field or tab in an application to certain users.

You can also set access to application options, controls, or data elements.

Examples include:

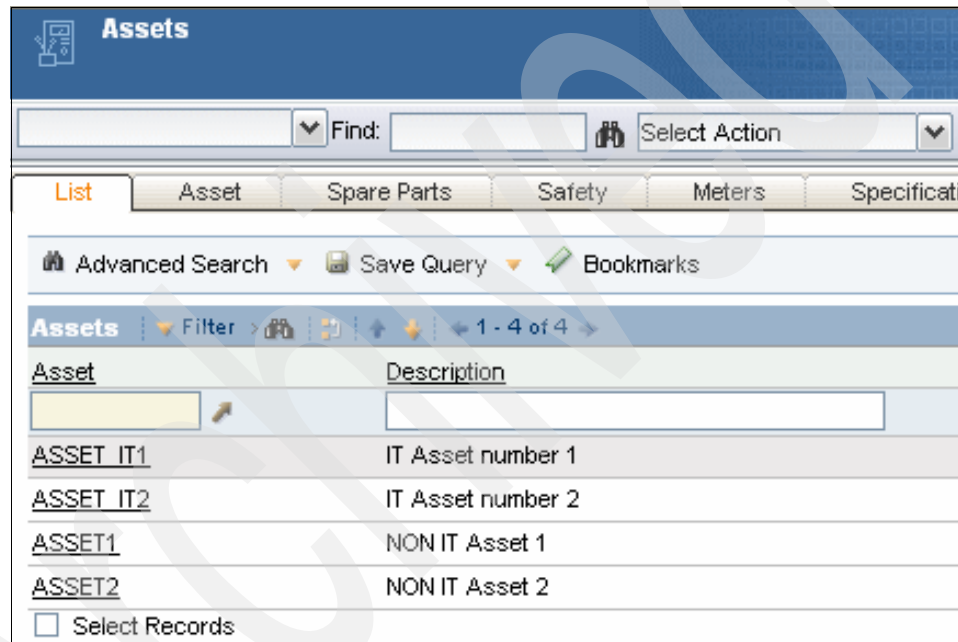
- ▶ Grant access to application options in the Select Action menu for a security group
- ▶ Configure any property in a control for a group, such as making a control hidden, masked, read-only, or required
- ▶ Configure other properties, such as color, label, and application link, to differ according to group and different conditions
- ▶ Show or hide a data attribute globally or for a security group

Creating and using a Conditional Expression

You use the Conditional Expression Manager application to define conditions used in data restrictions. The system uses a syntax like SQL. However, the syntax of the system uses additional variables.

You can create a condition in the Conditional Expression Manager application. In the following example we illustrate the behavior of an application using the Conditional Expression Manager function. We only allow the assets of type *IT* to be listed in the Asset application.

The current asset list looks as shown in Figure 5-23.



The screenshot shows a web application titled "Assets". It features a search bar with a "Find:" label and a "Select Action" dropdown. Below the search bar are tabs for "List", "Asset", "Spare Parts", "Safety", "Meters", and "Specifications". The "List" tab is active. Below the tabs are links for "Advanced Search", "Save Query", and "Bookmarks". A "Filter" dropdown is set to "Assets", and a pagination indicator shows "1 - 4 of 4". The main content is a table with two columns: "Asset" and "Description". The table contains four rows of data. Below the table is a checkbox labeled "Select Records".

Asset	Description
ASSET IT1	IT Asset number 1
ASSET IT2	IT Asset number 2
ASSET1	NON IT Asset 1
ASSET2	NON IT Asset 2

Figure 5-23 Assets list

To create a condition:

1. In the Conditional Expression Manager application, All Conditions table window, click **New Row**. The Row Details pane opens. For our example we have used the following:
 - Object = :assettype = 'IT'
 - Description = Asset type is IT
 - Type = Expression
 - Expression = :assettype = 'IT'

2. Type a value in the **Condition** field. By default, the condition is assigned a number. You can, however, modify this field. See Figure 5-24 on page 111.
3. Type text in the **Description** field.
4. In the **Type** field, specify a value or click **Select Value** to choose a type.
5. In the **Expression** field, click **SQL Expression Builder** to build a condition. The SQL Expression Builder dialog box opens.

Note: The value that you specified in the Type field determines whether you can edit the field or if it is read-only. If you selected **Class** in the Type field, the Expression field is read-only. If you specified **Expression** in the Type field, then you can edit the Expression field.

6. Enter a file name in the **Class** field. The file must be in a folder under the root of the product installation.

The screenshot shows the 'Conditional Expression Manager' window. At the top, there's a 'Select Action' dropdown. Below it, a table lists conditions. The first condition is selected, showing its details in a lower pane.

Condition	Description	Type	Reference Count
ITASSET	Asset type is IT	EXPRESSION	1

The details pane for the selected condition shows:

- Condition: ITASSET
- Type: EXPRESSION
- Expression: 'ASSETTYPE = "IT"'
- Class: (empty field)
- Reference Count: 1

Figure 5-24 Conditional Expression Manager

Note: The value that you specified in the Type field determines whether you can edit the Class field or if it is read-only. If you selected **Expression** in the Type field, the Class field is read-only. If you specified **Class** in the Type field, then you can edit the Class field.

7. Click **Save Condition Expression**.

Note: The **Reference Count** field is not editable. The value in this field automatically increments when the condition is specified in another application.

8. Go to **Security Groups**.

9. On the Object Restrictions sub-tab, select **New Row** to create a new data restriction.
- Object = ASSET
 - Application = Null
 - Type = Qualified
 - Reevaluate = checked (this is the default)
 - Condition = ITASSET (This is the conditional expression created previously.) See Figure 5-25 on page 112.

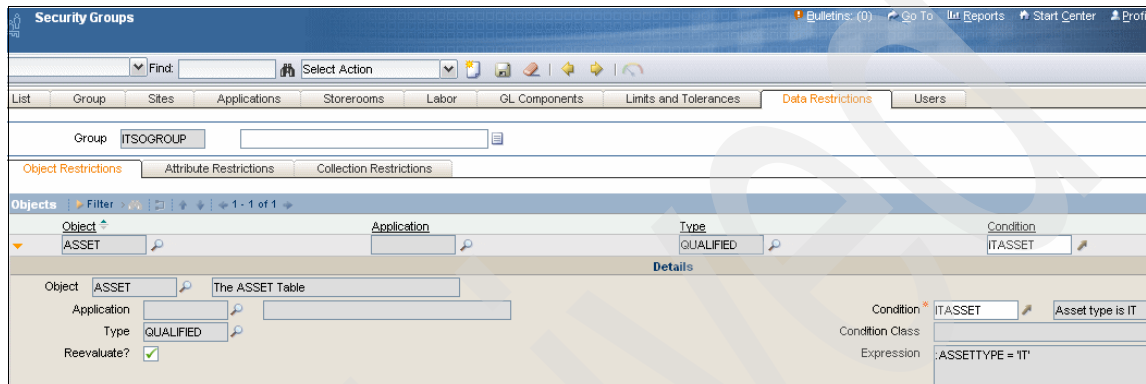


Figure 5-25 Conditional UI for security groups

10. Log out, then log in again as the user in the security group this restriction applies to. Only “IT Assets” will be displayed, as shown in Figure 5-26.

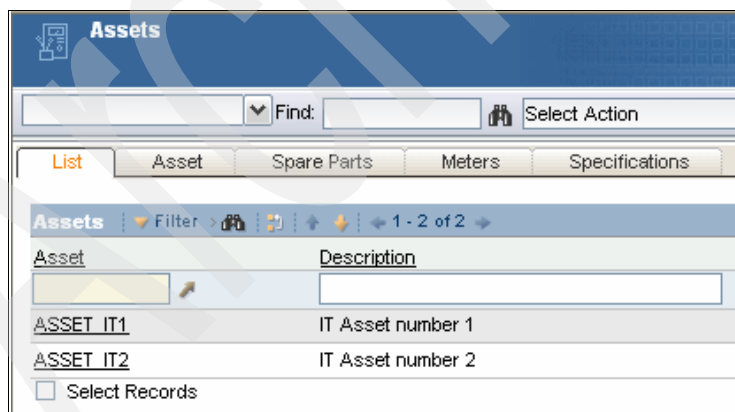


Figure 5-26 Conditional expression list

Creating a Signature Option

In the following example we use the Signature Option to modify the look of the Asset application by showing and hiding the Safety tab based on the security groups.

To create a SIGOPTION proceed as follows:

1. Go to **Application Designer** and open the application.
2. Create a SIGOPTION called **SAFTAB** with the description **Safety Tab**.
3. Navigate to the **Safety Tab** of Assets.
4. Open the control properties dialog and add SAFTAB signature option to the control. See Figure 5-27.

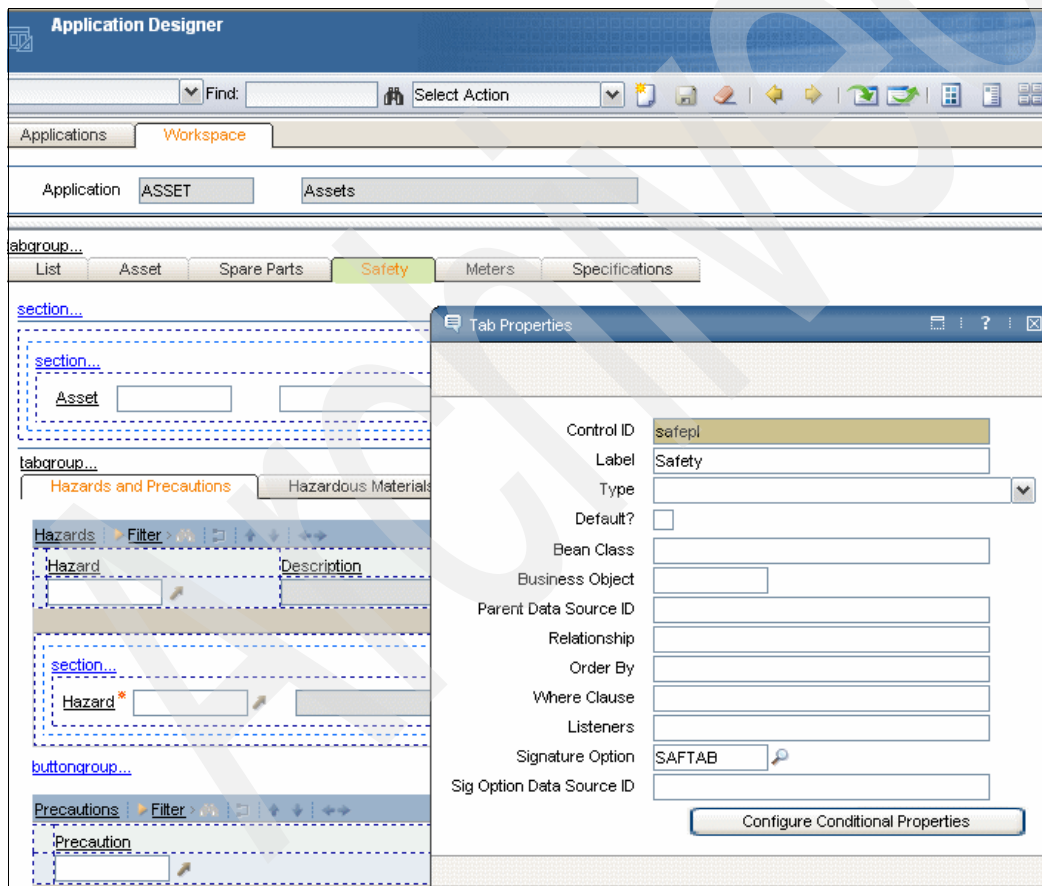


Figure 5-27 Signature option

5. Go to **Security Groups**.

6. Find the security group you are intending to use, then go to the **Applications** tab.
7. Select **Asset** application.
8. Find the Safety tab option and Grant it. See Figure 5-28 on page 114.

Security Groups

Find: Select Action:

List Group Sites **Applications** Storerooms Labor GL Components Limits and Tolerances Data Restrict

Group: ITSOGROUP

Applications Filter: 1 - 10 of 153

Description	Main Object/Table
Actions	Table to hold actions.
Activities and Tasks	The WOACTIVITY view.
Actual Configuration Items	Actual CI Table
Adapter Conversion	Deployed Assets Adapter Conversion Target
Application Designer	The MAXAPPS Table
Asset Link Results	Asset Link Result view.
Asset Reconciliation Results	Asset Result of Link and/or Comparison
Assets	The ASSET Table
Assignment Manager	The ASSIGNMENT Table
Bulletin Board	Table to store and maintain bulletin mes

Options for Assets Filter: 1 - 4 of 4

Description	Grant Access?
Delete Asset	<input checked="" type="checkbox"/>
New Asset	<input checked="" type="checkbox"/>
Read access to Asset	<input checked="" type="checkbox"/>
Save Asset	<input checked="" type="checkbox"/>

Filter: 1 - 2 of 2

Description	Grant Access?
SAfety Tab	<input checked="" type="checkbox"/>
Save Current Query	<input type="checkbox"/>

Details

Description: SAfety Tab

Grant Access? ☒

Condition:

Type:

Expression:

Figure 5-28 Security Groups for SIGOPTION

9. Log out, then log in as the user belonging to the security group to whom the condition applies. You will notice that the safety tab does not display, as shown in Figure 5-29 on page 115.

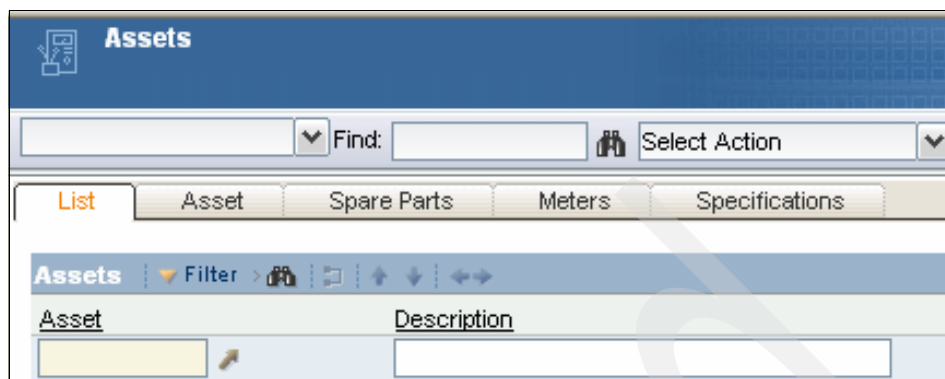


Figure 5-29 Sigoption for Asset tab

Archived

Migration configuration

This chapter provides some basic guidelines for using the Integration Framework for data exchange with external systems, and also discusses the Migration Manager application. The functionality described in this chapter is in the context of the Certification Test; for more detailed information refer to the *Migration Manager Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic=/com.ibm.ccmb.doc_7.1.1/ccmb_welcome.htm

This chapter covers the following topics:

- ▶ Integration Framework
- ▶ Basic integration configuration
- ▶ Migration Manager

6.1 Integration Framework

The Integration Framework includes the Maximo adapters that are part of IBM Tivoli process automation engine and are provided with IBM Tivoli Maximo Asset Management, IBM Tivoli Change and Configuration Management Database (CCMDB), IBM Tivoli Service Request Manager (SRM), and IBM Tivoli Asset Management for IT (TAMIT).

Furthermore, IBM provides additional add-on adapters to Maximo Asset Management for Oracle® and SAP® applications, which can be implemented within the Integration Framework. This add-on to Maximo provides an end-to-end integration solution, thus enabling business to more quickly and easily connect Maximo Asset Management to their Oracle or SAP suite and leverage approved integration tools and processes on both ends.

The different components of an Integration Framework solution can be arranged in a layered “stack” in a way that each layer builds on the layers below. The *object structure* is the basis for applications and adapters to communicate. It is used to define message content encapsulating business objects. The processing layers operate on top of the object structure to transform and standardize messages between Maximo data exchange format and an external system’s data exchange format.

The Integration Framework, as shown in Figure 6-1 on page 119, comes with advanced integration functionality, including:

- ▶ A real-time engine for real-time inbound Web services queries.
- ▶ Synchronous and asynchronous Java Message Service (JMS) based message exchange.
- ▶ Ability to build, transform, and customize message content.
- ▶ Means to configure, predefine, and create new integration definitions based on Maximo’s out of the box pre-configured integration contents:
 - Object structures
 - Publish channels
 - Enterprise services
 - External system (EXTSYS1)
 - Adapter (MAXIMO)
 - Endpoints
- ▶ Defining and managing multiple integration triggers, message formats (XML Flat File, Integration Table), and systems.

- ▶ Real-time user notifications and alerts on integration issues.
- ▶ Rules-based message processing and routing through a *rules engine*. The rule processor can act on message values, destination, and sending system processing rules.
- ▶ Running as a native Maximo application server component for tighter alignment with enterprise service bus architecture and better performance (see Figure 6-1).

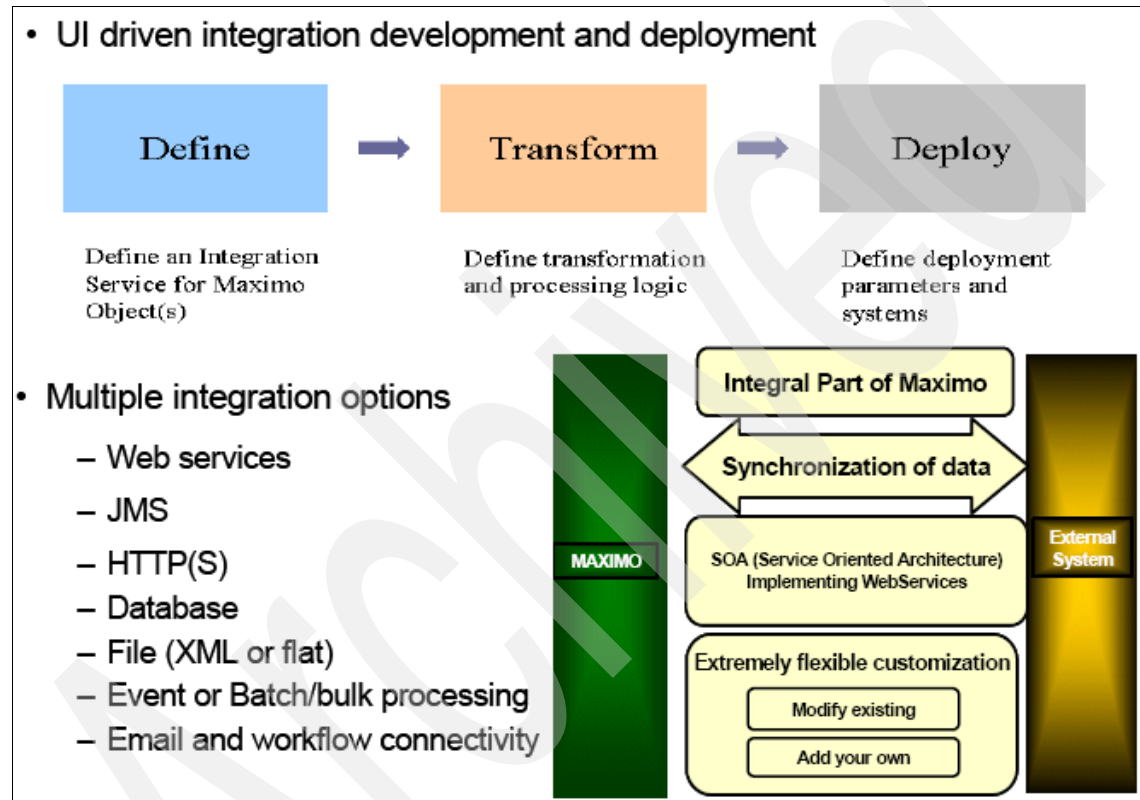


Figure 6-1 Integration Framework overview

6.2 Basic integration configuration

Basic configuration tasks involve:

- ▶ Validating system properties
- ▶ Validating queue and cron setup
- ▶ Validating Web Services/Schema setup

► Validating Security setup

We briefly go through the options available in the Integration module. To view these options click **Go To** → **Integration** (Figure 6-2).

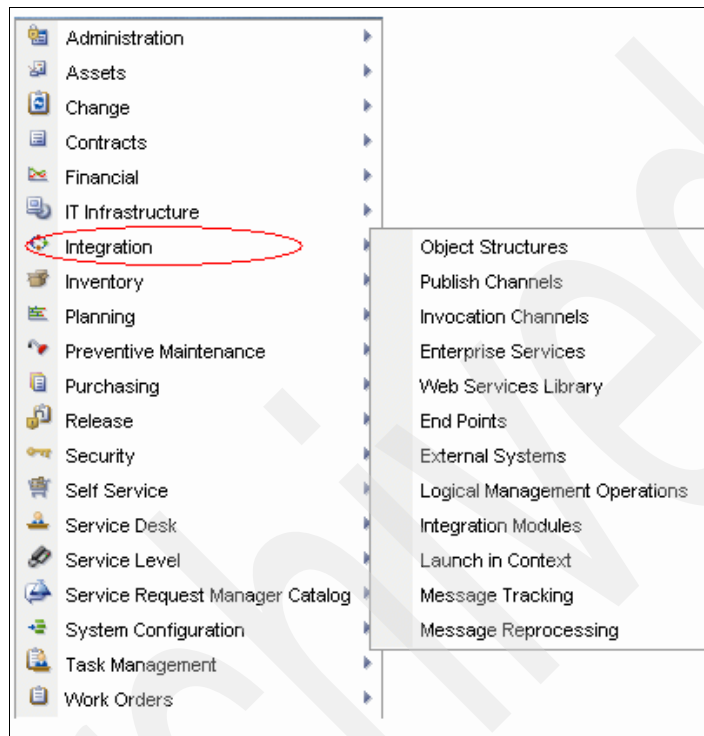


Figure 6-2 Integration module

6.2.1 Object structures

The object structure is the building block of the Integration Framework that lets integration applications perform the following functions:

- Publish and query application data
- Add, update, and delete application data via the following operations:
 - Sync
 - Create
 - Update
 - Delete
 - Query
- Import and export application data

Each Integration Object can include any or all of these data types:

- ▶ Persistent
- ▶ Non-Persistent
- ▶ User-defined field

The product includes various pre-defined object structures out of the box, to facilitate the development of integration contents. In creating object structures, instead of having to create new components, you can duplicate and use the existing ones.

Configuring object structures

Use the Object Structure tab in the Object Structures application (**Go To** → **Integration** → **Object Structures**) to perform the following configuration activities:

1. Create an object structure.
2. Add the system objects to the object structure.
3. Assign the processing classes (inbound or outbound) to the object structure.
4. Specify whether the object structure supports a flat file representation.
5. Restrict object structure supported operations to QUERY.
6. Use the **Select Action** menu in the Object Structures application to perform the following configuration activities:
 - a. Configure the column aliases to resolve alias conflicts in the object structure.
 - b. Include and exclude the system object columns from the object structure.

6.2.2 Publish channels

Publish channels are used to create and manage asynchronous outbound data flow from the integration framework to an external system (see Figure 6-3 on page 122).

The publish channel provides the Integration Framework to:

- ▶ Transform object structures to service input
- ▶ Associate an End Point
- ▶ Transform service response to object structures

Events that initiate publish channel processing are:

- ▶ Object events (insert, update, and delete)

- ▶ Application-initiated calls
- ▶ Data export.

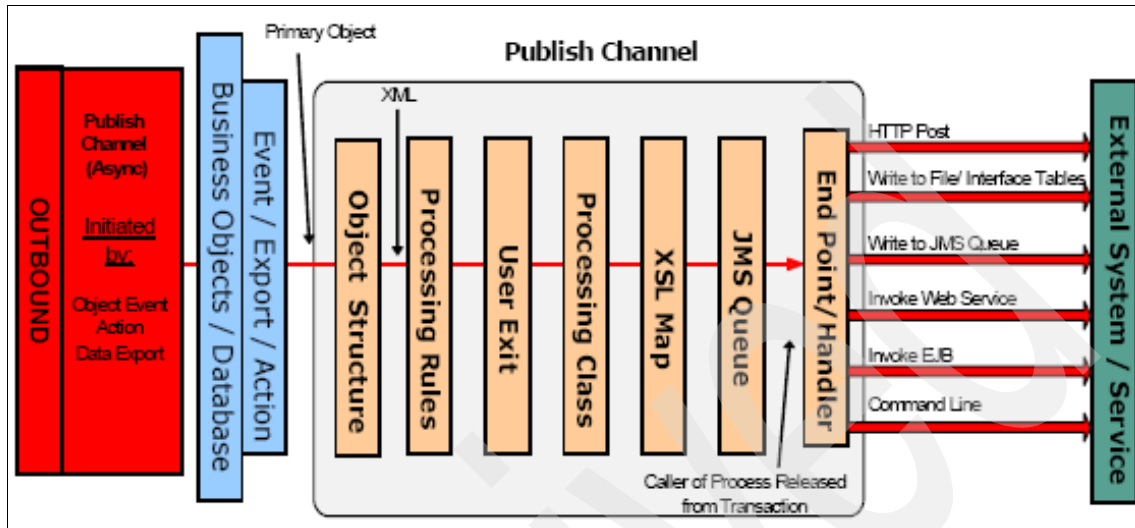


Figure 6-3 Publish channels

The publish channel can use the following processing layers to map the XML to the external system XML:

- ▶ Processing class
- ▶ User exit class
- ▶ XSL map file

The publish channel can apply any specified processing rules to objects before it saves the objects. Processing rules are used to access and retrieve pertinent data from objects that are not included in the object structure.

You can override the behavior of predefined data processing that the enterprise service supports through the integration controls. This integration control behavior is implemented through enterprise service processing rules and Java processing classes.

6.2.3 Invocation channels

The *Invocation Channels application* is used to create and manage synchronous (does not go through the outbound queue) outbound data flow from the Integration Framework to an external system (Figure 6-4 on page 123). The

invocation channels application is similar to publish channels, but it is initiated via a Custom Action Class (Java).

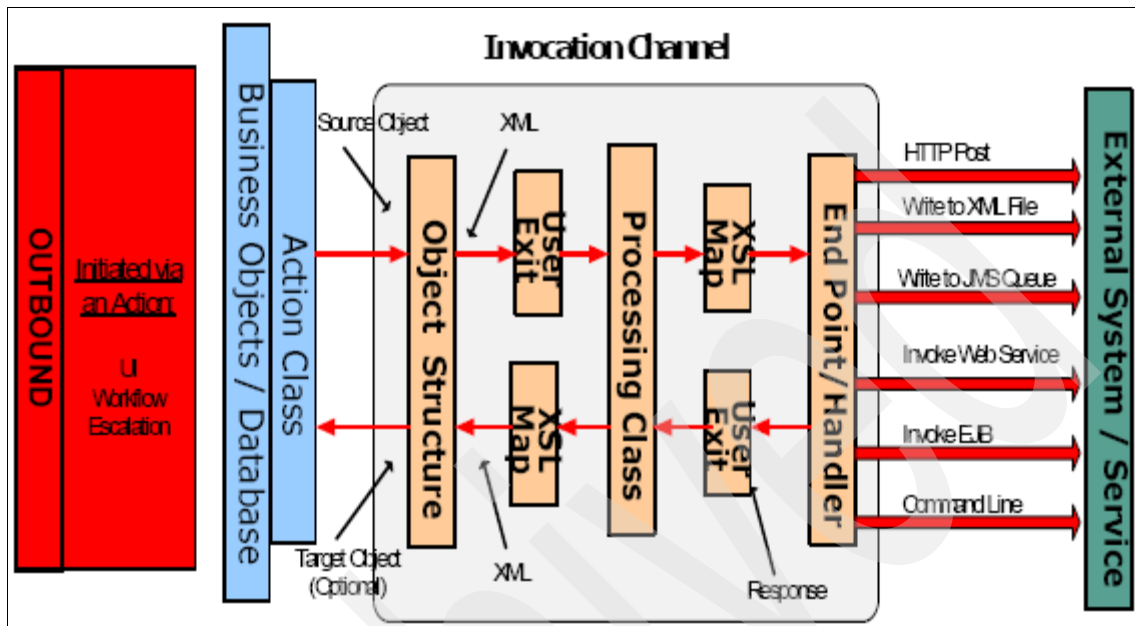


Figure 6-4 Invocation channels

6.2.4 Enterprise services

Use the *Enterprise Services application* to create, view, modify, or delete enterprise service records.

An enterprise service is the pipeline for importing data to the integration framework from an external system. Enterprise services processing can be triggered by the following system events (event-driven) or user actions (user-driven):

- ▶ Scheduled cron tasks
- ▶ User initiated queries
- ▶ Data Import

The content of an enterprise service data structure is based on the content of the associated object structure. When you trigger enterprise service processing, the system moves the integration framework message data into the inbound queue.

If necessary, you can use the object structure processing rules to define conditions under which the integration framework can skip or stop a message.

When you use processing rules, you also can change data in the enterprise service, before the creation of the objects. You can accomplish this task without having to use Java class files.

You also can alter the logic of predefined inbound processing, inbound channel mapping, and event filtering through the use of Java class files. These alterations are specific to the enterprise service record and overwrite any predefined processing logic you define at the object structure level.

The Enterprise Service application contains the following tabs:

- ▶ **List:** To search for enterprise service records.
- ▶ **Enterprise Service:** To add, view, modify, or delete enterprise service records.

6.2.5 External systems

External systems let you synchronize inbound and outbound data through the enterprise services and publish channels, respectively.

6.2.6 Endpoints

Outbound transactions (publish channels or invocation channels) for your business processes need endpoint values. The endpoints specify how the transactions are delivered and the handler that will route the transactions to the endpoint.

6.2.7 Importing data

The following steps describe the inbound process that uses the data import feature. Before importing data, be sure to cross check all fields and data for validity.

1. The Integration Framework checks that the external system and the enterprise service are valid and enabled. If you are importing flat files, the integration framework also checks that the enterprise service object structure supports flat structures. If the verification fails, the integration framework issues an error and does not process the message.
2. If the verification is successful, the integration framework identifies the inbound JMS queue that is assigned to the enterprise service and the external system.
3. The integration framework writes the message to the inbound queue. If the message contains multiple instances of a document, for example, if a single

message contains 10 person records, the application writes 10 messages to the queue. If one of the referred records has a processing error, a single message processing exception is identified and none of the other messages that can be successfully processed are committed to the database.

4. The integration framework updates the message header with the external system and enterprise service names. You have the option to preview the data that you want to import to check the format and the data validity of a source file. It is a synchronous validation mechanism that presents all the source file processing errors without committing data to the database.

The preview data process verifies that the data structure of the selected file complies with the integration XML or flat file definitions.

6.2.8 Integration Framework summary

With the Integration Framework platform, you can connect Maximo with other external systems using different integration mediums such as: file systems, databases, message queues, and Web services. This allows for bidirectional synchronous and asynchronous data exchange more easily and effectively. Another benefit of Integration Framework is the vast array of pre-defined out of the box integration libraries that support various integration scenarios between Maximo and external systems, thus allowing for quicker implementation with less complex integration procedures.

The Integration Framework is used to create and manage integration modules. The Integration Modules application provides a mechanism for a process management product, such as a Change or Release, to call an external operational management product.

6.3 Migration Manager

In the context of Migration Manager, *migration* is the process of promoting product configuration content from one product environment to another. *Configuration content* is the data that the system requires to construct and run a business application in the application server and make it available to end users in the enterprise. Product environments can include development, test, and production.

For example, you might want to extend the Purchase Order application by making the following configuration changes:

- Add a new table and several columns to the database (using the Database Configuration application)

- ▶ Add a new domain that contains several lookup values (using the Domains application)
- ▶ Add a new tab in the Purchase Order application screen presentation (using the Application Designer application)
- ▶ Develop a workflow process to automate an approval of data managed through the new table (using the Workflow Designer application)

All of these configuration changes are product configurations that are typically created in a development environment and promoted to production.

6.3.1 Overview

Migration Manager is a set of applications that enables a structured series of steps to promote your configurations from one product environment to another.

You can use the Migration Manager to perform the following tasks:

- ▶ Organize and consolidate all the configurations and customizations for a new product environment
- ▶ Promote your configurations from a development environment to a test environment for validation
- ▶ Promote your validated configurations from a test environment to a production environment

6.3.2 Migration Manager concepts and components

In this section we discuss Migration Manager concepts and components.

Package definitions and packages

You manage the configuration content that you want to migrate in the form of package definitions and packages. This configuration data that you have grouped together will constitute the configuration data in the form of a package. A *package* is an instance of a package definition. A *package definition* serves as a template from which you create unique packages. A package definition organizes the content to be migrated.

A package contains data either from the product database or from files that are deployed on the application server. Data from the product database is organized in migration objects and migration groups. Files are organized as compiled sources.

Note: The *batch size* of a package is the number of records that are retrieved at one time from each object in a migration group. The default value is 100.

Package contents

A package contains the following:

- ▶ Package manifest - Contains important information about a package, such as the source environment versions, the migration objects whose data is included in the package, the types of content in the package, the record count for each migration object, and README information entered in the source environment by an administrator to help during deployment to a target environment.
- ▶ Package metadata - Defines metadata information that pertains to the package definition of the package to be deployed in a target environment.
- ▶ Structural configuration content - Data that must be used to create or update database tables, columns, views, keys, indexes, and sequences.
- ▶ Non-structural configuration content - Configuration content that resides in the form of records of various configuration tables.
- ▶ Compiled sources - Files that include source code customizations, libraries, configuration files, and report executable files.
- ▶ History data - Life cycle information regarding the package.

Types of package definitions and packages

There are two types of package definitions and packages:

- ▶ Snapshot™ package
- ▶ Change package

A *snapshot package* contains “as is” configuration content collected for a package on demand. You define the snapshot package at any time, even after the configuration changes have been made.

A *change package* contains configuration content collected over a period of time. The data collected is based on database inserts, updates, and deletes that occur between the time you activate the package definition and the time that you create the package. A change package can contain configuration records inserted, updated, or deleted by designated users. You define the change package before the changes occur.

6.3.3 Migration objects and migration groups

Configuration content is organized into migration objects and migration groups.

Migration objects

A migration object is a group of one or more related business objects that represents one or more database tables (for example, workflow process, action, role). You define migration objects in a development instance and then move them into test and production environments. The product includes a comprehensive set of migration objects. Migration objects are implemented using the Object Structures application. You can also create your own migration objects using this application.

Migration groups

A migration group is a collection of related migration objects. It allows one to organize and group configuration content that will need to be migrated. A migration group can be either internal or user-defined. Internal migration groups are included with the product and are linked to other logically related migration groups called dependencies. You cannot modify internal migration groups. User-defined migration groups are migration groups that you create.

Note: You can select which Migration Groups are to be migrated.

6.3.4 Compiled sources

You can include compiled sources in a package definition.

Compiled sources define content from outside the database that packages contain when they are migrated. Compiled sources are files that must be part of the Enterprise Archive (EAR) file of the product. They can include many types of files, such as class files, archive files, image files, and properties files. They can also be aggregations of files from the server file system that must be migrated with configuration data from the database.

If you need to migrate multiple compiled source files, aggregate them into a single compressed file to simplify the migration process.

Sources and target environments

The environment from which you are migrating content is the source environment. The environment to which you are migrating content is the target environment. Migration Manager identifies sources and targets uniquely across all of your product environments. Migration Manager generates this identification

in the form of a string comprising three parts. The identification is the combination of the database host name, the database identifier, and the database schema name.

A package definition can be associated with any target. However, you can set inbound restrictions in a target environment to prevent the distribution and deployment of packages to that environment from restricted sources.

6.3.5 Migration Manager applications

Migration Manager consists of the following three applications. These applications are in the Migration module, which is in the System Configuration module of the product:

- ▶ Object Structures
- ▶ Migration Groups
- ▶ Migration Manager

Object Structures application

Use the *Object Structures application* (Figure 6-5) to view, create, and modify an object structure. One or more related *business objects* comprise an object structure. A business object is an object-relational representation that corresponds to a database table of the product. You can use the object structures that are included with the product, or you can create custom object structures to meet your business needs.

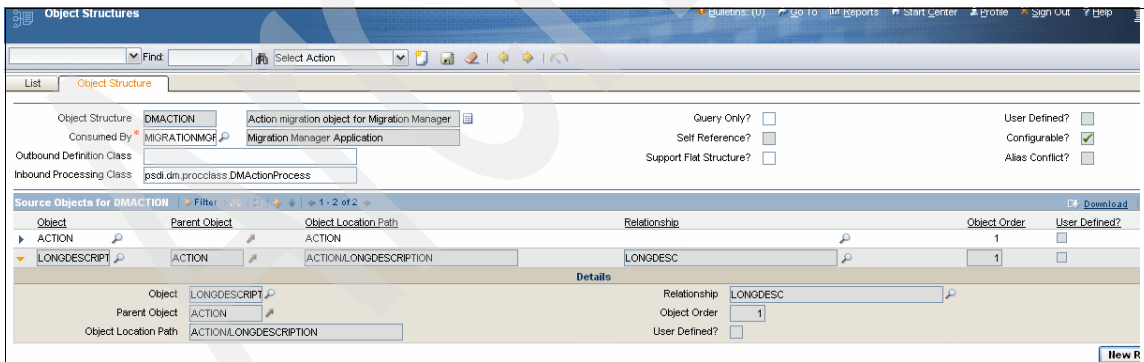


Figure 6-5 Object structure application

Migration Groups application

You use the *Migration Groups application* (Figure 6-6) to view, create, modify or delete a migration group. One or more migration objects (object structures)

comprise a migration group (Figure 6-7). You can include one or more migration groups in a package.

Each migration group can be linked to other related migration groups. This relationship between migration groups is called a *dependency*. A dependency ensures that all dependent configuration content is collected from source environments and distributed to target environments.

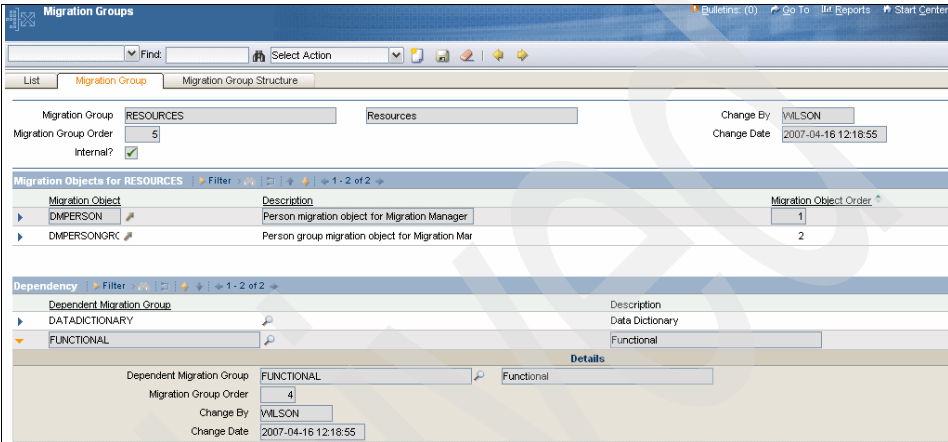


Figure 6-6 Migration groups application

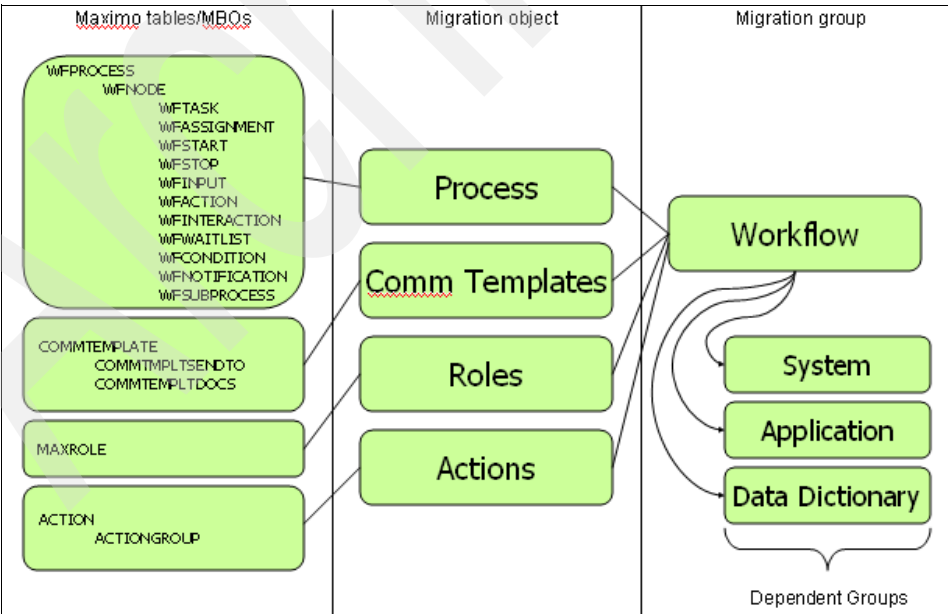


Figure 6-7 Content of a migration group

Migration Manager application

Use the *Migration Manager application*, shown in Figure 6-9 on page 132, to migrate your configuration content between product environments. Use this application in both your source and target environments. In a source environment, you define, create, and distribute packages. In a target environment, you deploy packages.

Specify the type when you create a package definition. Every package that is created from a package definition is of the same type as the package definition. Two types of packages can be defined in the Migration Manager application:

- ▶ Snapshot
- ▶ Change

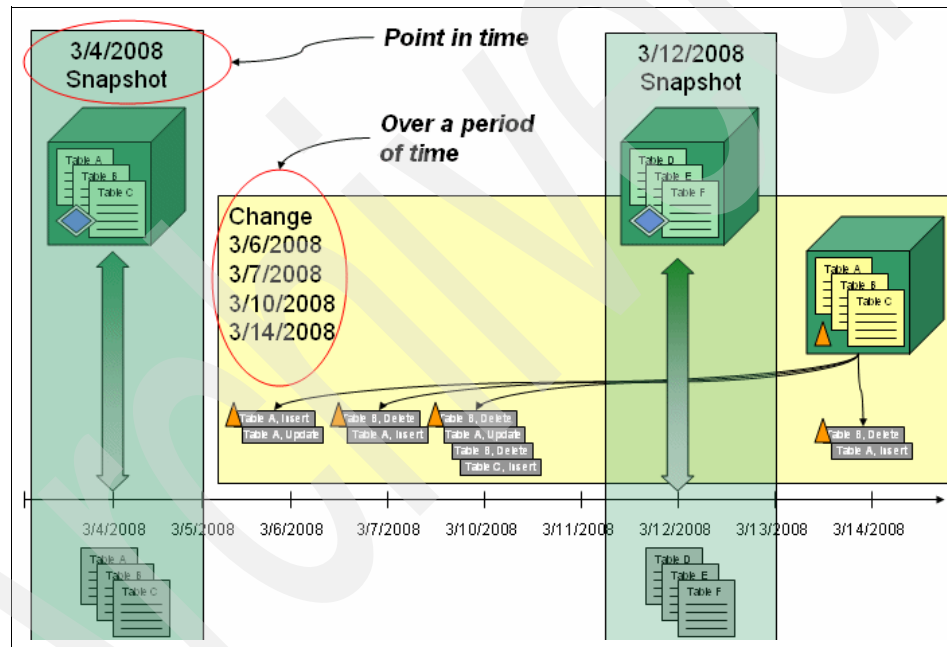


Figure 6-8 Types of packages

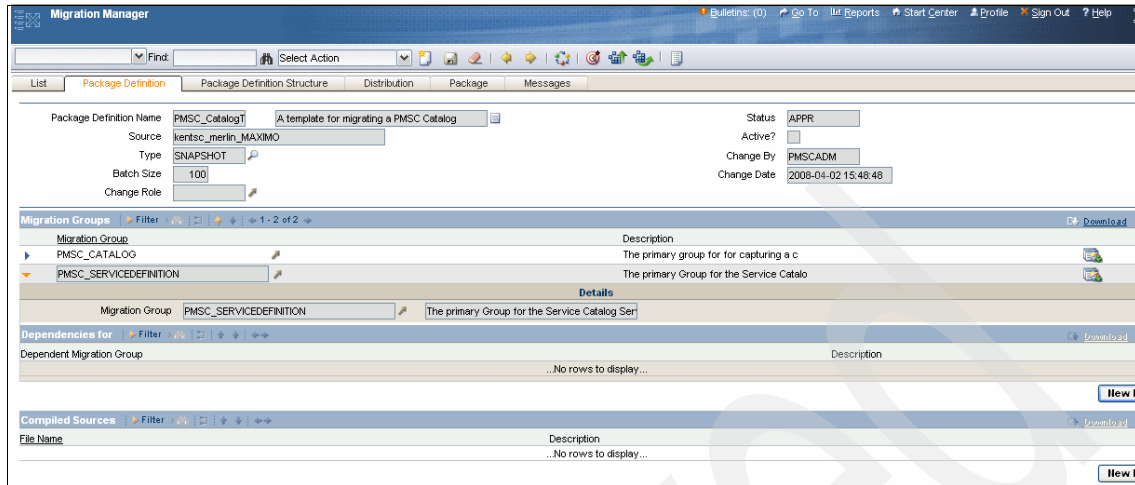


Figure 6-9 Migration Manager application

6.3.6 Migration planning

You need to determine the types of configuration changes. You will be organizing tasks by affected configuration applications, for example, you will be grouping all screen presentations tasks under the Application Designer application.

Another aspect of planning the migration is the organization of your configuration content. Configuration content can come from two types of sources:

- ▶ Content in the database
- ▶ Content outside the database

Note: Migration Manager gives you the flexibility to have all or a subset of your configurations defined, created, distributed, and deployed at one time.

6.3.7 Migration flow

You migrate the configuration content in four stages as depicted in Figure 6-10; the migration task flow is shown in Figure 6-11.

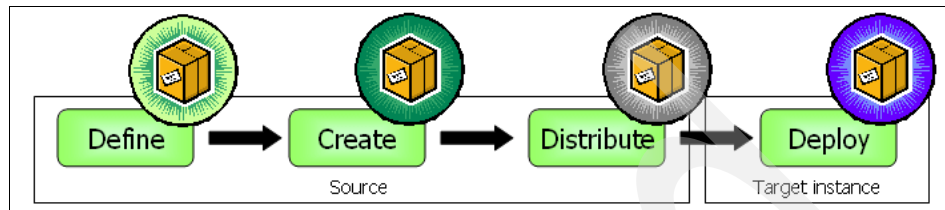


Figure 6-10 Migration process flow

Note: You can migrate configuration content between any two product environments.

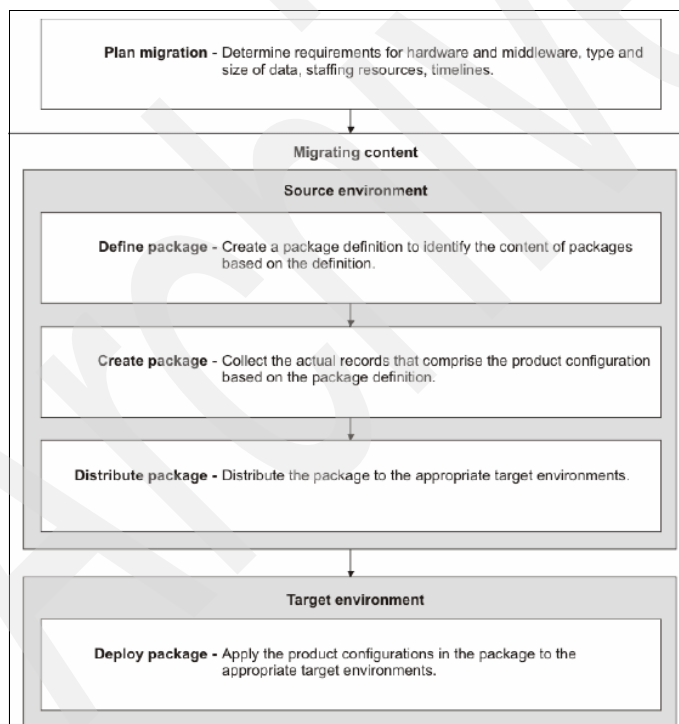


Figure 6-11 Migration task flow

Note: To preserve the integrity of structural changes, you can only deploy one package at a time.

6.3.8 Migration Manager summary

Use the Migration Manager application to migrate configuration content from one product environment to another. You manage the configuration content that you want to migrate in the form of package definitions and packages. As part of your implementation of a migration process, you use the Migration Manager application to define and create the package definitions, and then distribute and deploy the packages.

For example, you can migrate configuration from a development environment to a test environment. After testing, you can migrate the configuration to a production environment. The development environment is the source and the test and production environments are targets. You can use this approach during the initial configuration of the product or at any time when you want to change your configuration of the product.

Start Center configuration

This chapter provides details regarding the configuration and administration of the Start Center within Tivoli Process Automation Engine. Following the installation an administrator or privileged user can configure Start Centers to provide shortcuts to applications, quick inserts, and display data and key performance indicators within the portlets.

This section includes the following topics:

- ▶ Start Center templates
 - Start Center permissions
 - Creating a new Start Center template
 - Modifying an existing Start Center template
 - Modifying a portlet
 - Associating a Start Center template to a security group
- ▶ Key Performance Indicators
 - Creating a KPI
 - KPI Cron Task

7.1 Start Center templates

Start Center templates are configurable dashboards that provide easy access to the applications, result sets, and KPIs a user or administrator would be most likely to use.

7.1.1 Start Center permissions

Once the installation is complete and the system is populated with the necessary basic data, Start Center creation can begin.

Upon first login a user is not presented with a Start Center; one needs to be either be created or associated with their particular security group, as shown in Figure 7-1.

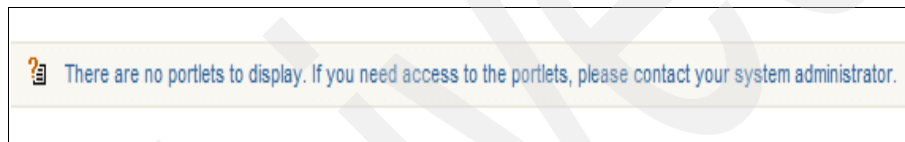


Figure 7-1 No Start Center to display

An Administrator such as maxadmin must access the security groups module to provide access to the appropriate groups, who will then be able to create and modify Start Centers.

To access security groups, select **Go To** → **Security** → **Security Groups**.

Select the group you would like to apply the permissions to from the List tab and then select the Applications tab to apply permissions for layout and configuration as well as the necessary Start Center portlets.

The following are the security group applications or, as referred to within the Start Center, *portlets* associated with Start Center configuration:

- ▶ Layout and Configuration - Administrator users can modify and configure the layout of the portlets display on the Start Center.
- ▶ Inbox/Assignments Setup - Administrators can define and edit which columns are displayed in the Workflow assignments inbox on the Start Center.
- ▶ KPI Graph Setup - Administrators can define and edit a KPI graph-style portlet to display on the Start Center.
- ▶ KPI List Setup - Administrators can define and edit a KPI list-style portlet to display on the Start Center.

- ▶ Result Set Setup - Administrators can define and edit the query used and columns displayed on the Start Center.
- ▶ Favorite Applications Setup - Administrators can define and edit the list of applications displayed in a Favorite Application portlet.
- ▶ Quick Insert - Administrators can define and edit the list of applications displayed in a Quick Insert portlet.
- ▶ Quick Insert Setup - Administrators can define and edit the list of applications in a Quick Insert portlet.
- ▶ Bulletin Board - View messages from the Maximo system.

7.1.2 Creating a new Start Center template



Figure 7-2 Layout and configuration options

Once provided with access to layout and configuration, the user will have the following options displayed on their Start Center upon login, as shown in Figure 7-2:

- ▶ Change Content/Layout - Use Change Content/Layout to add, remove, or to reconfigure the portlets displayed on your Start Center page.
- ▶ Display Settings - When you have more than one Start Center page available to you, the system displays tabs for each page. You can set which ones appear as tabs and which is the default.
- ▶ Create New Template - When you create a template, it must be assigned to a group before users in a group can access it.
- ▶ Modify Existing Template - If you have the Administrator permissions you can modify existing templates, even if you are not currently viewing that template.
- ▶ Update Start Center - If a system administrator notifies you that they have made changes to your Start Center template, you can update the Start Center page. When you update the Start Center page, you will lose any configurations that you made, for example, specific quick inserts or result sets. If you update the Start Center page and there are no changes to your original template, the latest changes you made to the Start Center are discarded. Also, the template on which the Start Center was originally based is reapplied.

Perform the following steps to create a new Start Center template:

1. Select **Create New Template**.

2. Select the desired layout (Narrow-Wide, Wide-Narrow or Equal Width).
3. Specify the portlets you would like to display in the appropriate left or right column section of the dialog box, as shown in Figure 7-3.

Layout * **Narrow-Wide**

Left Column Filter > 1 - 2 of 2

Portlet	Display Name
Favorite Applications	Favorite Applications
Quick Insert	Quick Insert

Right Column Filter > 1 - 3 of 3

Portlet	Display Name
KPI List	KPI List
Result Set	Result Set
Inbox / Assignments	Inbox / Assignments

Figure 7-3 Start Center Portlet Selection

4. Portlet ordering is configured as shown in Figure 7-4.

Download ?

Order

1

2

Select Content

Download ?

Order

1

2

3

Select Content

Finished Cancel

Figure 7-4 Start Center portlet ordering

7.1.3 Modifying a portlet

Once you have selected which portlets you would like to use in the Start Center, edit each one by selecting the **Edit portlet** icon as shown in Figure 7-5.

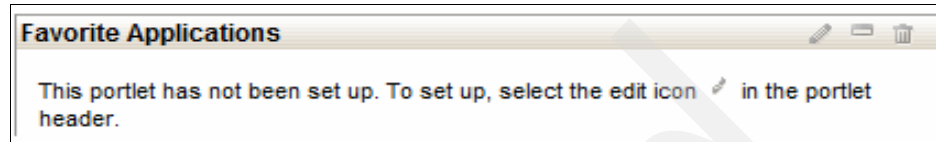


Figure 7-5 Start Center Edit portlet

Within each type of portlet there are several configurable options. For example, the Result Set portlet has the ability to select a user-defined or public query and then display its results with colored conditions on a bar or pie chart.

The following tabs are available within the Result Set setup:

- ▶ Available Queries - Lists all of the queries from which you can select one to display.
- ▶ Column Display - Select which columns to display and their order.
- ▶ Display Options - Set a color to indicate a status level.
- ▶ Chart Options - Set the parameters for a graph, if you choose to display one.

For example, if you would like to display all *NEW* work orders in the color red, configure the color parameters with an expression of *equal to*, an *expression value* of *NEW*, and a color of *red*, as shown in Figure 7-6.

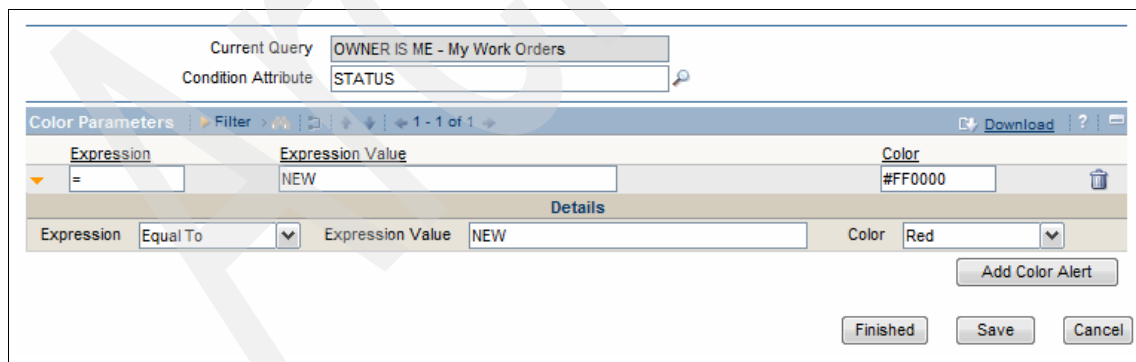


Figure 7-6 Result Set Setup Color Parameters

When the results are returned in the Start Center, those work orders with a status of *NEW* will be shown in the color red.

7.1.4 Modifying an existing Start Center template

With the appropriate security group permissions (layout and configuration) a user or Administrator can modify an existing Start Center template by selecting **Modify Existing Template**, as shown in Figure 7-7.



Figure 7-7 Start Center Modify Existing Template

1. You will be presented with the list of Start Centers you can modify, as shown in Figure 7-8.

The screenshot shows a window titled "Modify A Template". Inside, there is a table of "Start Center Templates". The table has three columns: "Start Center Template", "Description", and "Created On". There are 11 rows of templates, each with a red 'X' in the right margin. A "Filter" button and a "Download" button are at the top right of the table. A "Cancel" button is at the bottom right of the window.

Start Center Template	Description	Created On
Template-5	Administration	8/11/04
Template-36	Asset Manager	3/2/05
Template-8	Contracts	8/11/04
Template-39	Executives	8/22/07
Template-38	Finance	8/22/07
Template-37	HR	8/22/07
Template-12	Inventory	8/11/04
Template-2	Maintenance	3/2/05
Template-3	My Service Requests	8/11/04
Template-11	Operations Manager	8/11/04

Figure 7-8 Start Center Modify a Template

2. Select the Start Center you want to modify and make your changes.
3. Choose **Save Changes** to save your modifications.

7.1.5 Associating a Start Center template to a security group

Start Center template assignments are driven by the users security group. Select **Go to** → **Security** → **Security Groups** and then choose the appropriate group from the list tab.

You can then populate the Start Center template field and this will now be the default Start Center for that particular group, as shown in 7.2, “Key Performance Indicators” on page 142.

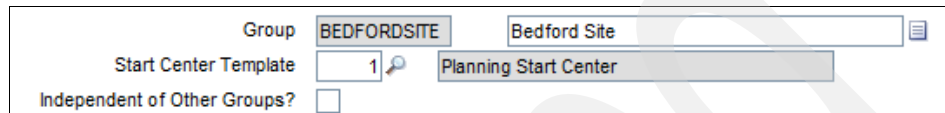
A screenshot of a web interface for configuring security groups. It features a 'Group' dropdown menu with 'BEDFORDSITE' selected, a text field containing 'Bedford Site', and a 'Start Center Template' dropdown with '1' selected. Below these is a checkbox labeled 'Independent of Other Groups?' which is unchecked. A 'Planning Start Center' button is also visible.

Figure 7-9 Start Center Security Group

If a user is part of multiple security groups, they will see a tabbed view of these Start Centers, as shown in Figure 7-10.


A screenshot of a tabbed interface with three tabs: 'Administration' (highlighted in orange), 'Inventory', and 'Process Management Requester'.

Figure 7-10 Multiple Start Center Templates

The user is able to navigate between their Start Centers and can also select to hide or set a particular Start Center as their user default by selecting **Display Settings**, as shown in Figure 7-11 and Figure 7-12 on page 142.

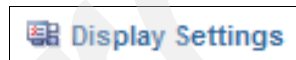


Figure 7-11 Start Center Display Settings Icon

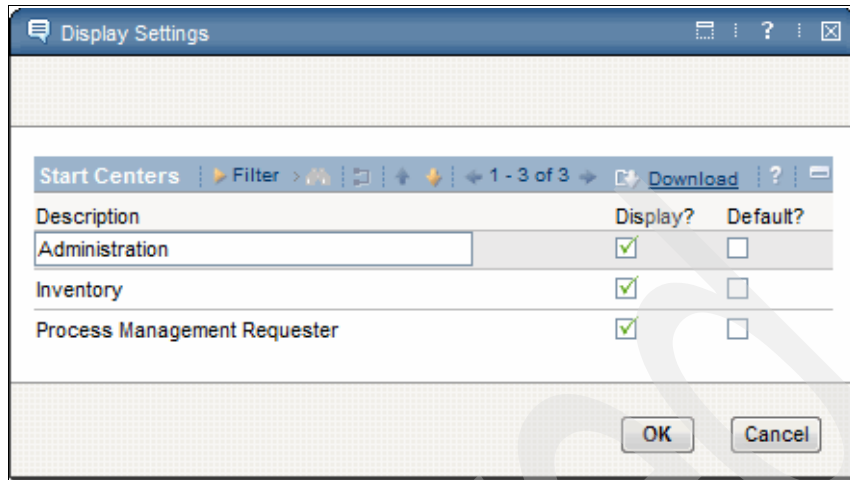


Figure 7-12 Display Settings

7.2 Key Performance Indicators

Key Performance Indicators (KPIs) provide the ability to track critical performance variables over time.

7.2.1 Creating a Key Performance Indicator

In order to display a Key Performance Indicator or KPI within the Start Center, the KPI must first be created from within the **KPI Manager** application.

To access the **KPI Manager** select **Go To** → **Administration** → **Reporting** → **KPI Manager**.

Within the KPI Manager select the **New KPI** icon on the toolbar as seen in Figure 7-13.



Figure 7-13 New KPI Icon

To create a KPI the user must define a select statement for the query and set the following parameters:

- ▶ Target - Target value
- ▶ Caution At - Caution value, which will be displayed in yellow
- ▶ Alert At - The alert value, which will be displayed in red

Figure 7-14 is an example of a KPI graph:

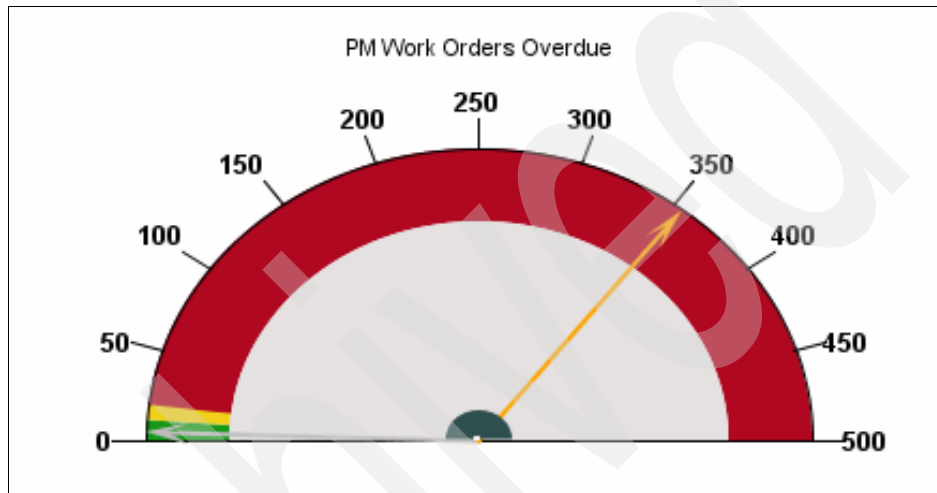


Figure 7-14 Sample KPI Graph

7.2.2 KPI Crontask

In order for a KPI to stay current with live data, a crontask must be established to facilitate and poll on a schedule.

To access the **Cron Task Setup** application, select **Go to** → **System Configuration** → **Platform Configuration** → **Cron Task Setup**.

Out of the box a crontask named *KPICronTask* is available to use for keeping KPI data current.

To enable this cron task, select the task from the list tab, then within the instance define the schedule (default is 1 day), the administrative user to run the cron task under, and set it to active as shown in Figure 7-15.

Cron Task Instances			
Filter > 1 - 1 of 1			
Cron Task Instance Name	Schedule	Run as User	Active?
KPINONREALTI	1d,0,0,0,*****	MAXADMIN	<input type="checkbox"/>

Figure 7-15 KPI Cron Task Instance

The KPI data will now be updated on the schedule you have established.

Work management configuration and administration

This chapter describes how to properly configure the work management functions. It goes through the applications that should be set up before you start using the system.

The following topics are covered:

- ▶ Work order settings
- ▶ Setting up job plan templates
- ▶ Work Order module
- ▶ Work management capabilities

8.1 Work order settings

This section describes some settings that are required in order to start using the system, and some other useful settings.

8.1.1 Organizations application

Most of the settings can be accessed from the Organizations application. From the Start Center, select **Go To** → **Administration** → **Organizations**.

Note: All of the settings should be set for *each* organization in the system.

Work order options

Select an organization that was already created in the system and open the **Work order options** in the Select Action menu, as shown in Figure 8-1.

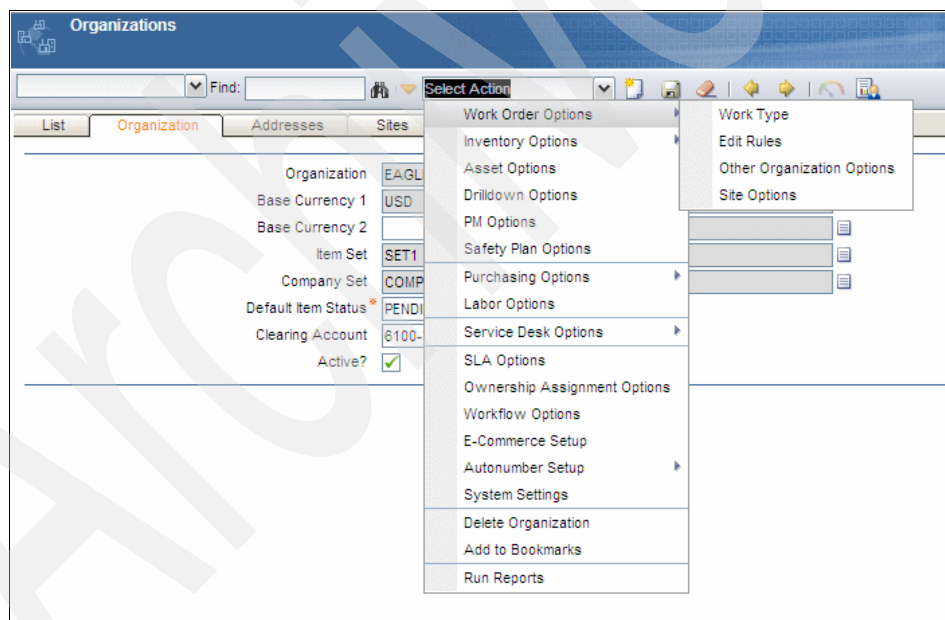
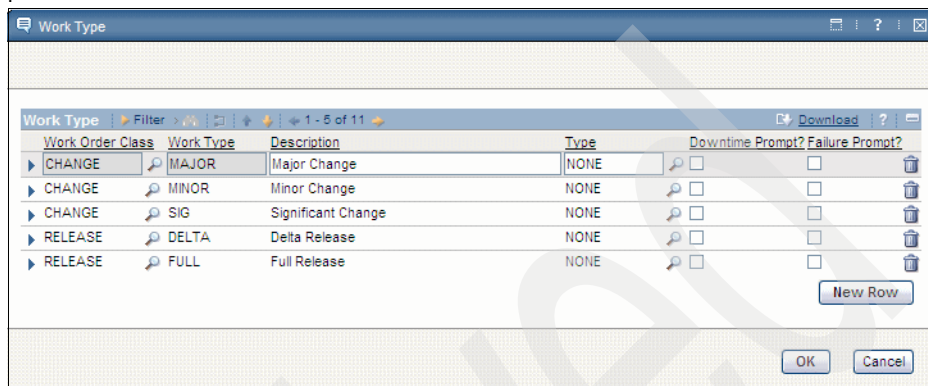


Figure 8-1 Work order options menu

Work type

The first step to configure the work orders is to define the work types. You will not be able to create a work order unless the work types are configured because work type is a required field in the Work Order application.



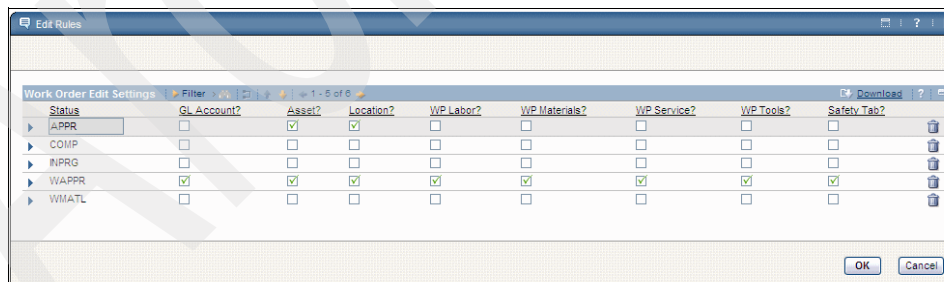
Work Order Class	Work Type	Description	Type	Downtime Prompt?	Failure Prompt?
CHANGE	MAJOR	Major Change	NONE	<input type="checkbox"/>	<input type="checkbox"/>
CHANGE	MINOR	Minor Change	NONE	<input type="checkbox"/>	<input type="checkbox"/>
CHANGE	SIG	Significant Change	NONE	<input type="checkbox"/>	<input type="checkbox"/>
RELEASE	DELTA	Delta Release	NONE	<input type="checkbox"/>	<input type="checkbox"/>
RELEASE	FULL	Full Release	NONE	<input type="checkbox"/>	<input type="checkbox"/>

Figure 8-2 Work Type dialog

Note: Remember that the work order work types are *not* configured in the Domains application, as is usual for value lists. Work types are set up in the Organizations application.

Edit rules

Edit rules are tied to the work order status. Depending on the status, you are able to edit some predefined fields but not others, as shown in Figure 8-3.



Status	GL Account?	Asset?	Location?	WP Labor?	WP Materials?	WP Service?	WP Tools?	Safety Tab?
APPR	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
COMP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
INPRG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAPPR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WMATL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 8-3 Edit rules dialog

Other organization options

There are other configurable options related to the organization. They are described in the following paragraphs and illustrated in Figure 8-4 on page 148.

- ▶ **Default Downtime Start:** Specifies which date appears by default in the start date field when Maximo displays the downtime report message
- ▶ **Actual Start Date:** Specifies the actual start date for a work order on status changes
- ▶ **Display Warranty Status:** Specifies whether Maximo will display a message if the asset is under warranty when entered on a work order
- ▶ **Display Downtime report prompt upon WO Completion for Asset in Down Status:** Specifies whether Maximo will display the Change Asset Status dialog box when the work order status for a down asset changes to complete or closed
- ▶ **Clear Material Reservation when WO status changes:** Specifies when Maximo will clear a work plan reservation used on a work order on status changes
- ▶ **Display Duplicate Problem Warning:** Specifies whether Maximo will display the duplicate problem dialog box when a user enters a work order for an asset or location that is already entered on another open work order with the same problem code

Other Organization Options

Default Downtime Start

☒ On Reported Date
☐ On Actual Start Date
☐ None

Set Actual Start Date

☒ On Change Status Initiate
☐ On Change Status Complete

Display Warranty Status? ☒

Display Downtime Report Prompt upon WO Completion for Asset in a 'Down' Status? ☐

Clear Material Reservation When WO Status Changes

☐ To Complete
☒ To Closed

Display Duplicate Problem Warning

On Asset? ☒ On Location? ☒

OK Cancel

Figure 8-4 Other organization options dialog

Note: In this section we presented a couple of options to be configured related to reporting asset downtime. This is an important action used to keep track of asset problems for further maintenance. It can be found in the following applications:

- ▶ Work Order Tracking
- ▶ Quick Reporting
- ▶ Assets
- ▶ Activities and Tasks

Site options

Figure 8-5 shows settings tied to the sites included in the current organization. The only options you can set here are the task numbering start and increment by.

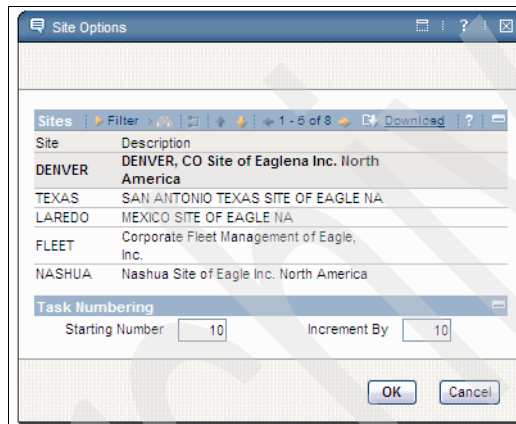


Figure 8-5 Site Options dialog

Autonumber setup

The Autokey feature is related to more than just work management applications, but the discussion of it is particularly relevant here because most users use it to customize the auto-numbering patterns for each type of work order.

An example is a company that wants to set a different prefix on the autonumber for each site in the organization, or even to set a prefix for each type of work order. This is a good practice for tracking and identifying how the work orders were generated.

To create or modify an autokey, in the Organizations application click **Select Action** → **Autonumber setup** as shown in Figure 8-6 on page 150.

There are four types of autokeys. Each one refers to a specific object level: System, Set, Organization, and Site.

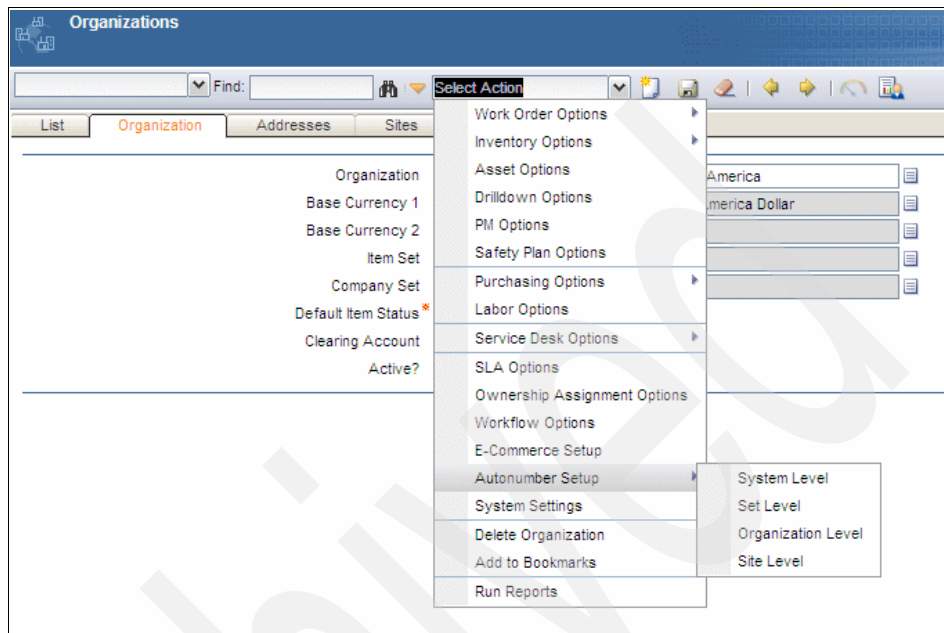


Figure 8-6 Autonumber setup menu

Figure 8-7 on page 151 shows the Site level dialog as an example. Here it is possible to create and modify the autokey attributes for each site of the current organization record.

- ▶ *Seed* is the starting number of the sequence.
- ▶ *Prefix* is the user-defined character or word that is inserted before the number so that the records can be identified easily.

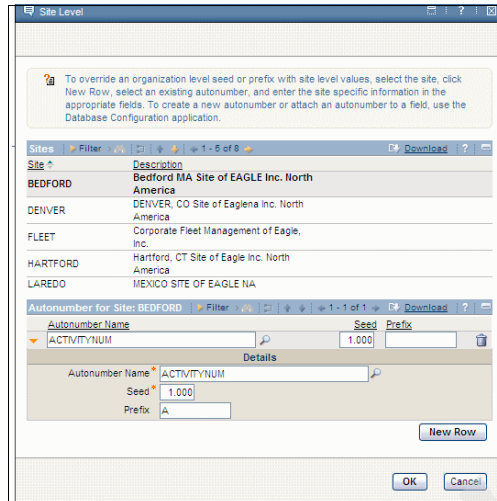


Figure 8-7 Site level autonumber dialog

8.1.2 Start Center setup for work management

This section describes useful functionality that can be set up in the Start Centers to display to the user a list of all the tickets, work orders, and activities that the user owns.

The Start Center is composed of portlets, and each portlet has an application that controls the content and configuration of the portlet. This section is focused on the work management public queries.

In most of the applications you have a list tab that can be used to create queries to be used in the Start Center.

The following steps provide an example of how to create a query to retrieve your tasks:

1. Select **Go To → Work Orders → Activities and Tasks**.
2. In the List tab, filter out the tasks you want to show in the Start Center.
3. Save the query, as shown in Figure 8-8 on page 152.
4. Set up the query as explained in Chapter 5, “Security configuration” on page 75.

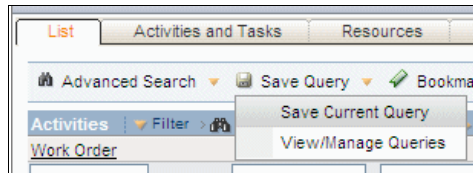


Figure 8-8 Save query menu

8.2 Setting up job plan templates

In this section we delve into the details of creating job plan templates.

A *job plan* is a work template that contains detailed information about the work to be done on an asset, item, or location. It has all the necessary information about the work such as a task list, the labor or crafts involved, and the materials and tools used to perform the work.

It is useful when you need to enter the same information many times in many work orders. Using job plans, it is not necessary to create a new work plan every time a new work order is created. Applying the job plan to a work order, all the tasks and resource estimates are copied into the work plan for the work order.

Some key considerations and features of job plans are:

- ▶ Working with job plans allows for standardization of work orders, but it does *not* restrict the work orders to being identical to the template.
- ▶ After applying a job plan to the work order, it is still possible to modify the work plan so that the procedures, labor, materials, services, and tools are more specific to the particular work order – without affecting the original template.
- ▶ Job plans are at the system level, but you can optionally set an organization and even a site for it. The same is true for tasks, labor, materials, services and tools.

For example, you can create a job plan at the organization level, and add specific tasks at the site level. This feature allows you to set up standardized job plans across all sites and make the work plan inherit specific tasks for each site.

Note: Tasks are not the only objects that can be defined for a specific site. It is also possible to define and set up the other related objects like labor, materials, services, and tools.

To access the Job Plan application, select **Go To → Planning → Job Plans**.

The job plan status can be:

- ▶ *DRAFT*: Default status for new records
- ▶ *ACTIVE*: Approved job plans that can be used in work orders
- ▶ *INACTIVE*: Job plans that are not used in work orders anymore

8.2.1 Job plan concepts

The following definitions apply to job plans:

- ▶ *Task* is a step that must be performed to complete the job. The information that comes along with each task is the description of the work to be done and the duration of the task. You can also attach a meter or set a nested job plan for more complicated work.
- ▶ *Craft* is the necessary skill to do the job. There are some procedures that require specialized skills like working with chemical products or electrical current.
- ▶ *Labor* is the person who will perform the work. It is usually not set in the job plans because, to allow for templates to be reused, most planners specify crafts rather than laborers when planning labor.
- ▶ *Material* is some item required to do the work, like replacement parts. You can set the quantity, the issuing storeroom, and other fields like the task that this material will be used for.
- ▶ *Tool* should be used when you know that a certain tool is needed to perform the work, like pliers and cutters. You can set the task that requires it and also check whether a reservation for that tool is required before the start of the work.
- ▶ *Service* is necessary, for example, when your company cannot provide something that you need to do the job, so you specify the service, quantity, and the vendor that provides the service.

8.3 Work Order module

This section describes the Work Order module. It does not go into detail about each application. Instead, it provides an overview of the work management capability and functionality that you should know.

Work orders are the core of maintenance management. A work order is a request for work to be performed and this module has the applications that

describe the work to be done, who will do the work, and when the work will start and finish.

8.3.1 Work Order applications

The module contains the following applications, which are described in the following sections:

- ▶ Work Order Tracking
- ▶ Labor Reporting
- ▶ Quick Reporting
- ▶ Activities and Tasks
- ▶ Assignment Manager
- ▶ Service Requests

Work Order Tracking

The *Work Order Tracking application* is used to create, review, approve, and manage work on assets and locations. To access it, select **Go To → Work Orders → Work Order Tracking**.

The application is organized in tabs to perform the following functions:

- ▶ **List** - Search for existing work order records.
- ▶ **Work Order** - Add, view, or modify information related to the assets and locations needed, scheduling, job plans, and PMs.
- ▶ **Plans** - Add, view, or modify information related to the work order children, tasks needed to perform the work and all the material, labor, services, and tools associated with the work order.
- ▶ **Related Records** - Add, view or delete related ticket and work order records.
- ▶ **Actuals** - Very similar to the plans tab, but used to report the actual work that was done in the work order.
- ▶ **Safety Plan** - Add, view, and modify safety information associated with a work order, like hazards and precautions.
- ▶ **Log** - Create, view, and edit Work Log and Communication Log entries.
- ▶ **Failure Reporting** - Enter information that helps to analyze failure trends for the company's assets, locations, and CIs.

Note: Entering *Failure Class* data is a way you can analyze failure trends for the company's assets, locations or configuration items.

Labor Reporting

The *Labor Reporting application* is used to report and keep track of the labor hours, such as type and the total number of hours of work that were performed by external or internal employees.

Quick Reporting

The *Quick Reporting application* is a simplified version of the Work Order Tracking application that can simplify reporting the actuals and other data after the work has been completed.

Activities and Tasks

The *Activities and Tasks application* is a subset of Work Order Tracking functionality to support single task specific work orders.

It is used to review and manage activities and tasks created by the other applications. It is important to know that an activity or a task does not exist by itself, so you cannot create records from this application.

Activities are created from the Service Desk module in the Incidents and Problems applications, while Tasks are created in the Work Order tracking.

Assignment Manager

The *Assignment Manager application* is used to manage work schedules, labor requirements, and dispatching of the work.

You can view work order assignments; labor, craft, and skill levels; dispatch labor according to work priority; and schedule work according to labor availability. It is also possible to filter labor to match work and vice versa.

Another important functionality of the Assignment Manager application is to record the time spent by the labor on the task. This can be done by the actions: *Start Assignment*, *Interrupt Assignment* and *Finish Assignment*.

Service Requests

The *Service Requests application* is used to create, view, and resolve service requests from customers. Records created from this application are a type of ticket.

Service requests in Maximo are created to resolve issues, obtain information, and obtain or change services. Either a service desk agent or a customer can create a service request.

8.3.2 Creating work orders

This section shows several applications that can be used to create work orders using Maximo:

- ▶ *Changes* - Use to create work orders related to service desk tickets.
- ▶ *Condition Monitoring* - Use to generate work orders to correct problem conditions found during monitoring procedures.
- ▶ *Incidents* - Use to create work orders related to service desk tickets.
- ▶ *Preventive Maintenance* - Use to generate scheduled maintenance work orders.
- ▶ *Problems* - Use to create work orders related to service desk tickets.
- ▶ *Quick Reporting* - Use to create work orders and report actual work done for simple jobs, unplanned work, or work not performed by the maintenance department.
- ▶ *Releases* - Use to create work orders related to service desk tickets.
- ▶ *Service Requests* - Use to create work orders related to service desk tickets.
- ▶ *Work Order Tracking* - Use to create and report on high-volume or complex work orders.

8.4 Work management capabilities

This section describes some of the new and enhanced work management configuration functionalities included in Maximo V7.1 that you should know for the certification exam.

8.4.1 Nested job plans

This functionality allows job plans to be nested within a hierarchical relationship. Users can create a job plan that refers to other job plans. These plans are nested and generate a work order hierarchy when applied to a work order (not just to tasks). Job plans can be nested in as many levels as needed.

8.4.2 Job plan template

Another enhancement to the Job Plan application is the addition of the Template Type field. This field has a domain associated with it, pre-populated with three choices:

- ▶ Maintenance
- ▶ Activity
- ▶ Process

This is a *required* field for the Job Plan application.

8.4.3 Work management status flow control

Maximo V7.1 provides the capability to define precedence relationships between work orders and tasks. This then initiates the resulting network of records automatically applied with a finish-to-start action, thus automating the flow of status changes between them. For example, if flow control sequencing is enabled at the job plan level, each task generated when applying the Job Plan to a work order evaluates the one before it to determine if it has completed. If the predecessor has completed, its status is automatically changed to “In Progress.” Any successive task cannot have its status changed to “In Progress” until its immediate predecessor has completed. As such, the status on the work order cannot be changed to “Complete” until all tasks have been completed in the order in which they are sequenced. When all tasks are completed, the work order status is automatically changed to “Complete.”

Reporting configuration

Reporting is an important component of the product because the information produced can have an impact on business decisions. This chapter discusses the reporting capabilities of the Tivoli process automation engine.

The application is integrated with the Business Intelligence Reporting Tool (BIRT). This open source reporting system integrates with Java/J2EE applications and will produce custom reports.

The following topics are covered in this chapter:

- ▶ Report administration
- ▶ Report configuration
- ▶ Running reports

9.1 Report administration

The report administration assists the Administrator in:

- ▶ Viewing a list of reports
- ▶ Defining the reports for the end users
- ▶ Changing the description of the reports
- ▶ Setting or viewing the security

As an Administrator, you can specify the following for the end users:

- ▶ Making the reports available and how to open, run, and print these reports
- ▶ Determining the outlook of the report titles and headings
- ▶ Setting the report security

The Report Administration contains the following tabs:

- ▶ List: To open a list of reports and perform a search on the list
- ▶ Report: To perform the following tasks:
 - Configure reporting options
 - Delete a report
 - Duplicate a report
 - Import report files
 - Import library files
 - Preview and print reports
 - Add a report to the database
 - Set and view the security settings for the report
- ▶ Security: Set and view the report security

You can set the security for an application in the Report Administration. Application security settings let you set group security for all reports in a selected application. The Maxadmin group has access to all “out of the box” reports. You must set up group or report access to each individual application or other new or customized reports.

To set the application security:

1. In the **Report Administration** application, select **Set Application Security** from the Select Action menu. The report Application Security dialog box opens.

2. Select an application name from the Application table window. Click **New Row**.
3. In the Application Level Security table window you can add, change, or delete security settings for a group. Security settings are defined by report type. For example, you can set report security so that Group A can see all reports in the classification application.
4. Click **Save**.

Prior to the deployment of the application, the Administrator can perform several customizations, described in the following sections.

9.1.1 Generating the Request pages

The *Request pages* are the parameter inputs required for each report. Before the reports can be accessed from with the application the request pages must be generated. To ensure the reports will be available to users, perform the following steps:

1. Log in to Maximo as the System Administrator.
2. From the Start Center navigate to the **Go To** function and select **Administration** → **Reporting Administration** (Figure 9-1).

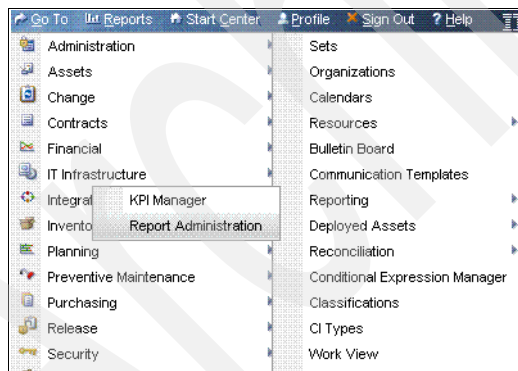


Figure 9-1 Report Administration option

3. Click the **Generate Request Pages** button at the bottom of the panel. A message box will be displayed, as shown in Figure 9-2 on page 162.

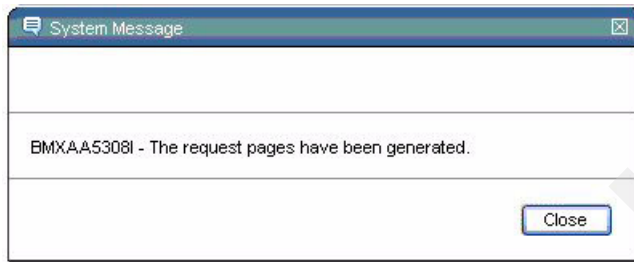


Figure 9-2 Generate Request Page notification box

At this stage the request pages have been successfully generated.

Note: Generating the request pages is a step you will only need to execute when you have a new installation or have uploaded a new report. We recommend that this step is done when other users have logged out of the system.

9.1.2 Importing a report

Use the *Report Administration application* to import a BIRT Report Design file (the report file). You perform this action to add a new report to your database or bring an updated version of an existing report into your database.

Before you import the report design file, you must import any associated library files. Use the Import Library File action from the Select Action menu to perform this operation.

This action is available only from the Report tab for the following reasons:

- ▶ If the report is new, you use the Report tab to add the report to the Report Administration application and then import the report to the database.
- ▶ If the report already exists, you import the report from the Report tab to be certain you chose a correct combination of Report Design file and Application name.

To import a report file follow these instructions:

1. Open the Report Administration application.
2. Select the **Report** tab.
3. From the Select Action menu, select **Import Report**. The Import Report dialog box opens. The existing report design file and the associated application name appears.

4. In the **Report Design File** field, enter the location of the report file you are importing. Click **Browse** to locate a Report Design file.
5. In the **Report Resource File** field, enter the location of any resource files. Resource files contain such items as images or external files. Click **Browse** to locate a Report Resource file. This is an optional field.
6. Click **OK**.

The application imports the report file.

9.1.3 Adding a report

You can add a report to the database using the following steps:

1. In the Report Administration application, click **New Report**.
2. In the resulting panel, shown in Figure 9-3 on page 164, enter the appropriate information:
 - **Report File Name:** The name of the report, with the file description as it was created in the Report Designer.
 - **Report Type:** Select the type of report. Click **Select Value** to view the list of available reports.
 - **Application:** Enter the application that end users use to run this report. Click **Select Value** to view a list of available application names. This setting specifies the application from which the end user can access the report, as well as the attribute names of any report parameters.
 - Select the **Report Folder** field. This field defaults to the value you entered in the Application field.
3. Click **Save Report**.
4. Click **Generate Request Page** to apply the changes.

- ▶ **Limit Records?:** This limits the number of records against which an end user can run a report. It prevents end users from executing large queries, which can cause negative performance impacts. Use the Report Administration application toolbar to open a report directly in the browser. When **Browser View** is checked, enter a value other than None in the browser **View Location** field. This field determines the application tabs that have an active Browser View icon.
- ▶ **Use Where Clause?:** Enables Current/Selected plus User-defined parameters.
- ▶ **No Request Page:** Disables Request Page for database updates.
- ▶ **Browser View and Browser View Location:** The Browser View feature lets you create a shortcut. With the shortcut, the end user can click an icon once in the application toolbar to open a report directly in the browser. When Browser View is checked, enter a value other than None in the Browser View Location field. This field determines the application tabs that can have an active Browser View icon.

The following options are available:

- **All:** The Browser View icon is available on a tab for the selected application.
 - **List:** The Browser View icon is only available on the List tab for the selected application.
 - **Main:** The Browser View icon is available on all tabs, except the list tab.
 - **None:** The Browser View icon does not appear in the selected application. None is the default.
- ▶ **Direct Print and Direct Print Location:** The Direct Print features let you create a shortcut so an end user can click an icon in the application toolbar to print the report. The configuration is the same as for Browser View Location.
 - ▶ **Direct Print with Attachments and Direct Print with Attachment Location:** The Direct Print with Attached Document feature lets you create a shortcut so an end user can click an application icon once (and select Yes in a message dialog box) to print the report and any associated attached documents. The configuration is the same as for Browser View Location.
 - ▶ **Generate Request Page:** Click **Generate Request Page** if you have not previously configured the report for Browser View. This option is available for all reports or at the individual report level.
 - ▶ **Preview:** In the Report Administration application, you can preview a request page and run a report. You can check for the following items:
 - The correct parameters, if any, appear to the end user on the request page.

- The generated report opens with the correct data and format.

To preview a report:

- In the Report Administration, select the report that you want to run.
 - Click **Preview**. The **Request Page** dialog box opens. The parameters displayed depend on the report that you select.
 - Enter values in any required fields. Required fields have an orange asterisk (*) next to them.
 - Click **Submit** to run the report. The report opens in a separate browser session.
- **Parameters:** From the parameters tab you can define ad hoc user parameters. Note that these parameters must also be specified in the report design itself.

9.3 Running reports

During the application installation process the BIRT default Report Writer is automatically configured to run reports from within the application.

Perform the following steps to open and work with a report:

- Use one of the following methods to open a report dialog box:
 - From the Reports menu in the application toolbar, select an application, as shown in Figure 9-5 on page 167.

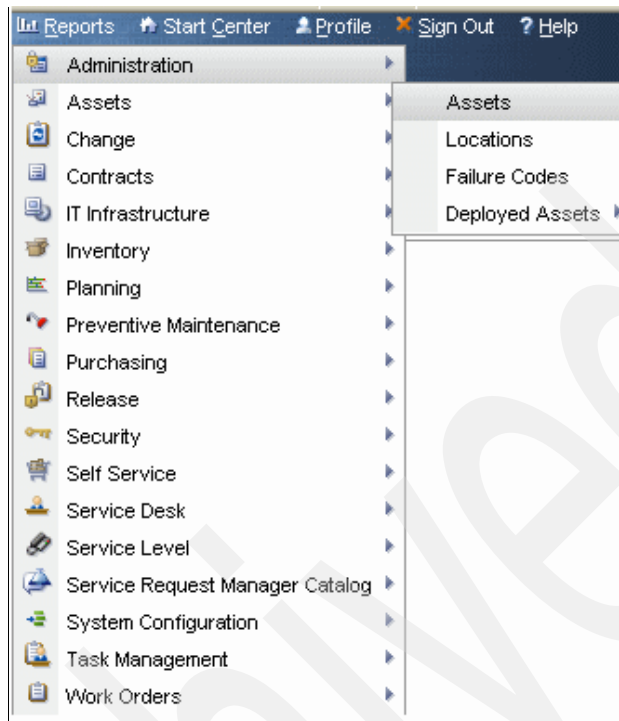


Figure 9-5 Report Menu

- b. From the **Select Action** menu, select **Run Reports**. The Report tab opens. The Report to Run window lists the available reports for the application. Click the report that you want to run (Figure 9-6).

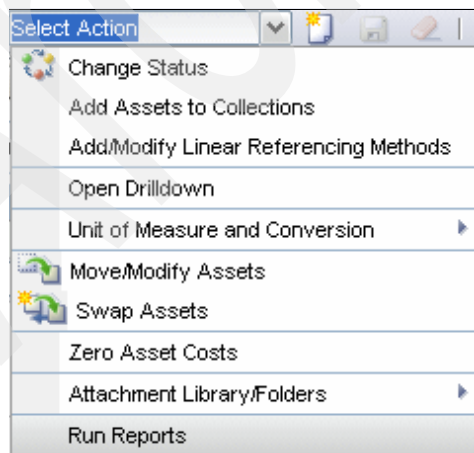


Figure 9-6 Select Action - Run Reports option

2. Select the report you want to see, for example, “Asset List” (Figure 9-7).

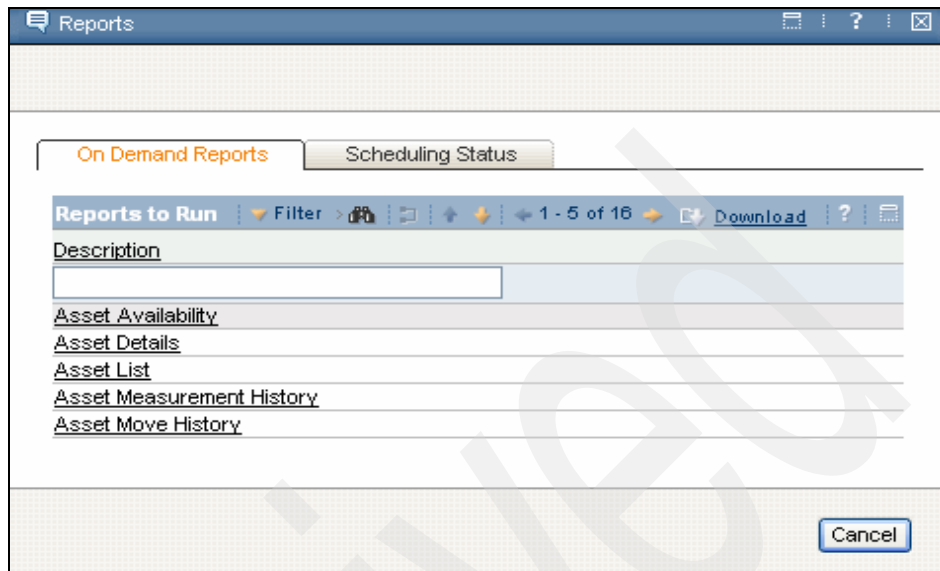


Figure 9-7 Selecting a report to run

3. Enter the required parameters in the Request Page dialog box (Figure 9-8).

Request Page

Fill in the fields in the Parameters section below and click Submit to run the report. If no parameters are displayed, the report will execute against the current/selected record set. Optionally, fill out the Schedule and Email Sections to schedule report run times and receive the scheduled report via email.

Parameters

Asset *

Site *

Start Date *

End Date *

Schedule

☒ Immediate

☐ At this Time

☐ Recurring

Email

To

Subject

Comments

Submit Cancel

Figure 9-8 Asset Lists report

4. Click **Submit** to run the report. The report opens in your browser.
5. On the reporting toolbar, perform any of the following actions:
 - a. Click the **Print Report as PDF** icon to print the report.
 - b. Click the **Export Data** icon to export the data in .CSV format.
 - c. Click the **Toggle table of contents** icon to see the table of contents for your report. The report you select determines the table of contents.

9.3.1 To schedule a report and send with e-mail

To schedule a report and send with e-mail, perform the following:

1. Open the Reports dialog box through one of the following methods:
 - a. From the Reports Menu in the application toolbar, select an application.
 - b. From the Select Action menu, select **Run Reports**.

2. Click the **Scheduling Status** tab. Select one of the following scheduling options:
 - **Once:** The report runs at a specific date and time in the future. Enter a date or click the select date icon. The date that you enter must be in (M or MM) / (D or DD) / YY format. Specify a time in HH:MM format and specify a.m. or p.m.

Recommendation: Use this option to schedule complex or lengthy reports to run during off-peak hours.

- **Recurring:** The report runs at regular intervals. Four fields let you specify when the report runs:
 - In the first field, enter a number from 1 through 365.
 - In the second field, enter the interval (day, week, or month).
 - In the third field, enter the day of the week or date of the month.
 - In the fourth field, enter the time in HH:MM format, along with AM or PM.

The following examples show the use of these fields:

- To run a report every day at 6:00 AM, select **1**, and then **Day**. Leave the third field blank and then **6:00 AM**.
 - To run a report every other Friday at 5:00 PM, select **2**, then **Weeks**, then **Friday**, and then **5:00 PM**.
 - To run a report every three months at 11:00 PM, on 15th of the month, select **3**, then **Months**, then **Day 15**, and then **11:00 PM**.
3. Use the following fields to send the report with e-mail. The system sends the report in .PDF format.
 - **To** – Enter one or more e-mail addresses to receive the report. Click Select Value to enter a system validated e-mail address.
 - **Subject** – Enter a subject for the report. If you do not enter a subject, this field defaults to the report name.
 - **Comments** – Enter any comments you want to include in the e-mail message.
 4. Click **Submit** to run the report. The report is sent to the e-mail address at the scheduled time.

9.3.2 To view and edit scheduled reports

You can use the Reports dialog box to view scheduled reports.

1. Open the Reports dialog box through one of the following methods:
 - a. From the Reports menu in the application toolbar, select an application.
 - b. From the Select Action menu, select **Run Reports**.
2. Click the **Scheduling Status** tab to open the Scheduling Status dialog box. In the Schedules You Can Edit section, you can view the type of report (once or recurring) and the next run time. You can delete a scheduled report and change schedule information.

Archived

Sample certification test questions

In this appendix, we provide sample questions that are representative of the ones you encounter on the actual certification test. We recommend you take this sample test after studying the chapters in this book.

Note: Each question has only one correct answer.

Questions

We provide the following questions to assist you in studying for the certification test:

1. Which configuration data is required while installing WebSphere Application server
 - a. Web Server Name, Port and Node name.
 - b. Web Server Name and Port.
 - c. Web Server Name, Port, Node Name and Cluster Name.
 - d. Web Server Name, Port and Cluster Name.
 - e. Web Server Port, Node Name and Cluster Name.
2. Which type of queues types are not supported by message engine in a Web Sphere application server?
 - a. Sequential Inbound and Outbound, Continuous Inbound Queues.
 - b. Sequential Outbound.
 - c. Continuous Inbound.
 - d. Continuous Inbound error.
 - e. Continuous Outbound.
3. What is the recommended maximum heap size for Maximo optimum performance?
 - a. 1.5 – 2.0 GB
 - b. 1.0 –1.5 GB
 - c. 2.0 – 2.5 GB
 - d. 0.5- 1.0 GB
4. Where do you define the conditions on source and destination of a crossover domain fields?
 - a. Crossover domain.
 - b. Domain application.
 - c. Condition Expression Manager.
 - d. System Properties.
 - e. Application Designer.
5. Which of the following describes the staging table?
 - a. Database view table where record set records are moved after execution of a query.

- b. Data stored after execution of multiple joins query.
 - c. Table in the system used to store the attributes of an incoming e-mail message.
 - d. Before report generation staging table is used to store result set.
 - e. None of the above.
6. Which of the following is not true?
- a. Indexes can be created on a persistent tables.
 - b. Clustered index can be created for Oracle Database.
 - c. Indexed table data can be searched in ascending or descending order.
 - d. It is possible to have an index status.
 - e. It is possible to create an unique index.
7. Vendor's labor costs are captured by using which default GL account?
- a. Labor Control Account.
 - b. External Labor Control Account.
 - c. No default GL Account exists.
 - d. No default GL Account exists, one has to define labor resource code for external.
 - e. None of the above.
8. Is it possible to define a Financial period as per user required tenures for example. 18 months or 3 months?
- a. Yes
 - b. No
 - c. You can only define up to 12 months
9. Which of the following are not an organization's default accounts?
- a. Global Rotating Suspense Account.
 - b. Global Ticket Account.
 - c. Tool Control Account.
 - d. External Labor Control Account.
 - e. Internal Labor Control Account.
10. Which of the following is not a part of Security Profile infrastructure?
- a. A user's security privileges controls a user's access to modules, applications, menu options, and data.

- b. The security group to which a user belongs controls the user's level of access and privileges within the system.
 - c. The security architecture is designed to use organization as the first level of security.
 - d. The profile tab in the users application displays the user's security profile.
 - e. The security profile information displays the access that has been granted to the selected user through the combination of their roles.
11. Which of the following is not a relevant for security groups?
- a. Security groups are two types Independent and non-independent.
 - b. It is possible to combine access rights and grants of one security group to another security group in one type of security group.
 - c. Using security controls action, you can specify EVERYONE group for all user fields.
 - d. It is necessary to create a security groups first before creation of a new user.
 - e. In short, security groups define authorizations and users inherit authorization of security groups.
12. User approval limits and tolerances are applied at organization level, but users inherit them to all the sites to which they have access. If a user that belongs to one group has invoice approval limits of \$1200 for site A and \$900 for site B under an organization, system gives invoice approval limits at Site A and Site B as:
- a. \$900 for both sites.
 - b. \$1200 for both sites.
 - c. \$1050 for both Sites.
 - d. \$1200 at Site A and \$900 at Site B.
 - e. \$1200 at Site A and \$1050 at Site B.
13. Which of the following is not a pre-migration task?
- a. Create Migration Objects.
 - b. Create Migration Groups.
 - c. Organize and upload compiled source.
 - d. Package Definition.
 - e. Package Deployment.
14. Which of the following is not the best practices using migration manager to deploy a package?

- a. Same base language in source and target environments.
 - b. No inbound restrictions in the target environment.
 - c. When one package at a time is deployed on the target environment
 - d. Administration mode turned on during Package Deployment.
 - e. Same product versions in source and target environments.
15. Which of the following is not a Start Center portlet?
- a. Bulletin Board.
 - b. Favorite Applications.
 - c. Inbox / Assignments.
 - d. Quick Insert.
 - e. Workflow.
16. If a user belongs to two security groups, after logging in, what is displayed when Start Center appears?
- a. Start Center will have two tabs each tab showing one Start Center application.
 - b. Only one Start Center application appears after user logins.
 - c. There is no relation between security groups memberships and Start Center.
 - d. User should login with two different credentials and configure each Start Center separately.
 - e. None of the above.
17. For which of the following we cannot set edit rules?
- a. GL Account.
 - b. Asset.
 - c. Location.
 - d. WP Labor.
 - e. Actions.

18. Which of the following is a Work Management configuration at organization level?
- a. Increment task numbering with start number under plan tab of work order tracking.
 - b. Under Flow Control.
 - c. Suspend Flow Control.
 - d. Flow Action Assist.
 - e. Inherit Status Changes.
19. Report Administration application allows to which of the following?
- i. Open a list of reports.
 - ii. Define reports to end users.
 - iii. Change the description of the report.
 - iv. Set or view security.
- a. i and iii
 - b. i, ii and iv
 - c. i, ii and iii
 - d. i, ii, iii and iv
 - e. None of the above
20. Where do you define number of records per report?
- a. Define number of records per page in the report code.
 - b. Once page size is defined, number of records per page is taken care of by reporting tool.
 - c. Using select action option define records per page.
 - d. Enter no of records that the Query returns value in Max Record Limit field.
 - e. None of the above.
21. How do you define Report Level authorization?
- a. Define authorizations for a groups under security tab.
 - b. Define authorizations under Report Administration.
 - c. System Administrator allows report designer to Authorize.
 - d. Using select action option define report authorizations.
 - e. None of the above.

Answers

The following list shows the correct answers to the sample questions in this appendix:

1. c
2. e
3. b
4. c
5. c
6. b
7. b
8. a
9. e
10. c
11. d
12. b
13. e
14. d
15. e
16. a
17. e
18. a
19. b
20. d
21. a

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

For information about ordering these publications, see “How to get Redbooks” on page 182. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *Deployment Guide Series: Maximo Enterprise Asset Management*, SG247640
- ▶ *IT Asset Management Processes using Tivoli Asset Manager for IT*, SG247601
- ▶ *Maximo Asset Management Essentials V7.1 Implementer's Guide*, SG247645

Online resources

These Web sites are also relevant as further information sources:

- ▶ IBM Professional Certification Program Web site
<http://www.ibm.com/certify/index.shtml>
- ▶ Test 017 objectives
<http://www-03.ibm.com/certify/tests/obj017.shtml>
- ▶ Tivoli process automation engine courses:
<http://www-03.ibm.com/certify/tests/edu017.shtml>
- ▶ Tivoli Asset Management for IT Release 7.1, Installation Guide:
<http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itmaxam.doc/welcome.htm>

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

A

- actions 48
- Actions application 47
- Activities and Tasks application 155
- add-on adapters 118
- Allow Generated Passwords to Be Displayed on Screen 98
- ALN domains 30
- Always E-mail Generated Passwords to Users 98
- Application Designer 113
- Application Designer applicatio 108
- Application Designer application 132
- application server 78
- Assignment Manager application 155
- autokey attributes 150
 - Prefix 150
 - Seed 150
- Autokey feature 149
- autokeys 150
- Autonumber setup 149
- Autonumbering application 35
- auto-numbering patterns 149

B

- BIRT default Report Writer 166
- built-in workflow process 41
- Bulletin Board 137
- Business Intelligence Reporting Tool (BIRT) 159
- business object 58

C

- calendars 37
 - create and modify calendars 37
 - holidays 38
 - organization level 38
 - referencing a calendar 38
- Calendars application 37
- Certification
 - benefits 3
 - checklist 5
 - IBM Professional Certification Program 2
 - process 7

- Tivoli Professional Certification Program 4
- Chart of Account application 69
- classification structure 39
- Classifications application 38–39
 - Associates Classifications 40
 - Attributes 40
 - Classification Structure / Hierachy 39
 - Other Systems 40
 - Sections 40
 - Separate Classification Hierachies 40
 - Using Classifications 39
- Clearing Account 35, 71
- Com Log Entry? 44
- Communication templates 42–43
 - associate file attachments 44
 - create e-mail notifications 44
 - create generic communication template 43
 - working with 43
- communication templates 42
- Condition field 46
- Conditional Expression Manager 57
- Conditional Expression Manager application 57
 - how to access 57
- Conditional Expression Manager. 87
- Conditional security
 - best place to create the restrictions 108
 - Conditional Expression Manager 109
 - creating 110
 - Creating a Signature Option 113
 - overview 108
- Conditional SQL Expression Builder 46
- configure the database 32
 - creating an object 32
 - modifying 32
- Cost Management 72
- Cost Management application
 - Budget 73
 - Parent Project 73
 - Project 73
 - Value 73
- courses 8
- create calendars 38
- Create Communication action 43
- Create New Template 137

- Cron Task Setup application 42
- cron tasks 42
- CROSSOVER Domains 31
- Currency Codes application 34, 66
 - Active? 66
 - Currency 66
 - Description 66
- Custom Action Class 123

D

- Data Restrictions 77
- Database Configuration application 32, 61, 69
- Database server 15
- deleting the TEMP and TMP directories 14
- Deployment manager 25
 - host name 24
 - operating system password 25
 - operating system user id 25
 - SOAP port 25
- deployment plan 16
- Direct Print 165
- Directory server 17
- disabling the firewall 14
- domains 30
 - types
 - ALN 30
 - CROSSOVER 30–31
 - NUMERIC 30
 - NUMERIC RANGE 30–31
 - SYNONYM 30
 - TABLE 30–31
- Domains application 126

E

- E-Mail Listener 41
- E-mail Listeners application 41
 - features 41
 - free form / formatted e-mails 41
 - Security 41
 - Storing attachments 41
 - The E-mail listener cron task 41
 - Workflow Process 41
- E-Mail Password to User? 98
- encapsulating business objects 118
- End Points 124
- enterprise service 123
- Enterprise Service application 123
 - tabs

- Enterprise Service 124
 - List 124
- Enterprise services processing 123
- enterprises 10
- escalation
 - deletion of rules 49
 - rules 49
 - schedule 50
 - validation 49
- Escalation application 45
 - actions and notifications 48
 - components 46
 - Actions 47
 - Escalation Point 47
 - Notifications 47
 - Object 46
 - Organization and or site 46
 - Schedule 47
 - SQL Statement 46
 - creating an escalation 45
 - escalation items
 - Actions 47
 - Escalation points 47
 - Header attributes 47
 - Notifications 47
 - maintaining 45
 - multiple escalation points 47
 - usage
 - IT Asset Management 45
 - Service Desk Management 45
 - Workflow processes 45
 - Workflow application action (APPACTION) 47
- Escalation Point Condition field 50
- Escalations 45
- Exchange Rates application 67
 - Active Date 68
 - Convert from Currency 68
 - Convert to Currency 68
 - Exchange Rate 68
 - Memo 68
- External systems 124

F

- Favorite Application Portlet 137
- Financial Configuration applications 66
- Financial Periods 69, 71
- Financial Periods application
 - Accounting Close Date 72

Actual Close Date 72
Closed by 72
From 72
To 72

G

General Ledger Account 69
Generate Request Page 163
GL Account 69
GL Account Configuration 69

I

IBM Certification Agreement 6
IBM Service Management (ISM) 10
IBM Tivoli Change and Configuration Management Database (CCMDB) 118
IBM Tivoli Directory Server 43
IBM Tivoli process automation engine 9
IBM Tivoli Service Request Manager 118
IBM WebSphere application server 24
Import Middleware Configuration Information 21
importing a report 162
Inbox / Assignments Setup 136
Independent of Other Groups? 80
integration configuration 119
Integration Framework 118, 120, 122, 124
 advanced integration functionality 118
 configuring object structures 121
 Importing data 124
 inbound Web services queries 118
 Invocation channels 122
 JMS based message exchange 118
 Object Structure tab 121
 Object structures 120
 pre-configured integration contents 118
 Adapter (MAXIMO) 118
 Endpoints 118
 Enterprise services 118
 External system (EXTSYS1) 118
 Object structures 118
 Publish channels 118
 real-time user notifications 119
 rules-based message processing and routing 119
 Publish channels 121
 summary 125
Invocation Channels application 122
ISM solution environment 12

middleware 12
 Administrative system 12
 Application server 12
 Database 12
 Directory server 12
 HTTP server 12

J

J2EE Application Server 24
J2EE server 15
J2EE technology 108
Java Message Service (JMS) 118
Job plan
 concepts 153
 Craft 153
 Labor 153
 Material 153
 Service 153
 Task 153
 Tool 153
 nested 156
 statuses
 DRAFT 153
 INACTIVE 153
 template 157
Job Plan application 153, 157
Job plan statuses 153

K

Key Performance Indicators (KPIs) 142
 creating 142
 crontask 143
 Graph Setup 136
 KPICronTask 143
 List Setup 136
KPICrontask 143

L

Labor Reporting application 155
Launch in Context 62
Launchpad 17
Layout and Configuration 136
LDAP (Lightweight Directory Access Protocol) 77
LDAP authentication 106
Limits and Tolerances 77
List 77
Locations 37

Locations application 37
Login Tracking 106

M

maxadmin 136
Maxadmin group 160
maximo.properties file 23
metadata 127
Microsoft® Active Directory 106
middleware 12
Middleware installation 15, 17
Middleware Installer 20
migration 125
 planning 132
Migration Configuration 117
Migration Manager 128
 applications 129
 Migration Groups 129
 Migration Groups application 129
 Migration Manager 131
 Change 131
 Snapshot 131
 Migration Manager application 131
 Object Structures 129
 Object Structures application 129
compiled sources 128
concepts and components 126
 package contents 127
 Compiled sources 127
 History data 127
 Non-structural configuration content 127
 Package manifest 127
 Package metadata 127
 Structural configuration content 127
package definitions 126
 types 127
packages 126
configuration content 132
example scenarios 125
Migration flow 133
Migration group 128
Migration objects 128
Migration planning 132
overview 126
summary 134
migration objects 128
multiple integration triggers 118

multiserver topology 14

N

notification 49
 Broadcast? field 49
notification types 49
 free-form 49
 template-based 49
Numeric 31
NUMERIC domains 31
NUMERIC RANGE domains 31
 continuous 31
 discrete 31
 lookups 31

O

object structure 120
Object Structures application 62
Oracle 118
Organizations 34
 create an organization 34
 create a company set 34
 create an item set 34
 delete an organization 35
 edit an organization 35
 working with 34
Organizations application 69, 71

P

People application 95
persist JMS messages 27
platform configuration options 29
Platform configuration summary 60
portlet 136, 151
Portlet Ordering 138
Processes table window 57
publish channels 121
Purchase Order application 126

Q

Quick Insert Portlet 137
Quick Reporting application 155

R

Redbooks Web site 182
 Contact us xii
Reporting 159

- Direct Print and Direct Print Location 165
- Direct Print with Attachments and Direct Print with Attachment Location 165
- Generate Request Page 165
- Parameters 166
- Preview 165
- schedule a report 169
- table of contents 169
- Request pages 161
- resources recommended for study 8
- return on investment (ROI) 5
- rules engine 119
- Run Reports 169

S

- Safety tab option 114
- sample questions 173
- SAP suite 118
- Security Controls action 105
- security group 76
- security group types
 - independent 93
 - non-independent 93
- Security Groups application 76
 - adding a new security group 78
 - adding applications to a security groups 81
 - adding Limits and Tolerances to security groups 86
 - adding storerooms to security groups 83
 - adding users to a security group 89
 - applying Data Restrictions to security groups 87
 - approval limits 86
 - assigning GL Components to security groups 85
 - Authorize Group for All Storerooms? check box 84
 - Authorize Group Reassignment 90
 - Base Currency field 87
 - Conditional Expression Manager 87
 - Grant Listed Applications 82
 - Grant Listed Options for This Application 83
 - groups
 - 76
 - DEFLTREG 76
 - EVERYONE 77
 - MAXADMIN 77
 - MAXREG 77
 - Independent of Other Groups? check box 80

- Revoke Listed Applications 82
- set restrictions 87
- Start Centers 92
- tabs
 - Applications 77
 - Data Restrictions 77
 - GL Components 77
 - Group 77
 - Labor 77
 - Limits and Tolerances 77
 - Sites 77
 - Storerooms 77
 - Users 77
- security profile 76
- Self registration 106
- self-registration 78
- Service Desk module 155
- service providers 10
- service requests 41
- Service Requests application 155
- Set Application Security 160
- Setting or changing passwords and password hints 106
- Setting up authentication 106
 - LDAP authentication 106
 - native authentication 107
- Signature Option 113
- Sites 36
 - active site 37
 - add a site 36
 - working with 36
- site-specific calendars 38
- Start Center
 - associating a template 141
 - creating a template 137
 - modifying an existing template 140
- Portlets
 - Bulletin Board 137
 - Favorite Applications Setup 137
 - Inbox / Assignments Setup 136
 - KPI Graph Setup 136
 - KPI List Setup 136
 - Layout and Configuration 136
 - modifying 139
 - Quick Insert 137
 - Quick Insert Setup 137
 - Result Set setup 137, 139
 - Chart Options 139
 - Column Display 139

- Column Display Available Queries 139
- Display Options 139
- templates 136
- Storerooms 77
- Synonym Domain 97
- SYNONYM domains 30

T

- TABLE domains 31
- Test 435 7
- Thomson Prometric 6
- TICKET table 32
- Tivoli base services 10
- Tivoli Certification benefits 4
- Tivoli environment 5
- Tivoli process automation engine 10, 14
 - database data 22
 - installation example 14
 - before you begin 14
 - Deployment plan 16
 - Logs 16
 - middleware installation 15
 - solution description 16
 - Tivoli middleware installer 15
 - Topology file 16
 - installation prerequisites 12
 - overview 10
 - portfolio 11
 - typical deployment environments 12
 - custom 13
 - simple 12
- topology file 16
- topology.properties file 19–20

U

- User approval limits 176
- Users application 76, 89, 91, 93
 - adding a new user 95
 - assigning a user to a security group 98
 - Authorize Group Reassignment 98
 - creating person records 96
 - Default Insert field 94
 - default insert site 94
 - DOMAINS option 97
 - E-Mail Password to User? check box 97
 - Generate Password 97
 - My Profile action 94
 - no matching person ID found 96

- Password Should Expire After First Login?
 - check box 98
- Personal section 95
- Security profile tab 100
- Set Security Profile action 94
- Site field 94
- Sites 100
- System level applications 100
- tabs

- Groups 91
- List 91
- Security Profile 92
- User 91

- user record statuses

- ACTIVE 92
- BLOCKED 92
- DELETED 92
- INACTIVE 92
- NEWREG 92
- SELFREG 92

V

- validation 50
- Validation Results table window 50

W

- Web-based courses 8
- WebLogic 108
- WebSphere connectivity data 24
- Windows 2003 Server 16
- wonum attribute 58
- Work management
 - administration 145
 - applying a job plan to a work order 152
 - Autonumber setup 149
 - capabilities 156
 - Edit rules 147
 - job plan 152
 - Other organization options 147
 - Actual Start Date 148
 - Clear Material Reservation when WO status changes 148
 - Default Downtime Start 148
 - Display Downtime report prompt upon WO Completion for Asset in Down Status 148
 - Display Duplicate Problem Warning 148
 - Display Warranty Status 148
 - settings 146

- Start Center setup 151
- status flow control 157
- work order options 146
- Work type 147
- work order 153
- Work Order module 153
 - applications 154
 - Activities and Tasks 155
 - Assignment Manager 155
 - Labor Reporting 155
 - Quick Reporting 155
 - Service Requests 155
 - Work Order Tracking 154
 - Actuals 154
 - Failure Reporting 154
 - List 154
 - Log 154
 - Plans 154
 - Related Records 154
 - Safety Plan 154
 - Work Order 154
 - creating work orders 156
 - applications
 - Condition Monitoring 156
 - Incidents 156
 - Preventive Maintenance 156
 - Problems 156
 - Quick Reporting 156
 - Releases 156
 - Service Requests 156
 - Work Order Tracking 156
 - work order definition 153
- work order number 44
- Work Order Tracking application 154
- work template 152
- Workflow Administration application 56
 - tasks
 - Delete Workflow assignments 57
 - Reassign Workflow assignments 57
 - Stop active processes 57
 - View Workflow assignments 57
- workflow and escalation processes 44
- Workflow Assignment (WFASSIGNMENT object) 47
- Workflow Designer 50
- Workflow Designer application 50
 - Condition Node 53
 - Connection Lines 55
 - Negative Connections 55
 - Positive Connections 55
 - creating workflows 55
 - Interaction Nodes 54
 - Manual Input Nodes 53
 - Process Node Types 51
 - Start Nodes 52
 - Stop Nodes 55
 - Subprocess Nodes 53
 - tabs 50
 - Canvas 50
 - List 50
 - Process 51
 - Task Nodes 52
 - Wait Nodes 53
 - Workflow Process 41
 - workspace 15–17



Certification Study Guide Series: Foundations of Tivoli Process Automation Engine



**Helps you achieve
Foundations of Tivoli
Process Automation
Engine certification**

**Explains the
certification path
and prerequisites**

**Introduces sample
test questions**

This IBM Redbooks publication is a study guide for Test 000-017: Foundations of Tivoli Process Automation Engine and is aimed at individuals who want to get an IBM Professional Certification on Tivoli Process Automation Engine.

The Foundations of Tivoli Process Automation Engine Professional Certification, offered through the Professional Certification Program from IBM, is designed to validate the skills required of technical professionals who work in the implementation of the Tivoli Process Automation Engine. Note that this test is a prerequisite for several other certifications, such as IBM Tivoli Maximo Asset Management for IT V7.1 Implementation

This book provides a combination of theory and practical experience needed for a general understanding of the subject matter. It also provides sample questions that will help in the evaluation of personal progress and provide familiarity with the types of questions that you will encounter in the exam.

This publication does not replace practical experience, nor is it designed to be a stand-alone guide for any subject. Instead, it is an effective tool that, when combined with educational activities and experience, can be an extremely useful preparation guide for the exam.

For your convenience, we structure the chapters based on the sections of the Test 000-017, such as Prerequisites and Installation, Platform Configuration and so on, so studying each chapter will help you prepare for one section of the exam.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks