

Peregrine

ServiceCenter

Application Administration Guide

Release 5.1

Copyright © 2003 Peregrine Systems, Inc. or its subsidiaries. All rights reserved.

Information contained in this document is proprietary to Peregrine Systems, Incorporated, and may be used or disclosed only with written permission from Peregrine Systems, Inc. This book, or any part thereof, may not be reproduced without the prior written permission of Peregrine Systems, Inc. This document refers to numerous products by their trade names. In most, if not all, cases these designations are claimed as Trademarks or Registered Trademarks by their respective companies.

Peregrine Systems® and ServiceCenter® are registered trademarks of Peregrine Systems, Inc. or its subsidiaries.

This document and the related software described in this manual are supplied under license or nondisclosure agreement and may be used or copied only in accordance with the terms of the agreement. The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document.

The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental.

If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by email at support@peregrine.com.

If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com.

This edition applies to version 5.1 of the licensed program.

Peregrine Systems, Inc.
Worldwide Corporate Headquarters
3611 Valley Centre Drive San Diego, CA 92130
Tel 800.638.5231 or 858.481.5000
Fax 858.481.1751
www.peregrine.com



Contents

	About This Guide	13
	Knowledge Requirements	14
	Examples	14
	Contacting Customer Support	14
	Peregrine's CenterPoint Web Site	14
	Corporate Headquarters	15
	North America and South America	15
	Europe, Asia/Pacific, Africa.	15
	Contacting Education Services	15
Chapter 1	Overview	17
	ServiceCenter Modules	18
	Sample Data	19
Chapter 2	User Profiles	21
	Operators	22
	User Roles	22
	User Profiles	22
	Types of User Profiles	22
	How the System Determines a User's Profile	23
	Out-of-the Box User Profiles	23
	Adding a Profile	32
	Editing Profiles	39

Chapter 3	Service Management	41
	Accessing Service Management	42
	Administering Service Management	43
	Security Files	43
	Accessing the Security Files	44
	Security Files Tab	45
	Environment Tab	46
	Managing User Information	49
	Setting Privileges and Views in the Service Management Profile	53
	Maintaining Inboxes	56
	Accessing the Macro List Editor	57
	Accessing Probable Cause Records	58
	Accessing the Knowledge Base	60
 Chapter 4	 Incident Management	 61
	Incident Management Overview	62
	How Incident Management Works	62
	Accessing Incident Management	64
	Administering Incident Management	66
	Security Files	66
	Accessing the Security Files	67
	Security Files Tab	68
	Environment Tab	69
	Managing User Information	69
	Setting Privileges and Views in the Incident Management Profile	73
	Assignment Groups	76
	Categories	81
	Maintaining Inboxes	94
	Probable Cause	99
	Macro Editor	104
	Downtime	104
	Summary Link	106
	Cost Management	107
	Configuring the Incident Management Environment	108
	Status, Alerts, and Escalation	111
	Alerts and Calendars	112

What is Escalation?	112
Severity Levels	113
The Two-Step Close	113
General Information	114
Setting Up the Two-Step Close	114
Accessing Other Utilities	121
Reset Downtime	122
Build/Refresh Summary	123
Downtime	127
Summary Link	128
Probable Cause	129
Subcategory	129
Problem Type	130
Product Type	131
Chapter 5 Root Cause Analysis	133
RCA Overview	134
Terms Used in this Chapter	135
Implementing Root Cause Analysis	135
Root Cause Analysis Flow	137
Accessing Root Cause Analysis	138
Administering Root Cause Analysis	139
Security Files	139
Accessing the Security Files	140
Security Files tab	141
Environment tab	142
Managing the Root Cause Environment	143
Managing User Information	143
Setting Privileges and Views in the Root Cause Profile	148
Maintaining Inboxes.	151
Accessing the Macro List Editor	151
Accessing the Knowledge Base.	152

Chapter 6	Scheduled Maintenance	155
	Scheduled Maintenance Overview	156
	Creating a Scheduled Maintenance Task	156
	Automated Task Generation	157
	Generating Tasks From an Existing Ticket	157
	Scheduled Maintenance in Inventory Management	159
	Generating Tasks from Scheduled Maintenance	161
	Using a Template	161
	Template Administration	162
	Adding Data Using Expressions	164
	Scheduled Maintenance Overhead	165
	Load Balancing	165
	Calling a Format Control Record	166
	Scheduled Maintenance Workflow	167
 Chapter 7	 Inventory Management	 169
	The ICM Repository	170
	Primary and Attribute Files	170
	Database Dictionaries	171
	Device Files	171
	Attribute Files	172
	Join Files	172
	Example	174
	Hierarchy	174
	Forms	175
	Creating Subtables from an Array of Structures	175
	Accessing Inventory Management	176
	Assets Tab	177
	Contracts Tab	177
	Administration Tab	178
	Organizing Inventory Records	178
	Administering Inventory Management	180
	ICM Environment	181
	Profiles	182
	Adding ICM Capability to the Operator Record	182
	Adding an ICM Profile	186

Device Types	190
Creating a New Device Type	193
Updating a Device Type Record	200
Deleting a Device Type Record	200
Adding a New User	203
Where to Find More Information	204
Inventory Records.	205
Where to Find More Information	206
Chapter 8 Inventory Management Service Information	207
Accessing Service Level Agreements	208
Contract Management Environment Records	209
Contract Management Permission	210
Adding a Contract Management Profile	210
Alerts	215
Contract Status	215
Currency Conversion Utility	215
Currency Definitions	217
Calculating Payments	220
Software Tracking and Compliance	221
License and Installation Models in the Catalog.	222
The Software Tab	222
Managing Different Types of Multiple Licenses	226
Adding Software Licenses as Asset Records	227
Software Installations	230
Software Counters	232
Choosing a Calculation Method.	233
Compliance	236
The Compliance Message Log.	236
Checking Compliance	236
Software Tracking and Compliance Example	238
Step 1: Add Items to the Catalog	240
Step 2: Add Records to the Inventory Management Database	243
Step 3: Create a Software Contract.	246
Step 4: Associate the Software License to the Contract	248

Step 5: Create a Support Contract for the Software License	251
Step 6: Create a Software Installation Record	253
Step 7: Check Software Compliance	255
Where to Find More Information	257
Chapter 9 Service Level Management	259
What Is a Service Level Agreement?	260
The Value of SLAs	260
Using SLAs	260
SLM Concepts	261
Using Clocks	261
Natural Progression	261
SLA Response Phase.	262
The SLM Module	262
Interfacing with External Sources	263
The SLA Configuration Record	263
SLA Options	265
Graphing	266
Thresholds.	266
Status Progression.	267
Natural Progression State	267
Intermediate States	267
Rules for Natural Progression and Intermediate States	268
Creating a Service Level Agreement	269
Description Tab	272
Availability Tab.	272
Response Times Tab.	274
Misc. Tab	276
Attachments Tab	277
SLA Maintenance Tasks	279
Editing an SLA Record.	280
Deleting an SLA Record	281
Recalculating Outage Data	282
Assigning an SLA to a Department.	283
Category and Priority Mapping	285
Performance Views	287

	Service Level Contracts.	311
	Features of Contract Management.	311
	Setup	312
	Service Contracts	319
	Accessing a Contract	319
	Expense Lines	329
	Cost Assessment	332
	Entitlement Checking	336
	Viewing Contract Overruns	339
	Contract Wizard	340
Chapter 10	Change Management	345
	Relationship to Service Management	346
	Glossary.	346
	Components of Change	348
	Workflow	348
	Security and Access Control	352
	Capability Words	353
	Using Change Management.	354
	Environment.	357
	Security Profiles	358
	Message Group Definition Record.	366
	Managing Categories and Phases	370
	Change Categories	371
	Task Categories.	374
	Creating a Category	378
	Updating a Category Record	381
	Deleting a Category Record.	382
	Printing a Category Record.	384
	Change and Task Phases	384
	Accessing Phase Records	386
	Phase Record Fields	390
	Creating a Phase	400
	Change and Task Phase Functionality	407

Change Records.	409
Searching for an Existing Change	409
Updating an Existing Change	418
Closing a Change Phase	418
Reopening a Change Request	423
Tasks	425
Searching for an Existing Task	425
Updating an Existing Task	433
Closing a Task Phase	433
Reopening a Task	434
Approvals	435
Approval Sequence	435
Approvals tab	436
Risk Calculation	446
Example	447
Events, Alerts, and Messages	450
Alerts	451
Alert Processing	453
Alert Definitions	453
Alert Log	458
Events.	460
Event Controls	460
Change Management Events File	461
Event Names and Definitions	463
Adding New Events	464
Messages	465
Message Classes	465
Adding msgclass Records.	466
Background Processing	467
Notifications	470
Appendix A Process Flow Diagrams.	473
Change Management Open	474
Change Management Update	475
Change Management Approval	476
Change Management Denial	477

Change Management Close	478
Change Management Reopen	479
Change Management Retract	480
Incident Management Open	481
Incident Management Update	482
Incident Management Close	483
Service Management Quick-Open	484
Service Management Create Incident	485
Service Management Update	486
Service Management Close	487
Inventory Management Open	488
Inventory Management Update	489
Inventory Management Delete	490
Appendix B	
Field-Level Details.	491
Overview	491
Table 1: New call — Call Detail tab	492
Table 2: New Call - Resolution Detail Tab.	497
Table 3: Existing call — Update tab	498
Table 4: Existing call — Resolution Detail tab	500
Table 5: New incident — Incident Details tab	501
Table 6: New incident — Actions/Resolutions tab	503
Table 7: New incident — Contact tab	504
Table 8: New incident — Asset tab.	505
Table 9: Update incident — Incident Details tab	508
Table 10: Update incident — Activities tab/Site Visit tab	511
Table 11: Update incident — Activities tab/Historic Activities tab.	513
Table 12: Update incident — Activities tab/Action Resolution tab	514
Table 13: Update incident — Contact tab	515
Table 14: Update incident — Asset tab	515
Table 15: Update incident — Attachment tab	515
Table 16: Update incident — SLA tab	516
Table 17: Update incident — Parts & Labor tab	518
Table 18: Update Incident — History tab	519
Table 19: Update Incident — Alerts tab.	520

	Update incident — Related Records tab	521
	Table 20: Calls tab	521
	Table 21: Related Incidents tab	521
	Table 22: Related Changes tab	522
	Table 23: Related Quotes tab	522
	Table 24: Related Root Cause tab	523
	Table 25: Billing Information tab	523
Appendix C	SLM-Related Reports	525
	SLA Reports	526
	Device Availability	527
	Device Outages (Top Ten)	528
	Change History	529
	SLA Device Availability Performance	530
	SLA Response Time Performance	531
Appendix D	Events	533
	Introduction	533
	Availability events	533
	Response event	534
	Index	535



About This Guide

The *Application Administration Guide* is an introduction to the principal ServiceCenter modules from an Application Administrator's perspective. To get started, read the [Overview](#) on page 17. For an in-depth understanding of ServiceCenter modules, see the [Process Flow Diagrams](#) on page 473.

Read these sections for information about ServiceCenter components:

- [User Profiles](#) on page 21
- [Service Management](#) on page 41
- [Incident Management](#) on page 61
- [Root Cause Analysis](#) on page 133
- [Scheduled Maintenance](#) on page 155
- [Inventory Management](#) on page 169
- [Inventory Management Service Information](#) on page 207
- [Change Management](#) on page 345
- [Service Level Management](#) on page 259

Read these appendices for supplemental information:

- [Process Flow Diagrams](#) on page 473
- [Field-Level Details](#) on page 491
- [SLM-Related Reports](#) on page 525
- [Events](#) on page 533

Knowledge Requirements

The instructions in this guide assume a working knowledge of Peregrine Systems ServiceCenter. You can find more information in the following guides.

- For administration and configuration information, see the *ServiceCenter System Administrator's Guide* or the *ServiceCenter Application Administration Guide*.
- For database configuration information, see the *ServiceCenter Database Management and Administration Guide*.
- For copies of the guides, download PDF versions from the CenterPoint web site using the Adobe Acrobat Reader, which is also available on the CenterPoint Web Site. For more information, see *Peregrine's CenterPoint Web Site* on page 14. You can also order printed copies of the documentation through your Peregrine Systems sales representative.

Examples

The sample windows and the examples included in this guide are for illustration only, and may differ from those at your site.

Contacting Customer Support

For more information and help with this new release or with ServiceCenter in general, contact Peregrine Systems' Customer Support.

Peregrine's CenterPoint Web Site

You can also find information about version compatibility, hardware and software requirements, and other configuration issues at Peregrine's Centerpoint web site: <http://support.peregrine.com>

- 1 Log in with your login ID and password.
- 2 Select **Go for CenterPoint**.
- 3 Select **ServiceCenter** from **My Products** at the top of the page for configuration and compatibility information.

Note: For information about local support offices, select **Whom Do I Call?** from **Contents** on the left side of the page to display the **Peregrine Worldwide Contact Information**.

Corporate Headquarters

Corporate headquarters contact information:

Address:	Peregrine Systems, Inc. Attn: Customer Support 3611 Valley Centre Drive San Diego, CA 92130
Telephone:	+1 (858) 794-7428
Fax:	+1 (858) 480-3928

North America and South America

North and South America contact information:

Telephone:	+1 (800) 960-9998 (US and Canada only, toll free) +1 (858) 794-7428 (Mexico, Central America, and South America)
Fax:	+1 (858) 480-3928
E-mail:	support@peregrine.com

Europe, Asia/Pacific, Africa

For information about local offices, see *Peregrine's CenterPoint Web Site*. You can also contact *Corporate Headquarters*.

Contacting Education Services

Training services are available for the full spectrum of Peregrine Products including ServiceCenter.

Current details of our training services are available through the following main contacts or at:

<http://www.peregrine.com/education>

Address: Peregrine Systems, Inc.
Attn: Education Services
3611 Valley Centre Drive
San Diego, CA 92130

Telephone: +1 (858) 794-5009

Fax: +1 (858) 480-3928

1 Overview

CHAPTER

The *ServiceCenter Application Administration Guide* introduces the principal ServiceCenter modules. It has instructions to set up and manage those modules, and instructions to tailor each module for your environment. Read the *ServiceCenter User's Guide* to learn how to start and use ServiceCenter modules. ServiceCenter operates as a client/server system. This guide concentrates on the client portion of the product.

Read this chapter for information about:

- *ServiceCenter Modules* on page 18
- *Sample Data* on page 19

ServiceCenter Modules

ServiceCenter provides a suite of modules to oversee your enterprise. It consists of a series of integrated modules and utilities designed to manage specific parts of your enterprise. These modules work together to create a complete system, not just a series of stand-alone products. For example, Incident Management and Change Managements use the inventory database contained within ICM.

The modules covered in this guide include:

- *Service Management* enables you to create a call report for each call received at the help desk. Depending on the nature of the call, the call report can be used in other modules to create an incident ticket, change request, order, and so on.
- *Incident Management* enables you to report and track incidents. *Incident tickets* are routed to the personnel who can resolve the issue.
- *Root Cause Analysis* is a module that enables you to track, prioritize, and resolve recurring incidents and incipient problems by determining their Root Cause.
- *Scheduled Maintenance* enables you to schedule and track Scheduled Maintenance Tasks.
- *Inventory Management* enables you to keep track of hardware and software in your network. For example, a network administrator could look at a list of the PCs at the site.
- *Inventory Management Service Information* describes service level agreements and contract management.
- *Change Management* enables you to request, list and track changes at a facility. For example, a change can be opened to add a network line to an office.
- *Service Level Management* describes how to track performance and provide system feedback on service agreements between departments within a company.

Sample Data

ServiceCenter contains a set of sample data with you can work and learn the product. You can use these records as a model for your actual data. This guide uses the sample data to illustrate the modules and processes described. You can modify or delete these records as you learn the system. You can also add new records.

Users	The sample data includes a set of fictitious users with associated profiles, incident tickets, and other records.
Inventory	You do not have to add devices for the sample system. A simulated network inventory is included with the sample data. The sample inventory database includes modems, PCs, workstations, mainframe hosts, and so on.
Call Reports	A set of sample call reports is included. You can review, update, and close these reports as you would an incident ticket in a live system.
Incident Tickets	A set of sample incident tickets is included. You can review, update, and close these tickets as you would an incident ticket in a live system.
Changes	A set of sample Change tickets is included. You can review, update, and close these tickets as you would a request for change in a live system.
Contracts	Sample contracts have been added to the system, including client companies with company and location records. Contract information has been added to other modules that share links to Contract Management.

2 User Profiles

CHAPTER

There are three areas of security that allow administrators to control user access within ServiceCenter:

- Operators define user access to ServiceCenter and its applications and utilities.
- Roles are a predefined set of profiles and capability words that can be referenced from an operator record.
- Profiles store rights and privilege information for users within each ServiceCenter application.

Profile records allow administrators to grant functionality specific to ServiceCenter application. Multiple operators can use a single profile record to create job-specific privileges. You can enhance these job-specific privileges by creating roles.

Read this chapter for more information about:

- *Operators* on page 22
- *User Roles* on page 22
- *User Profiles* on page 22
- *Types of User Profiles* on page 22
- *How the System Determines a User's Profile* on page 23
- *Out-of-the Box User Profiles* on page 23
- *Adding a Profile* on page 32
- *Editing Profiles* on page 39

Operators

The Operator record designates specific settings for each logon name used in ServiceCenter. Information in the Operator record is evaluated to determine the:

- Logon names and passwords.
- Capabilities of the operator to execute applications and utilities. (Capability words grant access to applications and utilities. They are defined in the capability file and are assigned in the Operator record through the Execute Capabilities array.)
- Initial application user accesses when logging on.

User Roles

User roles serve as the basis for assigning user profiles to operators. The role is referenced in the user's Operator record. When you select the user's role, the user's access rights and privileges in the form of user profiles are assigned for each of the ServiceCenter applications.

Note: User roles are not required in order to assign user profiles to operators. User roles allow administrators to conveniently add a standard set of functionality for a new operator.

User Profiles

Profile records allow you to grant rights and functionality specific to ServiceCenter applications. Multiple operators can use a single profile record, creating job-specific privileges.

Types of User Profiles

- User Profiles store information about a user's rights and privileges in ServiceCenter. Each profile defines a specific level of functional access to a ServiceCenter application, from basic user with limited access to system administrator with full access.
- Each application is delivered with a profile record named Default which is used when a profile does not exist. With Default, the environment record allows access to the application without a profile record.

Note: If you turn off the ability to access an application without a profile, a user profile must be defined to grant access to the application. Otherwise, users are denied access to the applications.

How the System Determines a User's Profile

When a user attempts to access one of the ServiceCenter applications, the system follows these steps to determine which profile to use:

- The system retrieves the profile name from the Operator record and accesses the profile record for the specific application.
- If the system cannot find a user profile, the system uses the Default profile.
- If a profile is not found and the ability to use the Default profile is set to false, a user is denied access to the application.

Out-of-the Box User Profiles

User profiles have varied levels of module access to accommodate the different levels of ServiceCenter users. The following table describes the out-of-box User Profiles that have been set up within ServiceCenter that can be used when assigning User Roles to system users.

User Profile	Privileges
ADMIN	<p>Used in Service Management, Incident Management, Root Cause Analysis, Inventory Management, Change Management, and Request Management to grant full administrative access:</p> <ul style="list-style-type: none"> ■ All basic options, including open, update, view, and close Call reports, Incident tickets, and Root Cause Analysis tickets. ■ Search the ServiceCenter knowledge base. ■ Open, review, approve, deny, and retract changes within Change Management. ■ Open and close quotes and orders within Request Management. ■ Approvals. ■ All print options. ■ All query options.
APPROVER	<p>Used in Change Management and Request Management to grant approval authority for requests for change and Request Management quotes and orders. Other privileges include:</p> <ul style="list-style-type: none"> ■ Basic options, such as, count records, find, and notify. ■ All query options. ■ All print options.
ASSET MANAGEMENT	<p>Used in Change Management to manage all Inventory Management assets and grant full administrative access:</p> <ul style="list-style-type: none"> ■ All basic options, including open, update, view, and close change tickets. ■ Search the ServiceCenter knowledge base. ■ Open, review, approve, deny, and retract changes within Change Management. ■ Approve changes within the CA and ONSITE approval groups. ■ All print options. ■ All query options.
CLIENT SECURITY	<p>Used in Incident Management to grant the following:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close incident tickets. ■ Search the ServiceCenter knowledge base. ■ Reopen, log, print, and allow inefficient queries.

User Profile	Privileges
COORDINATOR	<p>Used in Change Management, Inventory Management, and Request Management to grant administrative access to coordinate Change Management requests for change and Request Management quotes and orders. Privileges include:</p> <ul style="list-style-type: none"> ■ All basic options, including open, update, and view requests for change and quotes and orders. ■ Approvals and overrides. ■ All print options. ■ All query options.
DEFAULT	<p>Used in Service Management, Incident Management, Root Cause Analysis, Inventory Management, Change Management, and Request Management to grant the following access rights and privileges, including:</p> <ul style="list-style-type: none"> ■ View, log, find, fill, notify, count, search, override, allow inefficient queries, and check for duplicates for Call reports, Incident tickets, Root Cause Analysis tickets, requests for change, and quotes and orders. ■ Search the ServiceCenter knowledge base. ■ Within Change Management, all basic options, as well as all approval, print, and query options. ■ Within Request Management, most basic options, as well as all approval and print options and most query options.
EMERGENCY GROUP	<p>Used in Change Management to expedite a change from within the Change Management module. All basic, approval, print, and query options are granted.</p>
FACILITIES	<p>Used in Incident Management and Change Management to coordinate facilities activities. The following privileges are granted:</p> <ul style="list-style-type: none"> ■ Most basic options, including view, log, find, fill, notify, count, search, override, allow inefficient queries, and check for duplicates for Incident tickets and requests for change. ■ Approvals without override. ■ All print and query options. ■ Search the ServiceCenter knowledge base.
FIELD ENG	<p>Used in Incident Management to grant the following access rights and privileges:</p> <ul style="list-style-type: none"> ■ Some of the basic options, including view, log, find, fill, notify, count, search, override, allow inefficient queries, and check for duplicates for Incident tickets. ■ Search the ServiceCenter knowledge base.

User Profile	Privileges
HELPDESK	<p>Used in Change Management to grant the following access rights and privileges:</p> <ul style="list-style-type: none"> ■ Track alerts. ■ Calculate the risks. ■ Some of the basic options, including view, log, find, fill, notify, save, count, search, override, allow inefficient queries, review, find parents changes, open tasks, and check for duplicates for requests for change. ■ Search the ServiceCenter knowledge base. ■ Approvals without override. ■ All print options. ■ All query options.
HELPDESK TECH	<p>Used in Service Management and Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, close, and inactivate Incident tickets. ■ Search the ServiceCenter knowledge base. ■ Reopen, log, print, and allow inefficient queries. ■ Gain database access. ■ Create new categories.
INITIATOR	<p>Used in Service Management, Incident Management, Root Cause Analysis, Inventory Management, and Change Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, view, log, find, fill, and notify call reports and tickets. ■ Search the ServiceCenter knowledge base. ■ Log, print, count, and allow inefficient queries. ■ Create duplicates, new categories, and notes.
ISP	<p>Used in Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, close, and inactivate Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device.

User Profile	Privileges
ISPADMIN	<p>Used in Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, close, and inactivate Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device. ■ Inactivate and mass inactivate tickets. ■ Create new categories.
LAN SUPPORT	<p>Used in Change Management and Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device.
M/F SUPPORT	<p>Used in Change Management and Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create categories, allow inefficient queries, and check for incident duplicates on a device.
MANAGEMENT	<p>Used in Change Management to manage all requests for change. Grants full administrative access privileges, including:</p> <ul style="list-style-type: none"> ■ All basic options, including open, update, view, and close change tickets. ■ Search the ServiceCenter knowledge base. ■ Open, review, approve, deny, and retract changes within Change Management. ■ Approve changes within the ASSET MANAGEMENT and CA approval groups. ■ All print options. ■ All query options.

User Profile	Privileges
MASTER	<p>Used in Request Management and includes the following privileges:</p> <ul style="list-style-type: none"> ■ All basic functions, excluding database manager activities. ■ Alert log. ■ Approval options, including approve, mass approve, approval log, reevaluate, reset, and override. ■ All print options. ■ All query options.
ONSITE SUPPORT	<p>Used in Incident Management and Change Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Some of the basic options, including open, update, view, and close Incident tickets and requests for change. ■ Approvals for Change Management. ■ All print options. ■ All query options.
PROCUREMENT	<p>Used in Incident Management and Change Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Some of the basic options, including open, update, view, and close Incident tickets and requests for change. ■ Approvals for Change Management. ■ All print options. ■ All query options.
RECEIVER	<p>Used in Request Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Some of the basic options, including open, update, view, and close quotes and orders. ■ All approval options. ■ All print options. ■ Most query options.
REPLACEMENT	<p>Used in Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device.

User Profile	Privileges
REQUESTOR	<p>Used in Request Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Some of the basic options, including open, update, view, and close quotes and orders. ■ Log, reopen, find, and fill. ■ Post, reopen, generate orders, and so on. ■ Alert log. ■ All print options. ■ Some query options. ■ No approval options available.
REVIEWER	<p>Used in Service Management, Incident Management, Root Cause Analysis, Inventory Management, Change Management, and Request Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ A few of the basic options, including audit, close, count, find, and list pages. ■ Alert log. ■ All print options. ■ Most query options. ■ No approval options.
SEAGATE INFO	<p>Used in Incident Management to allow the following privileges:</p> <ul style="list-style-type: none"> ■ Browse. ■ Advanced search. ■ Print, views, and count.
SERVICE MANAGEMENT	<p>Used in Change Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Some of the basic options, including alerts, open, find, fill, notify, and save requests for change. ■ Approvals. ■ All print options. ■ All query options.

User Profile	Privileges
SERVICE TECH	<p>Used in Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Most of the basic options, including open, update, view, and close Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device.
SOFTWARE	<p>Used in Change Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Some of the basic options, including alerts, open, find, fill, notify, save requests for change, and IR query. ■ Approvals. ■ All print options. ■ All query options.
STANDARD	<p>Used in Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Most of the basic options, including open, update, view, and close Incident tickets. ■ Log, find, fill, and print tickets. ■ Create new categories and notes, allow inefficient queries, and check for incident duplicates on a device.
SYSADMIN	<p>Used in Incident Management, Service Management, Inventory Management, Root Cause Analysis, Change Management, and Request Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Call reports, Incident tickets, and Root Cause Analysis tickets. ■ Search the ServiceCenter knowledge base. ■ Open, review, approve, deny, and retract changes within Change Management. ■ Open and close quotes and orders within Request Management.
SYSTEMS ADMIN	<p>Used in Incident Management and Change Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, and view Incident tickets and requests for change. ■ Search the ServiceCenter knowledge base. ■ Open, review, approve, deny, and retract changes.

User Profile	Privileges
SYSTEMS SUPPORT	<p>Used in Change Management and Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device.
TECH	<p>Used in Inventory Management, Root Cause Analysis, Change Management, and Request Management....</p> <ul style="list-style-type: none"> ■ Open, update, and view Root Cause Analysis tickets. ■ Reopen, find, and fill tickets. ■ Perform advanced search. ■ Create personal inboxes. ■ Approvals and alerts within Change Management. ■ All print and query options within Change Management. ■ All approval and print options within Request Management. ■ Most query options within Request Management.
TECH LEVEL 2	<p>Used in Root Cause Analysis to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, and view Root Cause Analysis tickets. ■ Reopen, find, and fill tickets. ■ Perform advanced search. ■ Create personal inboxes.
TELECOMS	<p>Used in Change Management and Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device.

User Profile	Privileges
TRAINING	<p>Used in Change Management and Incident Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Incident tickets. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device.
WAN SUPPORT	<p>Used in Incident Management and Change Management to grant the following privileges:</p> <ul style="list-style-type: none"> ■ Open, update, view, and close Incident tickets and requests for change. ■ Log, reopen, find, fill, and print tickets. ■ Perform advanced search. ■ Gain database access. ■ Create duplicates, allow inefficient queries, and check for incident duplicates on a device. ■ Alerts and approvals within Change Management. ■ All print and query options within Change Management.

Adding a Profile

There are two ways to add user profiles in ServiceCenter. You can use the Central Administration Utilities (CAU) or individual ServiceCenter applications. For more information about adding a profile from within a ServiceCenter application, see the individual application chapters in this guide. The CAU allows you to:

- Add and edit users, profiles, assignment groups, and message groups from one central place.
- View a summary of a user's security information.
- Access application-specific profile configurations.

To add a new profile to an operator record using the CAU:

- 1 Log in to ServiceCenter with an administrator profile, such as falcon. Figure 2-1 shows the ServiceCenter home menu.



Figure 2-1: ServiceCenter home menu

- 2 Click the **Utilities** tab shown in Figure 2-2.

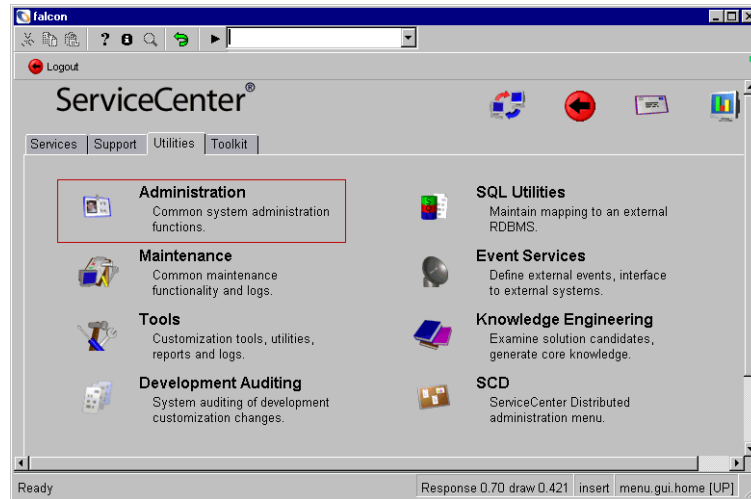


Figure 2-2: ServiceCenter home menu: Utilities tab

- 3 From the Utilities tab, click **Administration**. Figure 2-3 shows the Administration menu and the Information/Security/Insight tab.

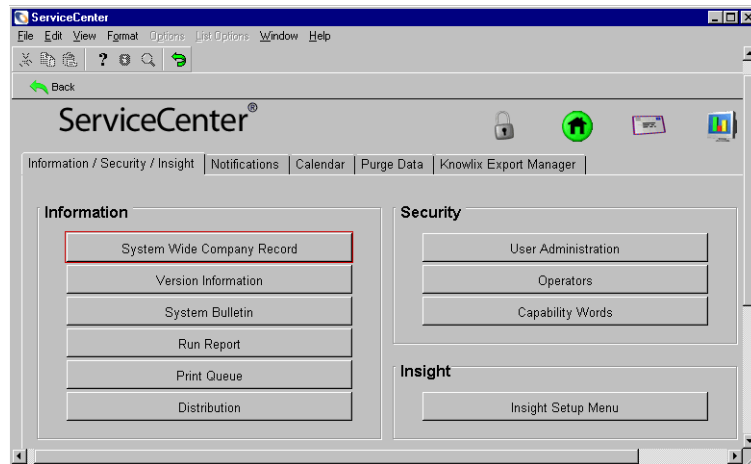


Figure 2-3: Information/Security/Insight tab

- 4 Click **User Administration**. Figure 2-4 shows the CAU menu.

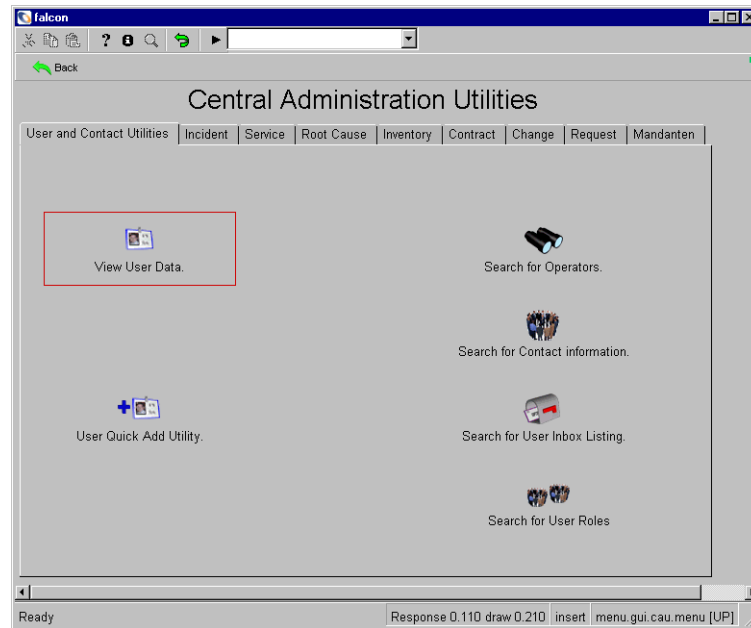


Figure 2-4: CAU menu

- 5 The tabs in the form represent the options available to centrally manage user access and privileges, and to conduct searches for contacts and operators.
- 6 From the CAU menu, click **View User Data**.
- 7 Type the user's name in the dialog box and click **OK**. You can choose a sample user, BOB.HELPDESK, from the drop-down list.

- 8 The Operator record for BOB.HELPDESK displays. Notice that BOB has an Root Cause profile of TECH.

ServiceCenter
File Edit View Format Options List Options Window Help

OK Cancel Save Delete Views Find Fill

OPERATOR RECORD

General Assignment/Message Groups

Login Name: BOB.HELPDESK Edit Op Info
Contact Name: HELPDESK, BOB Edit Contact
Email Addr: _____

Application Profiles

User Role: HELPDESK TECH LEVEL 1

Service Profile: HELPDESK TECH
Incident Profile: HELPDESK TECH
Root Cause Profile: TECH
Inventory Profile: INITIATOR
Contract Profile: DEFAULT
Change Profiles: HELPDESK
Request Profiles: REQUESTOR

Find

Add New Profile

Figure 2-5: Bob.Helpdesk operator record

- 9 Click the Find icon, a magnifying glass, to the right of the Root Cause Profile field.
- 10 Double-click the TECH profile shown in Figure 2-6.

User Rootcause Profile

Back Refresh 3/2 Count

name	full.name	initial.format
TECH	false	

Selected line is row 1 of 2 records insert rcenv.qbe(profile.list) [UP]

Figure 2-6: User Root cause Profile

- 11 The Privileges for the TECH profile appear. If you want Bob to close Root Cause records, you must create a new profile that allows him to do so.

- a Type a new profile name in the **Profile Name** field, or choose a pre-defined profile from the drop-down list. For this example, type **TECH 2**, as shown in Figure 2-7.

User Rootcause Profile: TECH 2

OK Cancel Previous Next Add Save Delete Find Fill

Root Cause Security Profile **Profile Name**

Privileges and Views

<input checked="" type="checkbox"/> Browse	Initial Inbox <input type="text"/>
<input checked="" type="checkbox"/> Open	Initial Format <input type="text"/>
<input checked="" type="checkbox"/> Update	Edit Format <input type="text"/>
<input type="checkbox"/> Close	Search Format <input type="text"/>
<input checked="" type="checkbox"/> Reopen	List Format <input type="text"/>
<input checked="" type="checkbox"/> Find	Manage Format <input type="text"/>
<input checked="" type="checkbox"/> Fill	Print Format <input type="text"/>
<input type="checkbox"/> Print	Open Script <input type="text"/>
<input checked="" type="checkbox"/> Views	Resolution Script <input type="text"/>
<input checked="" type="checkbox"/> Count	
<input checked="" type="checkbox"/> Advanced Search	
<input type="checkbox"/> Use Operator Full Name	<input checked="" type="checkbox"/> New Thread: Inbox -> Search
<input checked="" type="checkbox"/> Can Create Personal Inboxes	<input checked="" type="checkbox"/> New Thread: Search -> List
<input type="checkbox"/> Can Create Global Inboxes	<input checked="" type="checkbox"/> New Thread: List -> Edit
<input type="checkbox"/> Lock on Display	<input checked="" type="checkbox"/> New Thread: Inbox -> Edit
<input type="checkbox"/> Allow Inefficient Query	
<input type="checkbox"/> Skip Query Warning	

0 User Rootcause Profile record added. Response 0.40 draw 0.90 insert rc.profile.g(profile.view) [UP]

Figure 2-7: Profile Name



- b Click **Add**. The status bar displays this message: **User Rootcause Profile record added.**

Click **Add** to create a new profile with the same privileges, but with a new name in the **Profile Name** field.

Click **Save** to overwrite the original profile with the changes to the privileges and a new profile name.

You have added a new profile for BOB.HELPDESK, which is Root Cause Profile: **TECH 2**.

To add a new profile to a user role:

In the previous task you added a new Root Cause profile, TECH 2, for BOB.HELPDESK. You can also add the Root Cause profile to BOB.HELPDESK's user role, HELPDESK TECH LEVEL 2.

- 1 Complete step 1 on page 33 through step 5 on page 35.
- 2 From the CAU menu, click **Search for User Roles**. The User Role Search form appears.
- 3 From his operator record, you know that BOB belongs to the HELPDESK TECH LEVEL 2 user role. If you do not know the exact name of the user role, you can click Search to locate it, or you can click Find from the operator record. Type HELPDESK TECH LEVEL 2 in the User Role field. Click Search.
- 4 Figure 2-8 shows the User Role form for HELPDESK TECH LEVEL 2. Select TECH 2 from the Root Cause Profile drop-down list.

The screenshot shows a software window titled "userrole: HELPDESK TECH LEVEL 2". The window has a menu bar with icons for OK, Cancel, Add, Save, Delete, Find, and Fill. Below the menu bar, the "User Role:" field is set to "HELPDESK TECH LEVEL 2". The "Description:" field contains "Second Level helpdesk support. Transaction of calls, and process more advanced tickets." The "Service Profile:" is "HELPDESK TECH", "Incident Profile:" is "HELPDESK TECH", "Root Cause Profile:" is "TECH", "Inventory Profile:" is "INITIATOR", "Contract Profile:" is "DEFAULT", "Change Profiles:" is "INITIATOR", and "Request Profiles:" is "REQUESTOR". The "Capability Words:" list includes "partial.key", "problem management", "query.stored", "inventory management", "change request", "change task", "OCMQ", and "OCML". The "Query Groups:" are set to "Basic", "Intermediate", and "Advanced". The status bar at the bottom displays "Ready" and "Response 0.90 draw 0.160 insert userrole.g(db.view) [UP]".

Figure 2-8: User Role form

- 5 Click Save. The status bar displays this message: **userrole record updated.**

Editing Profiles

ServiceCenter enables you to set operator profiles for users of each module. These profiles supplement and further restrict any rights defined in a user's operator record, based on the operator's assigned user role. These options enable you to control access to each ServiceCenter module. For more information, see the *System Administrator's Guide*.

To edit a Profile record:

- 1 Complete step 1 on page 33 through step 5 on page 35.
- 2 From the CAU menu, click the **Service** tab.
- 3 Click **SM Profiles**. Figure 2-9 shows the Service Management Security Profile form.

The screenshot shows a window titled "Search User Service Profile Records". Below the title bar is a toolbar with icons for Back, Add, Search, Find, and Fill. The main content area is titled "SM Security Profile" and contains a "Profile Name" field. Below this is a section titled "Privileges and Views" with a list of checkboxes: Browse, Open, Update, Close, Find, Fill, Print, Views, Count, Advanced Search, Use Operator Full Name, Can Create Personal Inboxes, Can Create Global Inboxes, Lock on Display, and Can Notify. To the right of these checkboxes are several input fields for "Initial Inbox:", "Initial Format:", "Edit Format:", "Search Format:", "List Format:", "Manage Format:", and "Print Format:". At the bottom right, there is a section for "New Thread" with checkboxes for "Inbox -> Search", "Inbox -> List", "List -> Edit", and "Inbox -> Edit". The status bar at the bottom shows "Ready", "Response 0.50 draw 0.70", and "insert cc.profile.g(profile.search) [UP]".

Figure 2-9: the SM Security Profile form

4 Do one of the following:

- Type the name of the Profile you want to edit and press **Enter**. For example, type HELPDESK TECH. Remember that profile names are case-sensitive.
- Click **Search** to perform a true query that retrieves a list of all current profile records. Double-click the record you want to view.

The Profile record appears.

5 Edit the record.

When you edit Change Management and Request Management profiles, you must rebuild the Message group definitions. The Message group definition record stores the individual login IDs of the group's members (reviewers) and approvers who will receive notification and messages during a change or request project.

From the **Options** menu, click **Rebuild Group** to apply the Message group definition member list (reviewers and approvers) changes.

6 Click **OK** or **Save**. The status bar displays this message:

The User *profilename* Profile record updated

where *profilename* is the name of the application with the updated security profile.

Note: User groups or operators with this profile will have their access rights changed to reflect this updated profile as long as you do not change the profile name. If you change the profile name, the user group or operator retain the old assigned profile.

3

CHAPTER

Service Management

When a call comes in to a help desk to report an incident, the operator opens a *call report* in Service Management. All pertinent data regarding the call is recorded in the report and a category is assigned to the call. If the incident being reported can be resolved at the time by the help desk operator, the call is closed and no further action is required. If the incident being reported requires the attention of another technician, an incident ticket can be opened directly from the call report. Incident tickets opened in this manner are quickly generated since they contain all the necessary information recorded in the call (for example, SLA involved, contract affected). This chapter describes how to administer the Service Management module.

Read this chapter for information about:

- *Accessing Service Management* on page 42
- *Administering Service Management* on page 43
- *Accessing the Security Files* on page 44
- *Managing User Information* on page 49
- *Setting Privileges and Views in the Service Management Profile* on page 53
- *Maintaining Inboxes* on page 56
- *Accessing the Macro List Editor* on page 57
- *Accessing Probable Cause Records* on page 58
- *Accessing the Knowledge Base* on page 60

Accessing Service Management

You can access Service Management forms for administrative purposes from the Service Management section of the ServiceCenter home menu, or from the Central Administration Utilities.

Central Administration Utilities is a central control utility that allows a system administrator to access the operator's record for user and contact information, application profile privileges, and the Mandanten utility. This central control utility gives the system administrator the ability to access and control several users or a group from one central location, rather than having to go to the individual ServiceCenter modules.

To learn more about using Central Administration Utilities, see the *System Administrator's Guide*.

To access Service Management:

- 1 Click **Service Management** in the ServiceCenter home menu.



Figure 3-1: ServiceCenter home menu

Figure 3-2 shows the Service Management menu.

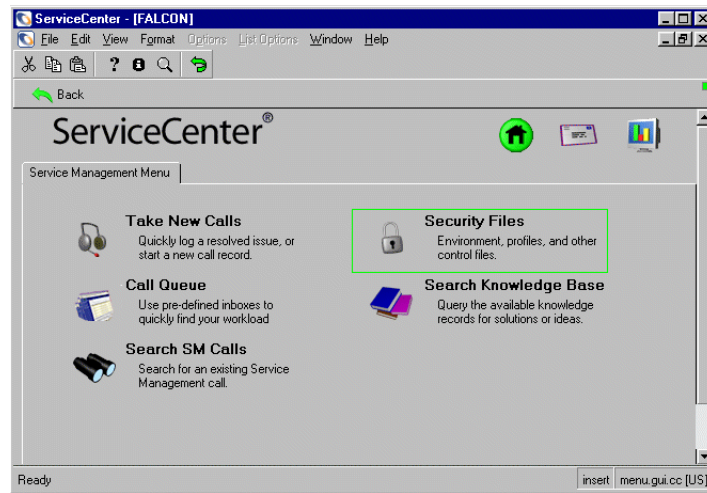


Figure 3-2: Service Management menu

The buttons on the Service Management menu allow you to open new Call records, access existing records, and configure the module.

Administering Service Management

This section discusses how to administer Service Management by adding and editing users and security profiles, and selecting Service Management Relationship Models. See the *System Administrator's Guide, Central Administration Utilities*, to learn about deleting users.

As a system administrator, you can add or edit ServiceCenter users from within Service Management and manage user profiles. You can restrict certain user rights and control the forms that your users see when accessing different parts of Service Management. The utilities that accomplish this are similar to those in Incident Management.

Security Files

Service Management contains built-in security. Through this security, you can define the capabilities for individual users (operators). For example, certain users may not have the rights to close call reports, while others may.

Users

Each person who logs onto ServiceCenter must have a personal information record stored in the **operator** file. Information associated with a user includes personal data, such as name, address, phone numbers, and login name, and password for ServiceCenter. ServiceCenter operator records also store *capability words* for a given user. Without an operator record, a user cannot log onto ServiceCenter. A user can belong to a group or utilize a Profile.

Profiles

Users must have a Service Management Profile in their operator record, or use the default, in order to gain access to the Service Management module. Records in the **smenv** file store Service Management rights and privileges information, such as, whether or not a user can close a call report. Profiles also store information that may affect the way Service Management looks and behaves. For example, a profile can define a personal search form for a specific user.

To learn more about application profiles, see [User Profiles](#) on page 21.

Environment Record

Service Management contains an environment record that defines options that affect the functionality of the Service Management module for all Service Management users. Some of the typical options stored in this record include:

- The relationship model
- Access rights
- A default category

Accessing the Security Files

To access security files from the Central Administration Utilities, see [User Profiles](#) on page 21.

To access security files from the Service Management Menu:

- 1 Click **Service Management** in the ServiceCenter home menu. The Service Management menu appears.

- 2 Click **Security Files**. Figure 3-3 shows the Service Management Security Administration Utility menu.

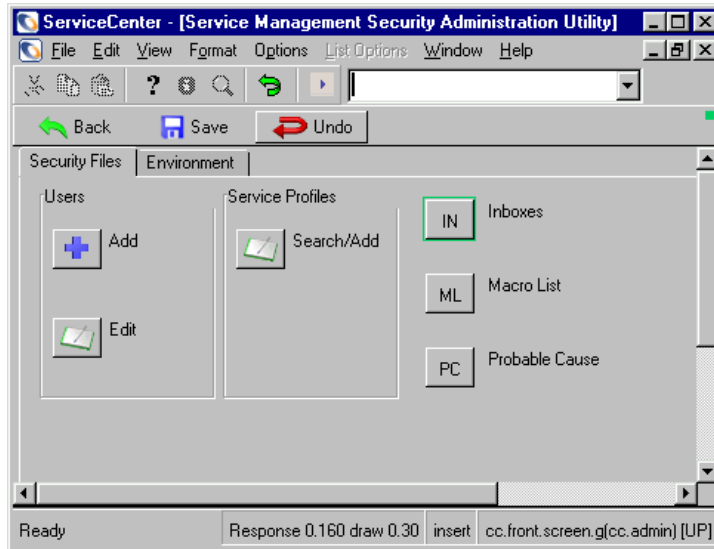


Figure 3-3: Service Management Security Administration Utility

- 3 Click **Back** or **Return** to return to the Service Management menu.

Security Files Tab

The Security Files tab enables you to:

- Add or edit ServiceCenter users.
- Search for and Add Service Profile records.
- Access the Inbox Maintenance Utility.
- Access the Macro Editor.
- Access the Probable Cause file.

Environment Tab

The **Environment** tab, shown in Figure 3-4, allows you to make general settings for all users of Service Management.

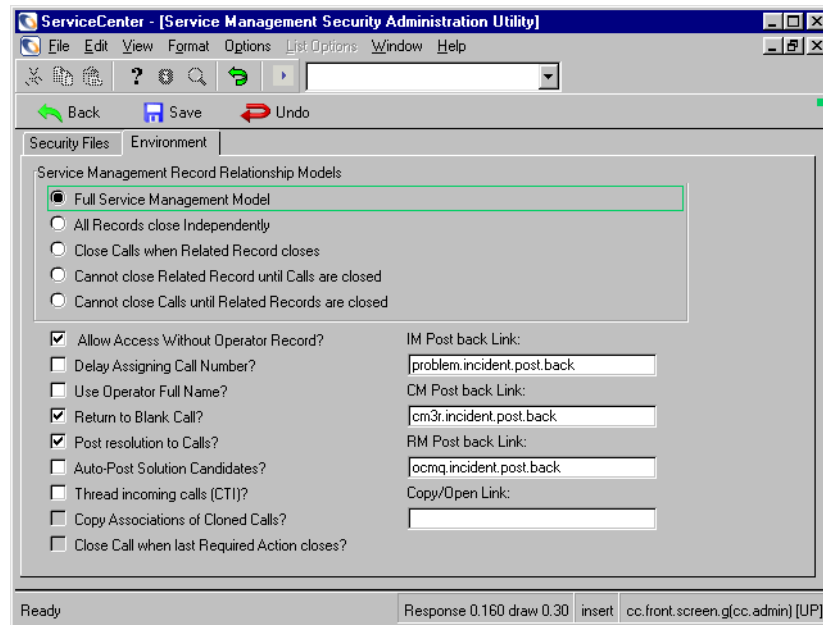


Figure 3-4: Environment tab

Service Management Record Relationship Models

The Service Management Relationship Models (SMRMs) are different methods that can be used to control the relationships between records inside ServiceCenter. Currently the SMRMs affect four record types: Service Management Calls, Incident Management Tickets, Change Management Changes, and Request Management Quotes.

ServiceCenter provides five models for managing the relationship between records in the principal modules:

- Full Service Management Model.
- All Records close Independently.
- Close Calls when Related Record closes.
- Cannot close Related Record until Calls are closed.
- Cannot close Calls until Related Records are closed.

Full Service Management Model

In this model, the state of a call is changed when each related record is closed, based on the value of the Notify By (callback) field in the call report.

The following callback options are available.

- **None.** The call is closed.
- **Email.** An e-mail is sent to the contact listed in the call informing contact that the related record has been closed. The call is then closed.
- **Page.** A page is sent to the contact listed in the call. The call is then closed.
- **Telephone.** A required action is added for the call. This action tells the user why the customer needs to be contacted. It also prevents the call from being closed until all required actions have been inactivated. The call then goes into the Open- Call back state.

All Records Close Independently

In this model, all Call records close independently. The state of related records has no bearing on whether a record can be closed. Closing the Call record does not affect records that are related to it.

Close Calls when Related Record Closes

In this model, when the last related record closes, the call is closed.

Cannot close Related Record until Calls are closed. In this model, records related to a call cannot be closed until the call is closed.

Cannot Close Calls Until Related Records are Closed

In this model, a call cannot be closed until all related incident tickets, change requests, and request management quotes are closed.

General User Options

The following table lists general user options.

Option	Description
Allow Access Without Operator Record	Permits users who do not have a Profile for Service Management to access the module by using the DEFAULT profile. See the <i>System Administrator's guide</i> for more information.
Delay Assigning Call Number?	No reference number is assigned to a call until after New is clicked in the initial call report form. Note: When this delay number is set to <i>true</i> , there is no unique identifier to tie an attachment within the file. Attachments cannot be saved when you open an incident, but only when saving an update to the file after the unique identifier has been assigned.
Use Operator Full Name?	System uses the name entered in the Full Name field of the operator record when time stamping call reports (on open, update, and so on) instead of using the operator's login name.
Return to Blank Call?	System returns the user to a blank (new) call form after the creation of an incident ticket.
Post resolution to Calls?	System posts the resolution of a closed ticket to the related call report.
Auto-Post Solution Candidates?	System automatically posts solutions from an incident ticket to the Global Knowledge feature if the Solution Candidate check box is selected.
Thread incoming calls (CTI)?	If this check box evaluates to <i>true</i> (selected) for users of Computer Telephony Integration, a Take New Call form opens each time a call is received. If this option evaluates to <i>false</i> , the current call is saved and replaced by the information from the incoming call.
Copy Associations of Cloned Calls?	Whether or not you want to copy the associations to other records when cloning a call.
IM Post back Link	Link record used to post information from a related Incident to the Call when the Incident is closed.
CM Post back Link	Link record used to post information from a related Incident to the Call when the Change is closed.

Option	Description
RM Post back Link	Link record used to post information from a related Incident to the Call when the Request is closed.
Copy/Open Link	When you copy a ticket, data from the ticket specified here will be copied to the new ticket based on the link record.


Managing User Information

You can add or edit a ServiceCenter user from the Central Administration Utilities. Within these utilities, you can add or edit a user's information, including contacts, user profiles, and passwords. See the *System Administrator's Guide* for detailed information about user access and security administration from the Central Administration Utilities.

To add and edit a user within the Service Management Security Administration Utility form, see the steps described in *Adding a User* on page 49 and *Editing User Records* on page 51.

Adding a User

To add a user in Service Management:

- 1 Click **Service Management** in the ServiceCenter home menu. The Service Management menu appears.
- 2 Click **Security Files**. The Service Management Security Administration form appears.
-  3 Click **Add in the Users structure**. A dialog box prompts you to type the name of the user you want to add.
- 4 Type the name of the new Service Management user. For example, you can add a user named Joe.User.
- 5 Click **OK** or press **Enter**.
- 6 A dialog box displays a prompt to clone another user. Click **Yes** to clone another user and do one of the following:
 - Select an existing operator record to copy and modify. Either click the drop-down arrow to display a QBE list of existing user records or type the name of the user you want to copy. As you type the first few letters, the name is placed in the field. For this example, type **B** and **BOB.HELPDESK** fills the field.
 - Select a blank record.

7 Click OK.

The new operator record appears with the new operator's name in the Login Name text box.

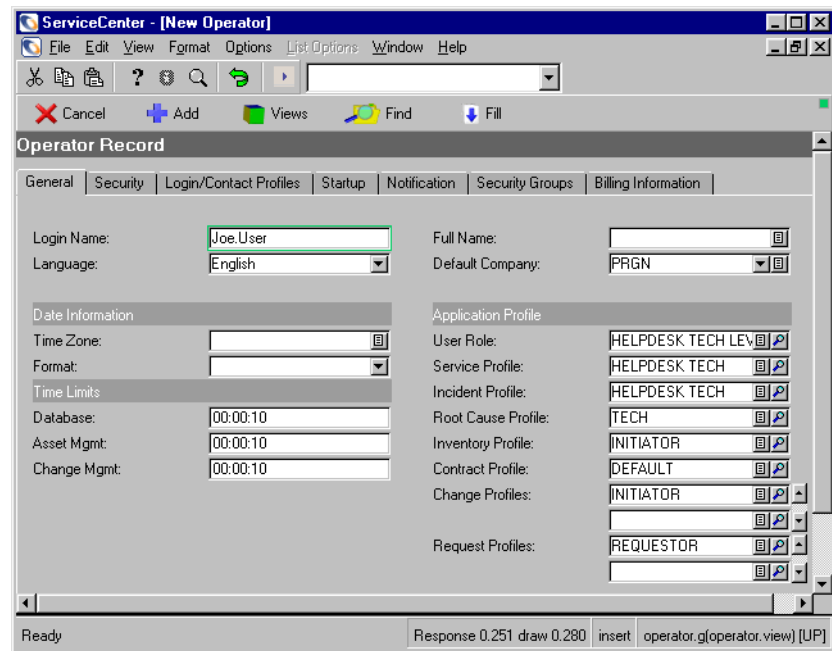


Figure 3-5: Operator record

- 8 Modify the operator record as needed. Refer to the *System Administrator's Guide* for instructions on creating new operator records.
- 9 Specify a Resource Type on the Login/Contact Profiles tab.
- 10 Click Add to save the new operator record.
- 11 A dialog box displays a prompt to ask if the new user already has a contact record.
 - a Click No.
 - b Enter the user's contact name by typing it in, or by selecting it from the drop-down list.
 - c Click OK.
 - d Modify the contact information as needed.
 - e Click Add to save the contact record. The status bar displays this message: Contact Information record added.

- 12 Click OK to return to the Service Management Security Administration Utility menu. The status bar displays this message: **The New User Process is finished.**

Based upon the User Role selected when the Operator record was added, the Service profile application access privileges and views are assigned.

Editing User Records

Controls in the security files allow you to edit a user's Service Management Profile records and operator record.

Note: To add a new user by copying an existing profile, see [Adding a User](#) on page 49.

To edit existing user records:

- 1 Click **Service Management** in the ServiceCenter home menu. The Service Management menu appears.
- 2 Click **Security Files** in the Service Management menu. The Service Management Security Administration form appears.
- 3 Click **Edit** in the Users area. A dialog box displays a prompt to select an operator record to edit.
- 4 Click **OK** or select an operator from the record list. The **CAU.operator** form appears and provides access to editing the operator's record, user profiles, and assignment/message groups.
- 5 Make any necessary changes to the various records, and then click **Save** or **OK**.



Adding or Editing Service Profiles

If the application profile settings need to be different, you can add a new profile or edit the existing profile.

To add a profile:

- 1 Click **Service Management** in the ServiceCenter home menu. The Service Management menu appears.
- 2 Click **Security Files**.
- 3 Click **Search/Add** in the Service Profiles structure. The Service Profile appears.
- 4 Enter the name of the Service Management profile you want to add.

- 5 Select the appropriate parameters for the user. For more information, see *Setting Privileges and Views in the Service Management Profile* on page 53.



- 6 Click **Add** to save the Profile record.

To add a new profile using an existing profile:

- 1 Check the User Role in the Operator record to make sure the appropriate profile settings apply, which are based on the User Role selected.

Note: If you select a different User Role, click **Fill** in the **User Role** field, so that the applicable Service profile access privileges and views are reset appropriately for each module.

- 2 Click **Find** to the right of the **Service Profile** field. The User Service Profile form displays.
- 3 Modify the privileges as necessary.
- 4 Enter a new name in the **Profile Name** field.
- 5 Click **Add**.

Note: Clicking **Add** keeps the original profile you modified and adds the new profile as long as you entered a new name in the Profile Name field. Clicking **Save** would overwrite the original profile with the changes to the privileges and a new profile name.

To edit a profile:

- 1 Check the User Role in the Operator record to make sure the appropriate profile settings apply, which are based on the User Role selected.

Note: If you select a different User Role, click **Fill** in the **User Role** field, so that the applicable Service profile access privileges and views are reset appropriately for each module.

- 2 Click **Find** to the right of the Service Profile field. The User Service Profile form displays.
- 3 Modify the privileges as necessary.
- 4 Click **Save**.

Setting Privileges and Views in the Service Management Profile

The Service Management profile form is used to define Profiles for users who plan to access Service Management. For an out-of-box defined solution, select the appropriate User Role for your new operator. (See the *System Administrator's Guide* for information on User Roles.) The selected User Role in an operator record plays an important part in deciding what application profiles are going to be assigned to the user.

For more information about the privileges and views assigned for this profile, see [Service Management Privileges and Views](#) on page 53. To learn about adding and editing user profiles, see [Adding a Profile](#) on page 32 and [Editing Profiles](#) on page 39.

Service Management Privileges and Views

Privileges and views define the user's access privileges and views within the Service Management module. Figure 3-6 shows the SM Security Profile form.

ServiceCenter - [Search User Service Profile Records]

File Edit View Format Options List Options Window Help

Back Add Search Find Fill

SM Security Profile Profile Name :

Privileges and Views

<input type="checkbox"/> Browse	Initial Inbox: <input type="text"/>
<input type="checkbox"/> Open	Initial Format: <input type="text"/>
<input type="checkbox"/> Update	Edit Format: <input type="text"/>
<input type="checkbox"/> Close	Search Format: <input type="text"/>
<input type="checkbox"/> Find	List Format: <input type="text"/>
<input type="checkbox"/> Fill	Manage Format: <input type="text"/>
<input type="checkbox"/> Print	Print Format: <input type="text"/>
<input type="checkbox"/> Views	
<input type="checkbox"/> Count	
<input type="checkbox"/> Advanced Search	
<input type="checkbox"/> Use Operator Full Name	
<input type="checkbox"/> Can Create Personal Inboxes	<input type="checkbox"/> New Thread: Inbox -> Search
<input type="checkbox"/> Can Create Global Inboxes	<input type="checkbox"/> New Thread: Search -> List
<input type="checkbox"/> Lock on Display	<input type="checkbox"/> New Thread: List -> Edit
<input type="checkbox"/> Can Notify	<input type="checkbox"/> New Thread: Inbox -> Edit

Ready Response 0.80 draw 0.111 insert cc.profile.g(profile.search) [UP]

Figure 3-6: SM Security Profile record

The following table lists Security Profile fields.

Field	Description
Browse	Allows the user or group to view existing call reports.
Open	Allows the user or group to create new call reports.
Update	Allows the user or group to change existing call reports.
Close	Allows the user or group to terminate existing call reports.
Find	Provides access to ServiceCenter's Find function in Service Management.
Fill	Provides access to ServiceCenter's Fill function in Service Management.
Print	User or group has print capabilities in ServiceCenter.
Views	Provides access to defined alternate forms when viewing a call report.
Count	User or group can count the number of tickets in a QBE list by clicking Count.
Advanced Search	Provides access to ServiceCenter's advanced search capabilities to query for information.
Use Operator Full Name	System uses the name from the Full Name field of the operator record when time stamping call reports (on open, update, and so on) instead of using an operator's login name.
Can Create Personal Inboxes	Allows the user or group to create personal inboxes for their own use. Creating inboxes is discussed in the <i>User's Guide</i> .
Can Create Global Inboxes	Allows the user or group to create global inboxes for all Service Management users. Creating inboxes is discussed in the <i>User's Guide</i> .
Lock on Display	Locks the incident ticket the user has displayed on the screen, whether or not any modifications are being made. No other users can display or modify the ticket. If Lock on Display is not selected, an exclusive lock is set on the record only when it is being modified. If the record is only being displayed, other users can display or modify that record.
Can Notify	Gives access to the Notify function
Initial Inbox	Defines the default inbox for the user or group in Service Management.

Field	Description
Initial Format	Form displayed to the user or group when opening a call report. The default is <i>cc.incquick</i> .
Edit Format	Form displayed to the user or group when editing an existing call report. The default is <i>cc.incidents</i> .
Search Format	QBE form displayed to the user or group when searching for existing call reports. The default is <i>cc.incidents</i> .
List Format	Form used to display a record list. The default is <i>incidents.qbe</i> .
Manage Format	Form displayed when the user or group presses Call Queue. The default is <i>sc.manage.call</i> .
Print Format	Form used by the system for printing call reports for the user of group.
New Thread: Inbox > Search	Keeps the inbox displayed in a different window after a search is run from that inbox.
New Thread: Search > List	Keeps the search form open after a QBE list displays.
New Thread: List > Edit	Keeps a QBE list form displayed when a record is accessed.
New Thread: Inbox > Edit	Keeps an inbox displayed after a record is accessed. Note: Threading allows the previous window to remain displayed when a new record is accessed. For example, when a record is accessed from a QBE list, the QBE list remains after the record opens in a new window.

Maintaining Inboxes

You may add, edit, and delete inboxes from the Service Management Security Administration Utility. These are the same inboxes used by Incident Management, and the procedures for maintaining them are identical. For detailed instructions on adding, editing, and deleting inboxes, see the *User's Guide*.

The screenshot shows a web application window titled "ServiceCenter - [Search Inbox Records]". The window has a menu bar with "File", "Edit", "View", "Format", "Options", "List Options", "Window", and "Help". Below the menu bar is a toolbar with icons for "Back", "Add", "Search", "Find", and "Fill". The main content area is titled "Inbox Maintenance" and contains four tabs: "Basic", "Advanced Options", "Sub Inbox Info", and "Information". The "Basic" tab is selected, showing the following fields:

- This is an inbox against this file: [Dropdown menu]
- Full Inbox Name: [Text input field]
- Parent Inbox: [Text input field with a small icon]
- Short Inbox Name: [Text input field]
- Inbox is owned by: [Dropdown menu]
- Available to these Groups: [Dropdown menu]
- Results sorted by: [Dropdown menu]

The status bar at the bottom of the window displays "Ready" and "Response 0.120 draw 0.110 insert apm.inbox.edit.g(inbox.search) [UP]".

Figure 3-7: Inbox Maintenance form

To access inbox maintenance features:

- 1 Click **Service Management** in the ServiceCenter home menu. The Service Management menu appears.
- 2 Click **Security Files**. The Service Management Security Administration Utility form appears.
- 3 Click **Inboxes**. The `apm.inbox.edit` form with add, edit, and search capabilities appears.



- 4 Click **Search**. Figure 3-8 shows a QBE list of available inboxes.

The screenshot shows the ServiceCenter - [Inbox] window. The top part is a QBE list with columns: Inbox Name, Operator Name, Query, Group Name, and Inbox Type. The bottom part is the Inbox Maintenance window with the Basic tab selected.

Inbox Name	Operator Name	Query	Group Name	Inbox Type
All my Approvals	%NONE%	(file.name="cm3t" and c		Approval
All Open Calls	%NONE%	open~="Closed"		call
Calls I Reported	%NONE%	contact.name=\$lo.ufnan		call
Calls My Dept Reported	%NONE%	dept=\$lo.dept		call
Calls Opened in the Last	%NONE%	open~="Closed" and op		call

Inbox Maintenance

Basic | Advanced Options | Sub Inbox Info | Information

This is an inbox against this file:

Full Inbox Name:

Parent Inbox:

Short Inbox Name:

Inbox is owned by:

Available to these Groups:

Results sorted by:

Selected line is row 1 of 32 records retrieved | Response 0.181 draw 0.200 | insert | inbox.qbe.g [UP]

Figure 3-8: Inbox Maintenance: Basic tab

- 5 Click the inbox you want to view. The Service Management Inbox Maintenance shown in Figure 3-7 on page 56 form appears.

Accessing the Macro List Editor

You can create, edit, and delete macros from the Service Management Security Administration Utility. For more information, see the *System Administrator's Guide* or the *System Tailoring Guides*.

To open the Macro List:



- Click Macro List in the Security Administration Utility form. Figure 3-9 shows the Macro List.

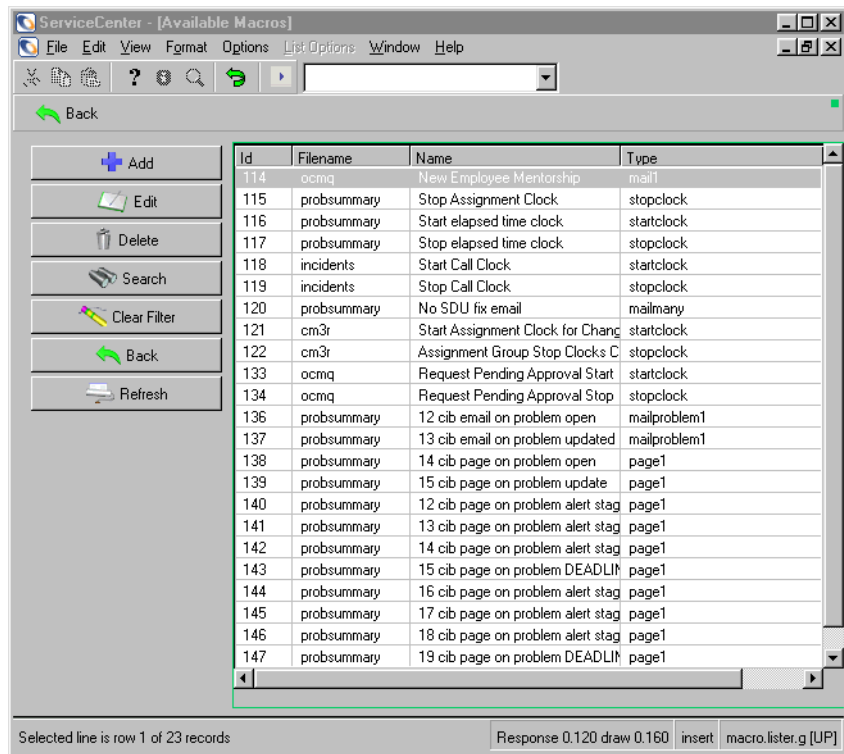


Figure 3-9: Available Macro list

Accessing Probable Cause Records

Call reports have a field called Cause Code, which performs a Find and Fill function that references data from probable cause records. The Cause Code can be used to categorize and assign incident tickets opened from call reports.

PC

- To access Probable Cause records:
- Click **Probable Cause** in the Security Administration Utility. Figure 3-10 shows the Probable Cause form.

The screenshot shows the ServiceCenter application window titled "ServiceCenter - [probcause]". It features a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for file operations and navigation. Below the toolbar is a table with five columns: Cause Code, Category, Resolution, Severity, and Incident Title. The table contains five rows of data. The second row is selected. Below the table is a form titled "PROBABLE CAUSE" with fields for Cause Code, Severity, Resolution Code, Category, Company, and Brief Description. There are also text areas for Key Words, Description, and Resolution. The bottom status bar indicates "Selected line is row 2 of 11 records" and "Response 0.50 draw 0.131 insert probcause.qbe.g [UP]".

Cause Code	Category	Resolution	Severity	Incident Title
Advice & Guidance		Advice & Guidance	2	Provision of advice and guidance to the user
Authentication Failure		Authentication Failure	4	User unable to provide adequate authentication of identity
Entitlement Failure		Entitlement Failure	4	User unable to provide adequate entitlement detail
Fault		Fault	2	Fault
No fault found		No fault found	2	Symptoms could not be reproduced or replicated

PROBABLE CAUSE

Cause Code: Advice & Guidance

Severity: 2

Resolution Code: Advice & Guidance

Category:

Company: DEFAULT

Brief Description: Provision of advice and guidance to the user

Key Words:

Description:

Resolution:

Resolution to this problem was achieved through the provision of advice and guidance to the user, either over the telephone by Email or at the users desk

Selected line is row 2 of 11 records

Response 0.50 draw 0.131 insert probcause.qbe.g [UP]

Figure 3-10: Probable Cause record

As the ServiceCenter administrator, you can modify these records or create new probable cause records tailored to your system. For more information, see [Probable Cause](#) on page 99.

Accessing the Knowledge Base

ServiceCenter allows you to make plain language queries for information (for example, information about an incident ticket or a question about equipment) using a Knowledge Base form. For example, a query can yield a list of incident tickets.

To access the Knowledge Base:

- Click **Search Knowledge Base** in the Service Management menu. Figure 3-11 shows the Knowledge Base search form.

Knowledge Area

ServiceCenter - [Knowledge Base]

File Edit View Format Options List Options Window Help

Back Search Clear

Find Solution - Knowledge Base

Select a Knowledge Area to begin search: Global Knowledge

Restrict Search to Which Field in IR key (blank=all fields):

What would you like to know?

Discovery Option:

☒ Shallow ☐ Complete Match

☐ Deep

Category: Subcategory: Product Type: Problem Type:

Device: Company: Location:

Ready Response 0.150 draw 0.20 insert sc.knowledge.prompt.core.g [UP]

Query Options Message Area Search Clear Data

Figure 3-11: Knowledge Base search form

For more information, see the *ServiceCenter User's Guide*.

4 Incident Management

CHAPTER

Incident Management allows help desk personnel to track reported incidents and spot trends before incidents become too large. The ServiceCenter Incident Management module allows a help desk operator to report various types of incidents: software, equipment, facilities, network, and so on. Support personnel can also track the progress of resolving these incidents. Incident Management automates the process of reporting and tracking an incident or groups of incidents associated with a business enterprise. This chapter describes administration of ServiceCenter's Incident Management module.

Read this chapter for more information about:

- *Incident Management Overview* on page 62
- *How Incident Management Works* on page 62
- *Accessing Incident Management* on page 64
- *Administering Incident Management* on page 66
- *Configuring the Incident Management Environment* on page 108
- *Status, Alerts, and Escalation* on page 111
- *The Two-Step Close* on page 113
- *Accessing Other Utilities* on page 121

For instructions about creating, updating, and closing incident reports, refer to the *ServiceCenter User's Guide*.

Incident Management Overview

Help desk operators open *incident tickets* (called problem tickets in earlier releases of ServiceCenter) for the type of incident reported.

A help desk operator can open a *call report* in Service Management to log a call without opening an incident ticket. A call record is useful when someone reports an incident to the help desk that requires no further action to resolve the incident. An incident ticket also can be opened from a call report.

Incident tickets are message carriers of incident information, like an e-mail system for incident communication. Incident tickets can be:

- Created and opened by help desk operators or automatically opened by ServiceCenter's Event Services utility. Refer to *Event Services Guide* for more information.
- Sent automatically to the proper system personnel.
- Tracked and resolved by those personnel and system managers.
- Sent by e-mail or fax to the user with a resolution to the incident.
- Linked to other modules, such as SLA or Contract Management, that deal with service agreements.

Incident tickets can be categorized to classify tickets by the type of incident or problem being reported. For example, an incident ticket describing a server incident stores different information than an incident ticket reporting a printer problem.

Incident tickets can be *prioritized*, *escalated*, and *assigned* to different personnel who are responsible for certain areas of a network or business. For administrative personnel, automatic escalation and other process control functions prevent incidents from exceeding service level agreements.

How Incident Management Works

Network users experience incidents with their computers or the services associated with the computer, such as printing. The users call their help desk to report such incidents. On a large network, support personnel are kept very busy, and you do not know if an incident is being fixed. The user may have to call again and leave a message, if the operator is not available. This process gets very frustrating for the user.

Service Management allows a help desk operator to keep track of calls by opening (creating) a call report. If a reported incident requires further action, an Incident Management ticket can be opened to track the incident. Forms are provided for various incident categories, and a Fill function allows an operator to complete portions of a ticket from a list of possible choices. The help desk operator then reviews the incident ticket to decide what action to take. If the incident needs to be resolved by another technician or department, the incident ticket can be forwarded. Once the incident is resolved, the incident ticket can be returned to the operator who opened it, with the resolution for confirmation. An incident ticket can also be reviewed before it is closed by anyone responsible for its resolution.

For example, if a user cannot print to the network printer, the user calls the help desk. From there, the help desk operator opens a call report to make a record of the call. In talking with the user, the operator discovers that the incident cannot be resolved during the phone call and must open an incident ticket. The operator sends the ticket to a technician, who discovers that the printer's network connection is broken. The technician updates the incident ticket and forwards the ticket to the network administrator, with a message that the printer connection is broken. The network administrator has the incident repaired, and closes the ticket. The service desk then informs the user that the ticket has been closed. All phases of this incident are covered from opening a call report and escalating the incident to having the problem resolved and closing the ticket.

Incident Management allows you to view related call reports and incident ticket records automatically. These dependent records can be selected and opened directly from the list view. Call reports and incident tickets are categorized to prevent different types of incidents from getting lost in the shuffle. For example, an incident ticket describing an e-mail incident stores different information than an incident ticket for a printer.

Incident Management is more than a message service. The appropriate personnel can escalate and reassign incident tickets. The system can also automatically issue alerts or escalate an incident that is not getting resolved. If a network printer is down, a technician or manager can escalate the incident to a higher priority to ensure the incident gets fixed quickly.

Accessing Incident Management

You can access Incident Management for administrative purposes from the Incident Management section of the ServiceCenter home menu, or from the Central Administration Utilities.

Central Administration Utilities allow a system administrator to access the operator's record for user and contact information, application profile privileges, and the Mandanten utility. This allows the administrator to control and access several users or a group's access from one central location, rather than having to control access from within each module or utility. For more information, see *User Profiles* on page 21 and the *System Administrator's Guide*.

To access Incident Management:

- 1 Log on to ServiceCenter with a system administrator profile, such as falcon.
- 2 From the ServiceCenter Home menu, click **Incident Management**, as shown in Figure 4-1.

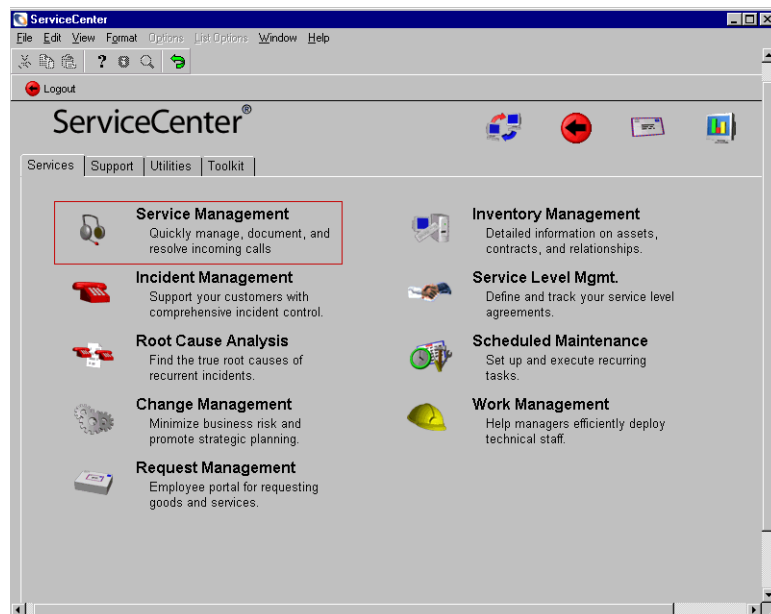


Figure 4-1: ServiceCenter home menu

Figure 4-2 shows the Incident Management menu.



Figure 4-2: Incident Management menu

Click a button to access Incident Management's various functions and utilities, such as incident ticketing, along with ServiceCenter functions, such as mail and system monitor.

The Tools tab accesses the Incident Management Tools (utilities). For more information, see the following sections:

- *Reset Downtime on page 122*
- *Build/Refresh Summary on page 123*
- *Alternate method on page 127*
- *Probable Cause on page 99*
- *Categories on page 81 and Predefined Incident Management Categories on page 82*
- *Inventory Management on page 169*

Administering Incident Management

This section discusses how to administer Incident Management by:

- adding and editing users, profiles, and category records.
- deleting profiles and category records.

Access is controlled through the application's security module.

Security Files

Incident Management contains built-in security. Through this security, you can define the capabilities of individual users (operators). For example, certain users may not have the rights to close incident tickets, while others may.

Environment

Incident Management contains an environment record that defines options that affect functionality of the Incident Management module for all Incident Management users. Some of the typical options stored in this record include:

- the default category for new incident tickets.
- Incident Management paging control.
- Distributed ticketing controls.

For more information, see [Configuring the Incident Management Environment](#) on page 108.

Users

Each person who logs into ServiceCenter is a user. Each user must have a personal information record stored in the **operator** file. Information associated with a user includes personal data such as name, address, phone numbers, login name, and password for ServiceCenter. ServiceCenter operator records also store *capability words* (as described below) for a given user. Without an operator record, a user cannot log onto ServiceCenter.

Profiles

Users must have an Incident Management Profile in their operator record, or use the default, in order to gain access to the Incident Management module. Records in the `pmenv` file store Incident Management rights and privileges information, such as, whether or not a user can close incident tickets. Profiles also store information that may affect the way Incident Management looks and behaves. For example, a profile can define a personal search form for a specific user. For more information, see [User Profiles](#) on page 21.

Capability Words

Incident Management security is mostly managed through profiles. In previous releases, capability words in the user's operator's record controlled a user's privileges. Incident Management uses the following capability words.

Capability Word	Description
SysAdmin	Grants the user system administrator authority to run administrative utilities for all ServiceCenter modules.
ProbAdmin	Grants the user administrative status <i>only</i> for the Incident Management module.
Problem Management	Grants use of the Incident Management module.

These capability words are entered in the user's operator record by an administrator to provide these privileges. For a complete list of capability words, see the *ServiceCenter System Administrator's Guide*.

Accessing the Security Files

To access security features from the Central Administration Utilities, see the *System Administrator's Guide*.

To access security features from the Incident Management menu:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files** in the Incident Management menu. Figure 4-3 on page 68 shows the Security Administration form.

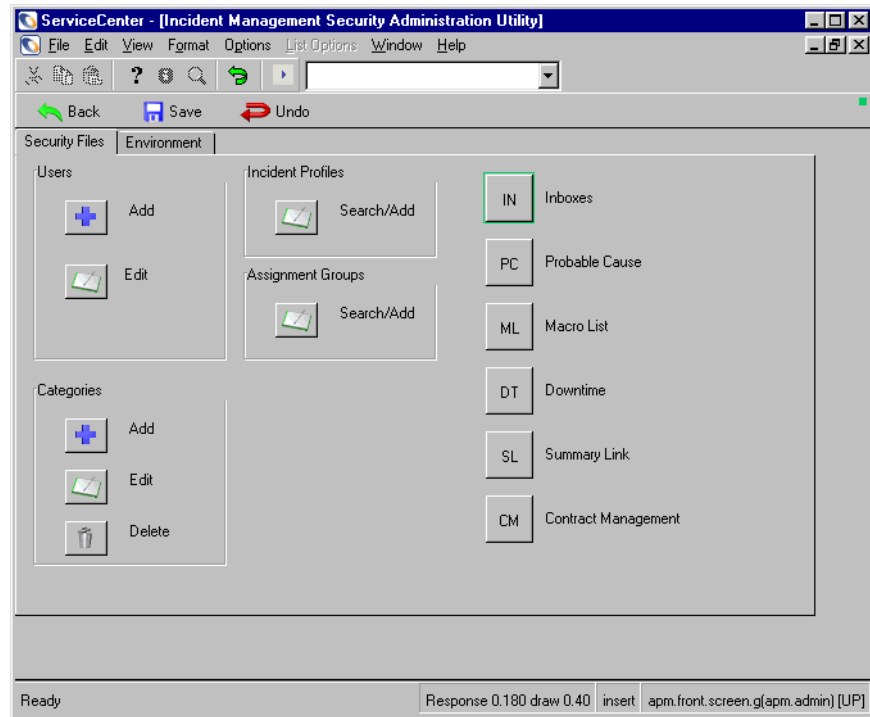


Figure 4-3: Incident Management Security Administration: Security Files tab

- 2 Select a security feature to edit, or click **Back** to return to the menu.

Security Files Tab

The **Security Files** tab allows you to add or edit:

- Incident profiles
- Assignment Groups
- Categories
- Downtime
- Summary Link
- Probable Cause
- Users (including the ServiceCenter operator record)
- Macro List
- Inboxes
- Cost Management

Environment Tab

The **Environment** tab allows you to make settings for the Incident Management Environment. For more information, see *Configuring the Incident Management Environment* on page 108.


Managing User Information

You can add or edit a ServiceCenter user from the Central Administration Utilities. Within these utilities, you can add or edit a user's information, including contacts, user profiles, and passwords. For more information about the CAU, see the *System Administrator's Guide*.

To add and edit a user within the Incident Management security files, see the steps described in *Adding a User* on page 69 and *Editing User Records* on page 71.

Adding a User

To add an Incident Management user:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. The Incident Management Security Administration utility appears.
-  2 Click **Add** in the Users section. A dialog box appears.
- 3 Type the name of the new Service Management user. For example, you can add a user named **Joe.User**.
- 4 Click **OK** or press **Enter**.
- 5 A dialog box displays a prompt to clone another user. Click **Yes** to clone another user.
- 6 Do one of the following:
 - Select an existing operator record to copy and modify. Either click the drop-down arrow to display a QBE list of existing user records or type the name of the user you want to copy. As you type the first few letters, the name is placed in the field. For this example, type **B** and **BOB.HELPDESK** fills the field.
 - Select a blank record.

- 7 Click OK. Figure 4-4 shows a new operator record with the new operator's name in the Login Name text box.

Figure 4-4: Operator Record


- 8 Modify the operator record as needed. For more information, see the *System Administrator's Guide*.
- 9 Specify a Resource Type on the Login/Contact Profiles tab.
- 10 Click **Add** to save the new operator record.
- 11 A dialog box displays a prompt that asks if the new user already has a contact record.
- 12 Click **No**.
- 13 Type the user's contact name, or select it from the drop-down list. Click **OK**.
- 14 Modify the contact information as needed. Click **Add** to save the contact record.
- 15 Click **OK** to return to the Incident Management Security Administration Utility menu. The status bar displays this message: **The New User Process is finished**.
- 16 Based upon the User Role selected when you added the Operator record, the Incident profile application access rights and privileges are assigned.

Editing User Records

Controls in the Security Administration Utility enable you to edit user Incident Management Profile records and the operator record.

Note: To add a new user by copying an existing profile, see [Adding a User](#) on page 69.


To edit existing user records:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. The Incident Management Security Administration utility appears.
-  2 Click **Edit** in the Users structure.
- 3 Select an operator from the drop-down list. The **CAU.operator** form displays the operators record, application profiles, and assignment/message groups.
- 4 Make any necessary changes to the various records, then click **Save** or **OK**.

Adding Incident Profiles

The IM Security Profile is used to define Incident Profiles and Assignment Groups for Incident Management users. The Profile form contains privileges and views parameters to help define user profiles. If the application profile settings need to be different, you can add a new profile or edit the existing profile.

To add a user profile:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. The Incident Management Security Administration utility appears.
- 2 Click **Search/Add** in the Incident Profiles structure. The Incident Profile appears.
- 3 Enter the name of the Incident Management profile you want to add.
- 4 Select the appropriate parameters for the user. For more information, see [Setting Privileges and Views in the Incident Management Profile](#) on page 73.
-  5 Click **Add** to save the Profile record.

To add a new profile using an existing profile:

- 1 Check the User Role in the Operator record to make sure the appropriate profile settings apply, which are based on the User Role selected.

Note: If you select a different User Role, click **Fill** in the **User Role** field, so that the applicable Service profile access privileges and views are reset appropriately for each module.

- 2 Click **Find** to the right of the **Incident Profile** field. The User Incident Profile form appears.
- 3 Modify the privileges as necessary.
- 4 Type a new name in the **Profile Name** field.
- 5 Click **Add**.

Note: Click **Add** to keep the original profile you modified and add the new profile as long as you entered a new name in the Profile Name field. Click **Save** to overwrite the original profile with the changes to the privileges and a new profile name.

Editing Incident Profiles

Incident Management allows you to set operator profiles for users of the module. These profiles supplement and further restrict any rights defined in a user's operator record. By default, no options are selected. These options allow you to control access to Incident Management.

Note: For more information, see *Adding a User* on page 69.

To edit a Profile record:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. The Incident Management Security Administration utility appears.



- 2 Click **Search/Add** in the Incident Profiles structure.
- 3 Do one of the following:
 - Enter the name of an Incident Management Profile you want to edit and press **Enter**.
 - Click **Search** to perform a *true* query and retrieve a list of all current Incident Management Profile records. From the displayed queue screen, select a record to view and modify by double-clicking on the Name in the record.
- 4 Update the fields you need to modify. Click **OK** or **Save**. The status bar displays this message: User Incident Profile record updated.

Setting Privileges and Views in the Incident Management Profile

The Privileges tab defines the user's rights in Incident Management. Figure 4-5 shows the Profile record on the Privileges tab.

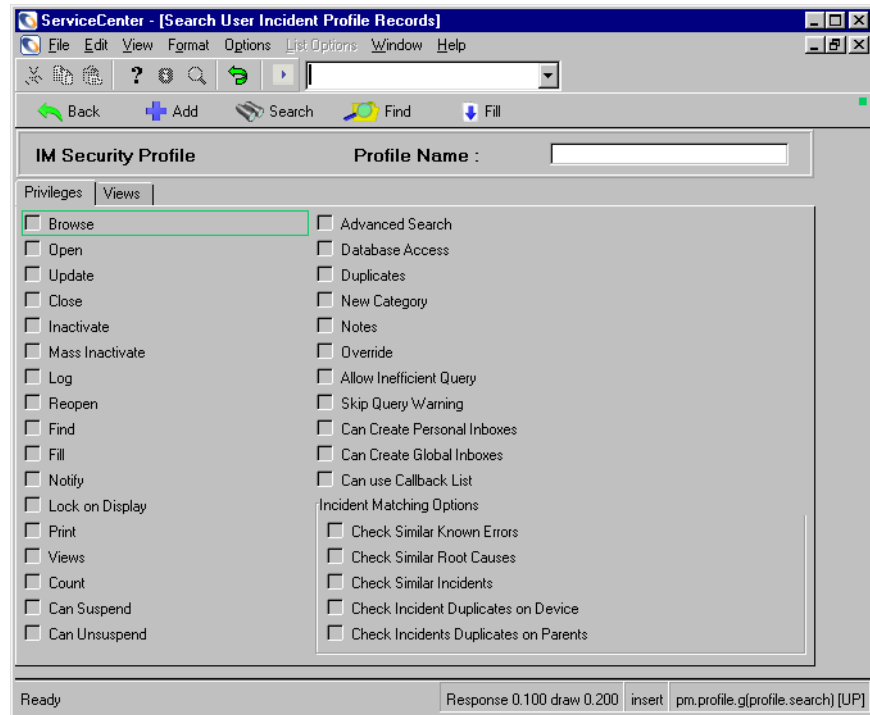


Figure 4-5: IM Security Profile record: Privileges tab

The following table describes the fields on the Privilege tab.

Privilege	Description
Browse	View existing incident tickets.
Open	Create new incident tickets.
Update	Change existing incident tickets.
Close	Close or resolve existing incident tickets.
Inactivate	Part of the two-step close process. Close or inactivate a resolved ticket after contacting the customer.

Privilege	Description
Mass Inactivate	Part of the two-step close process. Close or inactivate groups of resolved tickets. Be cautious in assigning this privilege, because tickets can be accidentally inactivated.
Log	Quick-Open an incident ticket.
Reopen	Reactivate a closed ticket.
Find	Use ServiceCenter's Find function in Incident Management.
Fill	Use ServiceCenter's Fill function in Incident Management.
Notify	Forward annotated tickets to other ServiceCenter users or to external e-mail.
Lock on Display	Locks the incident ticket on the screen, whether any modifications are being made. No other users can display or modify it. If you do not select Lock on Display , an exclusive lock is set on the record only when it is being modified. If you display the record without modifying it, other users can display or modify the record.
Print	Enable print capability in ServiceCenter.
Views	Use Incident Management's Views function to see incident tickets in defined alternate forms.
Count	Activates the count option in a QBE list to count the number of tickets in the list.
Can Suspend	Put a ticket into Suspend status.
Can Unsuspend	Take a ticket out of Suspend status
Advanced Search	Use advanced search capabilities to query for information.
Database Access	Access the Database Manager from the Options menu of an incident ticket.
Duplicates	Check for duplicate incident tickets when you open a new ticket.
New Category	Change the category of an incident ticket to another category.
Notes	Add notes to an incident ticket.

Privilege	Description
Override	<p>Close related call reports when closing an incident ticket. If this option is false (deselected), related calls are processed normally when an incident ticket is closed depending on the selected relationship model from the Incident Management Environment.</p> <p>Note: If you select Override in the Incident profile setting, then related calls will be closed, but no notifications will be sent out.</p>
Allow Inefficient Query	<p>Specify partially-keyed queries, which are queries without a complete set of information to do a search. Setting supersedes the setting in the Incident Management Environment Record.</p> <p>Note: If Skip Query Warning is true, ServiceCenter overrides this option.</p>
Skip Query Warning	Turn off the warning message normally sent when a partially-keyed query is entered. Setting to true (selected) overrides the option set in Inefficient Query.
Can Create Personal Inboxes	Create personal inboxes for personal use. For more information, see the <i>ServiceCenter User's Guide</i> .
Can Create Global Inboxes	Create global inboxes for all Incident Management users. For more information, see the <i>ServiceCenter User's Guide</i> .
Can use Callback List	Use the Callback List, which is a list of contacts who can be notified when an incident ticket is closed.
Check Similar Known Errors	Use IR Expert to search the rootcause file for existing Known Error tickets similar to the ticket being opened.
Check Similar Root Causes	Use IR Expert to search the rootcause file for existing Root Cause tickets that are similar to the ticket being opened.
Check Similar Incidents	Use IR Expert to search the probsummary file, based on the probsummary IR key, for existing incident tickets that are similar to the ticket being opened.
Check Incident Duplicates on Device	Search the probsummary file for existing open incident tickets on devices with the same logical name as the devices in a new ticket.
Check Incident Duplicates on Parents	Search the probsummary file for existing incident tickets on parent or grandparent devices for the device listed in a new ticket.

Views Tab

Figure 4-6 shows the IM Security profile record.

ServiceCenter - [User Incident Profile: SYSTEMS SUPPORT]

File Edit View Format Options List Options Window Help

OK Cancel Previous Next Add Save Delete Views Find Fill

IM Security Profile Profile Name : SYSTEMS SUPPORT

Privileges Views

Default Category: [Dropdown]
 QBE Format: [Text]
 Search Format: apm.search.probsummary
 Manage Format: sc.manage.problem
 Initial Inbox: [Dropdown]
 Initial Format: apm.quick
☐ Initial Script
☐ Resolution Script
 Auto-Notify Format: [Text]
 Browse Format: problem.template.browse
 Incident Macro Mail Format: [Text]

Assignment Groups
 SYSTEMS SUPPORT
 HELPDESK
 [Empty]
 [Empty]
 [Empty]
 [Empty]

Authorized Categories
 [Empty]
 [Empty]
 [Empty]
 [Empty]
 [Empty]
 [Empty]

☐ New Thread: Inbox -> Search
☐ New Thread: Search -> List
☐ New Thread: List -> Edit
☐ New Thread: Inbox -> Edit

Selected line is row 21 of 24 records Response 0.80 draw 0.261 insert pm.profile.g(profile.view) [UP]

Figure 4-6: IM Security Profile record: Views tab

Assignment Groups

An *Assignment Group* is a set of users responsible for an incident ticket. This group receives notification when an incident ticket is opened or escalates. The groups are added in Incident Management by a ServiceCenter administrator.

Assignment groups make the routing of incident tickets easier. For example, the help desk receives a call that a PC is not functioning properly. The incident is assigned to the IT Assignment Group. After looking at the PC, the IT technician determines that the hard drive needs replacing. Since the drive

needs to be purchased, the ticket is updated and assigned to a Materials Management group that takes care of acquisition. If the hard drive is not purchased and the ticket is not closed in a set amount of time, the ticket is automatically escalated and assigned to the operations manager.

Each Incident category definition includes a default Assignment Group for all tickets in that category.

For example, the **client system** category can list IT as the Assignment Group Name if the IT department is always the first group to handle client system incidents.

Field	Description
Default Category	Allows you to set a default Incident Management category for the user or group. The category's form appears when a user accesses the Incident Management module.
QBE Format	Name of the QBE form displayed when the user or group queries the probsummary file. The default is probsummary.qbe .
Search Format	Defines the default form used when the user or group executes a query in Incident Management. If this field is blank, the <i>apm.search.probsummary</i> form will display.
Manage Format	Allows the form displayed from the Incident Queue to be specified. The default is <i>sc.manage.problem</i> .
Initial Inbox	Defines the default inbox for the user or group in Incident Management. If this field is blank, all open tickets for the user's Assignment Groups will be displayed.
Initial Format	Causes the <i>problem.open</i> application to use the data entry form named in the adjacent field when the user or group opens an incident ticket. The default is <i>apm.quick</i> .
Initial Script	Causes the <i>problem.open</i> application to use the script named in the adjacent field to prompt the user or group for the required information.
Resolution Script	Causes Incident Management to use the script named in the adjacent field to automatically update the Incident summary record when an incident ticket is inactivated.
Auto-Notify Format	Name of the form displayed when a user is automatically notified of a resolved incident ticket.
Browse Format	Read only field. Name of the form the user or group sees when browsing incident tickets.

Field	Description
Incident Macro Mail Format	Used to store the format name that you wish to use when sending out an e-mail of a problem via macros. This field is also used when a call is set to notify by e-mail. If an incident is closed, and the related call is set to notify by e-mail, it will use the format identified by this field. This will override the default print/text format, however if left blank, it will use the incident print/text format.
New Thread: Inbox > Search	Keeps the inbox displayed after a search is run from that inbox. Note: Threading allows the previous window to remain displayed when a new record is accessed. For example, when a record is accessed from a QBE list, the QBE list remains displayed after the record is opened in a new window.
New Thread: Search > List	Keeps the search form open after a QBE list appears.
New Thread: List > Edit	Keeps a QBE list form displayed when a record is accessed.
New Thread: Inbox > Edit	Keeps an inbox displayed after a record is accessed.
Assignment Groups	Lists the Assignment Groups to which the user or group can reassign incident tickets.
Authorized Categories	Allows you to set the Incident Management and Service Management categories available to the user or group in this profile.

Adding a New Assignment Group

To add an Assignment Group:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. The Incident Management Security Administration utility appears.
- 2 Click **Search/Add** in the Assignment Groups structure.
- 3 To add a profile, type the name of the group in the **Assignment Group** field. For example, you can add a group called `assign.test`.



- 4 In the **Calendar Name** field, click **Browse** or **Fill** to enter the **Calendar Name**, if desired. **Calendar Name** identifies the work shift of the members of this group work, for example, *day shift*, *second shift*, and so on. A record is added from the *cal duty* file. Refer to *System Tailoring Guide* for details on ServiceCenter's Calendar function.
- 5 In the **Printer Name** field, enter the printer where you want this group's incident tickets printed. This is an optional field and can be left blank. If no printer is specified, the user's default printer is used.
- 6 In the **Alert Stage 2** field, use the **Fill** function to enter the group to whom you want this Assignment Group's notifications sent when an incident ticket is escalated to Alert Stage 2.
- 7 In the **Alert Stage 3** field, use the **Fill** function to enter the group to whom you want this Assignment Group's notifications sent when an incident ticket is escalated to Alert Stage 3.
- 8 In the **Reassignment Alert Group** field, use the **Fill** function to enter the Assignment Group to whom you want to send notification if a ticket got reassigned too often and a reassignment alert occurs.

When users reassign an incident ticket, that ticket is updated. Since the ticket is updated, the normal escalation process does not occur, even if no progress is made on resolving the ticket. An incident ticket can be passed around (reassigned) without getting resolved. Incident Management allows you to set a limit (threshold) on the number of times a ticket can be reassigned. This threshold value is set in the category record, which is discussed later in this chapter. When this threshold is reached, Incident Management notifies the group designated in this field.

- 9 Select **Reset Assignment Group** if you want incident tickets automatically reassigned to an above defined alert group when an alert is issued. This option is valid for all Alert levels, including Deadline Alert.

Note: When a ticket is reassigned, the assignment profile context changes.

If a ticket is reassigned to an assignment group on Alert Stage 2, the reassignment on Alert Stage 3 depends on the assignment profile definition of the group that received the ticket in the previous escalation.

If you do not set this flag, notifications will be sent, but no reassignments will be made.

10 Do one of the following:

- Type the name of the Assignment Group manager, or select it from the drop-down list, in the **Manager Name** field.
- Specify a location where to send incident tickets using ServiceCenter Distributed, under certain conditions:
 - In the **Route Tickets to This Site**, enter a location where tickets can be sent if an expression evaluates to true.
 - Enter a boolean expression to trigger the re-routing of tickets in the **If this is true** field. For more information, see the *Distributed Services Quick Start Guide*.

11 Select the **Operators** tab. Figure 4-7 shows the Assignment Group operators.

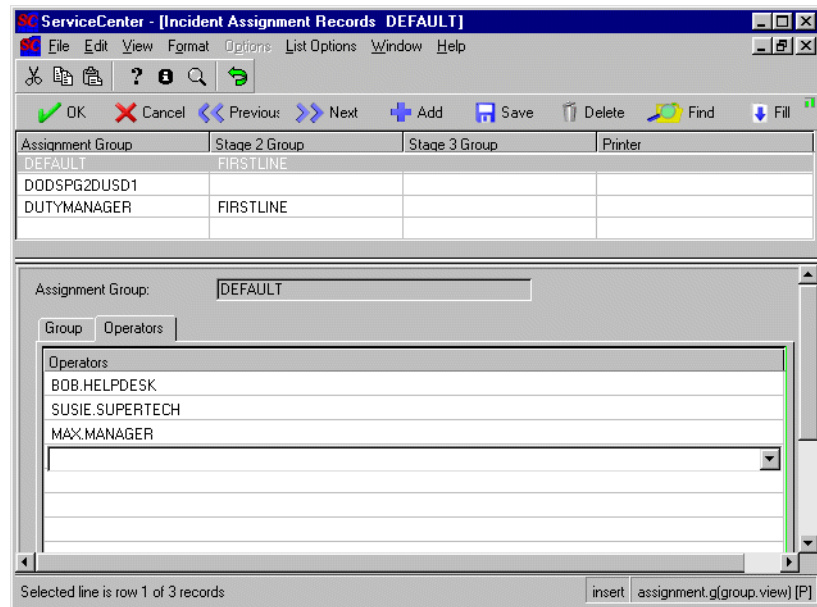


Figure 4-7: Assignment Group Utility: Operators tab

12 Type the ServiceCenter Operator IDs for prospective users in this Assignment Group. Do one of the following:

- Type Operator ID in each blank field.
- Choose the operator from the **Operators** field drop-down list.

There is no limit to the number of operators in an assignment group; however, consider how many users should respond to an incident when you create and populate a new assignment group.



- 13 Click **Add** or press **F2** to save the Profile record and return to the Incident Management Security Administration Utility.

Categories

Incident tickets, Call reports, Root Cause records, and Known Errors are assigned to a *category*. Categories classify tickets and reports by type.

A category can determine:

- who is responsible for resolving the call or incident (that is, the default Assignment Group).
- what information is needed to open an incident ticket.
- an incident ticket's severity.
- the incident ticket's priority.
- how quickly the incident ticket must be resolved.
- the time interval for escalating an incident ticket to a higher alert stage.
- who must be notified as the incident ticket is escalated.

Escalation and alerts are discussed later in this chapter. The processing logic for each category is essentially the same. However, ServiceCenter can use different incident ticket forms for each category. Different tabs contain category-specific information. For example, information needed to solve a software incident is different than information needed to solve an equipment incident. Some forms also have a Service Referral group of fields.

When you first enter information about an incident or call, you enter the information in an initial form and select a category.

In Incident Management, once you click **New** to add a record, the form associated with the category of the ticket appears. If a ticket is assigned the wrong category, the appropriate category can be assigned after the ticket is opened by someone with an appropriate Security Profile.

You may have other categories available in your initial incident form. A ServiceCenter administrator can add and revise incident categories. Categories also can be added and revised by a ServiceCenter user with administrative privileges.

Categories are also used to assign incidents to a designated group for that category. For more information, see [Adding a New Assignment Group](#) on page 78.

You can use the Category utility to:

- Update an existing category.
- Delete an existing category.
- Add a new category by modifying an existing category.
- Create a new category from scratch.

Predefined Incident Management Categories

Each category record contains a series of fields defining Assignment Groups for the Category, Open and Print options, Incident Management forms used with the category, and triggers for alert levels. The example category that is shipped with ServiceCenter is used in the samples in this section.

Category Tab

The following table lists predefined Incident Management categories.

Category	Description
business application	Indicates an incident with a large, system-wide application.
change	Indicates an incident that prompts a change request.
client system	Indicates a hardware or software incident with a client system.
enquiry	Indicates a request for information or a question.
example	Example category record in the standard ServiceCenter system that can be copied and renamed when creating a category.
network	Indicates a network incident.
other	Indicates a type of incident that does not fall into one of the other predefined categories.

Category	Description
printing	Indicates an incident with printers and related accessories (hardware, software and consummables, such as toner).
security	Indicates an incident with network, system or application security.
shared infrastructure	Indicates an incident with a shared hardware resource.
tbd	Indicates a type of incident that does not fall into one of the other predefined categories.
telecoms	Indicates an incident with a telephony component, either stationery or mobile.

Figure 4-8 shows the Category tab.

ServiceCenter - [ServiceCenter]

File Edit View Format Options List Options Window Help

OK Cancel Save Delete Copy Views Find Fill

Category | Formats | Alerts

Category Name: DEFAULT

Assignment Group Name: DEFAULT

Assignment Expressions:

☒ Disable Alert Paging?

☒ Post Downtime?

☐ Active Category?

Open Options:

Script Name:

Copy/Open Link:

Old Style Print Options:

☒ Override Default? ☐ Open Print Fmt? ☐ Update Print Fmt? ☐ Close Print Fmt?

Format Name:

Company: DEFAULT

Ready insert apm.category.g[apm.edit.category] [P]

Figure 4-8: Category record: Category tab

The following table lists category record fields.

Field	Description
Category Name	A unique name used to identify this category record. This field is read-only when editing category records.
Assignment Group Name	A default Assignment Group to which incident tickets are automatically assigned when using this category. You can use the Fill function in this field.
Assignment Expressions	An optional field Incident Management can evaluate before sending an incident ticket to an Assignment Group.
Disable Alert Paging?	Prevents new history page records from being added to an incident ticket record when a ticket is escalated to alert status. Instead, a line is added to the update.action field in the last page of a ticket. Normally an escalation adds a page to the incident document at each update.
Post Downtime	Requires Incident Management to calculate the downtime of the devices affected by this ticket when the ticket is closed.
Active Category	Controls whether or not this category shows up in the global lists and record lists.
Script Name	Identifies a ServiceCenter script to run when ever a ticket is opened in this category.
Copy/Open Link	When you copy a ticket, data from the old ticket will be copied to the new ticket based on the link record.
Override Default?	Overrides the Incident Management print option set in the Company Record, and allows Old Style Printing. If the print option is selected in the System Wide Company Record, a hard copy is printed of the current incident ticket when an open, update, or close is performed. Selecting the option here does the opposite of the setting in the System Wide Company Record. If printing is turned on in the System Wide Company Record, this option turns the printing off, and vice versa.
Format Name	Allows you to enter a form name that you want to use to print incident tickets opened in this category. You can also use the Fill function.
Open Print Fmt?	Prints incident tickets using the format specified when tickets are opened in this category.
Update Print Fmt?	Prints incident tickets using the format specified when tickets are updated in this category.

Field	Description
Close Print Fmt?	Prints incident tickets using the format specified when tickets are closed in this category.
Company	Indicates that a category can be used by the entered company. One help desk may be used for multiple companies. Indicate which company uses a category with this option. (This option can be set up to be used with Format Control or validity to enforce the use of a category by only certain companies.)

Formats tab

Each Incident Management form name on the Formats tab contains the category name. This unique name identifies the category subformat that is added to the appropriate Incident Management form. In the fields displayed above, *example* in each form name, such as **problem.example.open**, specifies which Incident Management form to display. An *example* subformat also appears when you select the **example** category for an incident ticket.

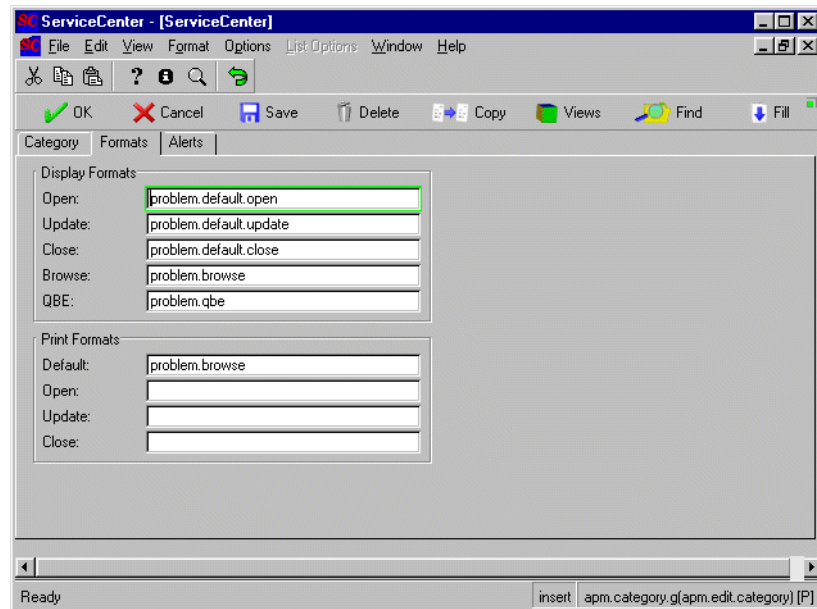


Figure 4-9: Category record: Formats tab

Note: Always use the base format name. Never enter the .g variation of the form.

The following table describes Display Formats options.

Display Format	Description
Open	Specifies the form to display when an incident ticket with this category is opened. You can use the Fill function in this field.
Update	Specifies the form to display when an incident ticket with this category is updated. Use the Fill function in this field.
Close	Specifies the form to display when an incident ticket with this category is closed. Use the Fill function in this field.
Browse	Specifies the form to display when an incident ticket with this category is being viewed in browse mode. Use the Fill function in this field.
QBE	Specifies the form for the QBE list to display when a query is run for an incident ticket with this category. Use the Fill function in this field.

The following table describes Print Formats options.

Print Format

Default	Specifies the form to print when a print command is issued against an opened, updated, or closed incident ticket with this category. It is active for any of the other print format fields that have been left blank.
Open	Specifies the form to print when a print command is issued against an opened incident ticket with this category.
Update	Specifies the form to print when a print command is issued against an updated incident ticket with this category.
Close	Specifies the form to print when a print command is issued against a closed incident ticket with this category.

Alerts tab

Figure 4-10 shows the alerts tab.

	Interval	Expression
Stage 1:	04:00:00	alert.time in \$file=tod()+<04:00:00>
Stage 2:	04:00:00	alert.time in \$file=tod()+<04:00:00>
Stage 3:	04:00:00	alert.time in \$file=tod()+<04:00:00>
Deadline:	2 00:00:00	deadline.alert in \$file=open.time in \$file+2 00:00:00'; if (priority.code in \$file='1'
Reassignment:	365 00:00:00	

Reassign Count Threshold: 2

Deadline Alert Group: DEFAULT

Figure 4-10: Category record: Alerts tab

The following table describes the fields on the Alerts tab.

Field	Description
Interval	Sets this category's time span for an incident ticket to be escalated to the next alert level, that is, Stage 1, Stage 2, Stage 3, Deadline and Reassignment. The format of this field is <i>DDD HH:MM:SS</i> .
Expression	Creates an expression to be used instead of the value in the Interval field to escalate a ticket from the corresponding alert to the next alert level. If no expression is entered, or if the expression evaluates to UNKNOWN or FALSE, the alert interval is used. Expressions should always be of the form: <code>alert.time in \$file = tod() + <interval></code> .

Field	Description
Reassign Count Threshold	Sets the number of times an incident ticket in this category can be reassigned. When users reassign an incident ticket, that ticket is updated. Since the ticket is updated, the normal escalation process does not occur, even if no progress is made on resolving the ticket. An incident ticket can be reassigned many times without getting resolved. This threshold value sets the number of times a ticket can be reassigned. When this threshold is reached, Incident Management notifies the Reassignment Group designated in the Assignment Group file after the reassignment interval has passed. See Adding a New Assignment Group on page 78.
Deadline Alert Group	Sets the Assignment Group to which an incident ticket in this category is set at a Deadline alert. You can use the Fill function in this field.

Options Menu

The following options appear in the Options menu when the Incident Management Category form is open.

Option	Description
Print Record	Prints the Category record to the user's default printer.
Edit Browse Format	Accesses Forms Designer to edit the browse form for this category.
Edit Category Format	Accesses Forms Designer to edit the structure this category adds to incident tickets.
Edit Open Format	Accesses Forms Designer to edit the open form that is opened on the Formats tab.
Edit Update Format	Accesses Forms Designer to edit the update form that is opened on the Formats tab. Accesses Forms Designer to edit the close form that is opened on the Formats tab.
Edit QBE Format	Accesses Forms Designer to edit the QBE list form for this category.

Adding a New Category

In creating a new category, you may add a *subformat* for that category. These subformats are joined to incident tickets using the new category, and the fields you have added are displayed in the ticket. The subformat may display as a new tab or in the place of a subformat designed for an existing category on which you have based your new category. The subformats are added in Forms Designer. The same categories are used in Incident Management and Service Management, and Root Cause Analysis.

Creating subforms saves a lot of work and time customizing the system. Header and update categories remain the same for all categories. Only category specific information has to be changed.

To add a new category record:



- 1 Click **Add** in the Categories area of the Incident Management Security Administration Utility form, shown in Figure 4-3 on page 68.
- 2 Type a unique name for the new category. For this example, add a category called **testcat**.
- 3 Click **OK**. Another prompt window appears.
- 4 Decided if you should base the new category on an existing category.
- 5 To base the new category on an existing category, select a category from the drop-down list and click **Yes**. For this example, select the *example* client system.

The status bar displays this message: **The problem.testcat.close formatctrl record was created**. Do not complete the remaining steps. The task is complete.


- 6 To create a new category, click **No**. A message asks if you want to edit the category subformat that is the basis of the new category. Creating subforms saves a lot of work and time customizing the system. Header and update categories remain the same for all categories. Only category specific information has to be changed.
- 7 To copy the subcategory as is, click **No**.
- 8 To edit the subcategory format, click **Yes**. The ServiceCenter Forms Designer utility appears.

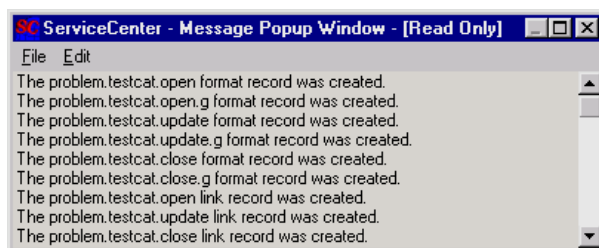


- 9 Click **Design**. The design form appears. See *System Tailoring* for information on how to use this utility. Make the changes and click **OK** to save them.
- 10 Click **OK** again to exit Forms Designer.

The new category record (`apm.category.g`) appears, as shown in Figure 4-8 on page 83. The data in many fields is automatically filled in based on values copied from your source category record and ServiceCenter defaults.

Warning: All category specific data is stored in the middle structure of the `problem dbdict`. All fields on your new category form must have matching data fields in the `problem dbdict`. *Do not* set the input control to a field which is not in the `problem dbdict`!

- 11 Edit or fill in the fields as necessary to complete the new record.
- 12  The status bar displays a short message. To display more messages, click the information button. The messages describe other necessary records the system has constructed automatically.



- 13 Click **Save** or press **F1** after you have entered the data. The status bar displays this message: **testcat has been updated.**

Editing Existing Categories

You can edit an existing category to match your system.



- 1 Click **Edit** in the Categories area of the Incident Management Security Administration Utility form, shown in Figure 4-3 on page 68. A message prompts you for the category to edit. For more information, see *Predefined Incident Management Categories* on page 82.
- 2 Select a category from the drop-down list. For this example, select the **example** category.
- 3 Click **OK**. The category record shown in Figure 4-8 on page 83 appears.
- 4 Modify the fields as necessary.
- 5 Click **Save** or press **F1**. The status bar displays this message: **category name has been updated.**

- 6 Click **Ok** to return to the Incident Management Security Administration Utility menu.

Creating New Categories from Existing Records

You can add a new category by copying an existing category. Use the Copy function to open the category record, modify that record and save it as a new category. The Copy option copies the existing category, substituting a user-defined category name in all forms, Format Control, and link records associated with the selected category. ServiceCenter adds the new category, forms, Format Control, and links to their corresponding tables.

To copy an existing category:



- 1 Click **Edit** in the Categories area of the Incident Management Security Administration Utility form, shown in Figure 4-3 on page 68.
- 2 A message prompts you to select a category to edit. For example, select the **example** category.
- 3 Click **OK**. The category record shown in Figure 4-8 on page 83 appears.



- 4 Click **Copy** or press F5 to make a copy of the current record that you can modify. A message prompts you to specify a New Category Name.
- 5 Type a unique name for the category. For example, name the new category **software**.
- 6 Click **OK**. A message asks if you want to edit the category subformat that is the basis for your new category. Creating subforms saves a lot of work and time customizing the system. Header and update categories remain the same for all categories. Only category specific information must be changed.
- 7 To copy the subcategory as is, click **No**.
- 8 To edit the subcategory format, click **Yes**. The ServiceCenter **Forms Designer** utility appears.



- 9 Click **Design**. The design form appears. For more information, see *System Tailoring, Volume 1*.
- 10 Make the changes and click **OK** to save them.
- 11 Click **OK** to exit Forms Designer. The new category record (`apm.category.g`) appears, as shown in Figure 4-8 on page 83. The data in many fields is automatically filled using values copied from your source category record and ServiceCenter default values.

Warning: All category specific data is stored in the middle structure of the **problem dbdict**. All fields on your new category form must have matching data fields in the **problem dbdict**. Do not set the input control to a field which is not in the **problem dbdict**.

- 12 Modify the data as necessary for the new record.
- 13 Click **Save** or press **F1** after you enter the data.

Deleting a Category

You can delete obsolete or unnecessary categories. During the process, a message prompts you to select an alternate category for the incident tickets.

To delete an existing category:



- 1 Click **Delete** in the Categories area of the Incident Management Security Administration Utility, as shown in Figure 4-3 on page 68. A message prompts you to identify a category to delete.
- 2 Select a record from the drop-down list. For this example, delete the **testcat** category.
- 3 Click **OK**.
- 4 If records exist that use this category, ServiceCenter prompts you for a replacement category. Select an existing category from the drop-down list to be used by all tickets previously assigned the deleted category and click **OK**.

A message prompts you to specify which forms related to the category can be deleted. Figure 4-11 shows a typical list of forms to delete.

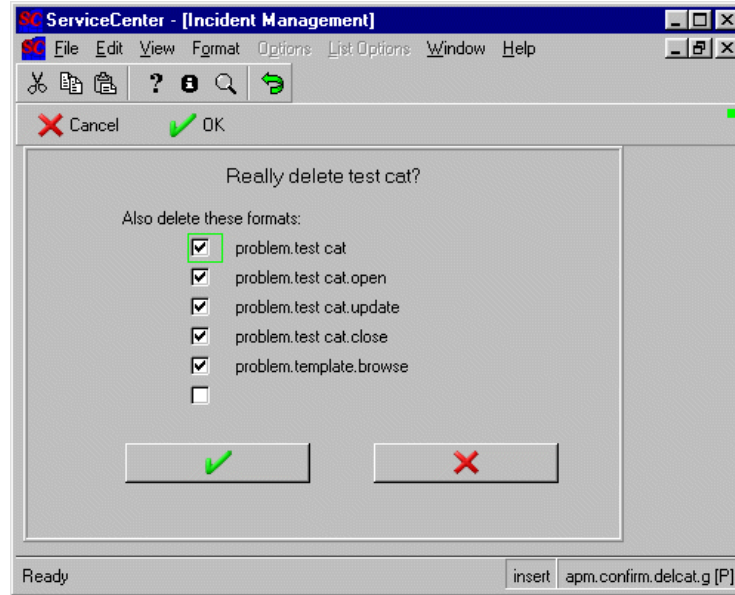


Figure 4-11: Incident Management delete category

- 5 Select the check boxes of all the forms that you want to delete with this category. Remember, ServiceCenter automatically adds forms specific to a category when a category is added.

Warning: Be careful not to delete forms (formats) that are used by other categories. For example, when deleting the `testcat` category, you will want to select only forms that contain `testcat` in the name, such as `problem.testcat.update`. You would not want to delete `problem.browse`, because this is a common form used by other Incident Management categories.

- 6 Click OK to delete the category and related forms. The status bar displays a message that ServiceCenter deleted the category and associated forms.

Maintaining Inboxes

Inboxes enable you to predefine a search for incident tickets, call reports, and other records. When you specify an specific inbox, the search runs using the search parameters defined in the inbox. The results are returned to the inbox table. For example, you can specify a search to look for all active incidents assigned to you. You can administer inboxes for Incident Management from the Security Files tab. Because an inbox is an object, you can edit it directly from the Database Manager. You can also copy an inbox that is available to all users and save it as a personal inbox that you can edit. For more information, see the *ServiceCenter User's Guide*.

To maintain inboxes:



- 1 Click **Inboxes** in the Incident Management Security Administration Utility menu, shown in Figure 4-3 on page 68. An Inbox form appears. Use the tabs in this form to define inboxes.
- 2 Click **Search** to perform a true query and retrieve a list of all current inbox records. A QBE list appears with the results of this search Figure 4-12 on page 95 shows the Inbox Maintenance form.

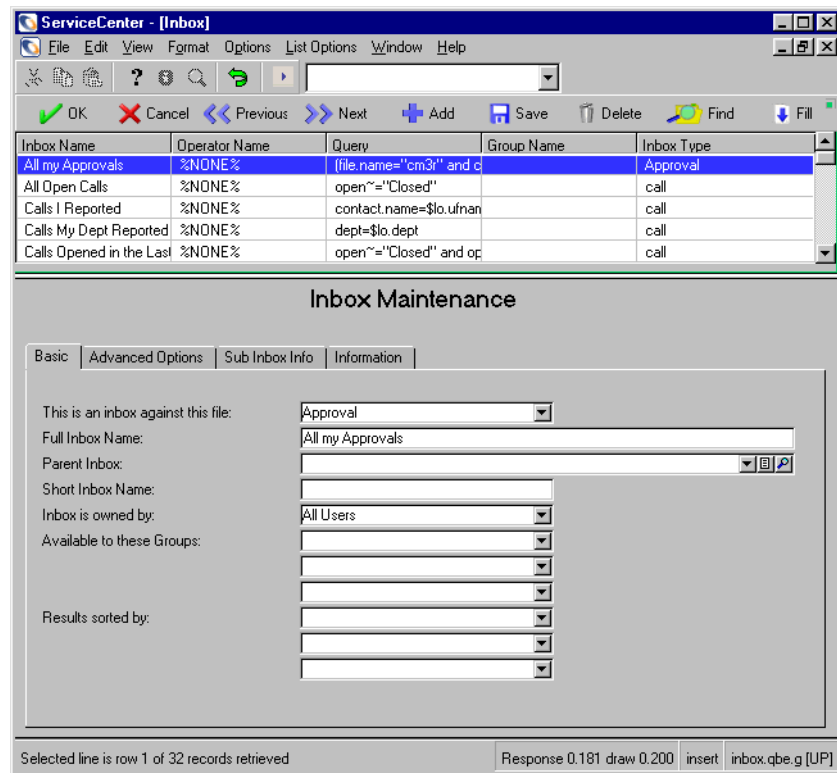


Figure 4-12: QBE Inbox list

3 Click an inbox record to select it.

Note: If you choose to add an inbox without using Search, select a file from the drop-down list in the **This is an inbox against this file** field. Your new inbox depends on the file you select. For example, if you select call, your new inbox is based on the call file.

Basic tab

The following table describes the fields on the Basic tab.

Field	Description
This is an inbox against this file	References the ServiceCenter file for which the inbox applies, for example, call , ocmq , or problem . Enter call for Service Management or problem for Incident Management. If the inbox is based on another inbox, the type is automatically entered.
Full Inbox Name	The name for your new inbox. If you are creating a new inbox, the name you entered earlier in the process is automatically displayed.
Parent Inbox	The parent inbox that this inbox should be linked to.
Short Inbox Name	The abbreviated name of this inbox.
Inbox is owned by	The name of the owner of this inbox.
Available to these Groups	Allows these users or groups to view the inbox.
Results sorted by	How records in the resulting QBE list can be sorted. For example, select category to sort the list by categories, select severity to sort the list by severity, and so on.

Warning: Sort criteria should match the search's query fields. If they do not, severe performance degradation may result. Do not specify sort criteria unless you understand the full effect of your selections.

Advanced Options tab

Figure 4-13 shows the Advanced Options tab.

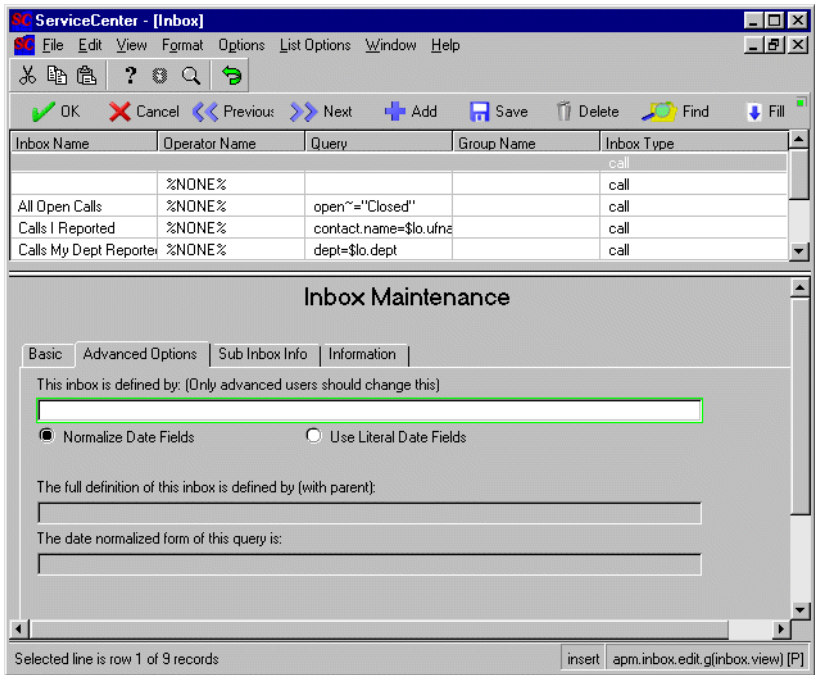


Figure 4-13: Incident Management Inbox Maintenance: Advanced Options tab

The following table describes fields on the Advanced Options tab.

Field	Description
This inbox is defined by (Only advanced users should change this)	Displays the syntax that defines the query.
Normalize Date Fields	Default setting that allows Incident Management to modify a query to search from the current date, not the date the inbox was added. If you select this option, the dates entered in the Inbox will be changed to reflect the time the each query is made rather than the specific time entered when the inbox was added.

Field	Description
Use Literal Date Fields	Causes the inbox to query from the date it was added. If you select this option, the dates entered in the inbox will be unchanged, and all queries to this inbox will return results based on the specific time entered when the inbox was added.
The full definition of this inbox is defined by (with Parent)	The definition of this inbox, including the parent inbox name.
The date normalized form of this query is	When creating an inbox manually, you must enter the normalizing query in this field.

Sub Inbox Info tab

When you create inboxes, you can also create sub inboxes to be contained within the initial inbox.

Sub-Inbox to display Information to display within the inbox you are creating, basing the information on the file you chose earlier.

Figure 4-14 shows the sub Inbox Info tab.

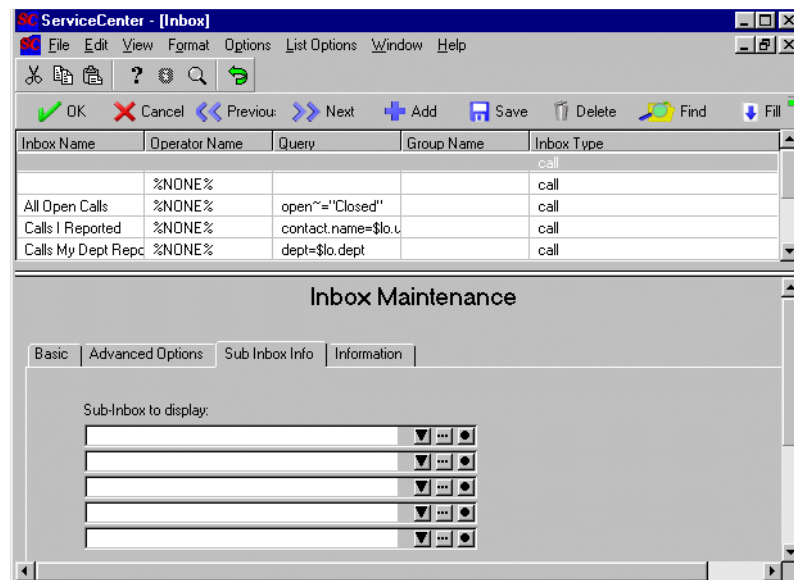


Figure 4-14: Incident Management Inbox Maintenance: Sub Inbox Info tab

Information tab

Figure 4-15 shows the Information tab that defines date field normalization and provides an example.

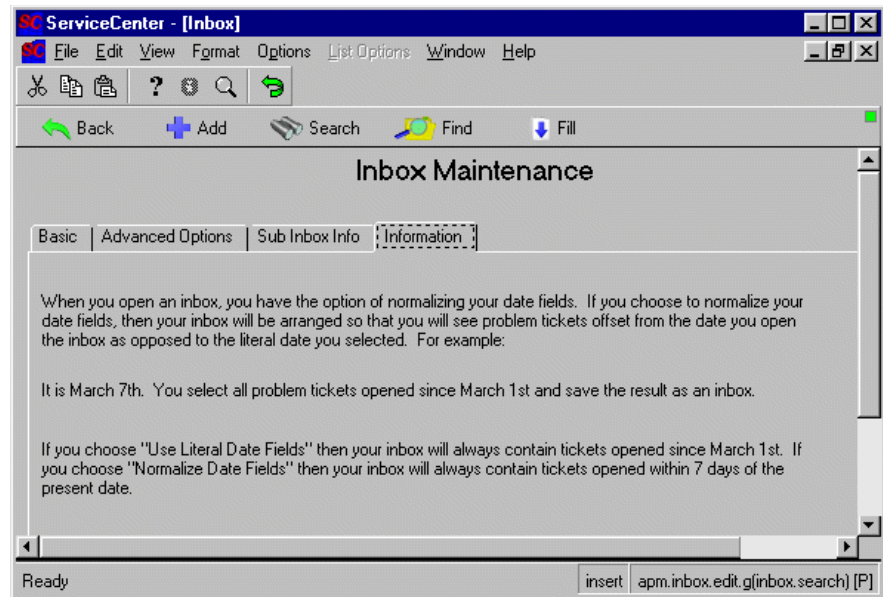


Figure 4-15: Incident Management Inbox Maintenance: Information tab

Saving an Inbox

To save an updated record or add an inbox:

- Click OK or Save to save your changes to an edited record.
- Click Add or press F2 to save the new record.

Probable Cause

Incident tickets contain an optional Cause Code field that links the ticket to a Probable Cause record. Cause codes allow incident tickets to be more easily categorized and assigned. Cause codes simplify incident reporting and tracking.

When a cause code is added to an incident ticket using the Fill function, accompanying information from the corresponding probable cause record can also be added.

ServiceCenter ships with a **probcause** file containing default probable cause records. As the ServiceCenter administrator, you can modify these records or add new probable cause records tailored to your system.

Editing a Probable Cause Record

To edit a Probable Cause record:

- 1 Click **Probable Cause** in the Incident Management Security Administration Utility form. Figure 4-16 shows a blank Probable Cause form.



Figure 4-16: Probable Cause form

- 2 Type the name of the device, or any other information you know, to simplify the search. For example, type User Training in the **Cause Code** field.
- 3 Click **Search** or press **Enter** to perform a true query and access a Probable Cause record list.

- 4 Select the Probable Cause record from the record list. The Probable Cause record appears. Figure 4-17 shows a Probable Cause record.

The screenshot shows a window titled "ServiceCenter - [probcause]". At the top is a menu bar with File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu is a toolbar with icons for OK, Cancel, Previous, Next, Add, Save, Delete, Find, and Fill. A table lists several probable causes:

Cause Code	Category	Resolution	Severity	Incident Title
Advice & Guidance	Advice & Guidance	2	Provision of advice and guidance to the user	
Authentication Failure	Authentication Failure	4	User unable to provide adequate authentication of identity	
Entitlement Failure	Entitlement Failure	4	User unable to provide adequate entitlement detail	
Fault	Fault	2	Fault	
No fault found	No fault found	2	Symptoms could not be reproduced or replicated	

Below the table is a form titled "PROBABLE CAUSE" for editing the selected record. The fields are:

- Cause Code: Advice & Guidance
- Severity: 2
- Resolution Code: Advice & Guidance
- Category: (empty)
- Company: DEFAULT
- Brief Description: Provision of advice and guidance to the user
- Description: (empty text area)
- Resolution: Resolution to this problem was achieved through the provision of advice and guidance to the user, either over the telephone by Email or at the users desk

At the bottom, it says "Selected line is row 2 of 11 records" and "Response 0.50 draw 0.131 insert probcause.qbe.g [UP]"

Figure 4-17: Probable Cause form

- 5 Modify the fields in the Probable Cause form.

Field	Description
Cause Code	A unique term that links this Probable Cause record to the incident tickets.
Severity	A numeric value indicating the impact on the network. You set these values as the administrator. For example, 1 is critical, 2 is less urgent but needs attention, and so on.
Resolution Code	The resolution code assigned to an incident ticket with this cause code when it is closed.
Category	The category this probable cause record uses.

Field	Description
Company	Indicates that a category can be used by the entered company. One help desk may be used for multiple companies. Indicate which company uses a category with this option. (This option can be set up to be used with Format Control or validity to enforce the use of a category by only certain companies.).
Brief Description	A short statement describing the incident that is automatically entered in the incident ticket when this cause code is selected.
Description	A longer statement about the probable cause.
Resolution	A statement describing a possible solution to an incident using this cause code.
Key Words	Words used to assist in querying for probable cause information.

- 6 Click **Save** or press **F4** to save the changes. The status bar displays this message: **Record updated in the probcause file.**

Options Menu

The Incident Management probable cause record form contains an Options menu with standard ServiceCenter menu options.

Field	Description
Print	Prints the probable cause record on the user's default printer.
Validity Lookup	Checks the data in the current field against the ServiceCenter <i>validity table</i> for that field.
Export/Unload	Allows you to export this record into a file for importing into a spreadsheet, or unload this data set for loading into another ServiceCenter system.
IR Query	Accesses ServiceCenter's IR Expert application.
Expand Array	Allows easy data entry to an array. A separate window is opened to enter the data.

Creating a New Probable Cause Record

Similar to editing a Probable Cause record, you can also add a new record.



To add a Probable Cause record:

- 1 Click **Probable Cause** in the Incident Management Security Administration Utility form, shown in Figure 4-3 on page 68. If you want to modify an existing record to add a new record, click **Search** and select that record from the record list.
- 2 Type a unique name in the **Cause Code** field.
- 3 Complete the other fields as described in *Editing a Probable Cause Record* on page 100.
- 4 Click **Save** or press F2. The status bar displays this message: **Record added to probcause file.**

Options Menu

The blank Incident Management probable cause setup form contains an Options menu with standard ServiceCenter menu options.

Option	Description
Clear	Clear the data entered in the form.
Restore	Return the fields in the form to the previous values. Only available in the initial form where you enter data.
Advanced Search	Display a list of possible search parameters. After a parameter is selected, a window is opened that allows you to set a time limit for a query. This time is entered in the hh:mm:ss format. Only available in the initial form in which you enter data.
IR Query	Access ServiceCenter's IR Expert application.
Export/Unload	Export this record into a file for importing into a spreadsheet, or unload this data set for loading into another ServiceCenter system.
Validity Lookup	Check the data in the current field against the ServiceCenter validity table for that field.
Reset	Delete all the records in the probcasue file. Do not use the Reset option unless you want to rebuild all the records in your Incident Management probcasue file.
Regen	Regenerate the indices for the probcasue file.
Open Inbox	Select a query to search for probable cause data.
Expand Array	Add a field to an array. A separate window is opened to allow you to enter the data.

Macro Editor

Macros are distinct actions, driven by predefined conditions, that are executed when a record is saved in the database. Macro actions are associated with files and reflect certain states in the records of those files. You can access ServiceCenter's Macro Editor from the Incident Management Security Administration Utility. Click Macro List to display the Macro List form. This is the access point for the Macro Editor. For instructions about this procedure, refer to *System Tailoring, Volume 2*.



Click **Macro List** in the Incident Management Security Administration Utility form shown in Figure 4-3 on page 68. Figure 4-18 shows the Macro List form. For more information, see *System Tailoring, Volume 1*.

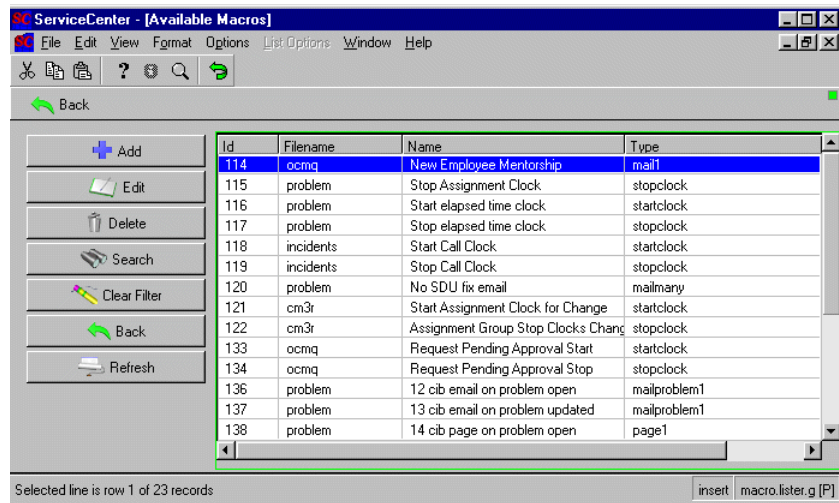


Figure 4-18: Macro List form

Downtime

You can access Incident Management downtime records from the Incident Management Security Administration utility form. These records display the availability of a selected device.

Availability measures a component's ability to provide service within a measured time frame. Incident Management provides three downtime measurements:

- | | |
|--------------------------|--|
| Explicit unavailability | Describes the downtime experienced by the failing device. |
| Implicit unavailability | Describes the downtime experienced because of the failure of a parent or controlling device. |
| Perceived unavailability | Describes the explicit or implicit downtime during normal business hours. Non-working hours are subtracted from the total. |

To access the downtime records:

DT

- 1 Click **Downtime** in the Incident Management Security Administration utility form shown in Figure 4-3 on page 68. Figure 4-19 shows a blank downtime record.

The screenshot shows a web application window titled "ServiceCenter - [downtime]". The window has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for Back, Add, Search, Find, and Fill. The main content area is titled "DOWNTIME" and contains several input fields and a table.

Logical Name field: Contains the text "pc001".

Location field: Empty.

Contact Name field: Empty.

Type field: Empty.

Table Name field: Empty.

Outage Totals section:

Last Reset	Explicit	Implicit	Perceived	Count

Details section:

Start Time	End Time	Type	Explicit	Implicit	Perceived	Incident No.

The status bar at the bottom shows "Ready" and "insert downtime.graph.g(db.search) [P]".

Figure 4-19: Downtime record

- 2 Type the name of the device, or any other information you know, to simplify the search. For example, type pc001 in the **Logical Name** field.
- 3 Click **Search** or press **Enter**.

- 4 Select the device record you want to view from the record list. The downtime record appears for the selected device. Figure 4-20 shows the downtime record.

The screenshot shows the ServiceCenter application window titled "[Search downtime Records]". The window has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for Back, Add, Search, Find, and Fill. The main content area is titled "DOWNTIME" and contains several sections:

- Logical Name:** A text field containing "ACME Phone 0002".
- Location:** An empty text field.
- Contact Name:** An empty text field.
- Type:** An empty text field.
- Table Name:** An empty text field.
- Outage Totals:** A section with five fields: "Last Reset", "Explicit", "Implicit", "Perceived", and "Count".
- Details:** A table with seven columns: "Start Time", "End Time", "Type", "Explicit", "Implicit", "Perceived", and "Incident No.". The table contains several empty rows for data entry.

The status bar at the bottom of the window displays "Ready" on the left and "Response 0.100 draw 0.71 insert downtime.graph.g(db.search) [UP]" on the right.

Figure 4-20: Downtime record

Summary Link

You can access the Incident Management's summary link record from the Incident Management Security Files tab. Links associate fields in one file or form with other records and other files. Fill and Find functions use links. Refer to the *System Tailoring Guide* for more information.

To access the summary link file:

- 1 From the ServiceCenter home menu, select **Incident Management**. Click the **Tools** tab.
- 2 Click **Summary Link**. Figure 4-21 shows the link file form.

Source Field Name	Format/File Name	Target Field Name	Add Query	Comments
number	probsummary	number		

Figure 4-21: Summary Link record

Cost Management

You can enable the module or set automatic labor and parts calculation features for Contract Management in the Contract Management configuration record. Contract Management integrates service contract information and tracking into the enterprise Service Desk. For more information, see [Service Level Management](#) on page 259.



- To access the Contract Management configuration record, click **Cost Management** in the Incident Management Security Administration Utility form shown in Figure 4-3 on page 68.

Figure 4-22 shows the Contract Management configuration record.

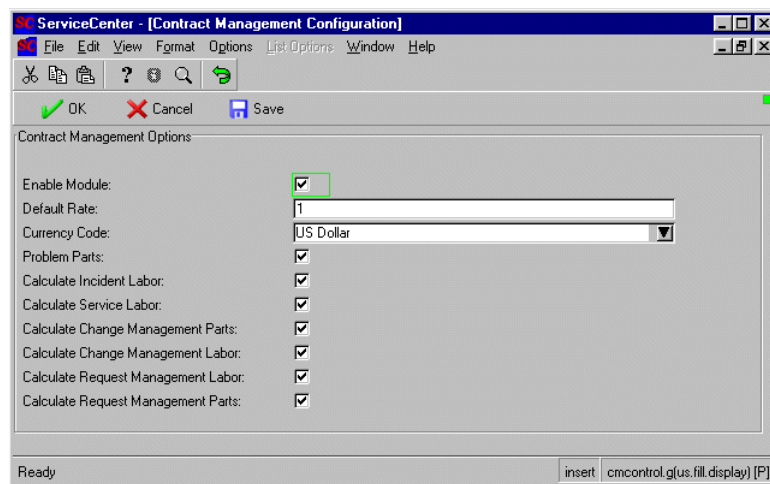


Figure 4-22: Contract Management Options

Configuring the Incident Management Environment

Incident Management contains an environment record that defines options that affect functionality of the Incident Management module for all Incident Management users. ServiceCenter is shipped with default environment records that you can modify for your system.

To configure the Incident Management environment for all users:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. The Incident Management Security Administration utility appears.
- 2 Select the **Environment** tab in the Incident Management Security Administration Utility form. Figure 4-23 on page 109 shows the Incident Management Environment Profile form.

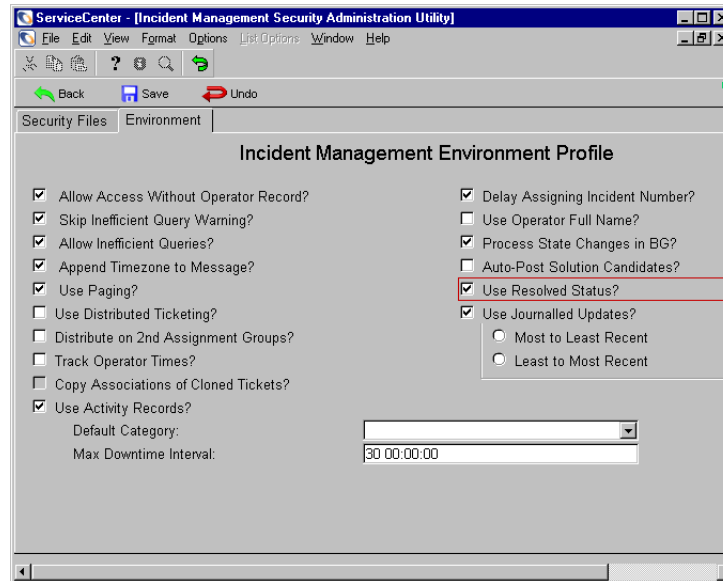


Figure 4-23: Incident Management Security Administration: Environment tab

- 3 Select the fields representing the parameters you want to apply to your Incident Management system.

Field	Description
Allow Access Without Operator Record	Permits users without an Incident Management profile to access the module using the DEFAULT profile. For more information, see the <i>System Administrator's Guide</i> .
Skip Inefficient Query Warning?	Disable the default message that a non-keyed query will be slow. Set to true (checked) to override the option set in Allow Inefficient Queries?.
Allow Inefficient Queries?	Execute a non-keyed query. Set Skip Inefficient Query Warning? to true (checked) to override the option.
Append Timezone to Message?	Add the date/time and time zone stamps to all Incident Management messages.
Use Paging?	Add a new history record (page) to the Incident Management database each time a ticket is updated.
Use Distributed Ticketing?	Activate Incident Management's distributed ticketing feature. For more information, see the <i>Distributed Services Quick Start Guide</i> .

Field	Description
Distribute on 2nd Assignment Groups?	Follow the standard distribution pattern in distributed ticketing, but based on the secondary Assignment Groups in the ticket as well as the primary Assignment Group.
Track Operator Times?	Automatically start a clock to track how long an operator has a lock on a record.
Copy Associations of Cloned Tickets?	Copy the associations to other records when cloning a ticket.
Use Activity Records?	Use activity records for text updates to the ticket.
Default Category	Set the category for an incident ticket opened from a device record (Inventory Management) that has no category listed. For more information, see Adding a New Category on page 89.
Max Downtime Interval	Limit the number of days for which availability can be calculated. The default is 30 days.
Delay Assigning Incident Number?	<p>Delay assigning an incident ID number to an incident ticket until you click New in the initial incident ticket form.</p> <p>Note: When this field is true, there is no unique identifier to tie an attachment within the file. Attachments cannot be saved when you open the ticket, but only when saving an update to the file after the unique identifier has been assigned.</p>
Use Operator Full Name?	Use the name entered in the Full Name field of the Operator File when stamping the ticket (on open, update, and so on) instead of the operator login name.
Process State Changes in BG?	Cause clocks associated with state changes to start and stop in the background. This feature makes the Windows interface work more efficiently.
Auto-Post Solution Candidates?	Post solutions automatically from an incident ticket to the Global Knowledge feature for tickets with the Solutions Candidate check box selected. For more information, see the <i>Database Management and Administration Guide</i> .
Use Resolved Status?	Activate the two-step close process in Incident Management.
Use Journalled Updates?	<p>Make any information entered in the Actions tab a permanent part of the record that cannot be deleted.</p> <ul style="list-style-type: none"> ■ Most to Least Recent: List updates to the record chronologically beginning with the most recent. ■ Least to Most Recent: List updates to the record chronologically beginning with the least recent.

- 4 Click **Save** or **OK**, or press **F2**, to save the changes. If you are modifying the default environment record, you cannot add a new environment record. ServiceCenter returns to the Incident or RCA Control Security Administration Utility form.

Status, Alerts, and Escalation

The status of an incident ticket is determined by the alert stage of the ticket. When an incident ticket is not updated within the specified time period, an alert message is automatically sent that an incident ticket has not been resolved. As an incident ticket passes through the alert stages, the ticket is escalated. Alert levels are displayed in the Status field of Incident forms.

ServiceCenter supports four *alert stages*:

- Alert Stage 1
- Alert Stage 2
- Alert Stage 3
- Deadline Alert

Alerts are triggered after a set period of time defined in a category record. Alert messages are displayed in a read-only escalation form. As various alert stages are reached, different Assignment Group is notified. For example, if an incident is not resolved by the Deadline Alert, the incident ticket may be escalated to an Assignment Group containing a manager.

An incident ticket reaches each alert stage after the specified time period passes without an update to the incident ticket. At this time interval, the next alert level is reached. A time interval is specified within each category record, for each alert level. This time interval can be adjusted according to the priority assigned to the ticket. For more information, see [Alerts tab](#) on page 87 and [Severity Levels](#) on page 113.

When each alert level is reached, ServiceCenter automatically notifies users that the incident ticket has reached that alert level, or it can reassign the ticket, depending on category definitions. The category record also contains flags that direct the system to notify specific users.

For example, the following list describes different users who might be notified.

- All contacts in the current contact list for the Assignment Group, except the manager.
- The user who opened the ticket.
- The current primary contact in the owner group.
- The current manager of the Assignment Group.
- The current manager of the owner group.
- The service level manager and client manager of the company and department specified in the ticket.

For alert stages 1, 2 and 3, the alerts are reset each time the ticket is updated. The Deadline Alert is always scheduled for an interval after the open time of the ticket, and is not affected by updates to the ticket.

Alerts and Calendars

The clocks that manage alerts do not need to run on a 24 hour schedule. For example, if your employees work from 9 am to 5 pm, set the alert clocks to run only during these hours. By default, all alert clocks run on a 24 hour, seven days a week schedule. However, if you select an availability calendar for a problem ticket Deadline Alert Group's calendar, the alert clocks for that ticket run only during the duty hours defined by the associated calendar.

What is Escalation?

Escalation is the process of increasing the urgency of an incident ticket. Escalation is accomplished automatically through alerts. As the various alert levels are reached, the escalation increases:

- Alert Stage 1 to Alert Stage 2
- Alert Stage 2 to Alert Stage 3
- Alert Stage 3 to DEADLINE ALERT

At each alert level, ServiceCenter forwards the incident ticket to the next Assignment Group. These groups are set by the ServiceCenter administrator.

Note: Whenever a ticket in Alert Stage 1, 2, or 3 is updated, its status reverts back to updated. The next auto-escalation goes to Alert Stage 1 again. However, once a ticket reaches DEADLINE ALERT, it remains on DEADLINE ALERT no matter how many times it is escalated.

The interval between alerts is set in the category records, and can be impacted by the priority set for the ticket.

Severity Levels

The severity of a ticket indicates the urgency of the problem. Severity is set by the user when an incident ticket is opened. Specify the severity in the Severity field of the initial incident form:

- 1 - Critical
- 2 - Urgent
- 3 - Normal
- 4 - Low
- 5 - Very low

Severity can be based on the impact the incident has on users and the category of the ticket. For example, an equipment incident that brings down a group of users is critical. A user wanting to know how to adjust the colors on a monitor is a less critical.

A ticket's severity level can be changed by the user as an incident ticket goes through updates. However, severity levels are not changed automatically as alerts progress.

The Two-Step Close

You can choose to close a ticket into two steps:

- *Resolving the Ticket on page 116*
- *Inactivating the Ticket on page 119*

A ticket is resolved when the technician has finished working on it and starts the closing process. A ticket is inactivated when the help desk finishes closing the ticket after contacting the customer and confirming the results.

General Information

There are a few things to remember about closing tickets.

- Resolved tickets appear as active tickets (flag=true) when searching, because they require further processing.
- Alerts are not processed for resolved or inactivated tickets.
- The option to resolve tickets is available for non-closed tickets.
- The close option (inactivation) is available on resolved tickets. However, you can also inactivate any ticket directly from the initial incident screen.
- Both Resolved and Closed tickets can be reopened.

Setting Up the Two-Step Close

To activate the two-step close feature, select an option in the environment record, and enable the appropriate users to perform each step.

To enable the two-step close feature:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. Click the **Environment** tab. Figure 4-24 on page 115 shows the Incident Management Environment Profile.

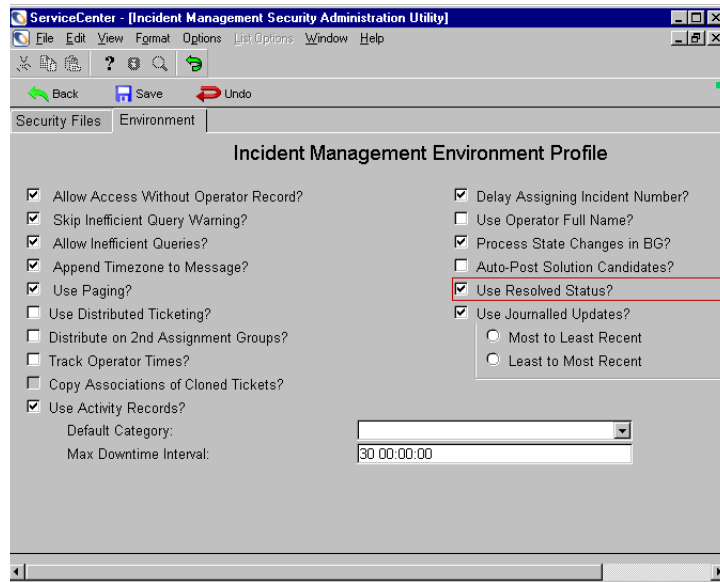


Figure 4-24: Incident Management Security Administration: Environment tab

- 2 Select the Use Resolved Status? check box
- 3 Click Save.

To set user rights for the two-step close:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**. The Incident Management Security Administration utility appears.



- 2 Click **Search/Add** in the Incident Profiles section. Figure 4-25 shows the Security Profile form.

The screenshot shows the 'ServiceCenter - [Search User Incident Profile Records]' application window. The title bar includes standard window controls and a menu bar with File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu bar is a toolbar with icons for Back, Add, Search, Find, and Fill. The main area is titled 'IM Security Profile' and contains a 'Profile Name' text box. Below this are two tabs: 'Privileges' and 'Views'. The 'Privileges' tab is active, showing a list of checkboxes for various permissions. The 'Browse' checkbox is highlighted with a green box. Other checkboxes include Open, Update, Close, Inactivate, Mass Inactivate, Log, Reopen, Find, Fill, Notify, Lock on Display, Print, Views, Count, Can Suspend, and Can Unsuspend. On the right side, there are checkboxes for Advanced Search, Database Access, Duplicates, New Category, Notes, Override, Allow Inefficient Query, Skip Query Warning, Can Create Personal Inboxes, Can Create Global Inboxes, Can use Callback List, and Incident Matching Options (Check Similar Known Errors, Check Similar Root Causes, Check Similar Incidents, Check Incident Duplicates on Device, Check Incidents Duplicates on Parents). The status bar at the bottom shows 'Ready' and 'Response 0.100 draw 0.200 insert pm.profile.g(profile.search) [UP]'.

Figure 4-25: Incident Management Security Profile form

- 3 Type the name of the profile in the Profile Name text box.
- 4 Click **OK**. The Profile record appears.
- 5 Check the **Close** box to allow the user or group to resolve tickets.
- 6 Check the **Inactivate** box to allow the user or group to inactivate tickets.
- 7 Click **OK** or **Save** to save the changes to the profile.
- 8 After updating a Profile record, stop and start your client to enable the changes to take effect.

Resolving the Ticket

A ticket is resolved when the technician has finished working on it and starts the closing process.

To resolve a ticket:

- 1 Display an open incident ticket.

Figure 4-26: Incident ticket

- 2 From the **Options** menu, click **Find Solution**. A list of potential solutions from the Knowledge Base appears. If one of the solutions resolves the ticket, select it and from the **Options** menu, click **Use Resolution**.
- 3 If none of the solutions resolves the issue, click **Back** and a dialog box appears asking if you are finished searching. Click **No**.

The Knowledge Base form appears, showing the description of your problem. The cursor is in the **Select a Knowledge Area to begin searching** field.

- 4 Change the search criteria in the **What would you like to know** field or change any of the filters to focus your search.

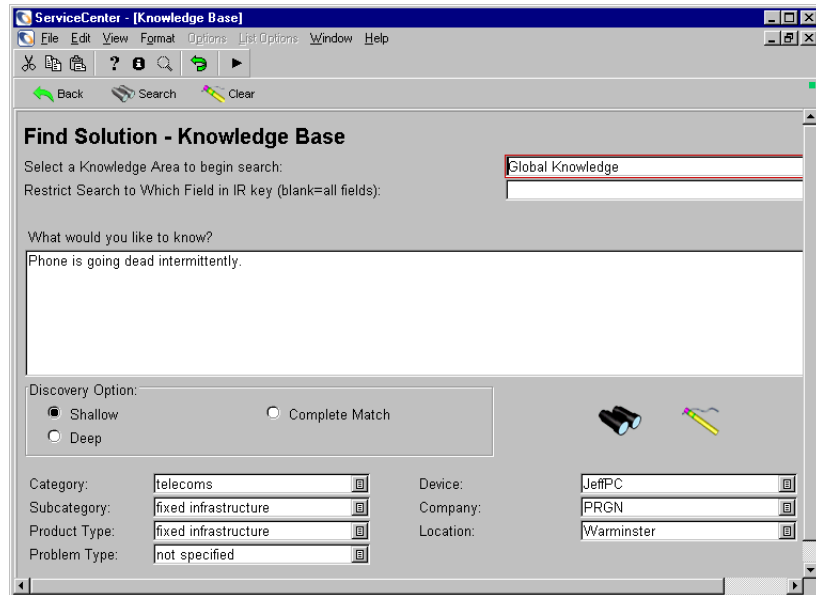


Figure 4-27: Recording a solution for an incident ticket

- 5 Click **Search**.
- 6 If one of the solutions resolves the ticket, select it and from the **Options** menu, click **Use Resolution**. Selecting Use Resolution does two things. It allows the help desk analyst to use a known solution and it begins a process whereby the Knowledge Base learns from the resolution being used. For more information, see the *User's Guide*.
- 7 Click **Save** to resolve the ticket. If your administrator enabled the SLM module and set it to post outages, an outage list appears. To set the post outages form appear rather than post outages automatically:
 - a From the ServiceCenter home menu, click **Service Level Mgmt**.
 - b Select **Configure Module**.
 - c Clear the **Auto Post Outages** check box.

- d When you set the **Auto Post Outages** check box to false, you have the option to post outages manually when resolving a ticket.

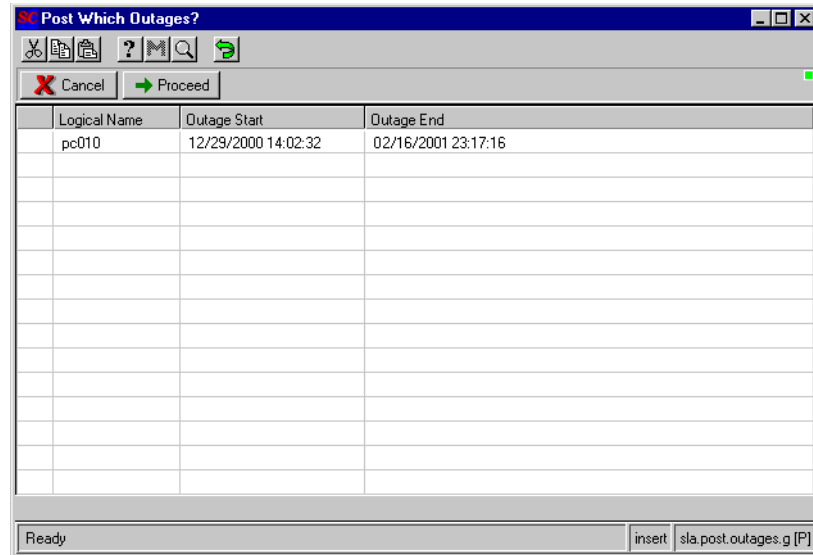


Figure 4-28: Outage list

- 8 Click **Proceed**. The system exits to the incident ticket. The status bar displays this message: Incident *incident unique ID* has been resolved by *operator name*.



- 9 The system tray displays a **Reopen** button. If you want to reopen the ticket, click **Reopen**.

Inactivating the Ticket

A ticket is inactivated when the help desk closes the ticket after contacting the customer.

To inactivate a ticket:

- 1 Open a resolved ticket. Figure 4-29 shows a resolved ticket.

ServiceCenter - [Update Incident Number IM1045]

File Edit View Format Options List Options Window Help

OK Cancel Previous Next Save Undo Close Find Fill Clocks

IM1045 Ticket Status: Open

Incident Title: Caller is complaining about glare from monitor.

Incident Details | Activities | Contact | Asset | Attachment | SLA | History | Alerts | Related Records | Billing Information

Alert Status: alert stage 3 Owner: BOB.HELPDESK

Category: client system Primary Asgn Group: ONSITE SUPPORT

Subcategory: hardware Assignee Name:

Product Type: desktop Second Asgn Group:

Problem Type: monitor Hot Ticket: ☐ Total Loss of Service: ☐

Manufacturer: Viewsonic Severity: 4 - Low

Class: class5 User Priority: Low

Contact Time: Site Category: B - Major Site

Contract: Cause Code:

Company: PRGN Site:

Contact: JENKINS, CAROL Phone / extension: (256) 455-7654

Incident Description: Caller is complaining about glare from monitor.

Figure 4-29: Inactivating an incident ticket

- 2 Edit the **Solution** field with any additional information.
- 3 Click **Close** to close the ticket. If the incident ticket you are trying to close is associated with open calls, a message appears asking if you want to force those calls to close.
- 4 Click **Yes** to force associated calls to close. The system exits to the incident ticket and the status bar displays this message: Incident *ticket unique ID* has been closed by *operator*. Any related calls will also be closed. The Ticket Status field now shows that the ticket is closed.

Accessing Other Utilities

The Tools tab in the Incident Management menu provides access to these Incident Management utilities:

- *Reset Downtime* on page 122
- *Build/Refresh Summary* on page 123
- *Downtime* on page 127
- *Summary Link* on page 128
- *Probable Cause* on page 129
- *Subcategory* on page 129
- *Problem Type* on page 130
- *Product Type* on page 131

Figure 4-30 shows the Tools tab choices.

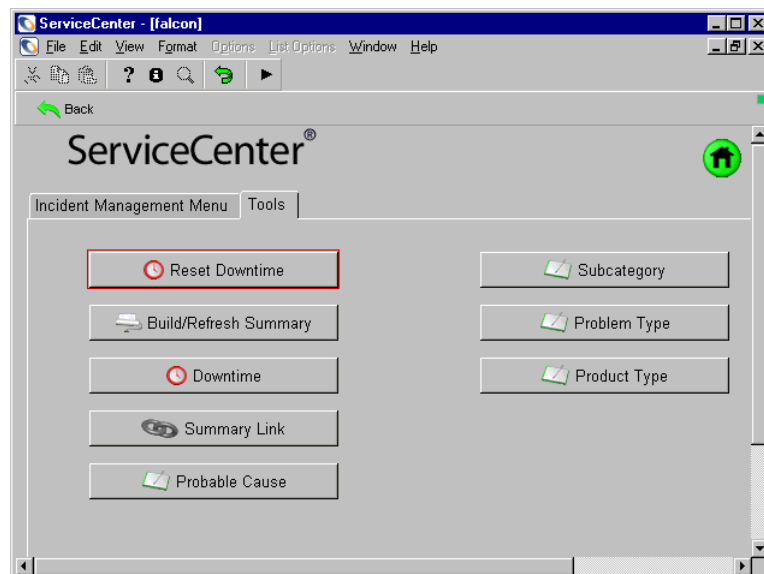


Figure 4-30: Incident Management menu: Tools tab

Reset Downtime

Reset Downtime allows you to reset the Incident Management downtime records for devices.

To reset the Downtime:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click the **Tools** tab. Click **Reset Downtime**. Figure 4-31 shows the Clear Availability Information form.

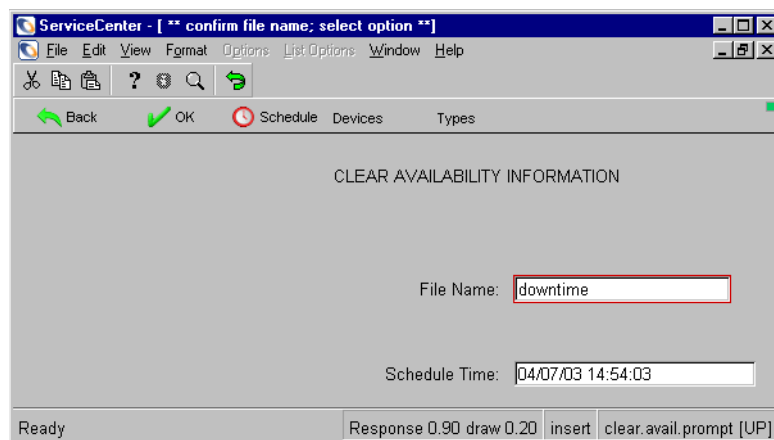


Figure 4-31: Resetting the Downtime record for a device

- 2 Click **Schedule** to set a time for the reset to occur.
- 3 Click **Devices** to add a list of devices whose downtime can be reset. Click **Types** to create a list of the types of devices whose downtime can be reset. Figure 4-32 on page 123 shows the logical names and device type lists.

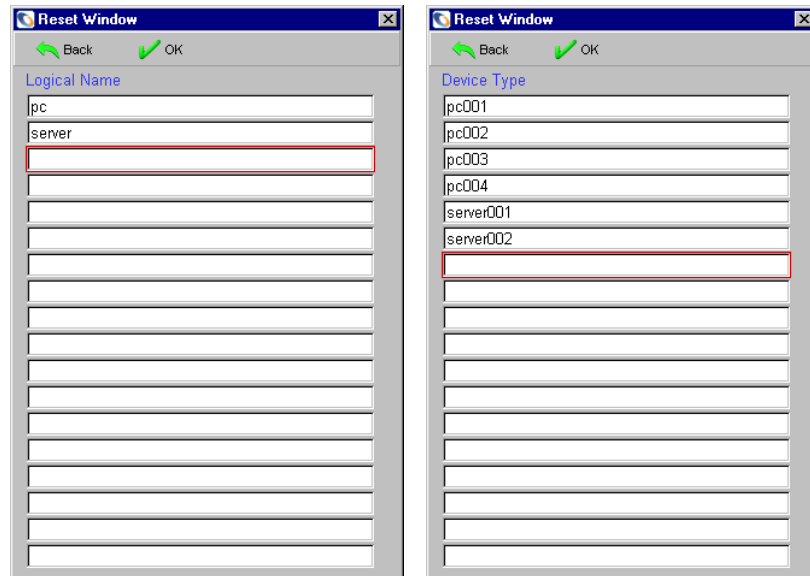


Figure 4-32: Logical Name and Device Type lists

- 4 Click **OK** to accept the downtime parameters you specified, or click **Back** to exit this form without resetting the downtime records.

Build/Refresh Summary

An incident summary (**probsummary**) record contains all the information related to an incident ticket, including previous updates. If you lose your incident summary file, you can build a new one from the incident ticket (**problem**) file. Build/Refresh Summary allows you to build a summary record for incident tickets within a specified range of incident ticket numbers.

To rebuild the summary properly, the link records **build.problem.summary** and **build.problem.convert** must be identical. The links in **build.problem.convert** are used only when you create a Build/Refresh Summary. The links in **build.problem.summary** define the fields to be copied from the **problem** record to the **probsummary** record with every incident ticket update.

If the links in `build.problem.convert` are not defined correctly, the new probsummary record will not have all the information available in the usual incident ticket updates. Therefore, before doing a Build/Refresh Summary, ensure that the file `build.prob.convert` is identical to `build.prob.summary`. To do this, copy `build.prob.summary` to `build.prob.convert`.

To correct the file `build.prob.convert`:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click the **Tools** tab. Click **Summary Link**. Figure 4-33 shows the Link file form.
- 2 Type `build.p` in the Name text box.
- 3 Click **Search**. A list of records appears, as shown in Figure 4-33.

Source Field Name	Format/File Name	Target Field Name	Add Query	Comments
number	probsummary	number		

Figure 4-33: Link File form

- 4 Double-click `build.problem.summary` record from the list.

- 5 The Link list appears, displaying the records **build.problem.summary** and **build.problem.convert**. Figure 4-34 shows the Link list.

name	system	sysmodtime	sysmoduser
build.problem.convert	PHD/PM	11/09/00 12:01:20	FALCON
build.problem.convert.old	PHD/PM UPGRADE	10/23/00 15:37:59	falcon
build.problem.summary	PHD/PM	03/01/01 13:57:32	FALCON

Link File

Name: System:

Description:

Source Field Name	Format/File Name	Target Field Name	Add Query	Comments
number	probsummary	number		

Selected line is row 1 of 5 records

Figure 4-34: Link File build.problem.convert

- 6 Click **build.problem.convert**. The Link record for **build.problem.convert** appears.



- 7 Click **Delete**.

- 8 A message asks if you want to delete this link. Click **Yes**. ServiceCenter returns you to the Link Maintenance file.

- 9 Click **build.problem.summary**.

- 10 In the Name text box, replace **build.problem.summary** with **build.problem.convert**.



- 11 Click **Add**

- 12 Click **OK** to return to the Link list.

- 13 To verify that the file copied, type **build.p** in the Name text box.

- 14 Click **Search**.

- 15 The records **build.problem.summary** and **build.problem.convert**, shown in Figure 4-34 should appear. If it does, proceed with the build/refresh.

To do a Build/Refresh Summary:

- 1 From the ServiceCenter home menu, click **Incident Management**. Click the **Tools** tab. Click **Build/Refresh Summary**. Figure 4-31 shows the Clear Availability Information form.

- 2 Figure 4-35 shows the dialog where you can specify a range of incident record numbers.

Figure 4-35: Build Problem Summary Records form

- 3 Type the range of record incident ticket numbers to build a new summary.
- 4 Do one of the following:
 - Click **Execute Now** to build your summary.

- Click **Schedule**. Figure 4-36 shows the Schedule Problem Conversion dialog box where you can specify a future date and time for the build.

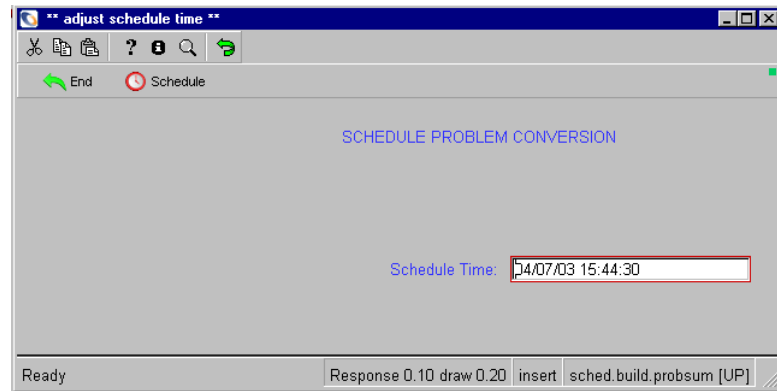


Figure 4-36: Schedule Problem Conversion form

- 5 Type a time and date (dd/mm/yy hh:mm:ss) for the build to take place.
- 6 Click **Schedule** to set the time. ServiceCenter returns you to the Incident Management Tools tab.

Alternate method

The **Downtime**, **Summary Link**, and **Probable Cause** functions can also be accessed through the Incident Management Security Administration Utility.

- 1 From the ServiceCenter home menu, click **Incident Management**. Click **Security Files**.
- 2 Click **Downtime**, **Summary Link**, or **Probable Cause**.

Downtime

- 1 From the ServiceCenter home menu, click **Incident Management**.
- 2 Click the **Tools** tab.
- 3 Click **Downtime**. Figure 4-37 on page 128 shows the Downtime form.

- 4 Click **Fill** to view a list of the logical names that you can choose.

ServiceCenter - [Search downtime Records]

File Edit View Format Options List Options Window Help

Back Add Search Find Fill

DOWNTIME

Logical Name Location Contact Name Type Table Name

ACME Phone 0002

Outage Totals

Last Reset Explicit Implicit Perceived Count

Details

Start Time	End Time	Type	Explicit	Implicit	Perceived	Incident No.

Ready Response 0.100 draw 0.71 insert downtime.graph.g(db.search) [UP]

Figure 4-37: Downtime

For more information, see the *ServiceCenter User's Guide*.

Summary Link

- 1 From the ServiceCenter home menu, click **Incident Management**.
- 2 Click the **Tools** tab.
- 3 Click **Summary Link**.

For more information, see [Summary Link](#) on page 128.

Probable Cause

- 1 From the ServiceCenter home menu, click **Incident Management**.
- 2 Click the **Tools** tab.
- 3 Click **Probable Cause**. Figure 4-38 shows the Probable Cause form.

Figure 4-38: Probable Cause form

For more information, see [Probable Cause](#) on page 99 and see the Service Management section in the *ServiceCenter User's Guide*.

Subcategory

- 1 From the ServiceCenter home menu, click **Incident Management**.
- 2 Click the **Tools** tab.
- 3 Click **Subcategory**.

- 4 Figure 4-39 shows the Subcategory form. Click **Search** to view a list of the subcategories and categories that you can choose.

Subcategory	Category
enquiry	business applications
client dependent	business applications
software	client system

Subcategory Information

Please enter the category and associated Subcategory

Category: business applications

Subcategory: enquiry

Active? ☒

Selected line is row 1 of 32 records retrieved Response 0.751 draw 0.431 insert subcategory.qbe.g [UP]

Figure 4-39: Subcategory Information

For more information, see the Service Management section in the *ServiceCenter User's Guide*.

Problem Type

- 1 From the ServiceCenter home menu, click **Incident Management**.
- 2 Click the **Tools** tab.
- 3 Click **Problem Type**.

- 4 Figure 4-40 shows the Problem Type form. Click **Search** to view a list of the problem types that you can choose.

The screenshot shows a web application window titled "ServiceCenter - [problemtyp]". The window has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with buttons for OK, Cancel, Previous, Next, Add, Save, Delete, Find, and Fill. Below the toolbar is a red header "Please Select a Problem Type". Under this header is a table with three columns: Problem Type, Product Type, and Given Level2. The table contains three rows: "business applications" (highlighted in blue), "applications", and "database". Below the table is a large gray area titled "Problem Type Information". Inside this area is a white box titled "Please enter associated Problem Type". This box contains four fields: "Product Type:" with a dropdown menu showing "applications", "Problem Type:" with a dropdown menu showing "business applications", "Subcategory:" with a dropdown menu showing "enterprise", and "Active:" with a checked checkbox. At the bottom of the window, there is a status bar with the text "Selected line is row 1 of 32 records retrieved" and "Response 0.150 draw 0.200 insert problemtyp.qbe.g [UP]".

Problem Type	Product Type	Given Level2
business applications	applications	enterprise
applications		
database	applications	

Problem Type Information

Please enter associated Problem Type

Product Type: applications

Problem Type: business applications

Subcategory: enterprise

Active: ☒

Selected line is row 1 of 32 records retrieved Response 0.150 draw 0.200 insert problemtyp.qbe.g [UP]

Figure 4-40: Subcategory Information

For more information, see the Service Management section in the *ServiceCenter User's Guide*.

Product Type

- 1 From the ServiceCenter home menu, click **Incident Management**.
- 2 Click the **Tools** tab.
- 3 Click **Product Type**.

- 4 Figure 4-41 shows the Subcategory form. Click Search to view a list. Select the Product Type record to populate the form.

ServiceCenter - [producttype]

File Edit View Format Options List Options Window Help

OK Cancel Previous Next Add Save Delete Find Fill

Please Select a Product Type

Product Type	Category	Subcategory
desktop	client system	hardware
external peripheral	client system	hardware

Product Type information

Please enter associated Product Type

Category: client system

Subcategory: hardware

Product Type: desktop

Severity: Low

Description:

Variable1:

Variable2:

Variable3:

Active? ☒

Assignment: ONSITE SUPPORT

Selected line is row 1 of 8 records

Response 0.80 draw 0.100 insert producttype2.qbe.g [UP]

Figure 4-41: Product Type

For more information, see the Service Management section in the *ServiceCenter User's Guide*.

5 Root Cause Analysis

CHAPTER

The goal of Root Cause Analysis is to minimize the effects of Incidents and Issues caused by errors in the IT infrastructure and to prevent their recurrence. Root Cause Analysis (RCA) allows users to identify the underlying root cause of the Issue or Incident, and initiate steps to correct that Root Cause with a permanent solution. This has the long term result of reducing the volume of Incidents and Issues that occur, saving the company time and money. RCA also allows users to improve their situation with a work around until a more permanent solution can be found, or when a permanent solution is costly in time or resources. This chapter describes administration of ServiceCenter's Root Cause Analysis module.

Read this chapter for information about:

- *RCA Overview* on page 134
- *Implementing Root Cause Analysis* on page 135
- *Root Cause Analysis Flow* on page 137
- *Accessing Root Cause Analysis* on page 138
- *Administering Root Cause Analysis* on page 139
- *Maintaining Inboxes* on page 151
- *Accessing the Macro List Editor* on page 151
- *Accessing the Knowledge Base* on page 152

For information about creating, updating, and closing Root Cause reports, see the *User's Guide*.

RCA Overview

The resolutions in RCA are documented and retained, so that first and second level support personnel can easily find and use the resolutions. Immediate availability of easy solutions is crucial to the effectiveness of support staff. The more Incidents that can be resolved on the first call, the happier the customer base. RCA is the bridge between Incidents and Known Errors and their solutions, allowing support personnel to resolve calls quickly and easily.

RCA determines weaknesses and errors in training and documentation by recording repeated customer errors that can be profitably addressed in training or documentation. Improved documentation and training helps customers avoid common mistakes that result in service calls, saving the organization time and money.

RCA documents resolutions in such a way that they can be easily found and added to the appropriate documentation and training materials by documentation and personnel. Complete and correct documentation and training have the long term result of reducing the volume of Incidents and Issues that occur, saving the company time and money.

RCA functions both reactively and proactively. It is reactive in that it is used to resolve situations related to Incidents. It is proactive in that it is used to identify and solve Issues and Known Errors, before Incidents occur. By taking action to prevent Incidents, rather than just reacting to them, an organization provides better service and is more efficient, making the customers happier and saving the organization time and money.

In summary, the goals of Root Cause Analysis are:

- To find errors in the IT infrastructure, record them, track their history, find resolutions for them, and prevent their recurrence.
- To record resolutions so that they are quickly and easily available to support, training, and documentation personnel.
- To find needs for improvements in training or documentation, and make the data to fix them easily accessible.
- To reactively resolve Issues related to Incidents
- To proactively resolve Issues before Incidents occur.

Terms Used in this Chapter

The following terms are used throughout the chapter.

Term	Description
Incident	A call to the service desk that is not immediately resolved and for which an Incident ticket has been issued.
Issue	A specific problem that may or may not have a set of related Incidents.
Known Error	An Issue for which the Root Cause has been diagnosed, and a solution or work-around has been determined.
Root Cause	The underlying cause of an Issue, or one or more Incidents.

Implementing Root Cause Analysis

Root Cause Analysis (RCA) should be implemented at the same time as Incident Management, or later, because it relies heavily on data gathered through the Incident Management process.

The quality of proactive Root Cause Analysis depends largely on successful service monitoring and the data recorded. Issues and Incidents must be identified, recorded, classified, investigated, and diagnosed by knowledgeable users.

In order to be effective, RCA requires the following input:

- Identify and detail Incidents and Issues
- Reactive analysis of Incidents & Issues
- Proactive analysis of the IT infrastructure
- Include input from support staff, developers, vendors, trainers, and so on
- Input discovered solutions

It often works well to begin with reactive analysis of incidents and issues, then continue with proactive analysis of the IT infrastructure after data have been gathered, because proactive RCA relies heavily on established service monitoring and data gathering.

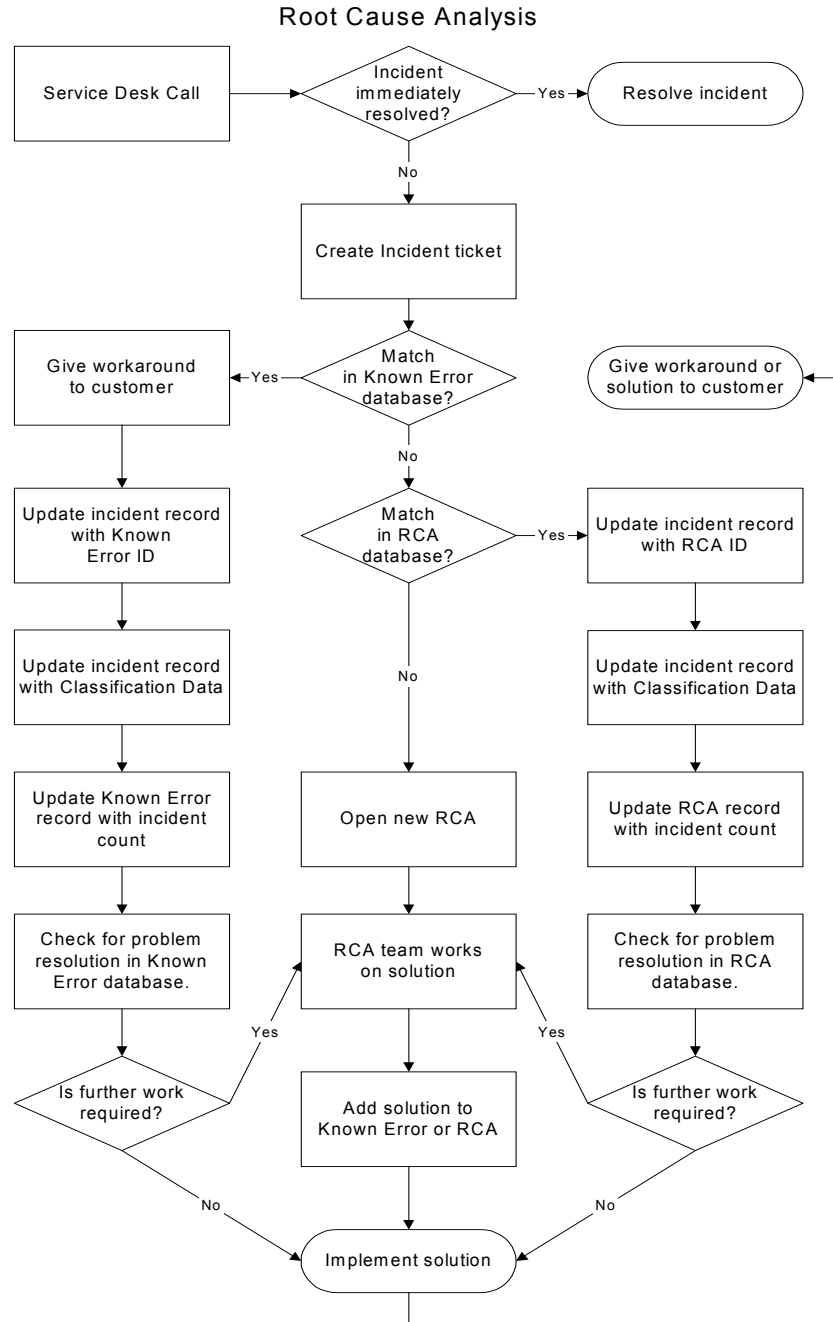
The goals of Incident Management and those of RCA can conflict somewhat. The main goal of Incident Management is to get the client up and running quickly. This is often done through a work around rather than through a permanent solution. The main goal of RCA is to find the underlying cause and a permanent solution that will prevent future Incidents. This takes more time, but improves performance in the long run.

It is important to make sure that your staff understands the differences between Root Cause Analysis and Incident Management and the importance of both.

When implementing Root Cause Analysis:

- Staff must be made aware of the benefits of both Incident and Issue solving activities.
- Incident records must include details and histories of Incidents for analysis purposes.
- Incident records must be linked with RCA records.
- Sufficient time must be allocated to both Incident and Issue solving activities.
- The knowledge base must be built and maintained.

Root Cause Analysis Flow



Accessing Root Cause Analysis

You can access Root Cause Analysis for administrative purposes from the Root Cause section of the ServiceCenter home menu, or from the Central Administration Utilities.

Central Administration Utilities allow a system administrator to access the operator's record for user and contact information, application profile privileges, and the Mandanten utility. This allows the administrator to control and access several users or a group's access from within each module or utility.

To administer Profiles from the Central Administration Utility, see the *System Administrator's Guide*.

To access Root Cause Analysis:

- 1 Click **Root Cause Analysis** in the ServiceCenter home menu, or enter `rca` on the command line.

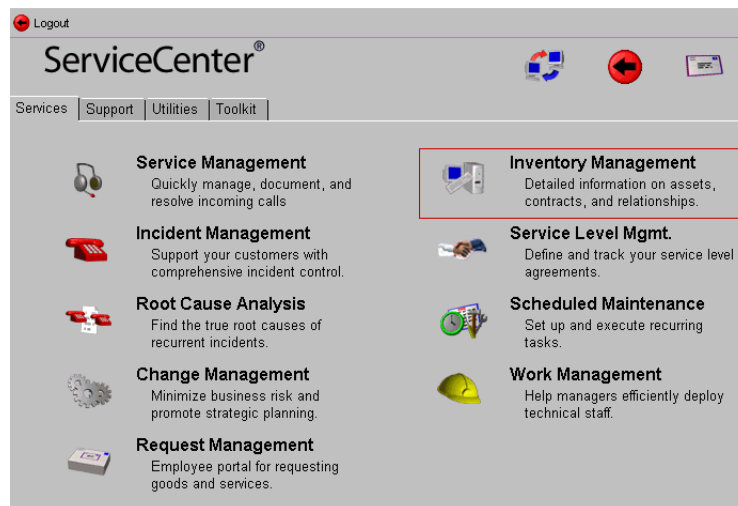


Figure 5-1: ServiceCenter home menu

Figure 5-2 shows the Root Cause Analysis menu appears.

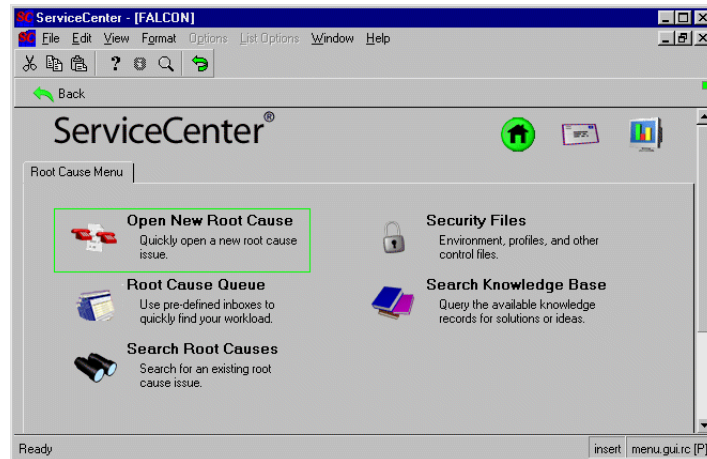


Figure 5-2: Root Cause menu

The Root Cause menu allows you to open new Root Cause records, access existing records, search Root Causes and the knowledge base, as well as configure the module.

Administering Root Cause Analysis

This section describes how to administer Root Cause Analysis by adding, editing, and deleting users and security profiles and by assigning certain display options to the viewer. It includes the following sections.

- *Accessing the Security Files* on page 140
- *Managing User Information* on page 143
- *Editing Profiles* on page 39
- *Maintaining Inboxes* on page 151
- *Managing the Root Cause Environment* on page 143

Security Files

Root Cause Analysis contains built-in security. Through this security, you can define the capabilities for individual users (operators). For example, certain users may not have the rights to close RCAs, while others may.

Users

Each person who logs into ServiceCenter is a user. Each user must have a personal information record stored in the **operator** file. Information associated with a user includes personal data such as name, address, phone numbers, login name, and password for ServiceCenter. ServiceCenter operator records also store capability words for a given user. Without an operator record, a user cannot log onto ServiceCenter. For a complete list of capability words, see the *ServiceCenter System Administrator's Guide*.

Profiles

Users must have a Root Cause Analysis Profile in their operator record, or use the default, to gain access to the Root Cause Analysis module. Profiles reflect the records in the **rcenv** file where Root Cause Analysis rights and privileges information is stored. For example, whether or not a user can close RCAs. Profiles also store information that may affect the way Root Cause Analysis looks and behaves. For example, a profile can list a personal search form for a specific user. For more information, see [User Profiles](#) on page 21.

Environment

Root Cause Analysis contains an environment record that defines options that affect functionality of the Root Cause Analysis module for all Root Cause Analysis users. Options stored in this record include Access rights.

Accessing the Security Files

To access security files from the Central Administration Utilities, see the *System Administrator's Guide*.

To access security files from the Root Cause Analysis menu:

- 1 From the ServiceCenter home menu, click **Root Cause Analysis**. The Root Cause Analysis menu appears.
- 2 Click **Security Files**. Figure 5-3 on page 141 shows the Root Cause Analysis Security Administration Utility appears.
- 3 Click **Back** to return to the Root Cause Analysis menu.

Security Files tab

Security options are selected on the Security Files tab shown in Figure 5-3.

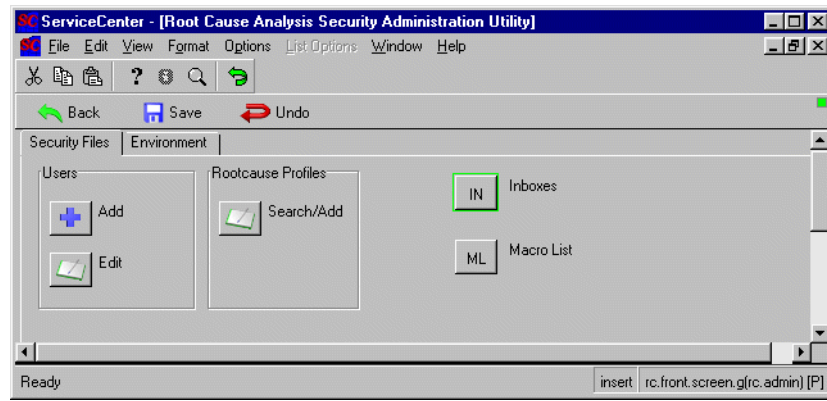


Figure 5-3: Security Administration Utility: Security Files tab

The Security Files tab allows:

- *Managing User Information* on page 143
- *Setting Privileges and Views in the Root Cause Profile* on page 148
- *Maintaining Inboxes* on page 151
- *Accessing the Macro List Editor* on page 151

Environment tab

Figure 5-4 shows the Environment tab.

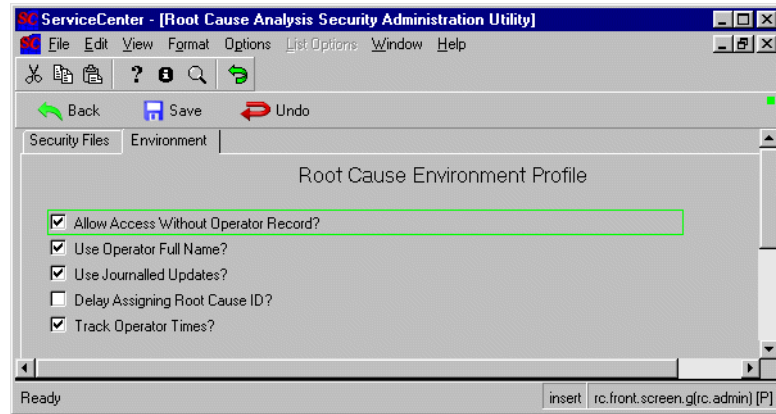


Figure 5-4: Security Administration Utility: Environment tab

The following table describes the parameters on the Environment tab.

Parameter	Definition
Allow Access Without Operator Record	Permits users without a Profile for Root Cause Analysis to access the module using the DEFAULT profile. See the <i>System Administrator's Guide</i> for more information.
Use Operator Full Name?	System uses the name entered in the Full Name field of the operator record when time stamping RCAs (on open, update, and so on) instead of using the operator's login name.
Use Journalled Updates?	Makes any information entered in the Action/Resolution tab a permanent part of the record that cannot be deleted. <ul style="list-style-type: none"> ■ Most to Least Recent: Lists updates to the record chronologically beginning with the most recent. ■ Least to Most Recent: Lists updates to the record chronologically beginning with the least recent.

Parameter	Definition
Delay Assigning Root Cause ID?	<p>No reference number is assigned to a Root Cause until after New is clicked in the initial Root Cause report form.</p> <p>Note: When this delay number is set to <i>true</i>, there is no unique identifier to tie an attachment within the file. Attachments cannot be saved when you open an incident, but only when saving an update to the file after the unique identifier has been assigned.</p>
Track Operator Times?	Turns on some default clocks that track how long a operator works on the record. SM and Incident Management have a similar field.

Managing the Root Cause Environment

You can configure general Environment Profile settings for all users via the Root Cause Environment tab. ServiceCenter is shipped with default environment records that you can modify for your system.

To set up the Root Cause environment:

- 1 Select the **Environment** tab in the Root Cause Analysis Security Administration Utility form. The Root Cause Environment Profile appears.
- 2 Select the parameters to apply to the Root Cause Analysis Environment. For more information, see *Environment tab* on page 142.
- 3 Click **Save** or press F2 to save the changes. If you are modifying the default environment record, you cannot add a new environment record. You will return to the RCA Control Security Administration Utility form.


Managing User Information

You can add or edit a ServiceCenter user from the Central Administration Utilities. Within these utilities, you can add or edit a user's information, including contacts, user profiles, and passwords. See the *System Administrator's Guide* for detailed information about user access and security administration from the Central Administration Utilities.

To add and edit a user within the Root Cause Analysis Security Administration Utility form, see *Adding a User* on page 144 and *Adding or Editing Root Cause Analysis Profiles* on page 146.

Adding a User

To add a user in Root Cause Analysis:

- 1 From in the ServiceCenter home menu, click Root Cause Analysis.
- 2 Click **Security Files** in the Root Cause Analysis menu. The Root Cause Analysis Security Administration utility appears.
-  3 Click **Add** in the Users structure of the Root Cause Security Administration Utility form. A dialog box prompts you to enter the name of the user you want to add.
- 4 Type the name of the new Root Cause user. For example, you can add a user named **Joe.User**.
- 5 Click **OK** or press **Enter**.
- 6 A dialog box displays a prompt to clone another user. Click **Yes** to clone another user.
- 7 Do one of the following:
 - Select an existing operator record to copy and modify. Either click the drop-down arrow to display a QBE list of existing user records or type the name of the user you want to copy. As you type the first few letters, the name is placed in the field. For this example, type **B** and **BOB.HELPDESK** fills the field.
 - Select a blank record.
- 8 Click **OK**.

The new operator record displays a new operator's name in the Login Name text box.

Figure 5-5: Operator Record

- 9 Modify the operator record as needed. Refer to the *System Administrator's Guide* for instructions on creating new operator records.
- 10 Specify a Resource Type on the Login/Contact Profiles tab.
- 11 Click **Add** to save the new operator record.
- 12 A dialog box displays a prompt that asks if the new user already has a contact record.
 - a Click **No**.
 - b Enter the user's contact name by typing it in, or by selecting it from the drop-down list.
 - c Click **OK**.
 - d Modify the contact information as needed.
 - e Click **Add** to save the contact record.

- 13 Click OK to return to the Root Cause Analysis Security Administration Utility menu. The status bar displays this message: **The New User Process is finished.**

Based on the user role selected when the operator record was added, the Root Cause profile application access rights and privileges are already assigned.
Editing User Records

Controls in the Security Administration Utility allow you to edit a user's Root Cause Analysis Profile records and operator record.

Note: For more information, see [Adding a User](#) on page 144.

To edit existing user records:

- 1 Click **Root Cause Analysis** in the ServiceCenter home menu.
- 2 Click **Security Files** in the Root Cause Analysis menu. The Root Cause Analysis Security Administration utility will display.
- 3 Click **Edit** in the Users structure. A dialog box displays a prompt to select an operator record for editing.
- 4 Select an operator from the drop-down list. The *CAU.operator* form displays, providing access to editing the operator's record, application profiles, and assignment/message groups.
- 5 Make any necessary changes to the various records, then click **Save** or **OK**.



Adding or Editing Root Cause Analysis Profiles

If you want to change the profile settings, you can either add a new profile or edit the existing profile.

Button	Definition
Add	Creates a new record in the <i>rcenv</i> file for the user. For more information, see Adding a Profile on page 32.
Edit	Edits the existing Root Cause Profile. For more information, see Editing Profiles on page 39.

If the application profile settings need to be different, you can add a new profile or edit the existing profile.

To add a profile:

- 1 From the ServiceCenter home menu, click **Root Cause Analysis**. The Root Cause Analysis menu appears.

- 2 Click **Security Files**.
- 3 Click **Search/Add** in the Rootcause Profiles structure. The Root Cause Security Profile appears.
- 4 Enter the name of the Root Cause profile you want to add.
- 5 Select the appropriate parameters for the user.



- 6 Click **Add** to save the Profile record.

To add a new profile using an existing profile:

- 1 Check the *User Role* in the Operator record to make sure the appropriate profile settings apply, which are based on the *User Role* selected.

Note: If you select a different *User Role*, click **Fill** in the **User Role** field, so that the applicable profile access privileges and views are reset appropriately for each module.

- 2 Click **Find** to the right of the **Root Cause Profile** field. The Root Cause Security Profile form displays.
- 3 Modify the privileges as necessary.
- 4 Enter a new name in the **Profile Name** field.
- 5 Click **Add**.

Note: Clicking **Add** keeps the original profile you modified and adds the new profile as long as you entered a new name in the Profile Name field. Clicking **Save** would overwrite the original profile with the changes to the privileges and a new profile name.

To edit a profile:

- 1 Check the *User Role* in the Operator record to make sure the appropriate profile settings apply, which are based on the *User Role* selected.

Note: If you select a different *User Role*, click **Fill** in the **User Role** field, so that the applicable Service profile access privileges and views are reset appropriately for each module.

- 2 Click **Find** to the right of the Root Cause Profile field. The Root Cause Security Profile form displays.
- 3 Modify the privileges as necessary.
- 4 Click **Save**.

Setting Privileges and Views in the Root Cause Profile

The Root Cause Analysis profile form is used to define Profiles for users who plan to access Root Cause Analysis. For an out-of-box defined solution, select the appropriate User Role for your new operator. (See the *System Administrator's Guide* for information on User Roles.) The selected User Role in an operator record plays an important part in deciding what application profiles are going to be assigned to the user. The Root Cause profiles supplement and further restrict any rights defined in a user's operator record, and allow you to control access to Root Cause Analysis.

Root Cause Analysis Privileges and Views

Privileges and views define the user's access privileges and views within the Root Cause Analysis module. Figure 5-6 shows the Root Cause Security Profile form. By default, no options are selected.

ServiceCenter - [User Rootcause Profile]

File Edit View Format Options List Options Window Help

Back Add Search Find Fill

Root Cause Security Profile **Profile Name**

Privileges and Views

<input type="checkbox"/> Browse	Initial Inbox	<input type="text"/>
<input type="checkbox"/> Open	Initial Format	<input type="text"/>
<input type="checkbox"/> Update	Edit Format	<input type="text"/>
<input type="checkbox"/> Close	Search Format	<input type="text"/>
<input type="checkbox"/> Reopen	List Format	<input type="text"/>
<input type="checkbox"/> Find	Manage Format	<input type="text"/>
<input type="checkbox"/> Fill	Print Format	<input type="text"/>
<input type="checkbox"/> Print	Open Script	<input type="text"/>
<input type="checkbox"/> Views	Resolution Script	<input type="text"/>
<input type="checkbox"/> Count		
<input type="checkbox"/> Advanced Search		
<input type="checkbox"/> Use Operator Full Name	<input type="checkbox"/> New Thread: Inbox -> Search	
<input type="checkbox"/> Can Create Personal Inboxes	<input type="checkbox"/> New Thread: Search -> List	
<input type="checkbox"/> Can Create Global Inboxes	<input type="checkbox"/> New Thread: List -> Edit	
<input type="checkbox"/> Lock on Display	<input type="checkbox"/> New Thread: Inbox -> Edit	
<input type="checkbox"/> Allow Inefficient Query		
<input type="checkbox"/> Skip Query Warning		

Ready insert rc.profile.g(profile.search) [P]

Figure 5-6: Root Cause Security Profile: Privileges and Views tab

The following table describes fields on the Privileges and Views tab.

Field	Description
Browse	Allows the user or group to view existing RCAs.
Open	Allows the user or group to add new RCAs.
Update	Allows the user or group to change existing RCAs.
Close	Allows the user or group to terminate existing RCAs.
Reopen	Allows the user or group to reactivate a closed ticket.
Find	Provides access to ServiceCenter's Find function in Root Cause Analysis.
Fill	Provides access to ServiceCenter's Fill function in Root Cause Analysis.
Print	User or group has print capabilities in ServiceCenter.
Views	Provides access to alternate forms when viewing a call report.
Count	User or group can count the number of tickets in a QBE list by pressing Count.
Advanced Search	Provides access to ServiceCenter's advanced search capabilities to query for information.
Use Operator Full Name	Tells the system to use the name from the Full Name field of the operator record when time stamping RCAs (on open, update, and so on) instead of using an operator's login name.
Can Create Personal Inboxes	Allows the user or group to create personal inboxes for their own use. Creating inboxes is discussed in Chapter 2 of the ServiceCenter User's Quick Start Guide.
Can Create Global Inboxes	Allows the user or group to create global inboxes for all Root Cause Analysis users. Creating inboxes is discussed in the <i>User's Guide</i> .
Lock on Display	Locks the call record a user has accessed.
Allow Inefficient Query	Allows the user or group to enter partially-keyed queries, that is, queries without a complete set of information to do a search. This setting supersedes the setting in the Root Cause Management Environment Record. This setting is overridden when Skip Query Warning set to <i>true</i> .
Skip Query Warning	Turns off the warning message normally sent when a partially-keyed query is entered. Setting to <i>true</i> (checked) overrides the option set in Allow Inefficient Query.

Field	Description
Initial Inbox	Defines the default inbox for the user or group in Root Cause Analysis.
Initial Format	Form displayed to the user or group when opening a call report. The default is <i>rootcause</i> .
Edit Format	Form displayed to the user or group when editing an existing root cause report.
Search Format	QBE form displayed to the user or group when searching for existing RCAs. The default is <i>rootcause.qbe</i> .
List Format	Form used to display a record list.
Manage Format	Form displayed when the user or group clicks Call Queue. The default is <i>sc.manage.call</i> .
Print Format	Form used by the system for printing call reports for the user of group.
Open Script	Script that runs when opening a root cause.
Resolution Script	Causes Root Cause Analysis to use the script named in the adjacent field to automatically update the Root Cause summary record when an Root Cause ticket is inactivated.
New Thread: Inbox > Search	Keeps the inbox displayed after a search is run from that inbox. Note: Threading allows the previous window to remain displayed when a new record is accessed. For example, when a record is accessed from a QBE list, the QBE list remains displayed and the record appears in a new window.
New Thread: Search > List	Keeps the search form open after a QBE list is opened.
New Thread: List > Edit	Keeps a QBE list form displayed when a record is accessed.
New Thread: Inbox > Edit	Keeps an inbox displayed after a record is accessed.

Maintaining Inboxes

You may add, edit, and delete inboxes from the Root Cause Analysis Security Administration Utility. These are the same inboxes used by Incident Management and other ServiceCenter modules. The procedures for maintaining them are identical. For more information, see the *ServiceCenter User's Guide*. Figure 5-7 shows the Basic tab.

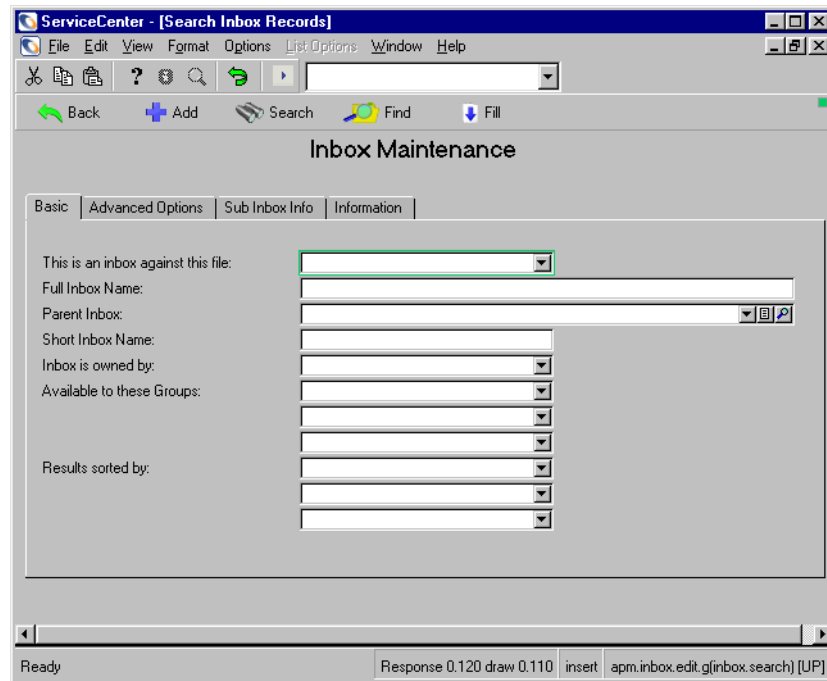


Figure 5-7: Inbox Maintenance: Basic tab

Accessing the Macro List Editor

You can access ServiceCenter's Macro Editor from the Root Cause Analysis Security Administration Utility. Click Macro List to display the Macro List form. This is the access point for the Macro Editor. For instructions about this procedure, refer to the *System Administrator's Guide*.

To open the Macro List:



- Click Macro List in the Security Administration Utility form.

Figure 5-8 shows the Macro List form.

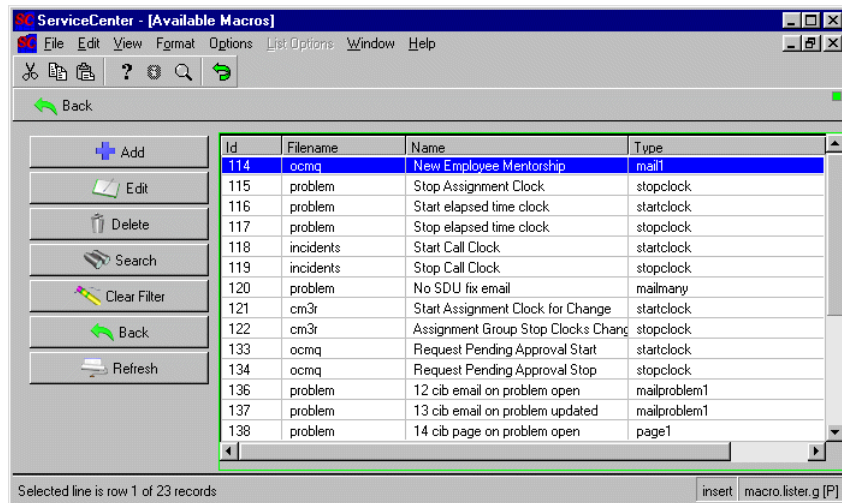


Figure 5-8: Macro List form

For more information, see the *ServiceCenter System Tailoring Guides*.

Accessing the Knowledge Base

ServiceCenter allows you to make plain language queries for information (for example, information about an incident ticket or a question about equipment) using a Knowledge Base form. For example, a query can yield a list of incident tickets.

To access the Knowledge Base:

- Click **Search Knowledge Base** in the Root Cause Analysis menu.

Figure 5-9 shows the Knowledge Base search form. To access the knowledge base, select Root Cause Database from the Select a Knowledge area to begin search drop-down list.

The screenshot shows a web application window titled "ServiceCenter - [Knowledge Base]". The interface includes a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for Back, Search, and Clear. The main content area is titled "Find Solution - Knowledge Base" and contains the following elements:

- A dropdown menu labeled "Select a Knowledge Area to begin search:" with "Global Knowledge" selected.
- A dropdown menu labeled "Restrict Search to Which Field in IR key (blank=all fields):".
- A text input field labeled "What would you like to know?".
- A "Discovery Option:" section with two radio buttons: "Shallow" (selected) and "Complete Match".
- A "Deep" radio button.
- Two icons: a flashlight and a pencil.
- Search criteria fields:
 - Category: [text box]
 - Subcategory: [text box]
 - Product Type: [text box]
 - Problem Type: [text box]
 - Device: [text box]
 - Company: [text box]
 - Location: [text box]

The status bar at the bottom shows "Ready", "Response 0.150 draw 0.20", "insert", and "sc.knowledge.prompt.core.g [L]".

Figure 5-9: Knowledge Base Search form

For more information, see the *ServiceCenter User's Guide*.

6 Scheduled Maintenance

CHAPTER

Scheduled Maintenance is a ServiceCenter module that enables you to establish a formal scheduled maintenance system to reduce unplanned outages and system failures by servicing systems before they fail rather than afterwards.

Scheduled Maintenance helps you administer, configure, and customize Scheduled Maintenance. You should have an understanding of the ServiceCenter expression syntax and Database Manager to administer Scheduled Maintenance.

Read this chapter for information about:

- *Scheduled Maintenance Overview* on page 156
- *Creating a Scheduled Maintenance Task* on page 156
- *Automated Task Generation* on page 157
- *Scheduled Maintenance in Inventory Management* on page 159
- *Adding Data Using Expressions* on page 164
- *Scheduled Maintenance Overhead* on page 165
- *Calling a Format Control Record* on page 166
- *Scheduled Maintenance Workflow* on page 167

Scheduled Maintenance Overview

Scheduled Maintenance makes it easy for you to define and store as many maintenance tasks as you need for your organization. Scheduled Maintenance includes these features:

- Enables you to defining and schedule recurring maintenance tasks, including incident tickets, change requests and Request Management quotes, using closed loop integration with ServiceCenter.
- Keeps all scheduled maintenance tasks in a central repository to ensure that important maintenance occurs on time. The stored maintenance tasks will automatically generate incident tickets, change requests, or Request Management quotes as they become due.
- Automatically notifies staff of all maintenance items as they become due using ServiceCenter.
- Creates and updates Scheduled Maintenance tasks even if you are unfamiliar with ServiceCenter. Scheduled Maintenance has an easy-to-use point and click task creation system. This enables users who are familiar with maintenance requirements to enter tasks, even if they are unfamiliar with ServiceCenter customization.
- Makes audit information available as necessary. The maintenance history and the auditing information for each task will be available if and when it is required.
- Creates sophisticated and detailed maintenance tasks.
- Maintains existing ServiceCenter customization and tailoring.
- Tracks scheduled maintenance tasks.

Scheduled Maintenance runs within the ServiceCenter system. It installs without requiring an upgrade, and has no impact on future ServiceCenter upgrades. It integrates into a pre-existing ServiceCenter installation, while maintaining all tailoring and customization.

Creating a Scheduled Maintenance Task

To create a Scheduled Maintenance task, follow these general steps:

- 1 Name and describe the task.
- 2 Define the task schedule.

- 3 Describe the effect of the task.
- 4 Optionally, you can create expressions to enter additional information into the incident ticket, change request, or Request Management quote.
- 5 Optionally, you can call a special Format Control Record to run in addition to the regular records that ServiceCenter runs automatically.
- 6 Save the task.
- 7 Verify that the task works correctly.

When the scheduled time occurs, Scheduled Maintenance automatically generates the appropriate incident tickets, change requests, or Request Management quotes. For more information and examples, see the *ServiceCenter User's Guide*.

Automated Task Generation

There are two ways that Scheduled Maintenance automatically generates tasks.

- Create the scheduled maintenance task from an existing incident ticket, change request, or Request Management quote. From the Options menu, select Generate Maintenance. The existing ticket becomes the basis for the scheduled maintenance task. For more information, see *Generating Tasks From an Existing Ticket* on page 157.
- Create the scheduled maintenance task from a default incident, change, or request template specified in Administrative Options for a device in Inventory Management. For more information, see *Generating Tasks from Scheduled Maintenance* on page 161

Generating Tasks From an Existing Ticket

Generating scheduled maintenance tasks can be tedious, especially if you must generate a large number of tasks to do approximately the same thing. For example, you might want to generate 10 scheduled maintenance tasks to back up 10 servers. The tasks are very similar in nature because the company uses a standard template for all server backups.

Scheduled Maintenance allows you to access Incident Management, Change Management, or Request Management, find a ticket, and generate a scheduled maintenance task. For example, you can create a default Change Management template for server backups. Instead of generating

10 scheduled maintenance tasks manually that are variations on the default template, you can access the template from Change Management and select Generate Maintenance 10 times. You must still specify a recurrence schedule for each task, but many of the details on the Change Request are already specified.

Migrated fields

All fields in the template do not migrate to the maintenance task and subsequently to the generated incident, change, or request.

Incidents

- category*
- brief.description
- assignment
- logical.name**
- ticket.owner
- priority.code
- problem.status

Changes

- description
- category
- logical.name**
- coordinator
- work.manager
- assigned.to
- priority

Requests

- description
- category
- requestor.name
- assigned.to
- coordinator
- priority
- action

* May be overridden if the device has a default problem management category.

** Overridden with the device name of the selected item within the Inventory module when you choose this option.

To generate a maintenance task from existing tickets:

- 1 From the ServiceCenter home menu, click **Incident Management**, **Change Management**, or **Request Management**.
- 2 To view an existing queue, click **Incident Queue**, **Change Queue**, or **Quote Queue**. Do one of the following:
 - Specify a ticket number. Click **Search** to view the ticket record.
 - Click **Search** to display all tickets in the queue. Double-click the selected ticket to view the ticket record.
- 3 To search for a ticket, click **Search IM Tickets**, **Search Changes**, or **Search Quotes**. Do one of the following:
 - Specify a ticket number. Click **Search** to view the ticket record.
 - Click **Search** to display all tickets in the queue. Double-click the selected ticket to view the ticket record.

- 4 From the **Options** menu, choose **General Maintenance**. Click the **Schedule** tab. The default schedule for a generated maintenance task is **Regularly: Every 1 00:00:00**, beginning at the current date and time. You can change this value to the recurrence model you want.

If this task is referenced in the Scheduled Maintenance Administrative Options, or the named template does not exist, the system creates a skeletal scheduled maintenance task. Skeletal maintenance tasks have an inactive state by default. Check the Active box to run the task.

Scheduled Maintenance in Inventory Management

Scheduled Maintenance is integrated with the ServiceCenter Inventory Management module.

To access Scheduled Maintenance commands:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 From the **Assets** tab, click **Assets**.
- 3 Do one of the following:
 - Type the Asset ID and click **Search**.
 - Click **Search** to view all assets, double-click the selected asset.
- 4 From the **Options** menu, choose **Scheduled Maintenance**, and click one of the following commands:
 - Maintenance Tasks
 - Maintenance History
 - Generate Recurring
 - Incidents
 - Changes
 - Requests

Maintenance Tasks

Choose this command to show any maintenance tasks that are bound to a specified device. A task that references a range of devices, such as every server in Topeka, will not appear.

Maintenance History

Choose this command to list how many incidents, changes, or requests are generated when a maintenance task runs. From this list, you can view the individual problem tickets, change requests and Request Management quotes in detail. Maintenance tasks that create one incident, change, or request show one entry. Maintenance tasks that create a collection of incidents, changes, or requests for every record in inventory matching certain parameters can generate different information each time the task runs.

For example, on May 1, there might be two servers in Topeka, but by June 1, there might be a third server installed. Therefore, a task that generates a change for every server in Topeka would generate two changes in May and three changes in June.

Generate Recurring > Incidents,

Choose this command to generate a scheduled maintenance task for the current device, which creates an incident ticket. This scheduled maintenance task is based on a template incident ticket and other information from Inventory Management.

Generate Recurring > Changes

Choose this command to generate a scheduled maintenance task for the current device, which creates a change request. This scheduled maintenance task is based on a template change request and other information from Inventory Management.

Generate Recurring > Requests

Choose this command to generate a scheduled maintenance task for the current device, which creates a Request Management quote. This scheduled maintenance task is based on a template Request Management quote and other information from Inventory Management.

Ticket Limitations

The Scheduled Maintenance Advanced Query has a built in anti-spam feature. By default, the system will only generate 50 tickets, regardless of how many records the advanced query returns. This is to prevent, for example, an errant user from creating a Scheduled Maintenance task that would open a

ticket for every device in inventory. However, if you want to be able to generate a larger number of tickets, you can increase that number. This threshold is user definable under the administrative options section of the Scheduled Maintenance menu.

Generating Tasks from Scheduled Maintenance

This feature generates maintenance tasks for a specific device. Maintenance tasks are relatively complex because they ultimately create incidents, changes, or requests. The type of incident, change, or request a scheduled maintenance task generates depends on a template ticket.

To access a template ticket:

- 1 From the ServiceCenter home menu, click **Scheduled Maintenance**.
- 2 From the **Scheduled Maintenance** menu, click **Administrative Options**. The Scheduled Maintenance Administrative Options form appears with a list of default templates.

Using a Template

ServiceCenter follows this series of steps when it applies a default template to a new scheduled maintenance task.

- A user selects Generate Recurring Incidents, Changes, or Requests. See *Scheduled Maintenance in Inventory Management* on page 159.
- In this example, ServiceCenter determines that the default incident template is IM1001. See *Template Administration* on page 162.
- ServiceCenter creates a scheduled maintenance task. When the task runs, it creates a new incident ticket that looks like IM1001.
- ServiceCenter enables a user to modify this maintenance task.

The new ticket is not entirely template based. The default template for IM1001 may reference another piece of hardware. ServiceCenter uses the values in IM1001 and modifies them. ServiceCenter overrides the category of IM1001 with the default problem management category for the device as it appears in its inventory record. ServiceCenter overrides the device referenced by IM1001 references with the new device.

Template Administration

You have the ability to identify templates for new scheduled maintenance tasks, or to change the maximum number of tickets.

To select templates for use in task generation:

- 1 Open the Scheduled Maintenance menu and select Administrative Options. Figure 6-1 shows the Edit Record dialog box.

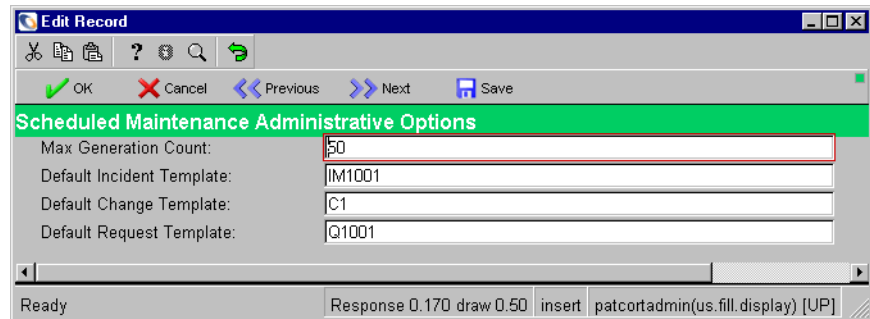


Figure 6-1: The Edit Record dialog box

- 2 You can specify a ticket number for each of the following:
 - Default incident template
 - Default change template
 - Default request template

The default incident, change and request templates listed here refer to existing incident, change, or request tickets. Choosing this option generates a scheduled maintenance task that will subsequently create an incident, change, or request based on the appropriate template ticket.

To define the maximum number of queries to be returned:

- 1 Open the Scheduled Maintenance menu and select Administrative Options. The Edit Record dialog box appears, as shown in Figure 6-1 on page 162.
- 2 Change the **Max Generation Count** field to a new value. Click **OK** to return to the Scheduled Maintenance Menu tab.
- 3 Click **Scheduled Maintenance**.
- 4 Do one of the following:
 - Type the name of the scheduled task in the Name text box and click **Find**.
 - Click **Search** to display a list of all scheduled tasks. Double-click the selected task. In this example, choose Shutdown Zombie Jobs.
- 5 Stop and restart the scheduler that executes Scheduled Maintenance tasks.

The screenshot shows the 'ServiceCenter - [Database: 42]' application window. The 'Scheduled Maintenance Tasks' dialog box is open, with the 'Details' tab selected. The 'Name' field is 'Shutdown Zombie Jobs'. The 'ID' field is '42'. The 'Next Scheduled at' field is '01/28/03 16:30:47'. The 'Description' field is 'Open Incident Tickets of Category: network'. The 'Assign To' field is 'LAN SUPPORT'. The 'Set Status To' field is 'Open'. The 'With Ticket Owner of' field is 'BOB.HELPDESK'. The 'With Priority Code of' field is '4 - Priority Four'. The 'With a Company of' field is 'ACME'. The 'Work on This Device' field is 'MF-000001'. The 'Use These Expressions to Fill the Task' section contains the text: 'Example: priority.code in \$L.file="1"', 'subcategory in \$L.file="applications"', and 'priority.code in \$L.file="4"'. The 'Call out to this format control record to finish filling the record; fc add routines will run' field is empty. The status bar at the bottom shows 'Ready', 'Response 0.120 draw 0.230 insert', and 'patcotask(task.view) [UP]'.

Figure 6-2: Scheduled Maintenance Tasks: Details tab

If you do not stop and restart the scheduler, the system does not recognize that this value has changed.

Adding Data Using Expressions

The *ServiceCenter User's Guide* describes how to populate fields on an incident ticket, change request, or Request Management quote. In addition to those fields, you can use expression syntax to auto-fill additional fields in the incident ticket, change request, or Request Management quote.

Expressions run after the simple information is filled in the incident ticket, change request, or Request Management quote. You can use expressions to override the category, assignee, or another field.

To fill fields using expression syntax:

- 1 Complete step 1 through step 4 on page 163.
- 2 Click the **Details** tab.
- 3 Figure 6-2 on page 163 shows the Advanced section on the Details tab.
- 4 Type the expressions that set selected fields to new values. The incident ticket, change request, or Request Management quote are called `$L.file` in these expressions. For example, to set the subcategory and priority code on incident tickets, add these two lines of expression code.

```
subcategory in $L.file="application"
priority.code in $L.file="4"
```

where `application` is the name of the subcategory and `4` is the priority code. Figure 6-3 shows how these expressions appear on the Details tab.

Use These Expressions to Fill the Task; the problem ticket or change request or quote in question will be `$L.file`
 Example: `priority.code in $L.file="1"`

<code>subcategory in \$L.file="applications"</code>
<code>priority.code in \$L.file="4"</code>
<input type="text"/>

Call out to this format control record to finish filling the record; fc add routines will run

Figure 6-3: Using Expressions

- 1 Click **Save**.

Scheduled Maintenance Overhead

Scheduled Maintenance relies on the Incident background scheduler to call into the Scheduled Maintenance code at regularly scheduled intervals. If the Incident scheduler is not running, no Scheduled Maintenance tasks run. When a Scheduled Maintenance task runs, it increases the load on the Incident scheduler by a marginal amount.

Scheduled Maintenance does not put a large load on your system unless you are using the Scheduled Maintenance system to generate extraordinarily large numbers of incident tickets, change requests, or Request Management quotes. The impact of Scheduled Maintenance on your system if it creates twenty tasks a day is approximately identical to the impact of one user opening twenty tasks a day.

If you set up a Scheduled Maintenance task to create 20,000 Incident tickets at 2:00 AM on January 1st, your system would slow down somewhat. Scheduled Maintenance will create all 20,000 tickets consecutively, much the same as one user opening 20,000 incident tickets consecutively. The increased load may be noticeable but it will not be crippling.

Load Balancing

You should not notice any change in your system load when you use Scheduled Maintenance. However, if you have unusually large numbers of task opening every day, such as 1000 each day, or over 100 in a 10-minute period, consider creating a private scheduler that runs only Scheduled Maintenance tasks. When you create this scheduler and have it up and running, change the class on the Scheduled Maintenance Hook schedule record to match your new scheduler. You can also change the repeat interval on the inhook schedule record to meet your site's needs.

To access the Scheduled Maintenance Hook schedule record:

- 1 From the ServiceCenter home menu, click the **Toolkit** tab.
- 2 Click **Database Manager**.
- 3 Type **schedule.looksee** in the **Form** field. Type **schedule** in the **File** field. Click **Search**.
- 4 The blank Schedule File form appears. Click **Search** for a list of all records.
- 5 Locate and select Scheduled Maintenance Hook to populate the form fields.

The minimum effective repeat interval is one minute because the system checks for tasks every minute. With adjustment, you can reduce this to about 10 seconds. You cannot reduce the interval to less than 10 seconds because of the internal structure of the ServiceCenter scheduling system.

Calling a Format Control Record

Scheduled Maintenance includes a hook to allow you to execute a particular Format Control record before it hands over control to the main ServiceCenter code.

The normal Format Control record specified inside of an incident ticket, change request, or Request Management quote always runs. However, you can add an additional Format Control record. If you leave the Format Control field blank, your normal Format Control record runs. If you specify a Format Control record, all of your normal Format Control still runs, but this named Format Control record runs first. Figure 6-4 shows the Format Control text box on the Details tab.

Use These Expressions to Fill the Task; the problem ticket or change request or quote in question will be \$L.file
 Example: priority.code in \$L.file="1"
 subcategory in \$L.file="applications"
 priority.code in \$Lfile="4"
 Call out to this format control record to finish filling the record; fc add routines will run

Figure 6-4: Using Expressions

This mechanism is a hook that enables you to manage Format Control, calculations (although task expressions can accomplish many of the same tasks more simply), validations, or calls to subroutines. All of this happens before the record is passed into the regular ServiceCenter incident, change or request code.

To specify an extra Format Control record:

- 1 Complete step 1 through step 4 on page 163.
- 2 Click the **Details** tab.
- 3 Figure 6-4 shows the Advanced section on the Details tab.
- 4 Type the name of a Format Control record in the text box.
- 5 Click **Save**.

The Add processes on this extra Format Control record will execute after the expressions are parsed, but before the regular incident ticket, change request, or Request Management quote management code.

Scheduled Maintenance Workflow

Figure 6-5 shows how information flows through Scheduled Maintenance.

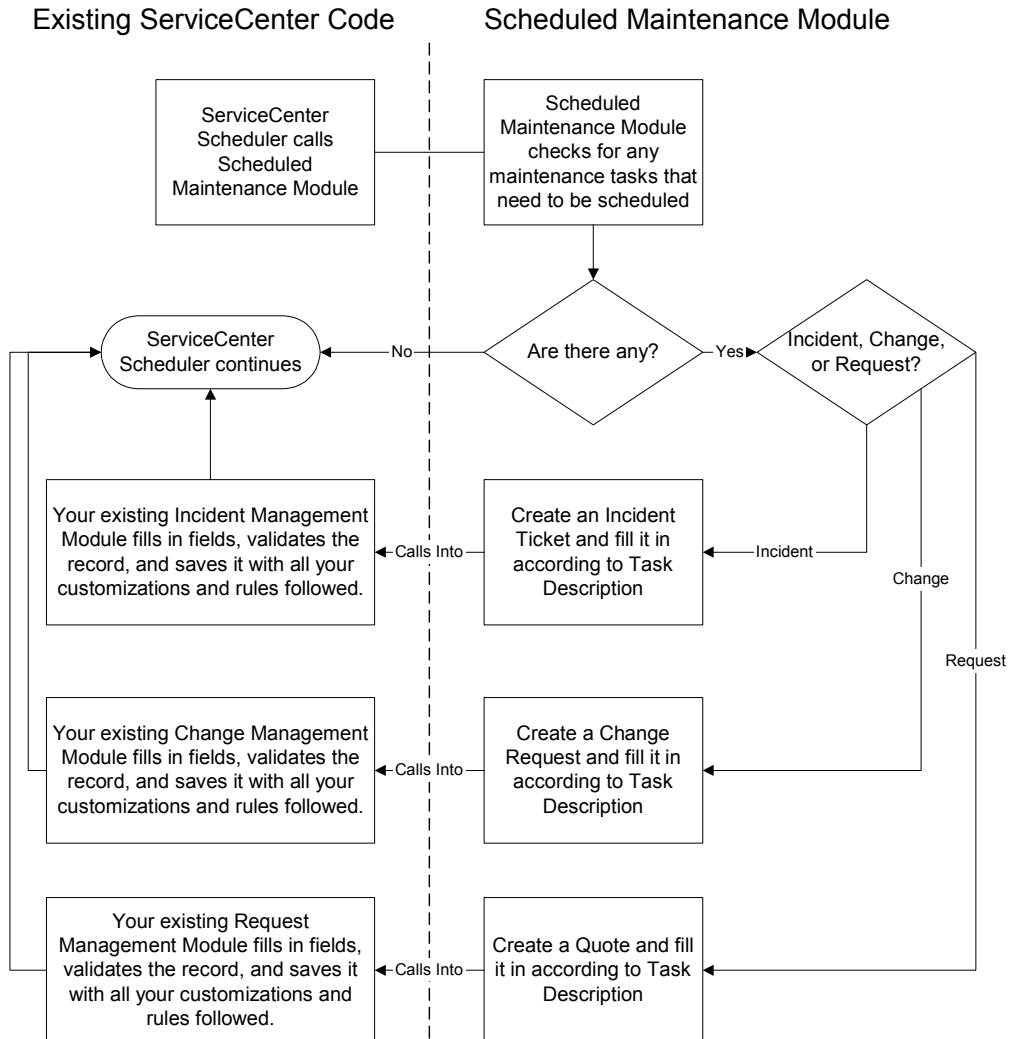


Figure 6-5: Scheduled Maintenance workflow

7 Inventory Management

CHAPTER

This chapter describes the administration of ServiceCenter's Inventory Management Module (ICM) helps you track organizational assets by creating asset inventory records. Other ServiceCenter modules can access the inventory records in ICM. For example, if you create an incident ticket, Incident Management can access the component information from the inventory database. Incident Management can insert this information in the new ticket. You can also create inventory records with ICM.

Through network discovery tools, inventory records can be added automatically and updated by network agents feeding device configuration information into Inventory Management. For more information about associated user tasks, see the ServiceCenter User's Guide.

Read this chapter for information about:

- *The ICM Repository* on page 170
- *Creating Subtables from an Array of Structures* on page 175
- *Accessing Inventory Management* on page 176
- *Organizing Inventory Records* on page 178
- *Administering Inventory Management* on page 180
- *Inventory Records* on page 205

The ICM Repository

ICM provides a data repository that describes the physical and logical network and any other assets you want to track in this way, such as furniture and fixtures. Other ServiceCenter modules such as Incident Management and Change Management use this data.

Although you may be constantly accessing ICM records, you will not necessarily be running ICM. Other ServiceCenter modules retrieve information from the ICM repository. Other ServiceCenter module records display only the relevant information. You can view a complete inventory record using the Find function from a field that is related to the inventory record.

The ICM modules share a set of inventory files that describe the common attributes of all devices, the specialized attributes of different device types, and the relationships between them.

Primary and Attribute Files

The primary files are:

File Name	Contents
device	Contains records for each device or facility in the network and serves as the device file for all network entities.
devtype	Creates the different device types and controls the relationships between the different files that make up the network, how they are displayed, and any script called when adding the device to the database.

A separate set of database descriptors defines all common and specific attributes that appear when you select a device.

Database Dictionaries

There are three database dictionaries (dbdicts) for each component with an attribute file:

- device dbdict
- attribute
- joinfile

The `logical.name` field in both the attribute and device dbdicts create a logical joinfile.

Device Files

The hardware and facilities in your network are *devices* that are described in device files. Device files contain common information about each component (hardware or software) in the system. There is a logical device record for each component in the network. Each logical device record can be retrieved from the device file. Depending on its type, the component may also have a logical record in an attribute file. For example, every PC has a logical device record in the `pcdevice` file, and also a logical attribute record in the `pc` file.

Device file characteristics include:

- Only one device file.
- A logical record in the device file for every device in the ICM.
- The `logical.name` field is the unique identifier in the dbdict.

The device dbdict is the general database dictionary. It contains a `logical.name` field that is the unique identifier for each device. Fields in the device file, except for `logical.name`, are not repeated in the attribute files.

Attribute Files

Most hardware or software device types have a set of descriptive attributes. Different device types can share a common set of attributes. The descriptive attributes are organized into logical attribute files, where each component matching a device type has a logical record. For example, PCs have an attribute file named `pc`. Not all device types have attribute files. Only information specific to the named device type resides in this file. Only information common to all network components resides in the device file.

Attribute file characteristics include:

- There is one attribute file for every device type.
- Attribute files have the same name as their device type.
- The `logical.name` field is the unique identifier in the `dbdict` for each of these files.

Attribute File Examples

There are associated attribute files that describe the specific features of each device type. Some of the files are:

- | | |
|--------------|---------------|
| ■ bridge | ■ multiplexer |
| ■ circuit | ■ path |
| ■ controller | ■ peripheral |
| ■ cpu | ■ port |
| ■ fep | ■ switch |
| ■ modem | ■ workstation |

Join Files

When a user accesses component data, ICM creates a `joinfile` for that component by extracting information from both the device and attribute files. The `joinfile` is a virtual (logical) file, residing only in memory and not written to the database. This file contains no records, but does have a `dbdict`. This file joins the fields in the component's device file record with the fields in the component's attribute file.

As a rule, the **joinfile** names have the prefix **device**. The name for this file is a combination of the prefix **device** and its attribute file name (**device<attribute file>**). For example, the virtual joinfile for a PC component would be named **devicepc**. The form to display this joined data is named **device.<attribute>**, for example, **device.pc**.

joinfile features include:

- A joinfile contains no records.
- A joinfile contains a combination of fields from the device file and related attribute file.
- The name for the joinfile is a combination of the device file and its attribute file name (*device<attribute name>*).
- The **logical.name** field is the unique identifier in the dbdict for each of these files.

Remember that joinfiles never populated; they only serve to define the extracted fields from the **device** file and the **attribute** files. Although ServiceCenter displays the field information in record format, it is the virtual joinfile that points to the original data.

When you make changes to the joinfile, ServiceCenter writes the changes to the original data in the device and attribute files.

Example

Figure 7-1 shows how this file system works for a user seeking inventory information about a PC.

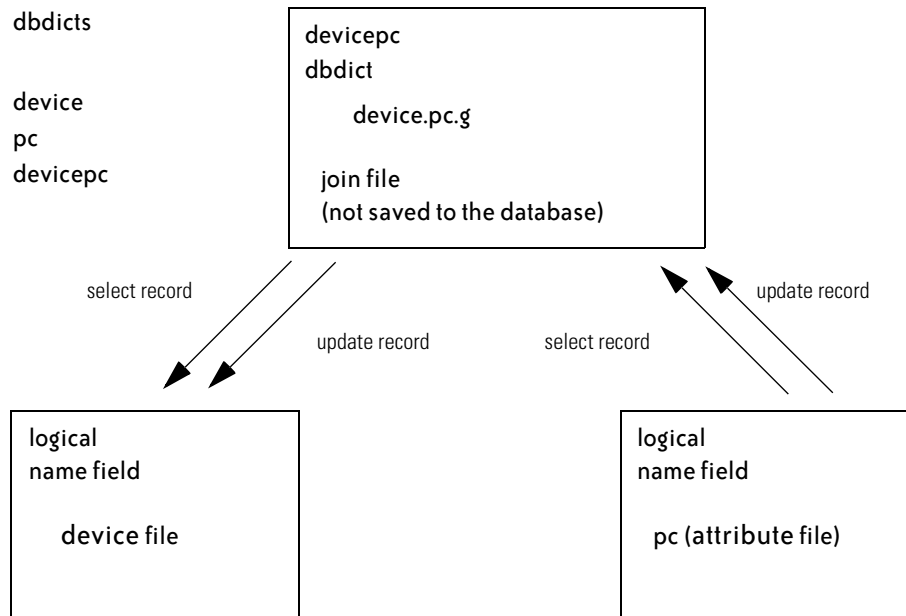


Figure 7-1: ICM Files

Hierarchy

ICM organizes components into an inventory hierarchy, according to their function in the network.

Hierarchy Function

Parent	The next component up the hierarchy from a selected component. A parent component must have an identified child component. For example, a server would be the parent of a PC.
--------	---

Hierarchy	Function
Child	The next component downward in the hierarchy. A child component must have an identified parent component. For example, a local printer would be a child of a PC.
Container	A device that contains other devices. A container can be thought of as a structure of other devices. A container is neither parent nor child, although it can contain one or more parents and/or children. For example, a network segment is the container for the PCs on that segment.

Forms

ICM uses three different types of forms.

- **Device forms** `device` and `device.g` are used for querying on fields common to all device types. For example: a PC record may appear using `device.g`.
- **Attribute forms** (one form for each attribute file) displays detailed attribute data and are the basis for creating each attribute file's Database Dictionary. For example: attribute file name = `circuit`, form name = `circuit`.
- **Join forms** (one form for each joinfile) enables you to simultaneously view, populate, and update fields in both `device` and `attribute` files. Normal functions are available to add, delete, and update the records. Special functions are available to access parents and children. For example: joinfile name = `devicecircuit`, form name = `device.circuit`.

Creating Subtables from an Array of Structures

ServiceCenter enables a dbdict administrator to manage data more effectively by creating subtables of unique and non-unique attributes within an array of structures. You can use this feature to:

- Improve mapping to external SQL database tables.
- Implement a more cost-effective solution for managing attribute information.
- Simplify queries.

The dbdict administrator can identify two subtable names for each array of structures in the dbdict. One table contains the names of unique attributes; the second table names non-unique attributes. A pop-up utility dialog box enables you to identify which attributes are unique.

The subtable feature helps you create queries that can return detailed information. This type of available detail can improve business and management decisions. You can create subtables for an array of structures in any dbdict. ServiceCenter ships with subtables already created for all arrays of structures in the inventory dbdicts.

For more information, see *ServiceCenter System Tailoring, Volume 2*.

Accessing Inventory Management

You can access Inventory Management from the ServiceCenter home menu.

To access Inventory Management:

- 1 From the ServiceCenter home menu, click **Inventory Management**. Figure 7-2 shows the Inventory Management menu.



Figure 7-2: Inventory Management menu

Assets Tab

The Assets tab, shown in Figure 7-2 enables you to manage assets and view and edit software installations and SLM (Service Level Management) information.

Contracts Tab

The Contracts tab enables you to manage the contract queue, terms and conditions, payments, and asset allocations. Figure 7-3 shows the Contracts tab.

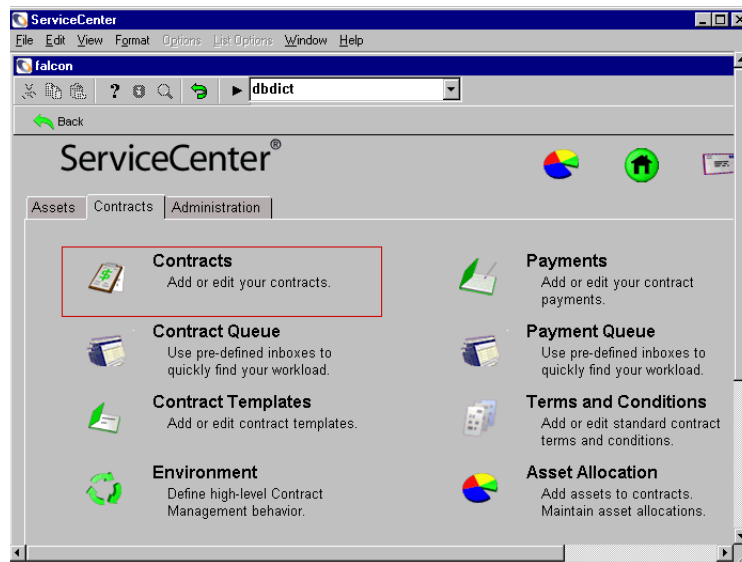


Figure 7-3: Inventory Management menu: Contracts tab

Administration Tab

The Administration tab enables you to add users to administer profiles, device types, and software compliance data. Figure 7-4 shows the Administration tab.

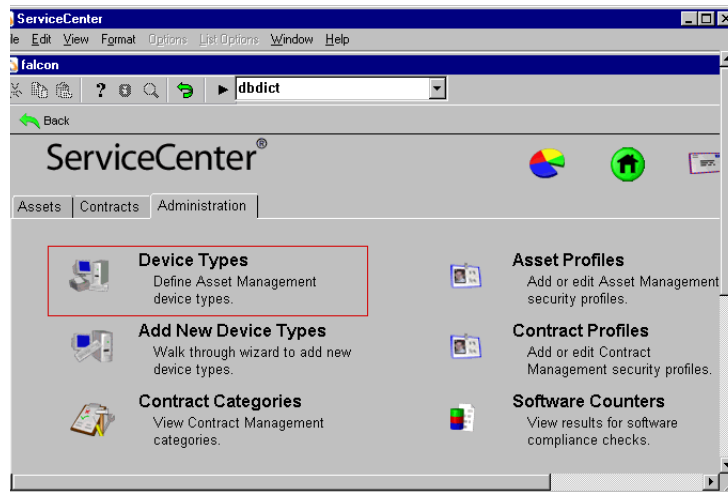


Figure 7-4: Inventory Management menu: Administration tab

Organizing Inventory Records

ServiceCenter uses parent/child relationships to organize inventory records. These relationships depend on how the devices are related in a network.

Networks are based on a hierarchy. This hierarchical structure contains parent-child relationships between devices. For example, Figure 7-5 on page 179 shows a server as the parent of the PC attached to it.

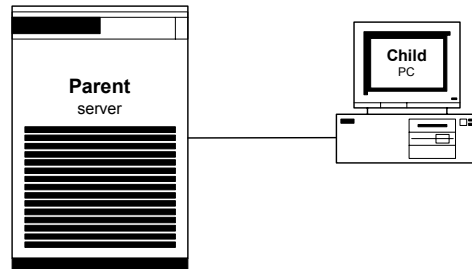


Figure 7-5: Parent device with a child

A parent device can have multiple children. The children do not have to be of the same device type. For example, Figure 7-6 shows a server with different types of PCs attached to it, a Pentium and a Macintosh. The same server has a network printer attached, which is another child with the same parent (the server) as the PCs.

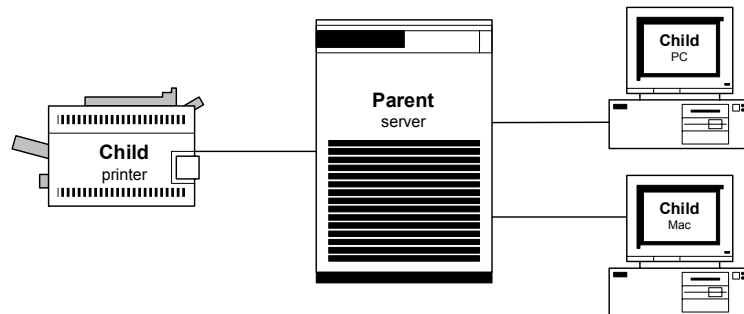


Figure 7-6: Parent device with multiple children

A child device can also have children. The child becomes both a parent and a child. For example, Figure 7-7 on page 180 shows a PC with a local printer directly attached. The PC is a child of the server and the parent of the local printer.

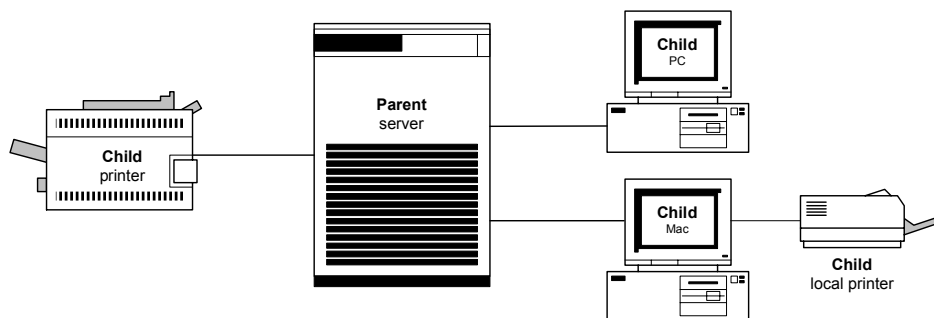


Figure 7-7: Child device with a child

ServiceCenter uses parent/child relationships to structure inventory records. Inventory records contain a field to list the parent device.

The inventory forms have choices in the Options menu to find parents and children for a selected device. For more information, see *Inventory Records* on page 205.

You can also have multiple parents for one device. Figure 7-8 shows how a PC can connect to multiple servers.

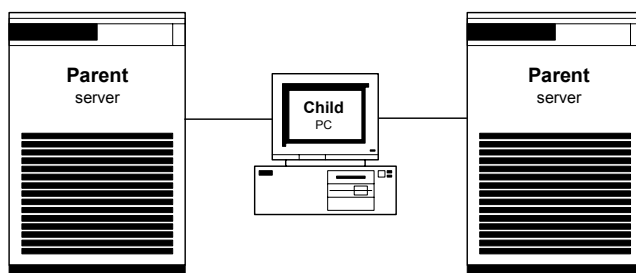


Figure 7-8: Child with multiple parents

Administering Inventory Management

You can access Inventory Management and Configuration Management for administrative purposes from the Service Management section of the ServiceCenter home menu, or from the Central Administration Utilities (CAU).

The CAU enables you to access the operator's record for user and contact information, application profile privileges, and the Mandanten utility. You can control and access several users or group access from within each module or utility.

Inventory Management has sample data to use while learning the product. Before putting ServiceCenter Inventory Management into your production system, you must make modifications to match your system. Use this sample data to test your modifications.

To administer users and security Profiles from the CAU, see the *System Administrator's Guide*.

ICM Environment

Inventory Management has an environment record to defines options that affect functionality of the overall ICM environment for all users. ServiceCenter ships with a default ICM environment record that you can modify for your system.

To access the ICM Environment record:

- 1 From the ServiceCenter home menu, click **Inventory Management** to access the Inventory Management menu.
- 2 From the **Assets** tab, click **Environment**. Figure 7-9 shows the Application Environment record.

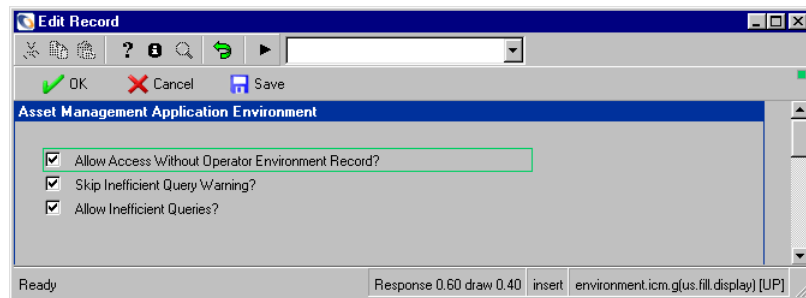


Figure 7-9: Asset Management Application Environment record

- 3 Select the fields that you want to apply to your Inventory Management system. Click **Save** or **OK**, or press F2, to save the changes.

Field	Description
Allow Access Without Operator Environment Record?	Permits users without an individual or Group Profile for ICM to access the module using the DEFAULT profile.
Skip Inefficient Query Warning?	Disables the message warning users that a non-keyed query will be slow. If you check this option, it overrides the setting in the Allow Inefficient Queries? option.
Allow Inefficient Queries?	Enables the user to execute a non-keyed query. if you check Skip Inefficient Query Warning?, it overrides this option.

Profiles

Just as with the other ServiceCenter modules, you can set up user profiles for ICM users. These profiles supplement and further restrict any rights defined in an operator record. There are no default options selected. For more information, see [User Profiles](#) on page 21 and [Adding a New User](#) on page 203.

Adding ICM Capability to the Operator Record

Before you can add an ICM profile, the user must have rights to ICM defined in the ServiceCenter operator record. Three capability words control access to ICM.

Capability Word	Function
SysAdmin	Access to all user and administrative functions in ICM, as well as the rest of ServiceCenter.
ICMAdmin	Access to all user and administrative functions in ICM.
Inventory management	Normal access to ICM user functions, as defined by the ICM profile.

The ICM profile adjusts ICM security access only for users with inventory management capability. SysAdmin and ICMAdmin capabilities both grant complete access to all ICM functionality. Read the following instructions to learn how to modify an operator record of an existing user to provide Inventory Management capability. For a complete list of capability words, see the *ServiceCenter System Administrator's Guide*.

Note: If the user does not have access to the ICM menu from the startup screen, you must add the necessary controls using Forms Designer and update the menu record.

To update an operator record:

- 1 Invoke the CAU using one of the following methods:
 - Type `cau` at the Command Line prompt.
 - From the ServiceCenter home menu, click the **Utilities** tab shown in Figure 7-10.

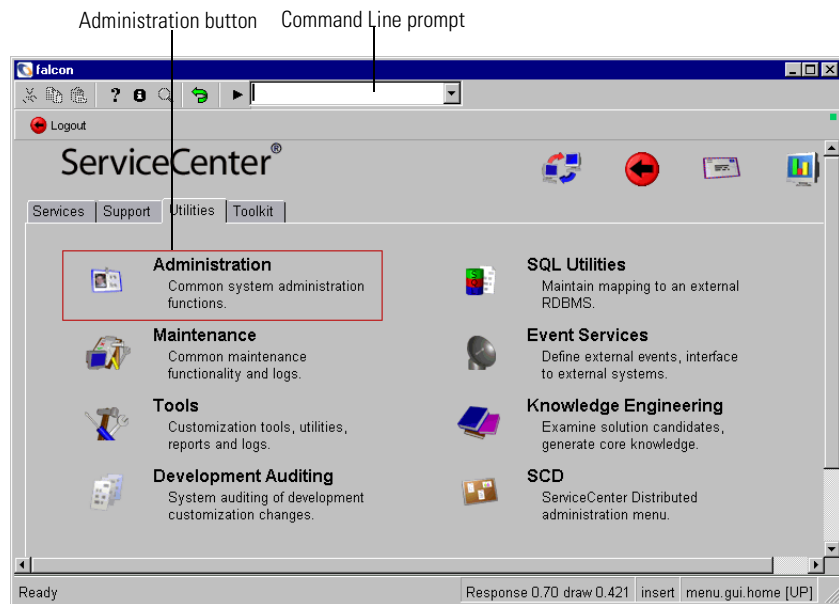


Figure 7-10: ServiceCenter home menu: Utilities tab

- 2 Click **Administration**. Figure 7-11 on page 184 shows the Administration menu.

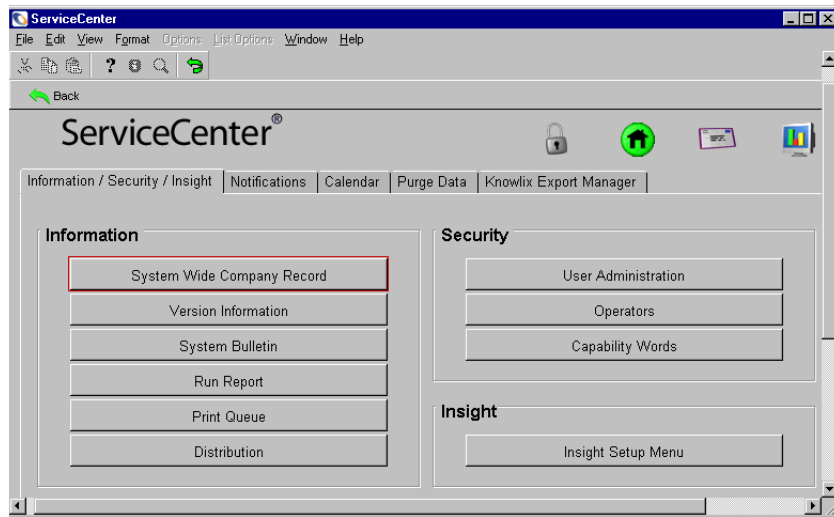


Figure 7-11: Information/Security/Insight tab

- 3 From the **Information/Security/Insight** menu tab, click **User Administration** in the Security area.

The Central Administration Utilities menu shown in Figure 7-12 appears. The tabs in the form shown represent the options available to the system administrator to centrally manage user access and privileges, and conduct searches on contacts and operators.

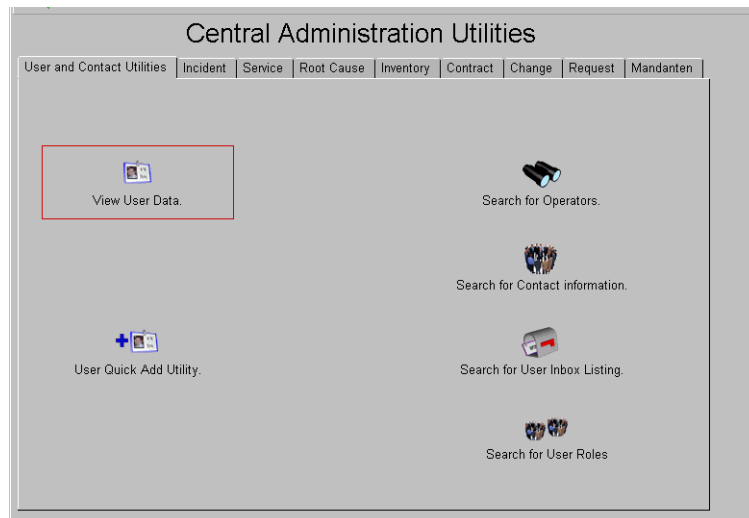


Figure 7-12: Central Administration Utilities home menu

- 4 Click **View User Data**.
- 5 Do one of the following.
 - Select BOB.HELPDESK from the drop-down list.
 - Type the ServiceCenter **Login Name** of the user whose operator record you want to modify. For this example, type BOB.HELPDESK. Remember that the user name is case-sensitive. Click **OK**.

Figure 7-13 shows the operator record for BOB.HELPDESK.

The screenshot shows the 'ServiceCenter' application window with the 'OPERATOR RECORD' dialog box open. The 'General' tab is active. The 'Login Name' is 'BOB.HELPDESK' and the 'Contact Name' is 'HELPDESK, BOB'. There are buttons for 'Edit Op Info' and 'Edit Contact'. An 'Email Addr.' field is present but empty. Under 'Application Profiles', several profiles are listed in dropdown menus: 'User Role' is 'HELPDESK TECH LEVEL 1', 'Service Profile' is 'HELPDESK TECH', 'Incident Profile' is 'HELPDESK TECH', 'Root Cause Profile' is 'TECH', 'Inventory Profile' is 'INITIATOR', 'Contract Profile' is 'DEFAULT', 'Change Profiles' is 'HELPDESK', and 'Request Profiles' is 'REQUESTOR'. Each dropdown has an 'Add New Profile' button next to it.

Figure 7-13: BOB.HELPDESK operator record

- 6 Click **Edit Op Info**.

Important: If the operator record is based on a template, adding the capability to the template will provide ICM capability to the user and all others who share the template.

- 7 Click the **Startup** tab. Figure 7-14 shows the Startup tab information and the list of capabilities.

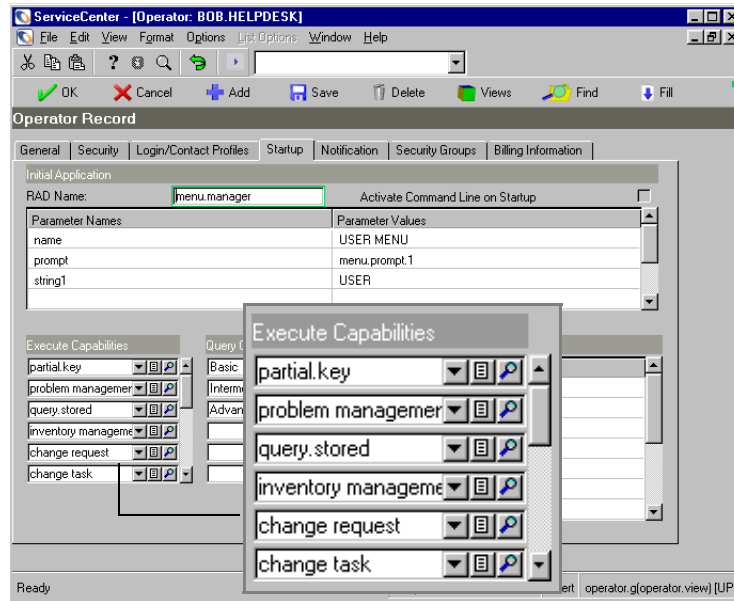


Figure 7-14: Operator Record: Startup tab

- 8 Scroll to a blank cell in the **Execute Capabilities** list.
- 9 Type **ICMAdmin** in the blank cell in the **Execute Capabilities** list. Remember that capability words are case-sensitive.
- 10 Click **Save**. The status bar displays a message that the record was updated. Now you can set the parameters of the user's access.

Adding an ICM Profile

After you modify the operator record to grant ICM rights to a user, you must add an ICM profile for that user.

ServiceCenter ships with a series of profiles, based on User Roles. The **DEFAULT** profile sets the parameters for users who are not defined by any other profile. Users can access ICM using only this profile if you selected the **Allows Access Without an Operator Environment Record** option in the Inventory Management Environment record. For more information, see *ICM Environment* on page 181.

To add and edit ICM profiles:

- 1 From the ServiceCenter home menu, click **Inventory Management** to access the Inventory Management menu.
- 2 From the Administration tab, click **Asset Profiles**. Figure 7-15 shows an inventory security profile form.

Figure 7-15: Inventory Security Profile form

- 3 Do one of the following:
 - Type a **Profile Name** for an existing user.
 - Click **Search** to display a list records. Double-click the record to be viewed or modified.
 - To create an entirely new profile, type a new name in the **Profile Name** field. Click **Add** or press F1. The status bar displays a message that the record is added.
 - To create a profile based on a currently existing profile:
 - Click **Search** to display a list of records.
 - Double-click the record to be copied.

- Type the new name in the **Profile Name** field.
- Click **Add** or press F1. The status bar displays a message that the record is added.

Example

- 1 Select the existing profile **TECH**, as shown in Figure 7-16.

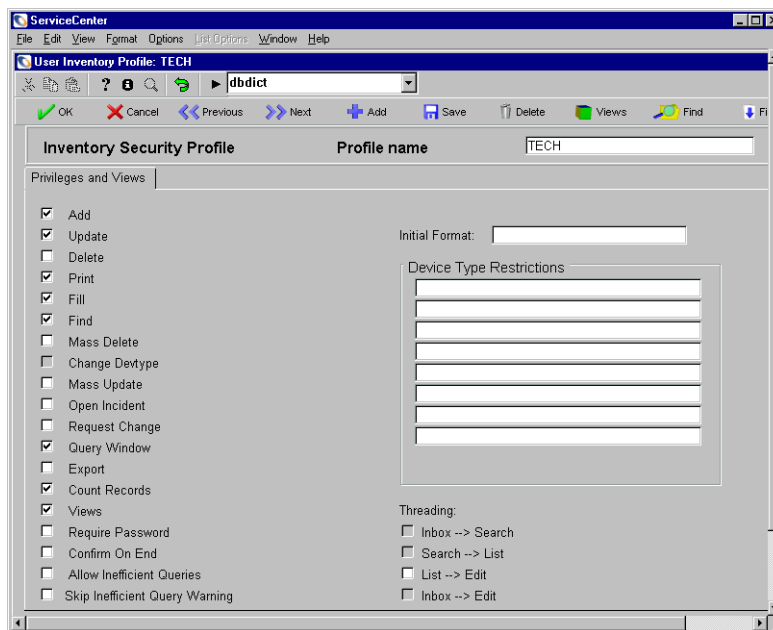


Figure 7-16: ICM Security Profile

- 2 Select the Inventory Management environment rights for the operators using this profile. For a list of options and their definitions, see *Inventory Security Profile options* on page 189.

For this example, select the **Allow Inefficient Queries** option. Leave all other options as they are.

- 3 In the **Initial Format** text box, type the name of the form that appears when the operators using this profile access Inventory Management. If you leave this field blank, the operator record defaults to the Startup menu for the user. To select from a list of existing formats, place your cursor in the **Initial Format** text box and click **Fill** or press F9. For this example, leave the field blank.

- 4 In the **Device Type Restrictions** area, type the device types that the operators using this profile cannot add, delete, or update. If this area is blank, all device types are available to this profile. To select from a list of existing formats, place your cursor in one of the **Device Type Restrictions** text boxes and click **Fill** or press **F9**. For this example, leave these fields blank.
- 5 Select the Threading options that you want to be available for this profile.

Option	Function
Inbox > Search	Displays the inbox in a different window after a search runs from that inbox.
Search > List	Keeps the search form open after a QBE list appears.
List > Edit	Causes a device selected from the search list, to appear in a new window. The user is able to view multiple devices from the same list. If you omit this option, the device appears in the same window as the list.
Inbox > Edit	Displays an inbox after you retrieve a record.

- 6 Click **Save** or press **F4**. The status bar displays a message that the record was updated.
- 7 Click **OK** or press **F2** to return to the blank ICM Profile record.
- 8 Click **Back** to exit ICM profiles.

A user, such as BOB.HELPDESK, can now log on to ServiceCenter with the TECH profile settings and access ICM.

Inventory Security Profile options

The options in this table are available to ServiceCenter System Administrators (SysAdmin capability) and ICM Administrators (ICMAdmin capability) regardless of the parameters are selected in this Profile record.

Field	Definition
Add	Add component records.
Update	Update component records.
Delete	Delete component records.
Print	Enables the print option for the user or group.

Field	Definition
Fill	Enables the Fill function for the user or group.
Find	Enables the Find function for the user or group.
Mass Delete	Select a group of inventory records and delete them.
Change Devtype	Change the device type of an asset.
Mass Update	Select a group of inventory records and modify fields in those records.
Open Incident	Open an incident ticket from within Incident Management.
Request Change	Open a change request in Change Management from within ICM. For more information, see Change Management on page 345.
Query Window	Run structured queries in ICM.
Export	Export component records to an external file.
Count Records	Count the records in a QBE list.
Views	View alternate forms in ICM.

The options in this table are available only when selected.

Field	Definition
Require Password	Require a password to access ICM.
Confirm on End	Display a confirmation form before exiting the primary ICM module.
Allow Inefficient Queries	Execute an incomplete or partially-keyed query. This option is overridden if you select Skip Inefficient Query Warning .
Skip Inefficient Query Warning	Disable the message warning the user that a non-keyed query will be slow. If you choose this option, you will override Allow Inefficient Queries .

Device Types

The **devtype** file contains a record for each type of component you are tracking in ICM. ServiceCenter ships with a series of device type records, which you can modify or delete. You also can add new device type records.

To access a device type record:

- 1 From the ServiceCenter home menu, click **Inventory Management** to access the Inventory Management menu.
- 2 From the Administration tab, click **Device Types**. Figure 7-17 shows the Device Type Definition form.

The screenshot shows a window titled "Search devtype Records". Inside, there's a toolbar with icons for Back, Search, Find, and Fill. Below the toolbar is a section titled "Device Type Definition". This section contains several input fields: "Device Name:", "Device Type:", "Bitmap:", "Format Name:", "Attr File:", "Join Def:", "Print Format Name:", and "Active:". Each field has a corresponding input box. To the right of the "Format Name:", "Attr File:", and "Print Format Name:" fields are small icons for file selection. Below these fields is a section labeled "Sub Types" which contains a list of subtypes. At the bottom of the window, a status bar displays "Ready", "Response 0.50 draw 0.70", and "insert devtype.g(devtype.search) [UP]".

Figure 7-17: Inventory Device Type Definition form

- 3 To search for a specific device type record, do one of the following:
 - Leave the fields blank and press **Enter** to perform a true query and retrieve a list of all current device type records. Select a record from the QBE record list.
 - Type a device type name in the **Device Type Name** field, which retrieves the record from the **devtype** file. Press **Enter**.

For this example, type **Computer** in the **Device Type Name** field and press **Enter**. Figure 7-18 shows the device type record.

Device Name	Device Type	Format Name	Attr File	Join Definition
Application	application	device.Application		
Computer	computer	device.computer	computer	joincomputer
Display Device	displaydevice	device.displaydevice	displaydevice	joindisplaydevice
Example	example	device.example		
Furnishings	furnishings	device.furnishings	furnishings	joinfurnishings

Device Type Definition	
Device Name:	Computer
Device Type:	computer
Bitmap:	ipc
Format Name:	device.computer
Attr File:	computer
Join Def:	joincomputer
Print Format Name:	device.computer
Active:	<input checked="" type="checkbox"/>
Sub Types	<ul style="list-style-type: none"> Desktop Dumb Terminal Laptop Tower MAC

Selected line is row 2 of 12 records

Response 0.60 draw 0.150 insert devtype.qbe.g [UP]

Figure 7-18: Inventory Device Type Definition record

The following table describes the fields in the Device Type Definition form.

Field	Description
Device Name	Descriptive name of the device type.
Device Type	Internal name of the device used by ServiceCenter.
Bitmap	Device bitmap name.
Format Name	Join format displayed for component of this device type.
Attr File	Attribute file associated with this device type.
Join Def	Join Definition record associated with this device type.
Print Format Name	Print format associated with this device type.
Active?	Whether or not this device type is active.
Sub Types:	Names of different types of this device.

Creating a New Device Type

You can use the Create a New Device Type wizard to create a device type, along with the accompanying attribute and join forms. You can create the attribute and join forms separately before you create the new device type.

To create a new device type:

- 1 From the ServiceCenter home menu, click **Inventory Management** to access the Inventory Management menu.
- 2 From the Administration tab, click **Add New Device Types**. Figure 7-17 shows the wizard splash screen. click **Next**.

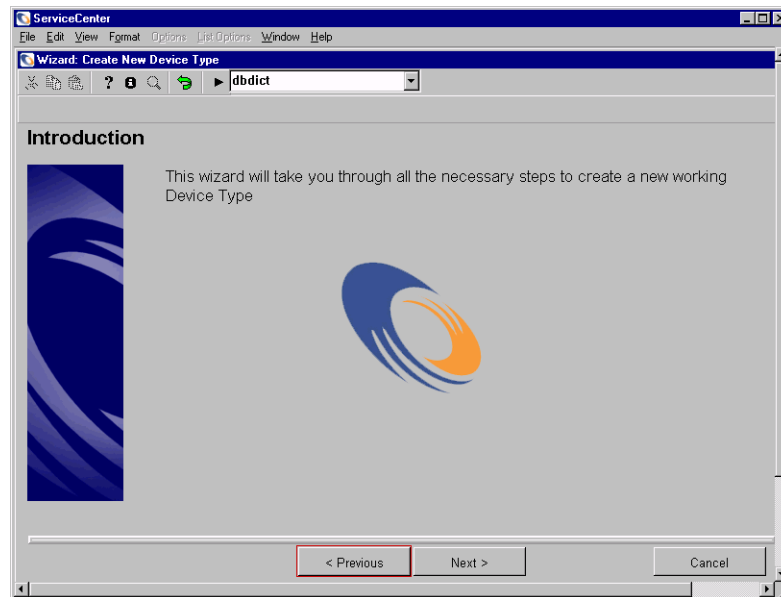


Figure 7-19: Introduction to the Create New Device Type wizard

- 3 Figure 7-20 shows where you can specify the device name. For example, type **UPS** in the Device Type Name field. ServiceCenter displays this name to the user.

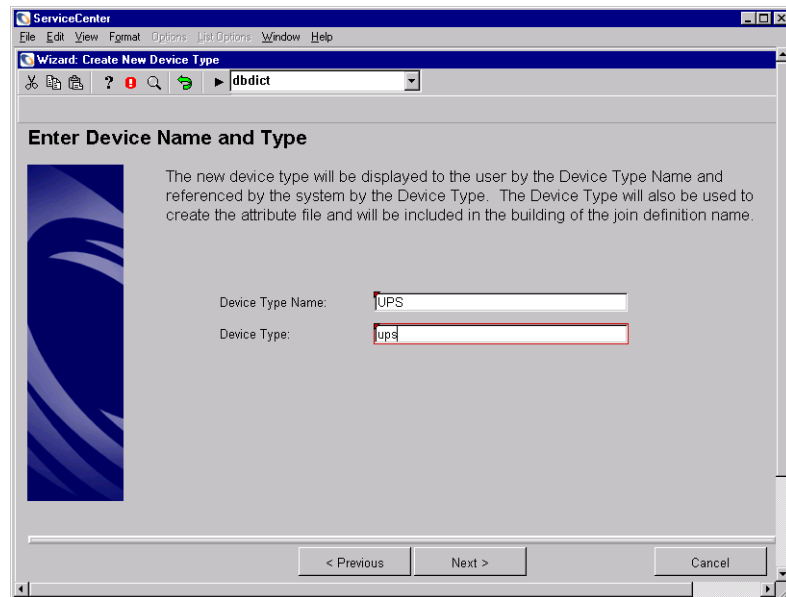


Figure 7-20: Specify the device name and type

- 4 Specify the Device Type name. For example, type **ups** to identify the attribute form to be used with this device type. ServiceCenter uses the device type to create the attribute file and to create the joinfile definition. Click Next.
- 5 Figure 7-21 on page 195 shows the form where you can specify the display and print format names. Do one of the following:
 - To select an existing format, click Fill, and double-click to select the name from the list.
 - To create a new format, type a new format name in the text box. The format name can adhere to any naming convention; however, Peregrine Systems uses: device.xxx.g.

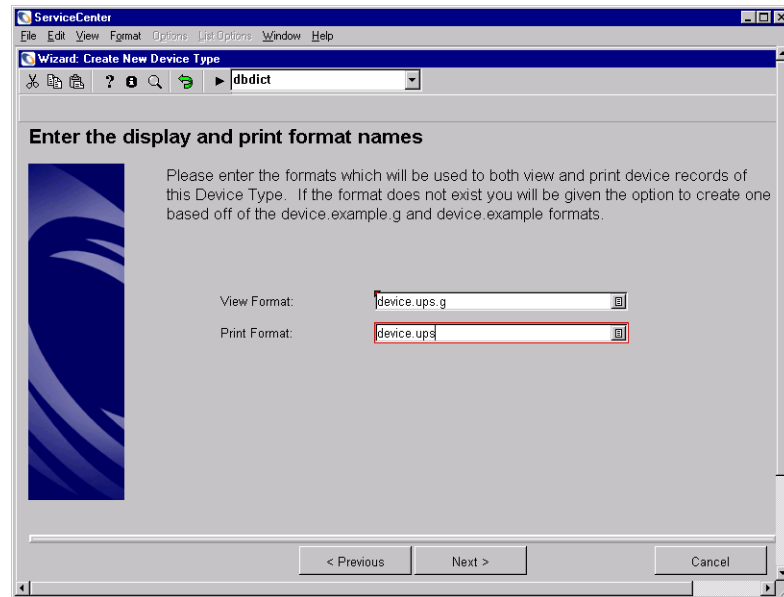


Figure 7-21: New format name

- 6 A message appears to ask if you want to use the `device.template` format as a template for your new format. For each new format name you enter, a corresponding message asks if you want to use the `device.template` format.
 - To use the format, click **Yes**.
 - To specify a different format name, click **Cancel** and type the new name in the New Format text box.
 - If a warning appears, click **OK** to proceed.

Note: If you click **No**, the format name will not be used but not created.

For the example, click **Yes**.

The Modify the formats associated with the new Device Type dialog box shown in Figure 7-22 appears.

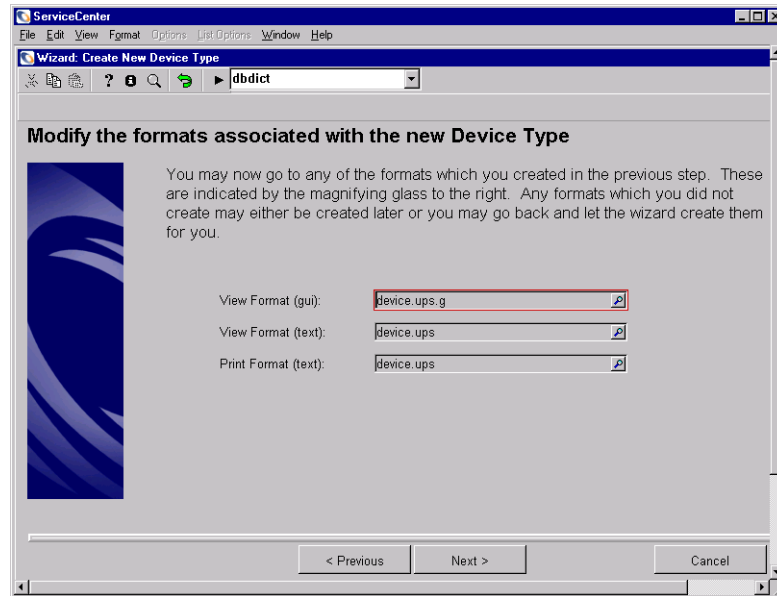


Figure 7-22: Modify the formats associated with the new device type

- 7 You can edit the display and print formats to give each format the appropriate appearance and function. To edit a form:
 - Click **Find** to open the template format with Forms Designer. ServiceCenter retrieves all fields on the template form from the device file. If you add a new field to the format, ServiceCenter also adds it to the attribute file.
 - Click **Design** to display your new format in design mode.
 - Modify the format as needed.
 - Click **OK** to save the changes and exit design mode.
 - Click **OK** to return to the Wizard.
- 8 Repeat step 7 as necessary. When you finish editing the display and print formats for each form, click **Next**.

- 9 Click **Next**. Figure 7-23 shows where you can specify an attribute file name.

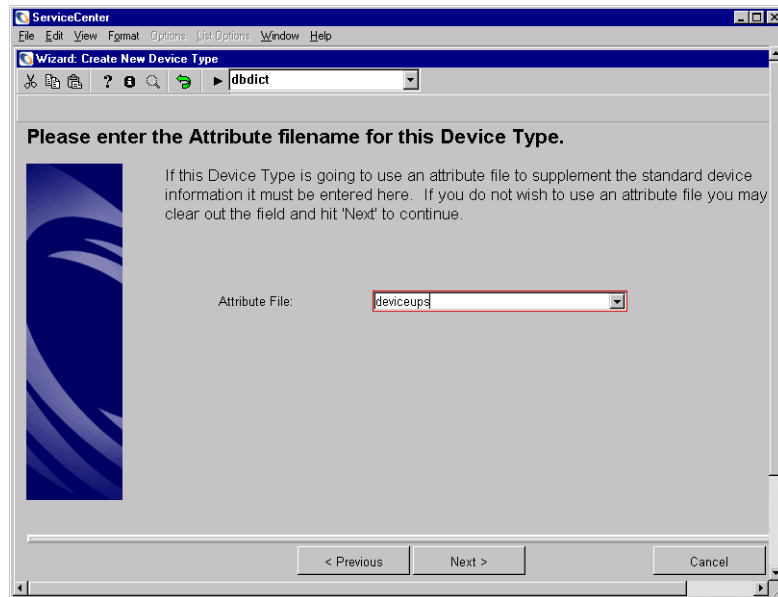


Figure 7-23: Attribute file name

Do one of the following:

- Select an existing file name from the drop-down list. Click **Next**. Skip to step 10 on page 198.
- Type a new name, omitting blank spaces and special characters. For example, **deviceups**. Click **Next**. A message informs you that the device does not exist. If you want to create the device, click **Yes**. Proceed to step 10 on page 198.
- To omit using an attribute file, leave the text box blank and click **Next**.

10 Figure 7-24 shows where you can specify a join definition source.

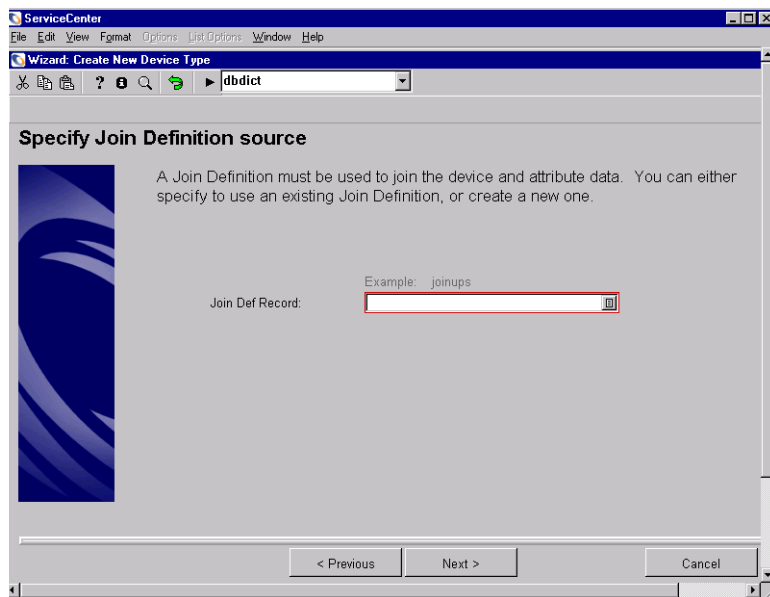


Figure 7-24: Joindef source

Do one of the following:

- Omit a Join Def record name and click **Next**. ServiceCenter suggests a name. To accept that name, click **Yes**.
 - Click **Fill** to view and select a Join Def from a list of available records. Click **Next**.
- 11 Figure 7-25 on page 199 shows where you can specify a list of subtypes to be associated with the new device type. These subtypes can be anything that makes sense for your configuration. Click **Next**.

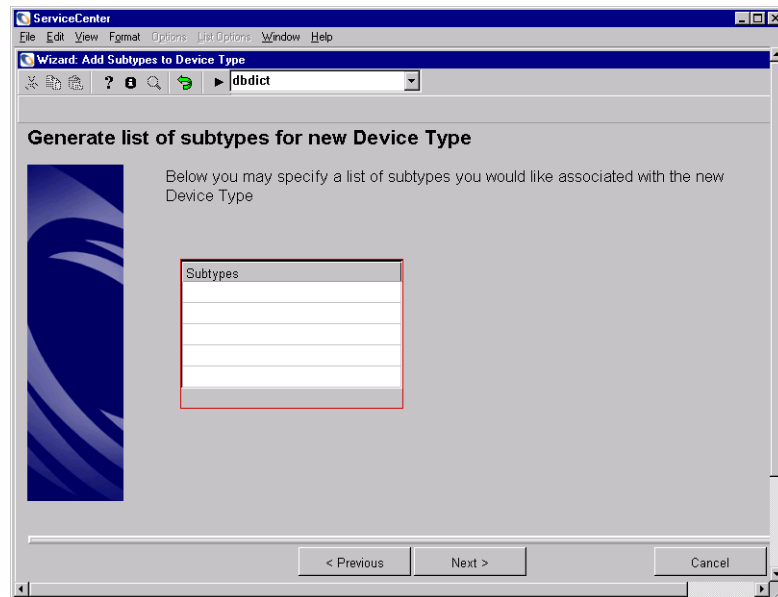


Figure 7-25: List of subtypes

- 12 Figure 7-26 shows where you can activate the new device type. You can choose to omit this step. Click **Next**.

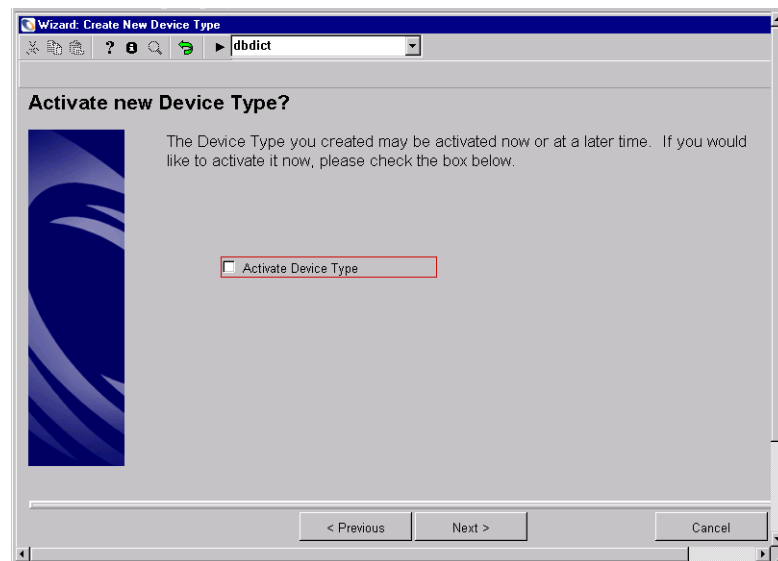



Figure 7-26: Activate the new device type

- 13 A message that the device type was added appears. Click OK to return to the **Administration** tab.
-  14 Click the information button **on** the toolbar to read any messages. ServiceCenter displays information about your new device type. If the icon is blue, there is a required action; if it is red, there is an error message.
- 15 You must log out and log back in for your new device type to be displayed in the drop-down list in the **Type** field of a device record.

Updating a Device Type Record

Follow these steps to update the device type record.

- 1 Complete *step 1 on page 191* through *step 3 on page 191*.
- 2 Edit the fields you need to change.
- 3 Click Save or press F4.

Deleting a Device Type Record

If the device type shares join forms with another device type, copy the shared forms first. Then after deleting the device type, rename the shared forms to their original names.

To delete device type records:

- 1 Click **Inventory Management** in the ServiceCenter home menu.
- 2 Select the Administration tab.

- 3 Click **Device Types**. A blank inventory device type form appears.

The screenshot shows a window titled "Search devtype Records". Inside, there's a toolbar with icons for Back, Search, Find, and Fill. Below the toolbar is a section titled "Device Type Definition". This section contains several input fields: "Device Name:", "Device Type:", "Bitmap:", "Format Name:", "Attr File:", "Join Def:", "Print Format Name:", and "Active:". Each field has a corresponding input box. To the right of the "Format Name:", "Attr File:", "Join Def:", and "Print Format Name:" fields are small icons for file selection. Below these fields is a "Sub Types" list box. At the bottom of the window, a status bar displays "Ready", "Response 0.30 draw 0.70", and "insert devtype.g(devtype.search) [UP]".

Figure 7-27: Device Type Definition form

- 4 Locate the device type you want to delete. You can do one of the following:
 - Leave the fields blank and press **Enter** to perform a *true* query and retrieve a list of all current device type records. Select a record from the QBE record list that is opened.
 - Type a device name in the **Device Type Name** field, which pulls the record from the `devtype` file, and press **Enter**.
- 5 When the record displays, click **Delete** or press **F5**. A message appears to confirm the deletion of the record.
Click **Yes** to delete the record. Click **No** to cancel the action and return to the record.

- 6 Figure 7-28 shows the Confirm Delete Action form.

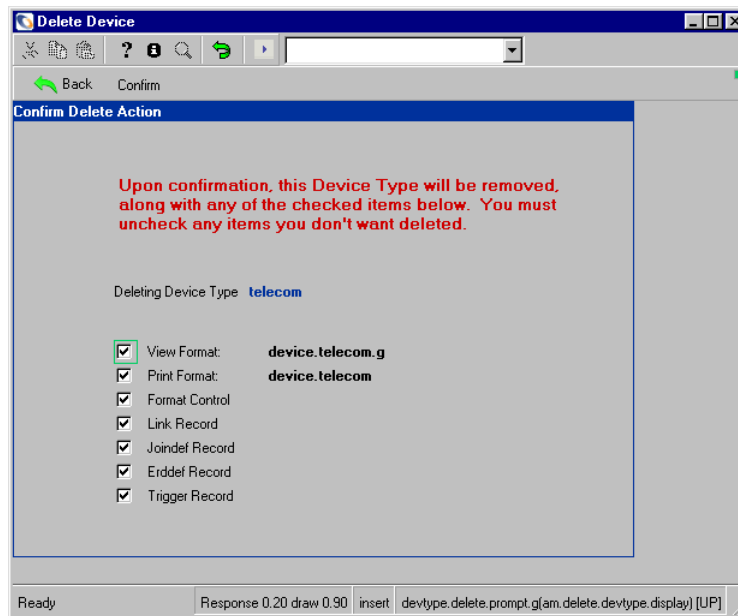


Figure 7-28: Confirm Delete Action form

- 7 Clear any items you don't want deleted.

Note: ServiceCenter selects all items by default. Peregrine Systems recommends that you delete all components related to a particular device type. Be careful when you delete components because some components may be used by other device types. Deleting components used by other device types can prevent you from displaying assets tied to those device types.

- 8 Click **Confirm** or press F1 to delete the record. ServiceCenter returns you to the Device Type Definition form.



- 9 Click **View Messages** in the toolbar to view additional messages and instructions.

Adding a New User

The system creates the following records for the new user:

- Contact record
- Operator record with Inventory Management capabilities
- Inventory Management Profile record.

To add a new user to the system:

- ▶ Type **cau** on any menu command line or navigate through the ServiceCenter menu system:
 - 1 From the ServiceCenter home menu, click the **Utilities** tab.
 - 2 Click **Administration**. The **Administration** menu displays the Information/Security/Insight tab.
 - 3 Click **User Administration** in the Security area. The Central Administration Utilities menu appears. The tabs in the form represent the options available to the system administrator to centrally manage user access and privileges, and to conduct searches on contacts and operators.
 - 4 Click **User Quick Add Utility**. Type the name of the user to be added in the new dialog box. For example, type **JOE.USER** . Click **OK**.
 - 5 A dialog box appears to clone another user. Do one of the following:
 - Click **Yes** to clone another user. Select an existing User from the drop-down list.
 - Click **No** to create a user from scratch.

For this example, click **Yes**. A message asks you to type the name of the user to be cloned. Copy **BOB.HELPDESK**.
 - 6 Click **OK** or press **Enter**. The new operator record appears with the new operator name in the Login Name text box.
 - 7 Modify the operator record as needed.
 - 8 Click **Add** to save the new operator record.
 - 9 A message appears to ask if the user already has a contact record. Click **No**.
 - 10 Type the contact name of the new user.

Figure 7-29 shows the User Contact Information form.

Figure 7-29: User Contact Information template

- 11 Complete the record with all relevant data.
- 12 Click Add.
- 13 Complete any other administrative maintenance on the Operator Record.
- 14 Click Save and return to the Central Administration Utilities menu.

Where to Find More Information

For more information about the following subjects, see the Central Administration Utilities section in the *System Administrator's Guide*.

- creating, using, or updating operator records
- administration tasks
- ICM profiles

For more information about Forms Designer, see *System Tailoring, Volume 1*.

Inventory Records

The device file is a central repository for asset information and is referenced throughout ServiceCenter. Navigational buttons in the device form or device attribute join form allow you to access incident tickets, change records, and Request quotes for a particular asset. Each inventory record in ICM contains information about a particular device. Tabs and field data vary, depending on the asset selected.

To access an asset record:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click **Assets**.
- 3 Do one of the following to display an asset record:
 - Click **Search** to perform a true query and retrieve a list of all current device type records. From the generated list, double-click the Name in the record.
 - Specify data to narrow your search. For example, type the name of an asset in the **Asset** field or select a device type from the **Type** field. Click **Fill** to display a list for the named field.
- 4 Click **Search** or press **Enter**.

Figure 7-30 shows the list and the asset form.

Logical Name	Type	Network	Location	Model	Status
ACME Phone 0001	telecom	AT&T	ACME HQ		Warehouse
ACME Phone 0002	telecom	AT&T	ASIA HQ		Installed
ACME Phone 0003	telecom	AT&T	ACME HQ		Installed
ACME Phone 0004	telecom	AT&T	ACME HQ		Installed

Telecommunications	
System Summary Contact Location Vendor Relationships Financial Outage History Attachments	
Ownership	
Asset ID:	ACME Phone 0002
Subtype:	Desk Phone
Asset Tag:	
Network Name:	AT&T
Domain:	
Assignment:	
Serial Number:	
Part Number:	
Manufacturer:	
Model:	
Status:	Installed
Company:	ACME
Department:	
Cost Center:	
Service Contract:	
Incident Category:	lbd
Priority:	
Asset Pending Change?	<input type="checkbox"/>
Critical Asset?	<input type="checkbox"/>
System Down?	<input checked="" type="checkbox"/>

Selected line is row 2 of 32 records retrieved Response 0.061 draw 0.561 insert device.qbe.g [UP]

Figure 7-30: Asset record

Some fields in other ServiceCenter modules, such as Incident Management, are filled in with values specified in inventory records. For example, the inventory record Device Type field populates the Type field in an incident ticket. This provides consistency throughout the system.

You can also use the fields to create records for new devices. For more information, see [Creating a New Device Type](#) on page 193. The Options menu and system tray buttons are consistent throughout the various inventory device forms.

Where to Find More Information

For more information about options menus and fields, creating and updating an asset record, see the *ServiceCenter User's Guide*.

8 Inventory Management Service Information

CHAPTER

Service Information provides service level agreement data about devices in the inventory database. A Service Level Agreement (SLA) tracks device availability and response time guarantees for devices in the ICM database. For more information, see *Service Level Management* on page 259.

Read this chapter for information about:

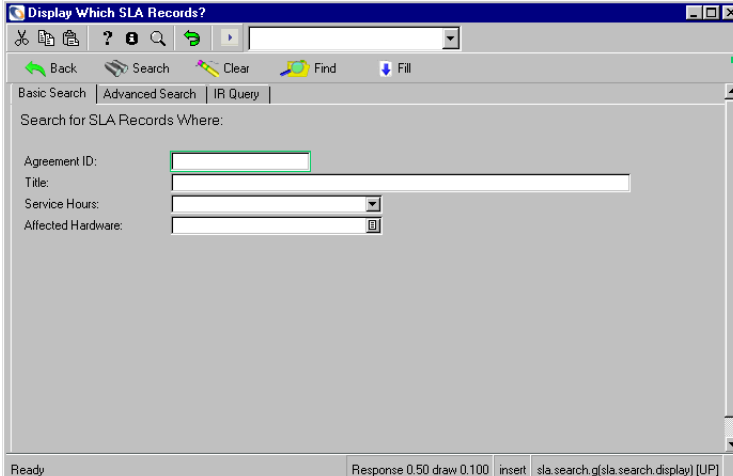
- *Accessing Service Level Agreements* on page 208
- *Contract Management Environment Records* on page 209
- *Adding a Contract Management Profile* on page 210
- *Alerts* on page 215
- *Contract Status* on page 215
- *Currency Conversion Utility* on page 215
- *Software Tracking and Compliance* on page 221
- *License and Installation Models in the Catalog* on page 222
- *Software Tracking and Compliance Example* on page 238

Accessing Service Level Agreements

You can access the Service Level Management (SLM) feature directly from the ICM menu.

To view Service Level Agreements:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click **SLA Information**. Figure 8-1 shows the SLA Search form.



The screenshot shows a web application window titled "Display Which SLA Records?". The window has a standard toolbar with icons for Cut, Copy, Paste, Help, Find, and Print. Below the toolbar is a navigation bar with tabs for "Basic Search", "Advanced Search", and "IR Query". The "Basic Search" tab is selected. The main area is titled "Search for SLA Records Where:" and contains four input fields: "Agreement ID:" (a text box), "Title:" (a text box), "Service Hours:" (a dropdown menu), and "Affected Hardware:" (a text box with a small icon to its right). The status bar at the bottom of the window displays "Ready", "Response 0.50 draw 0.100", and "insert sla.search.g(sla.search.display) [UP]".

Figure 8-1: SLA Search form

- 3 To view an SLA, do one of the following:
 - If you have any information about the SLA, type it into the appropriate fields and click **Search** or press **Enter**. A record list appears with all matching records. Double-click the record that you want to view.
 - Click **Search** to perform a true query and retrieve a list of all current SLM records. Double-click the record that you want to view.

Figure 8-2 shows an SLA record.

The screenshot shows the 'Edit SLA Record' window. At the top is a toolbar with icons for OK, Cancel, Previous, Next, Save, Add, Delete, Find, and Fill. Below the toolbar is a table with three columns: Agreement ID, Expiration, and Title. The table contains two rows: one for '155' with expiration '12/31/08 00:00:00' and title 'ACME Bronze', and another for '156' with expiration '12/31/08 00:00:00' and title 'ACME Gold'. A status bar at the bottom right of the table indicates '2/16'. Below the table is a detailed view of the selected record (Agreement ID: 156). It includes fields for Agreement ID, Expiration, Title, Service Hours, Target, and Dept Full Name. The 'Description' tab is selected, showing 'ACME Gold Service Level Agreement'. The status bar at the bottom of the window reads 'Ready' and 'Response 0.110 draw 0.170 insert sla.qbe.g [UP]'.

Agreement ID	Expiration	Title
155	12/31/08 00:00:00	ACME Bronze
156	12/31/08 00:00:00	ACME Gold

2/16

Agreement ID: 156 Expiration: 12/31/08 00:00:00

Title: ACME Gold

Service Hours: Target: 99

Dept Full Name:

Description Availability Response Times Misc. Attachments

ACME Gold Service Level Agreement

Ready Response 0.110 draw 0.170 insert sla.qbe.g [UP]

Figure 8-2: SLA Record with a record list

Contract Management Environment Records

Contract Management contains an environment record with options that affect functionality of the overall Contract Management environment for all users. ServiceCenter ships with a default Contract Management environment record that you can modify for your system.

To access the Contract Management Environment record:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click the **Contracts** tab.
- 3 Click **Environment**. For more information, see *ICM Environment* on page 181.

Contract Management Permission

Before a user can add a contract profile, the user must have Inventory Management rights defined in their ServiceCenter operator record. Three capability words control access to Inventory Management:

Capability Word	Function
SysAdmin	Access to all user and administrative functions in Inventory Management, as well as the rest of ServiceCenter.
ICMAdmin	Access to all user and administrative functions in Inventory Management.
inventory management	Normal access to Inventory Management user functions, as defined by the Inventory Management profile.

Note: The Inventory Management profile adjusts Inventory Management security access only for users with Inventory Management capability. SysAdmin and ICMAdmin capabilities both grant complete access to all ICM functionality.

For a complete list of capability words, see the *ServiceCenter System Administrator's Guide*.

Adding a Contract Management Profile

After you modify the operator record to give a user Contract Management rights, you must add a Contract Management profile for that user. ServiceCenter ships with a series of profiles, based on User Roles. The DEFAULT profile sets the parameters for users who are not defined by any other profile. Users can access Contract Management using this profile only if you select the **Allows Access Without an Operator Environment Record** option in the Inventory Management Environment record. For more information, see *ICM Environment* on page 181.

To add and edit ICM profiles:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click the **Administration** tab.
- 3 Click **Contract Profiles**.

Figure 8-3 shows a Contracts Security Profile form.

The screenshot shows a web application window titled "Search ctenv Records". Below the title bar is a toolbar with icons for Back, Add, and Search. The main content area is titled "Contracts Security Profile" and contains a "Profile Name:" text input field. Below this are several sections, each with a list of permissions represented by checkboxes:

- Threading**
 - ☐ Inbox -> Search
 - ☐ Search -> List
 - ☐ List -> Edit
 - ☐ Inbox -> Edit
- Contracts**
 - ☐ Add Contract
 - ☐ Update Contract
 - ☐ Cancel Contract
 - ☐ Renew Contract
- Contract Templates**
 - ☐ Create Template
 - ☐ Select Template
 - ☐ Update Template
 - ☐ Delete Template
- Software Counters**
 - ☐ Create Counter
 - ☐ Update Counter
 - ☐ Delete Counter
 - ☐ Compliance Check
- Payments**
 - ☐ Schedule Payment
 - ☐ Gen Payment Sched
 - ☐ Update Payment
 - ☐ Submit Payment
 - ☐ Cancel Payment
- Asset Allocation**
 - ☐ Add Asset
 - ☐ Gen Asset Allocation
 - ☐ Update Asset
 - ☐ Delete Asset
- Terms and Conditions**
 - ☐ Add Term/Condition
 - ☐ Update Term/Condition
 - ☐ Delete Term/Condition
- General Privileges**
 - ☐ Require Password
 - ☐ Confirm On End
 - ☐ Allow Inefficient Queries
 - ☐ Skip Inefficient Query Warning
 - ☐ Print
 - ☐ Fill
 - ☐ Find
 - ☐ Query Window
 - ☐ Export
 - ☐ Count Records
 - ☐ Mass Add
 - ☐ Mass Update
 - ☐ Mass Delete

The status bar at the bottom shows "Ready" and "Response 0.150 draw 0.141 insert ct.profile(db.search) [UP]"

Figure 8-3: Contracts Security Profile form

- 4 Do one of the following:
 - In the **Profile Name** field, type the profile name for the operator for whom you are building this profile.
 - If you are modifying an existing profile, click **Search** to perform a true query and find that profile. Double-click the record that you want to view and modify.
- 5 Threading allows the previous window to remain when you request a new record. For example, when you select a record from a QBE list, the QBE list remains after the record appears in a new window. Choose the Threading options that you want available for this profile.

Option	Function
Inbox > Search	Displays the inbox in a different window after running a search from that inbox.
Search > List	Deeps the search form open after displaying a QBE list.

List > Edit	Causes a device selected from the search list to appear in a new window. Therefore, you can access multiple devices from the same list. If you do not select this check box, the device information appears in the same window.
Inbox > Edit	Displays the inbox after you access the record.

6 Select the Contracts rights for the user.

Field	Function
Add Contract	Add contracts.
Update Contract	Edit an existing contract.
Cancel Contract	Cancel a contract (as long as it is in draft mode.)
Renew Contract	with renew contract capability, the Renewal Info tab appears on a contract form.

7 Select the Contract Templates rights for the user.

Field	Function
Create Template	Create a contract template.
Select Template	Select a template when creating a contract. The Wizard has only the contract type drop-down list.
Update Template	Access and make changes to a contract template.
Delete Template	Delete a contract template.

8 Select the Software Counters rights for the user.

Field	Function
Create Counter	Create a software counter.
Update Counter	Access and make changes to a software counter.
Delete Counter	Delete a software counter.
Compliance Check	Control the appearance of the Compliance Check and Create Schedule Record buttons on the Software Counter Information form.

9 Select the Payments rights for the user.

Field	Function
Schedule Payment	Control the appearance of the Schedule a Single Payment button on the Contract Information form. Also control the appearance of the Payments button on the Contracts tab.
Gen Payment Sched	Control appearance of the button on the contract on the Payment Information subtab of the Financial tab on the Contract Information form.
Update Payment	Access and make changes to a payment record.
Submit Payment	Control the appearance of the button on the Payment Information subtab on the Contract form. The contract must be in pending mode for this button to appear.
Cancel Payment	Control appearance of button on the Payment Information subtab on the Contract form. The contract must also be in pending mode for this button to appear.

10 Select the Asset Allocation rights for the user.

Field	Function
Add Asset	Add assets to a contract.
Gen Asset Allocation	Generate an allocation percentage spread against any assets that are attached to a contract.
Update Asset	Access and make changes to asset allocations on a contract.
Delete Asset	Delete assets from a contract.

11 Select the Terms and Conditions rights for the user.

Field	Function
Add Term/Condition	Add contract terms and conditions.
Update Term/Condition	Access and make changes to contract terms and conditions.
Delete Term/Condition	Delete terms and conditions.

12 Select the General Privileges for the user.

Field	Function
Require Password	Require a password to access ICM.
Confirm on End	Display a confirmation form before exiting the primary ICM module.
Allow Inefficient Queries	Execute an incomplete or partially-keyed query. This option is overridden when you select Skip Inefficient Query Warning.
Skip Inefficient Query Warning	Disable the message warning the user that a non-keyed query will be slow. Overrides the Allow Inefficient Queries setting.
Print	Enable the print option for the user or group.
Fill	Enable the Fill function for the user or group.
Find	Enable the Find function for the user or group.
Query Window	Run structured queries in ICM.
Export	Export component records to an external file.
Count Records	Count the records in a QBE list.
Mass Add	Select a group of inventory records and add them to the database.
Mass Update	Select a group of inventory records and modify fields in those records.
Mass Delete	Select a group of inventory records and delete them.



13 If you added a new profile, click **Add** or press **F1**. The status bar displays a message that the record is added.

14 Click **OK** or press **F2** to return to a blank ICM Profile record. If you modified an existing profile, click **Save** or press **F4**. The status bar displays a message that the record was updated.

Alerts

ServiceCenter comes with the following alerts out of the box:

- Contract expiration 30 days
- Contract renewal pending

Administrators can create additional alerts as needed. For more information, see the *System Tailoring* guide.

Contract Status

There is a schedule record named **Contract Status** and a background scheduler named **contract**. ServiceCenter uses the background scheduler and the information in the schedule record to check for start date, expiration date, and status to determine if updates are required.

For more information, see these guides:

- *ServiceCenter User's Guide*
- *ServiceCenter Client/Server Installation Guide for Windows*
- *ServiceCenter Request Management Guide*
- *ServiceCenter System Tailoring*
- *ServiceCenter Work Management*

Currency Conversion Utility

Contract Management has a currency conversion utility that automatically converts national currencies, depending on exchange rates at the time the contract is granted. You can enter daily exchange rates into the system to ensure accurate rate conversions. Contract Management manages all currencies in compliance with European Union currency regulations, and ships with the fixed inter-European exchange rates pre-loaded into the system.

To set daily exchange rates:

- 1 From the ServiceCenter home menu, click the **Support** tab.
- 2 Click **Conversion Rates**. Figure 8-4 shows a blank Conversion Rate Information form.

The screenshot shows a web browser window titled "ServiceCenter - [Search Currency Conversion Records]". The browser's address bar is empty, and the menu bar includes File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu bar is a toolbar with icons for Back, Add, Search, Find, and Fill. The main content area is titled "Conversion Rate Information" and contains the following fields:

- Root Currency Code:
- Date:
- Exchange Rate:
- Currency Code:

Below these fields is a section titled "1 Root Currency will buy rate other currency e.g." which contains the same four fields:

- Root Currency Code:
- Exchange Rate:
- Currency Code:

The status bar at the bottom of the browser window displays "Ready" on the left and "Response 0.230 draw 0.121 insert curconvert.gl(db.search) [UP]" on the right.

Figure 8-4: Blank Conversion Rates form

You can also access the Conversion Rate Information form by clicking **Service Level Mgmt.** on the ServiceCenter home menu and then clicking **Conversion Rates**.

- 3 Click **Search** or press **Enter** to perform a true query to retrieve a list of all current conversion records. Figure 8-5 shows a list of conversion rates.

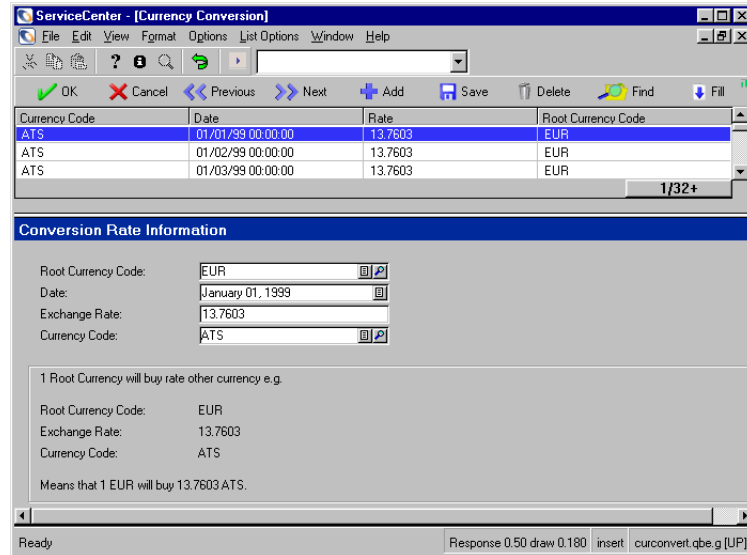


Figure 8-5: Conversion Rates QBE list

- 4 Choose a currency from the record list to update.
- 5 Click **Save**. The following table describes Currency Conversion record fields

Field	Description
Root Cur Code	The family of currencies on which you want to base all your contracts.
Date	Date of the exchange rate shown in the Rate field.
Rate	Rate of exchange between the currencies entered in the record as of the date in the Date field.
Currency Code	System codes for the specific currencies used in contracts.

Currency Definitions

Currency definition records define currency codes for each of the international currencies entered in the system and establish whether or not an individual currency has European Union Currency (EUR) as its root.

To view a currency definition record:

- 1 From the ServiceCenter home menu, click the **Support** tab.
- 2 Click **Currencies**. Figure 8-6 shows a blank Currency Information form.

Figure 8-6: Currency Information search form

You can also access the Currency Information form by clicking **Service Level Mgmt.** on the ServiceCenter home menu and then clicking **Currency Definitions**.

- 3 Do one of the following:
 - Type the name of a currency or other search criteria and click **Search** or press **Enter**.
 - Click **Search** to perform a true query and retrieve a list of all currency definition records.

- 4 The requested record or a QBE list of records appears. Double-click the record that you want to view or modify. Figure 8-7 shows a Currency Definition record.

The screenshot shows a window titled "ServiceCenter - [currency: Andorran Franc]". It has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with buttons for OK, Cancel, Previous, Next, Add, Save, and Delete. Below the toolbar is a table with columns "Currency Cdc", "Name", and "Symbol". The table contains four rows: ADF (Andorran Franc), ADP (Andorran Peseta), AED (United Arab Emirates Dirh), and AFA (Afghanistan Afghani). The "ADF" row is selected. Below the table is a section titled "Currency Information" with fields for Name (Andorran Franc), ISO 4217 Code (ADF), Active? (checkbox), EU Currency? (checkbox), and Notes (text area). To the right of these fields is a "Format" section with fields for Symbol (ADF), Prefix or Suffix (SYM XXX), Decimal Symbol, Digits After Decimal (2), and Grouping Separator. At the bottom of the window, a status bar shows "Selected line is row 1 of 32 records retrieved" and "Response 0.110 draw 0.80 insert currency.qbe.g [UP]".

Figure 8-7: Currency Definition record

- 5 Add, edit, or delete currency definitions in this form. The following table describes Currency Definition record fields.

Field	Description
Name	Common name of the currency (for example, German Mark).
ISO 4217 Code	International Standard Organization for currency codes
Active?	If a currency is selected as active in the currency definition record, the currency appears in the Currency field drop-down list wherever the Currency field displays.
EU Currency?	The selection of this check box identifies the currency as belonging to the European Union.
Notes	Users may enter any comments they want in this field.
Symbol	The international symbol for the currency (for example, \$ for US Dollars).
Prefix or Suffix	Display format of a currency shows the position of the symbol in relation to the number (for example, \$1, 1 DM)
Decimal Symbol	Symbol used in the currency to indicate decimal placement.

Field	Description
Digits After Decimal	The number of placeholders allowed after a decimal.
Grouping Separator	The group of large number. In USD, there is a comma (,) in a four-digit number (1,000). Other currencies may not use a grouping separator.

Calculating Payments

The Assets tab displays a line for each contract asset. Expense line amounts are based on the weighted allocations that are assigned to the assets. When you record payments, there is an internal application that adds the weighted amount allocation, compares the result to the total, and calculates the first payment. Figure 8-8 shows the Assets tab.

General	Lease Info	Lessor/Contact	Assets	Financial	Terms	Renewal Info	Notes	Attachments
Add Assets			Generate %					
Asset	ID	% Cost Allocation	Status					
device	TRAIN pc 100	33.3						
device	TRAIN pc 104	33.3						
device	TRAIN pc 105	33.3						

Figure 8-8: Assets tab

Example

If you make a payment of \$127.50(USD) for the three assets, there is an expense line created for each asset. Each expense line is allocated approximately one-third of the payment.

First asset	42.59
Second asset	42.46
Third asset	42.46
Total	127.51

When ServiceCenter adds the allocated amounts, the total is 127.51, which is one cent over the total payment amount.

ServiceCenter adjusts the first allocation amount to ensure the total allocated amount equals the actual payment amount. The final expense line amounts are as follows:

First asset	42.58
Second asset	42.46
Third asset	42.46
Total	127.50

For more information, see [Expense Lines](#) on page 329.

Software Tracking and Compliance

ServiceCenter includes functionality that empowers you to manage the software used in your organization. You can:

- Set up software inventories.
- Verify that the number of actual software installations is within the number of installations allowed by your licenses.
- Link each software license to a specified contract.
- Manage software suites.

Managing software includes managing the application, license, installations, and contracts. The following tables work together to manage software in an organization.

Table	Function
model	Track different software models, including software license and software installation models.
device	Track data about each application and software license.
contractsoftware	Document any financial and procurement information for licensing agreements. You can also attach multiple licenses to a software contract.
contractitem	Track the associations between contracts and assets.
pcsoftware	Track software installations.
softwarecounter	Verify that the number of software installations you actually have conforms with the number of installations allowed by your licenses.

License and Installation Models in the Catalog

Models are the different categories of assets contained in the catalog. To effectively track software licenses, there must be two types of models in the catalog:

- Software license model
- Software installation model

The Software Tab

The Software tab displays information for software licensing and installation. Use this tab only if the data in the LI Category field on the Catalog tab references a software license or software installation.

Field	Description
Application Name	Name of the software application you're licensing or installing.
Single-User	License that allows software to be installed on a single workstation to be used by a single user.

Field	Description
Multi-User	License that allows software to be installed on multiple workstations to be used by multiple users.
Per named workstation	A multi-user licensing type that allows multiple software installations across multiple workstations. This field only displays if the Multi-User option is selected.
Total No. of Installs	The maximum number of times you can install the software. This field only display if the multi-user licensing type, Per named workstation, is selected.
Per named user	A multi-user licensing type that allows a specified number of individuals to have access to the software. This field only displays if the Multi-User option is selected.
Total Number of Named Users	The maximum number of people who can be named to have access to the software.
Per concurrent accesses	A multi-user licensing type that allows a specific number of individuals to have access to the software at the same time. This field only displays if the Multi-User option is selected.
Concurrent Accesses	The number of people who can access the software at the same time.
Evaluation Rights	The maximum number of installations allowed for demonstration or evaluation purposes.
Number of Points	For certain types of licenses, the number of points each license right consumes.
Version	The current version of the software application.
Authorized	Whether the software application has been authorized for use.

To add a software license model to the catalog:

- 1 From the ServiceCenter home menu, click the **Support** tab.
- 2 Click **Models**. The Model Information form appears.

- 3 On the General tab of the Model Information form, supply any necessary information, which may include:

Option	Function
Part No.	Unique identifier for each model in the catalog.
Brief Description	A short statement describing the incident that is automatically entered in the incident ticket when you select this cause code.
Manufacturer	Name of the manufacturer. Data in this field is read-only since it displays based on the Part Number you enter.
Model	Manufacturer's model number for the asset. Data in this field is read-only because it depends on the Part Number.
Cost	Purchase amount of the model.
Currency	Currency on which the cost is based.

Your organization may require that you complete additional fields. Figure 8-9 shows the General tab on the Model Information form.

The screenshot shows the 'ServiceCenter - model: 530' window. The 'Model Information' form is open, with the 'General' tab selected. The form contains the following fields and values:

- Part No.: 530
- Brief Description: Norton Antivirus 7.5
- Manufacturer: Symantec
- Model: Norton Antivirus 7.5
- Model Ext.: (empty)
- Serialized: ☐
- Cost: 50.00
- Currency: USD
- GL Number: (empty)
- Default Priority: (empty)
- Default Quantity: 1
- Config. File: (empty)

The 'Detailed Description' section contains the text 'Purchase Norton Antivirus 7.5'. The 'Instructions' section is empty. The status bar at the bottom indicates 'Ready' and 'Response 0.201 draw 0.290 insert model.g(db.view) [UP]'.

Figure 8-9: Model Information form: General tab

- 4 Click the Catalog tab.

- 5 On the **Catalog Information** subtab, type the line item category name, such as **Software License**, in the **LI Category** field. For more information, see the *ServiceCenter Request Management Guide*.

Figure 8-10 shows the Catalog Information subtab.

The screenshot shows the 'ServiceCenter - model: 530' application window. The 'Model Information' form is open, and the 'Catalog Information' subtab is selected. The form includes fields for 'LI Category' (set to 'Software License') and 'Assigned Dept'. Below these are two tables: 'Components' and 'Dependencies'. The 'Components' table has columns for Group, Part Number, Description, Quantity, Category, and Option Type. The 'Dependencies' table has columns for Group Name, Dependent On, and Dependency Type. The status bar at the bottom indicates 'Ready' and 'Response 0.201 draw 0.290 insert model.g(db.view) [UP]'.

Figure 8-10: Model Information form: Catalog Information subtab (Catalog tab)

- 6 Click the **Software** tab and type the following data:
 - Application Name
 - License Information
 - Multi-User License Type
 - Total Number of Installs
 - Evaluation Rights
- 7 Click **Add** or press **F2**.

To add a software installation model to the catalog:

 - 1 Complete step 1 on page 223 through step 5 on page 225.

- 2 On the Catalog tab and its associated subtabs, there are two fields that require entries appropriate for a software installation model.

Field	Function
Part No.	Must be a unique number.
LI Category	The line item category for a software installation model is software installation .

- 3 Click the Software tab and type the following information:
 - Application Name
 - Installation Information
 - No. of points
 - Version
 - Authorized?
- 4 Click **Add** or press F2.

Managing Different Types of Multiple Licenses

ServiceCenter allows you to choose one of three types of multiple licenses:

- **Per named workstation** enables you to install a software application on a given number of identified workstations. For example, a license for an office automation suite that can be installed on 1,000 workstations.
- **Per named user** enables access to an application or database for a given number of users. For example, a license enabling access to a database for 500 named users.
- **Per concurrent accesses** enables a specified number of concurrent accesses to a database. For example, a license enabling 1,000 concurrent users access to the database.

For each multiple license, ServiceCenter has a Rights field, which specifies the number corresponding to the number of:

- Workstations on which the software can be installed.
- Named users.
- Simultaneous accesses.

Software counters use these values to verify that your company has not exceeded the number of installations or concurrent users granted by a license.

Adding Software Licenses as Asset Records

A software license is an asset stored in the device table. It represents the number of authorized software uses within an organization. For example, you may purchase a 50-user license for Microsoft Office that supports 50 installations of Microsoft Office.

To create a software license:

- 1 From the ServiceCenter home menu, click **Inventory Management**. Click **Assets**. Figure 8-11 shows the Asset Information form.

Figure 8-11: Asset Information form

- 2 Populate the fields with available information about the asset to create an asset record.
- 3 Select **Software License** in the **Type** field drop-down list.
- 4 Choose the appropriate subtype in the **Subtype** field drop-down list.

- 5 Click **New**. Figure 8-12 shows the Device Software License form.

The screenshot shows the 'ServiceCenter - [New Asset]' window. The 'Device Software License' form is displayed with the 'Summary' tab selected. The 'Subtype' dropdown is set to 'Project Management License'. The 'Part Number' field is highlighted with a red box. The status bar at the bottom shows 'Ready' and 'Response 0.761 draw 0.301 insert device.softwarelicense.g(am.new.device) [UP]'.

Figure 8-12: Asset Information form

- 6 On the **Summary** tab, type the part number in the **Part Number** field. The **Part Number** field retrieves license model information from the catalog.
- 7 Complete the appropriate fields on the **Summary**, **Financial**, **Contact**, and **Attachments** tabs. For more information, see the *ServiceCenter User's Guide*.
- 8 Click the **License** tab and complete the appropriate fields. The **License** tab includes the following subtabs and fields.

Field	Description
Application Name	Name of the software. This information comes from the model table based on the part number you entered on the Summary tab.
Where is the software resident?	Where the software resides, either the network or the client.
Can software be used in multi-OS environment?	Can the software be used on more than one operating system?
Current Version	The current version number of the software in the contract.
Past Versions	Previous version number of the software.

Click the **License Type** subtab

Fields and Options	Description
Single-User option	License that allows software to be installed on a single workstation to be used by a single user.
Multi-User option	License that allows software to be installed on multiple workstations to be used by multiple users.
Per named workstation option	A multi-user licensing type that allows multiple software installations across multiple workstations. This field only displays if the Multi-User option is selected.
Total No. of Installs Note: This the label for the rights field if the Multi-user licensing type field is Per named workstation.	The maximum number of times you can install the software. Note: This value is used for compliance checks.
Per named user option	A multi-user licensing type that allows a specified number of individuals to have access to the software. This field only displays if the Multi-User option is selected.
Total Number of Named Users Note: This the label for the rights field if the Multi-user licensing type field is Per named user.	The maximum number of people who can be named to have access to the software.
Per concurrent accesses option	A multi-user licensing type that allows a specific number of individuals to have access to the software at the same time. This field appears only if the Multi-User option is selected.
Concurrent Accesses	The number of people who can access the software at the same time.
Evaluation Rights Note: This the label for the rights field if the Multi-user licensing type field is Per concurrent accesses.	Informational field. The maximum number of installations allowed for demonstration or evaluation purposes.

Fields and Options	Description
Product Pool	Drop-down list with servers, applications, and systems. It is an informational field that dynamically controls the appearance of MIPS / # of Processors fields if servers or systems is selected.
MIPS / # of Processors	Reflects computer performance. Field is informational and only displays if servers or systems is selected in the Product Pool field drop-down list.

With the exception of the Product pool and MIPS / # of Processors fields, other data comes from the model table that depends on the part number specified on the Summary tab.

- 1 Complete the appropriate fields on the Regions/Languages subtab.

Field	Description
Regions	Fill function is available. Lists regions for which the software is applicable.
Languages	Fill function is available. Lists languages for which the software is applicable.

- 2 Click **Add** to save the new asset record.

Software Installations

In ServiceCenter, a software installation is tracked as an asset. When you create a software installation, it retrieves data from the model table, which depends on the specified part number. The Installed Software form enables you to create a record of the software, where it is installed, and who is using it. Typically, discovery tools populate Software Installation records.

The Installed Software form has two tabs:

- Application Information
- Installed Computer System

Figure 8-13 shows the Application Information tab.

Search pcsoftware Records

Back Add Search Find Fill

Installed Software Information

Application Information Installed Computer System

Application Name: [text box] Status: [dropdown]

Description: [text box]

Part Number: [text box] License ID: [text box]

Manufacturer: [text box] Counts For: [text box]

Model: [text box] File Name: [text box]

Serial No.: [text box] File Size: [text box]

Last Scanned: [text box] Installed Directory: [text box]

Last Update: [text box] Media Type: [text box]

Updated By: [text box] Execution Count: [text box]

Version: [text box] Last Execution: [text box]

Fingerprint [text box]

Suite Component? ☐

Authorized? ☐

Ready Response 0.190 draw 0.100 insert pc.software.files.g(db.search) [UP]

Figure 8-13: Installed Software form: Application Information tab

Figure 8-14 shows the Installed Computer System tab.

Installed Software Information

Application Information Installed Computer System

Installed System: [text box]

Installation Date: [text box]

Installed By: [text box]

Contact Name: [text box]

Network Name: [text box]

Removal Date: [text box]

Model: [text box]

Type: [text box]

Removed By: [text box]

Serial Number: [text box]

Figure 8-14: Installed Computer System tab

For more information, see the *ServiceCenter User's Guide*.

To create a software installation record:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click the **Assets** tab.

- 3 Click **Installed Software**.
- 4 Populate the fields of the different tabs according to your needs.
Note: **Application Name** on the Application Information tab is a required field.
- 5 Click **Save** or **Add**, or press F2, to save the record and leave it displayed.

Software Counters

Software counters enable you to verify that the number of software installations you actually have does not exceed the number authorized by your license. The number of software installations or access rights authorized by a license is indicated by a number of rights.

For certain licenses, the software installation corresponds to the consumption of a certain number of points. For example, a Microsoft Select license specifies that installing Microsoft Word uses 10 points. Therefore, 100 of these installations uses 1,000 points. When you use software installation counters, you can specify if the installation count should also count the number of points allocated to each installation.

To create a software counter:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click the **Administration** tab.
- 3 Click **Software Counters** to display the Software Counter Information form.
- 4 Do one of the following:
 - Type the name of the application in the **Name** field.
 - Click **Search** to select the appropriate software.
- 5 The Licenses tab has these fields.

Field	Description
All License Models	Checks compliance of all licenses.
License Models	Checks compliance of the number of selected licenses that you specify.

- 6 Click the **Installs** tab.

The Installs tab has the following fields:

Field	Description
All Installation Models	Checks compliance of all installations.
Calculation Method	Checks compliance of selected installations.
Count Software Suite Components?	Count each application in a suite. (e.g. Microsoft Office is a suite that includes Word, Excel, PowerPoint, Access).
Count Removed or Unknown Installs?	Count any installations that have a status of removed or uninstalled.
Count Non-Authorized Install?	Count any unauthorized installations.

- 7 Choose the calculation method in the **Calculation Method** drop-down list field.
- 8 Select any other appropriate options.
- 9 Click **Add**.

Choosing a Calculation Method

Choosing the calculation method for the number of installations enables you to verify that you have not exceeded the number of rights specified in the software license. For example, an office software license credits you 1,000 rights. Each software installation consumes 10 points. The software installation counter enables you to verify that the software has not been installed more than 100 times ($100 \times 10 = 1,000$). ServiceCenter has three calculation methods:

- Count each installation
- Count each workstation
- Count each user.

Each installation

Count each installation regardless of the number of workstations or users.

Figure 8-15 on page 234 shows that there are three installations counted (Installation 1, Installation 2, and Installation 3).

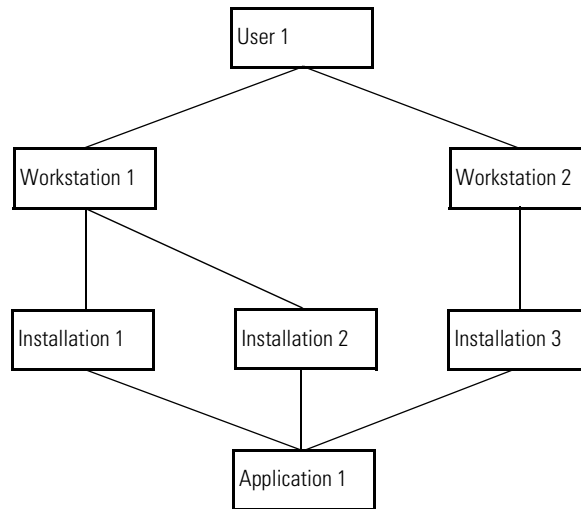


Figure 8-15: Installation example

Each Workstation

Figure 8-16 shows an example that counts by workstation, not by the number of installations.

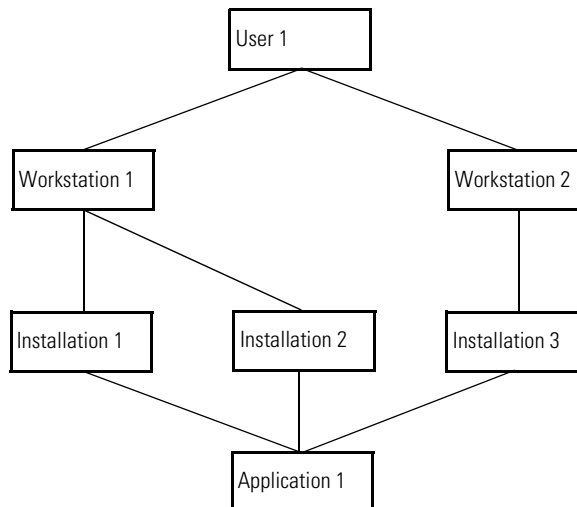


Figure 8-16: Workstation example

If you install the same application multiple times on a workstation, ServiceCenter counts only one of those installations. Figure 8-16 on page 234 shows that Workstation 1 has Installation 1 and Installation 2 of Application 1. Because the count is by each workstation and there is only one workstation, there is one installation of Application 1 counted. For Workstation 1 and Workstation 2, each has an installation (Installation 1 and Installation 3). There are two installations counted.

Each User

ServiceCenter counts one installation for each user on the workstation where the application resides.

Figure 8-17 shows that User 1 has two installations (Installation 1 and Installation 2) on his workstation (Workstation 1). Also notice that User 1 has another workstation (Workstation 2) with a third installation on it. Although there are three installations, the count is by each user. Therefore, ServiceCenter counts only one installation for User 1. There is also a second user. Figure 8-17 shows two installations counted.

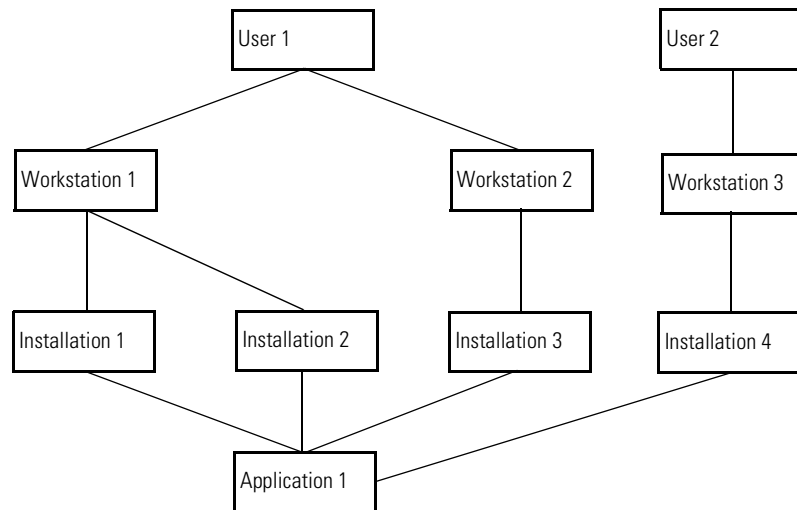


Figure 8-17: Count by user

Compliance

When you click **Add** to create the software counter, the form adds Results and Message Log tabs and Compliance Check and Create Schedule Record buttons. The Results tab has the following fields.

Field	Description
No. of Rights	Indicates the total number of rights acquired for a particular software license.
Rights Counted	Locates the number of instances of the software that are in use.
Last Processed	Indicates the last time a compliance check was performed.

The Compliance Message Log

The Message log tab displays one of the following error messages about the data entered for which you are checking compliance:

No license models have been selected for the software counter.

No installation models have been selected for the software counter.

There are no license models in the model table.

A software license does not exist for the license model with Part No.= %S.

Asset ID= %S is not a software license but is linked to license model with Part No.= %S.

The software license with Asset ID= %S does not indicate any rights.

There are not software install models in the model table.

A software install does not exist for the software installation model with Part No.= %S.

Installed system= %S does not exist for the software install with the License ID= %S and Application Name= %S.

To clear the message log:

- Choose **Options > Clear Message Log**.

Checking Compliance

You can manually check compliance or you can schedule compliance checking to occur automatically.

- To check compliance manually, click **Compliance Check**. If the compliance check is successful, a message appears. Click **OK**.

To check compliance automatically:

- 1 Click **Create Schedule Record** to launch the Schedule Software Compliance Check Wizard.
- 2 **When should the initial check be performed?** Type the date when you want the first compliance check to occur.
- 3 Do one of the following:
 - Type the relative date/time (DDD HH:MM:SS) format in the next available field. For example, type 7 for DDD to indicate every seven days, and 11:55:00 for HH:MM:SS to indicate the hour, minutes, and seconds.)
 - Select **Monthly**, **Quarterly**, **Semi-Annually**, or **Annually**.

Figure 8-18 shows the Schedule Software Compliance Check Wizard.

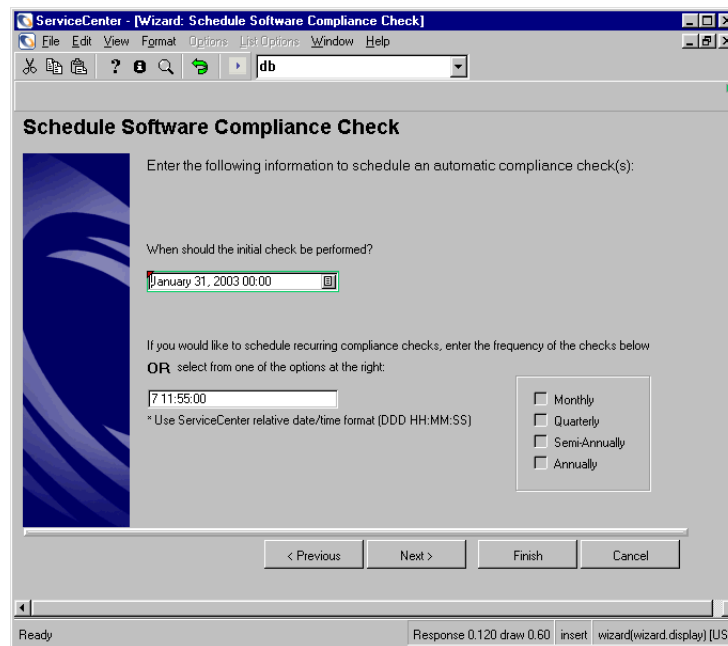


Figure 8-18: Schedule Software Compliance Check wizard

- 4 Click **Finish**. ServiceCenter creates a schedule record with the same name as the software counter record. For more information, see *System Tailoring*.
After ServiceCenter completes a compliance check, it displays all results on the Results tab. Click **No. of Rights** on the **Results** tab to display a list of all the software licenses counted during the compliance check.

Software Tracking and Compliance Example

Your organization needs Norton AntiVirus software. You submitted a Change Request ticket that is approved. As part of the Change Request process, you must add the software license and software installation information to the catalog. An order ticket exists to obtain the software. The order ticket includes two line items: one for the purchase of the software license and another to procure software installation services.

- Step 1** Add the software license and software installation information to the catalog. See *Step 1: Add Items to the Catalog on page 240*.
- Step 2** When you receive the software license, you should add an Application type asset record and a Software License type asset record to the Inventory Management database. See *Step 2: Add Records to the Inventory Management Database on page 243*.
- Step 3** The next step is to create a software contract. See *Step 3: Create a Software Contract on page 246*.
- Step 4** Associate the software license you created to the contract. See *Step 4: Associate the Software License to the Contract on page 248*.
- Step 5** Create a support contract and associate the application asset to the contract. See *Step 5: Create a Support Contract for the Software License on page 251*.
- Step 6** Install the software and create install records in the Software Installation table, one record for each installation. See *Step 6: Create a Software Installation Record on page 253*.
- Step 7** After time has passed, you should check to verify that the organization is compliant with the Norton AntiVirus license. Create a software counter to verify that the number of installations you actually have conforms with the number of installations you have for the licenses. See *Step 7: Check Software Compliance on page 255*.

Figure 8-19 on page 239 shows the interrelated table and record relationships that enable software tracking and compliance checking.

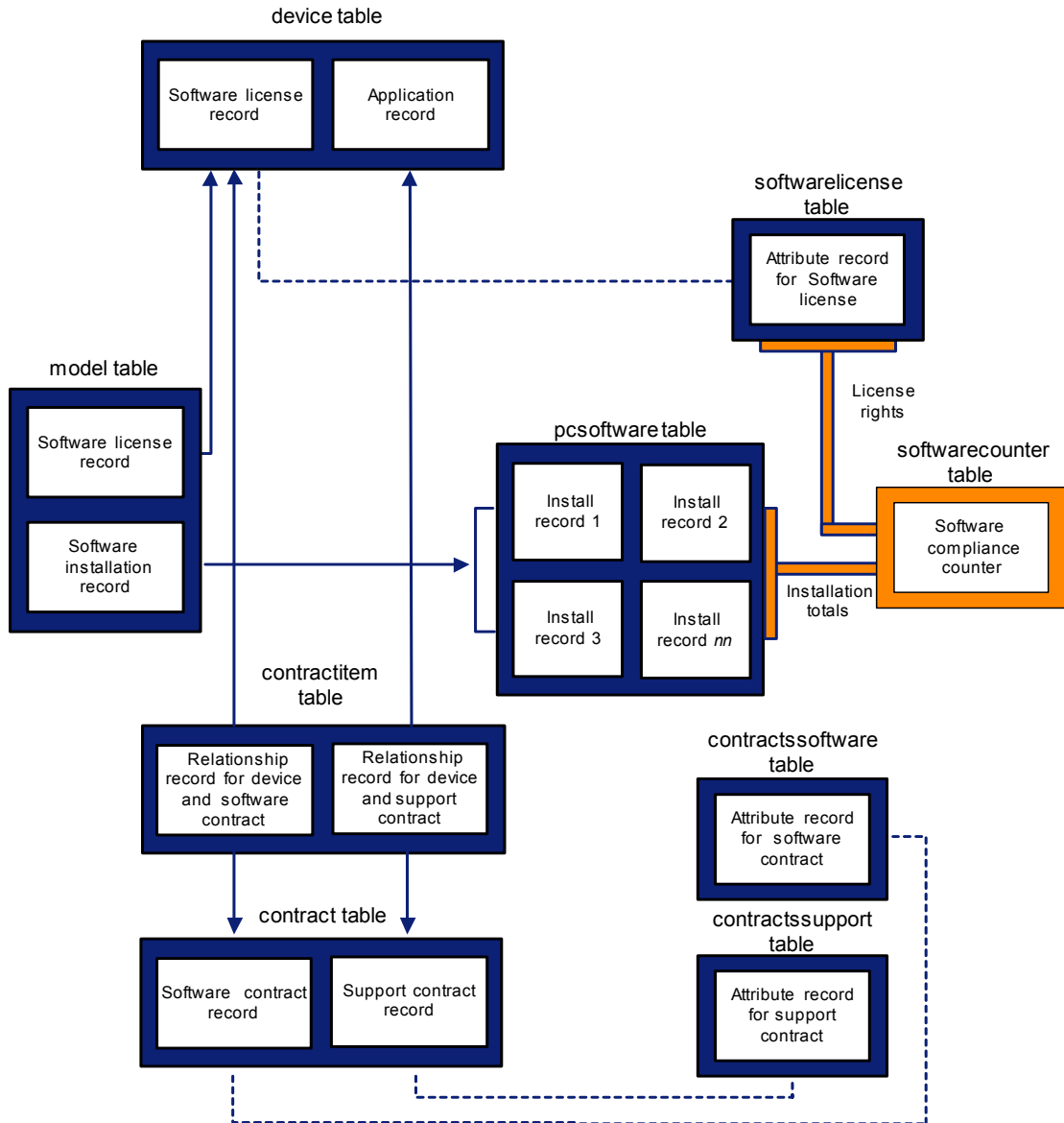


Figure 8-19: Software tracking and compliance check relationships

Step 1: Add Items to the Catalog

In this example, you are adding a software license model to the catalog.

To add an asset to the catalog:

- 1 From the ServiceCenter home menu, click the **Support** tab.
- 2 Click **Models**. Figure 8-20 shows the Model Information form.

The screenshot shows a web application window titled "ServiceCenter - Search model Records". The window has a menu bar with "File", "Edit", "View", "Format", "Options", "List Options", and "Help". Below the menu bar is a toolbar with icons for "Back", "Add", "Search", "Find", and "Fill". The main content area is titled "Model Information" and has several tabs: "General", "Current Quantities", "Reorder", "Vendors", "Catalog", "Software", and "Picture". The "General" tab is selected, showing a "General Information" section with the following fields: "Part No." (text input), "Brief Description" (text input), "Manufacturer" (text input with a small icon), "Model" (text input), "Model Ext." (text input), "Serialized" (checkbox), "Cost" (text input), "Currency" (text input), "GL Number" (text input), "Default Priority" (text input), "Default Quantity" (text input), and "Config. File" (text input). Below the "General Information" section are two more sections: "Detailed Description" and "Instructions", each with a large text area. The status bar at the bottom of the window shows "Ready" on the left and "Response 0.180 draw 0.281 insert model.g(db.search) [UP]" on the right.

Figure 8-20: Model Information form

For more information, see the Support Files section in the *ServiceCenter System Administrator's Guide*.

- 3 Type the required information on the **General** tab on the **Model Information** form, as shown in Figure 8-21 on page 241.

Note: If you are actually adding an item to the catalog, complete any additional fields that are required by your organization's business rules and practices.

The screenshot shows the 'ServiceCenter - model: 530' window with the 'Model Information' form open. The 'General' tab is selected. The form contains the following fields:

Part No.:	530	Cost:	50.00
Brief Description:	Norton Antivirus 7.5	Currency:	USD
Manufacturer:	Symantec	GL Number:	
Model:	Norton Antivirus 7.5	Default Priority:	
Model Ext.:		Default Quantity:	1
Serialized:	<input type="checkbox"/>	Config. File:	

Below the 'General Information' section is the 'Detailed Description' section with the text 'Purchase Norton Antivirus 7.5'. The 'Instructions' section is empty. The status bar at the bottom shows 'Ready', 'Response 0.201 draw 0.290', and 'insert model.gldb.view [UP]'.

Figure 8-21: Model Information form: General tab

- 4 Click the Catalog tab.
- 5 On the Catalog Information subtab, type the line item category name, **Software License**, in the LI Category field. Figure 8-22 shows the Catalog Information subtab.

The screenshot shows the 'ServiceCenter - model: 530' window with the 'Model Information' form open. The 'Catalog' tab is selected, and the 'Catalog Information' subtab is active. The form contains the following fields:

LI Category:	Software License	Assigned Dept:	
Sequence:			

Below the 'Catalog Information' section is the 'Components' section, which is a table with the following columns: Group, Part Number, Description, Quantity, Category, and Option Type. The table is currently empty.

Below the 'Components' section is the 'Dependencies' section, which is a table with the following columns: Group Name, Dependent On, and Dependency Type. The table is currently empty.

The status bar at the bottom shows 'Ready', 'Response 0.201 draw 0.290', and 'insert model.gldb.view [UP]'.

Figure 8-22: Model Information form: Catalog Information subtab (Catalog tab)

- 6 Click the **Software** tab and type the information shown in Figure 8-23.

The screenshot shows a window titled "ServiceCenter - model: 530". The menu bar includes File, Edit, View, Format, Options, List Options, and Help. The toolbar contains icons for OK, Cancel, Previous, Next, Add, Save, Delete, Views, Find, and Fill. The "Model Information" form has several tabs: General, Current Quantities, Reorder, Vendors, Catalog, Software, and Picture. The "Software" tab is selected. The form contains the following fields:

- Software Information:** Application Name: Norton AntiVirus Corporate Edition
- License Information:**
 - Single-User: ☐
 - Multi-User: ☒ Per named workstation
 - Total No. of Installs: 1
 - Evaluation Rights:
- Installation Information:**
 - Points per Install:
 - Version:
 - Authorized?: ☐

The status bar at the bottom shows "Ready" and "Response 0.201 draw 0.290 insert model.g(db.view) [UP]"

Figure 8-23: Model Information form: Software tab

- 7 Click Add or press F2.
- 8 Next, you must add a software installation model to the catalog. You can do so by modifying the record you just created for the software license model. Click the **General** tab of the **Model Information** form. Type the new part number **531** in the **Part Number** field.
- 9 Click the **Catalog** tab and change the line item category name in the **LI Category** field to **Software Installation**.
- 10 Click Add or press F2.
- 11 Click OK.
- 12 Click Back to return to the ServiceCenter home menu.

Step 2: Add Records to the Inventory Management Database

In this step, you will add two types of assets to the device table. You will add an Application asset for the Norton AntiVirus application and a Software License asset for the Norton AntiVirus license

To add the application asset:

- 1 From the ServiceCenter home menu, click **Inventory Management**. Click **Assets**. Populate the fields with information about the asset record you are creating.
- 2 Because you are creating a software license, select:
 - **Application** in the **Type** field drop-down list.
 - **Anti-Virus/Security** in **Subtype** field drop-down list.
- 3 Click **New**. The Application form appears. Complete the fields on the **System Summary** tab as shown in Figure 8-24.

The screenshot shows the 'ServiceCenter - New Asset' window with the 'System Summary' tab selected. The 'Ownership' section contains the following fields and values:

Field	Value
Asset ID:	Norton AntiVirus 7.5
Subtype:	Anti-Virus/Security
Asset Tag:	
Network Name:	
Domain:	
Assignment:	
Serial Number:	
Version:	
Status:	Available
Company:	
Department:	
Cost Center:	
Service Contract:	
Incident Category:	
Priority:	
Asset Pending Change:	<input type="checkbox"/>
Critical Asset:	<input type="checkbox"/>

Figure 8-24: Application form: System Summary tab

- 4 Click **Add**.

To add the software license asset:

- 1 From the ServiceCenter home menu, click **Inventory Management**. Click **Assets**. Populate the fields with information about the asset record you are creating.
- 2 Because you are creating a software license, select:
 - **Software License** in the **Type** field drop-down list.
 - **Utility Software License** in the **Subtype** field drop-down list.

- 3 Click **New**. The Device Software License form appears. Complete the fields on the Summary tab, as shown in Figure 8-25.

ServiceCenter - New Asset

File Edit View Format Options List Options Help

OK Cancel Add Find Fill

Device Software License

Summary License Contact Financial Attachments

Ownership

Asset ID: NAV License Status: Available

Subtype: Utility Software License Company:

Description: Department:

Assignment: Cost Center:

Part Number: 530 Incident Category:

Manufacturer: Priority:

Model: Asset Pending Change? ☐

Critical Asset? ☐

Ready Response 0.200 draw 0.320 insert device.softwarelicense.gl(am.new.device) [UP]

Figure 8-25: Device Software License form: Summary tab

- 4 Click the **License** tab. Complete the appropriate fields on the License tab shown in Figure 8-26.

ServiceCenter - New Asset

File Edit View Format Options List Options Help

OK Cancel Add Find Fill

Device Software License

Summary License Contact Financial Attachments

License Information

General License Type Regions/Languages

Application Name: NoroIn AntiVirus Current Version: 7.5

Where is the software resident? network

Can software be used in multi-OS environment? ☐

Past Versions

Ready Response 0.200 draw 0.320 insert device.softwarelicense.gl(am.new.device) [UP]

Figure 8-26: Device Software License form: General subtab (License tab)

- 5 Click the **License Type** subtab and complete the appropriate fields, as shown in Figure 8-27.

The screenshot shows the 'ServiceCenter - New Asset' window with the 'License Information' subtab selected. The 'License Type' subtab is active, displaying the following fields:

License Type		Rights	
Single-User	<input type="radio"/>	Total No. of Installs:	500
Multi-User	<input checked="" type="radio"/>	Evaluation Rights:	5
Per named workstation		Product Pool:	applications

Figure 8-27: Device Software License form: License Type subtab (License tab)

- 6 Click the **Regions/Languages** subtab and complete the appropriate fields. Figure 8-28 shows the Regions/Languages subtab.

The screenshot shows the 'ServiceCenter - New Asset' window with the 'License Information' subtab selected. The 'Regions/Languages' subtab is active, displaying the following fields:

Regions	Languages
North America	English
Asia	Japanese

Figure 8-28: Device Software License form: Regions/Languages subtab (License tab)

- 7 Click **Add** or press F1 to save the new asset record.

Step 3: Create a Software Contract

The next step is to create a contract for the Norton AntiVirus software.

To create a software contract:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click the **Contracts** tab.
- 3 Click **Contracts**. The General Contract Information form appears.
- 4 Click **New** to launch the Add New Contract Wizard.
- 5 Click the **Create what type of contract?** option.
- 6 Figure 8-29 shows the drop-down list to choose a contract type. Choose **software**. Click **Next**.

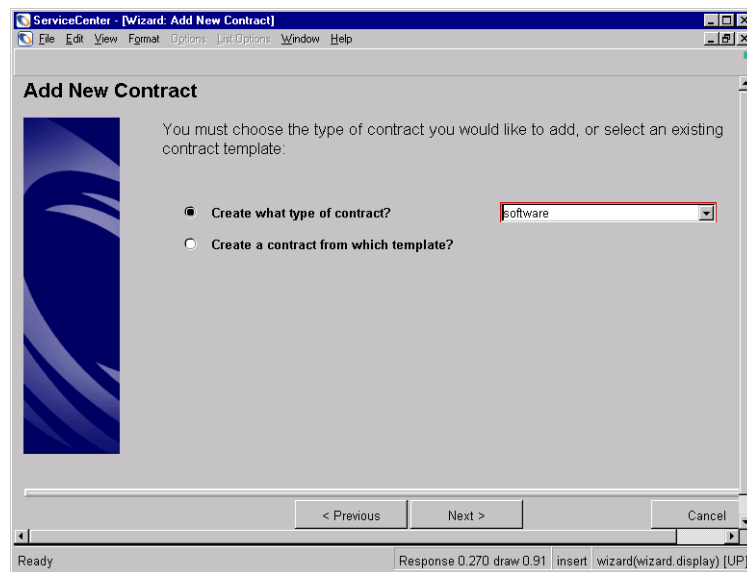


Figure 8-29: Add New Contract wizard

- 7 The General Contract Information form displays.

8 Complete the fields shown in Figure 8-30.

The screenshot shows a software application window titled "ServiceCenter - [New Contract]". The window has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar (Back, Add, Find, Fill). The main content area is titled "Software Contract Information" and contains two columns of fields. The left column includes Contract ID (NAV), Creation Date (April 14, 2003 11:01), Submitted By (falcon), Negotiated By, Assignee, and Brief Description. The right column includes Status (draft), Contract Type (software), Signed Date, Start Date, and Expiration Date. Below these fields is a tabbed interface with tabs for General, Vendor/Contract, Financial, Terms, Renewal Info, Notes, and Attachments. The General tab is active and contains fields for Company (ACME), Department (Administration), Budget Center, Budget Code, Project ID, Accounting Code, Language, Notification Group, Notification Contact, Product No., Part No., Manufacturer, Model, Purchase Order No. (02002), Purchase Req No. (Q1003), and Invoice No. At the bottom of the window, there is a status bar showing "Ready", "Response 0.310 draw 0.281", and "insert | contract software(contract.open) [UP]".

Figure 8-30: Software Contract form: General tab

Note: The data in the Purchase Order No. and the Purchase Req No. fields are sample data and do not reflect actual request tickets.

- 9 Type today's date in the **Start Date** field.
- 10 Type a date one year in the future in the **Expiration Date** field.
- 11 Click the **Financial** tab and complete the fields shown in Figure 8-31 on page 248.

ServiceCenter - New Contract

File Edit View Format Options List Options Help

Back Add Find Fill

Software Contract Information

Contract ID: NAV Status: **draft**
 Creation Date: February 26, 2003 17:31 Contract Type: software
 Submitted By: FALCON Signed Date:
 Negotiated By: Start Date: <your start date>
 Assignee: Expiration Date: <your expiration date>
 Brief Description:

General Vendor/Contact Financial Terms Renewal Info Notes Attachments

Cost

Cost Center:

Purchase Cost

Cost: 25000
 Currency: US Dollar
 Currency EX Date:

One-Time Charge

Cost:
 Currency:
 Currency EX Date:

Renewal Cost

Cost:
 Currency:
 Currency EX Date:

Ready Response 0.211 draw 0.340 insert contract:software(contract.open) [UP]

Figure 8-31: Software Contract form: Financial tab

- 12 Click **Add**. ServiceCenter adds the Licenses tab to the Software Contract form.

Step 4: Associate the Software License to the Contract

On the contract you just created, you now will add the software license to it.

To add a software license to a contract:

- 1 Click the **Licenses** tab on the Software Contract form.
- 2 Click **Add Licenses**. The Select Assets to Add to Contract Wizard appears.
- 3 Click **Fill** next to the first field. A Search criteria form displays.

- 4 Access the software license you created previously. Fill the necessary fields to filter the list. For example, to locate the software license for this contract, type NAV in the Asset ID field, as shown in Figure 8-32. Click **Search**.

Figure 8-32: Asset Information

If there is only one license in the database, it automatically populates the first asset text box on the Select Assets to Add to Contract Wizard shown in Figure 8-33. Click **Next**.

Figure 8-33: Select Assets wizard

If you have more than one license in the database, the search returns a list. Double-click the correct license and it also populates the first field of the wizard. Click **Next**. Figure 8-34 shows the license you added at the bottom of the Asset list.

ServiceCenter - [Contract: NAV]

File Edit View Format Options List Options Window Help

Back Save Find Fill

Software Contract Information

Contract ID: NAV Status: current
 Creation Date: April 14, 2003 11:01 Contract Type: software
 Submitted By: falcon Signed Date:
 Negotiated By: Start Date: April 14, 2003 00:00
 Assignee: Expiration Date: April 14, 2004 00:00
 Brief Description:

General Licenses Vendor/Contact Financial Terms Renewal Info Notes Attachments

Add Licenses Generate %

Asset	ID	% Cost Allocation	Status
device	CarolPC	55.0	Available
device	DD-000002	35.6	Retired
device	DPC00005	45.0	Warehouse
device	NAV		Available

Ready Response 0.581 draw 0.581 insert contract.software(contract.view) [UP]

Figure 8-34: Select Assets wizard

- 1 If you want to allocate costs to this license or any other license, double-click the row where the asset appears. Figure 8-35 shows the form where you can specify an allocation percentage.

ServiceCenter - [Contract Item]

File Edit View Format Options List Options Window Help

Back Add Save Delete Find Fill

Available

Contract ID: NAV
 Asset: device
 ID: NAV
 % Cost Allocation:
 Asset Status: Available

Contract Information

Contract Type: software
 Contract Status: current
 Company: ACME
 Assignee:
 Start Date: April 14, 2003 00:00
 Expiration Date: April 14, 2004 00:00

Ready Response 0.180 draw 0.60 insert proration(contractitem.view) [UP]

Figure 8-35: Allocation Information form.

- 2 Type the percentage of the cost you are allocating to this license in the **% Cost Allocation** field.
- 3 Click **Save**.
- 4 Click **Back** to return to the Licenses tab of the Software Contract Information form. The allocation percentage appears in the **% Cost Allocation** column.

Step 5: Create a Support Contract for the Software License

The next step is to create a support contract for the Norton AntiVirus software.

To create a support contract:

- 1 From the ServiceCenter home menu, click the **Services** tab. Click **Inventory Management**.
- 2 Click the **Contracts** tab.
- 3 Click **Contracts**. The General Contract Information form appears.
- 4 Click **New**. The Add New Contract Wizard appears.
- 5 Click **Create what type of contract?** option.
- 6 Choose the **support** contract type from the drop-down list, as shown in Figure 8-36.

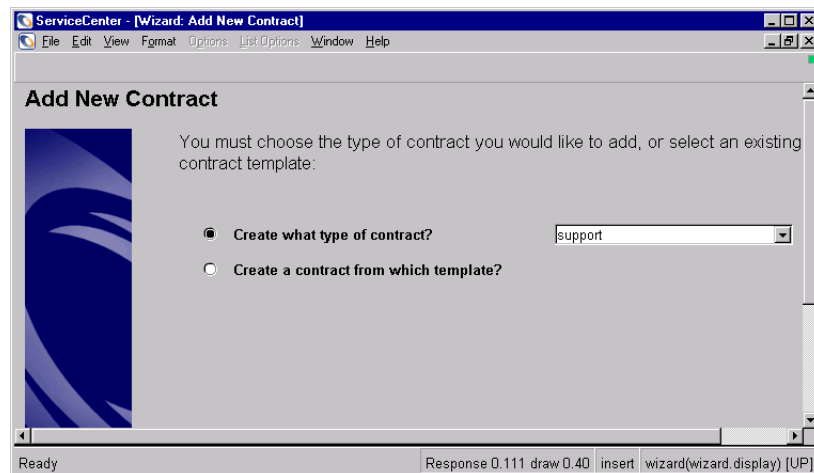


Figure 8-36: Add New Contract wizard

- 7 Click **Next**.

- 8 The General Contract Information form appears. Complete the fields using the information shown in Figure 8-37.

ServiceCenter - New Contract

File Edit View Format Options List Options Help

Back Add Find Fill

Support Contract Information

Contract ID: Status: **draft**

Creation Date: February 26, 2003 17:37 Contract Type: support

Submitted By: FALCON Signed Date:

Negotiated By: Start Date: <your start date>

Assignee: Expiration Date: <your expiration date>

Brief Description:

General | Support Info | Vendor/Contact | Financial | Terms | Renewal Info | Notes | Attachments

Customer ID: ACME Notification Group:

Department: Administration Notification Contact:

Budget Center:

Budget Code:

Product No.:

Project ID:

Part No.:

Accounting Code:

Manufacturer:

Model:

Language: English

Purchase Order No.:

Purchase Req No.:

Invoice No.:

Authorized Callers

Ready Response 0.211 draw 0.340 insert contract.support(contract.open) [UP]

Figure 8-37: Support Contract Information form: General tab

Note: The data in the Purchase Order No. and the Purchase Req No. fields are sample data and do not reflect actual request tickets

- 9 Type today's date in the Start Date field.
- 10 Type a date one year in the future in the Expiration Date field.
- 11 Click Add.

Adding an Application Asset to a Support Contract

The next step is to add the Norton AntiVirus 7.5 application asset to the support contract you just created.

To add an asset to a support contract:

- 1 Open the support contract you just created.
- 2 Follow the steps in *Step 4: Associate the Software License to the Contract* on page 248 to add the asset to a support contract. Use the asset ID Norton AntiVirus 7.5.

Step 6: Create a Software Installation Record

Next, you must create five installation records. Remember, that auto-discovery typically creates software installation records.

To create a PC software record:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 From the Assets tab, click **Installed Software**.
- 3 The Installed Software Information form appears. Complete the form with the information shown in Figure 8-38.

The screenshot shows the 'Installed Software Information' form in the 'pcsoftware' application. The form is titled 'Installed Software Information' and has two tabs: 'Application Information' and 'Installed Computer System'. The 'Application Information' tab is active. The form contains various fields for software details. The 'Application Name' is 'Norton AntiVirus 7.5', 'Description' is 'Norton AntiVirus 7.5', 'Part Number' is '531', 'Manufacturer' is 'Advanced Systems', and 'Model' is '7.5'. The 'Status' is 'Installed'. The 'License ID' is 'NAV01'. Other fields like 'Serial No.', 'Last Scanned', 'Last Update', 'Updated By', 'Version', 'File Name', 'File Size', 'Installed Directory', 'Media Type', 'Execution Count', 'Last Execution', 'Suite Component?', and 'Authorized?' are also present. The 'Fingerprint' field is empty. The bottom status bar shows 'Ready', 'Response 0.111 draw 0.200 insert', and 'pc.software.files.g(db.view) [UP]'.

Figure 8-38: Installed Software Information form: Application Information tab

- 4 Click the Installed Computer System tab and type CarolPC in the Installed System field, as shown in Figure 8-39.

The screenshot shows a window titled 'pcsoftware' with a menu bar (File, Edit, View, Tools, Window, Help) and a toolbar with icons for OK, Cancel, Previous, Next, Add, Save, Delete, Find, and Fill. The main area is titled 'Installed Software Information' and has two tabs: 'Application Information' and 'Installed Computer System'. The 'Installed Computer System' tab is selected. It contains several input fields: 'Installed System' (with 'CarolPC' entered), 'Installation Date', 'Installed By', 'Removal Date', and 'Removed By'. On the left, there are fields for 'Contact Name' (JENKINS, CAROL), 'Network Name', 'Model' (p500), 'Type' (computer), and 'Serial Number'. The status bar at the bottom shows 'Ready', 'Response 0.111 draw 0.200 insert pc.software.files.g(db.view) [UP]'.

Figure 8-39: Installed Software Information form

- 5 Click Add.
- 6 Repeat step 1 on page 253 through step 5 on page 254 to add four more installation records. Ensure that you:
 - Update the License ID field on the Application Information tab and the Installed System field on the Installed Computer System tab for each additional installation record.

Install record	License ID field on the Application Information tab	Installed System field on the Installed Computer System tab
#2	NAV002	BobPC
#3	NAV003	DavePC
#4	NAV004	JoePC
#5	NAV005	SarahPC

Step 7: Check Software Compliance

Assume that time has passed and according to the business practices of the organization, it is time to check the compliance of the Norton AntiVirus software.

The purpose of the compliance check is to verify that the organization adheres to the requirements of the software license. Compliance checks the number of rights in the license against the number of installs.

To create a software counter:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click the **Administration** tab.
- 3 Click **Software Counters**. The Software Counter Information form displays.
- 4 Type All Norton Licenses in the Name field.
- 5 Type 530 in the first row of the License Models field.

Note: Remember, 530 is the part number for the Norton Antivirus 7.5 software license.

The screenshot shows a web application window titled "ServiceCenter - [Search Software Counter Records]". The window has a menu bar with "File", "Edit", "View", "Format", "Options", "List Options", "Window", and "Help". Below the menu bar is a toolbar with icons for "Back", "Add", "Search", "Find", and "Fill". The main content area is titled "Software Counter Information". It contains a "Name:" label followed by a text input field containing "All Norton Licenses". Below this are two tabs: "Licensess" (selected) and "Installs". Under the "Licensess" tab, there is a section titled "Count the licenses linked to the following models:" followed by a checkbox labeled "All License Models?". Below this is a table with the heading "License Models" and one row containing the value "530". The status bar at the bottom shows "Ready", "Response 0.440 draw 0.100", "insert", and "software.counter.g(softwarecounter.search) [UP]".

Figure 8-40: Software Counter Information form: Licensess tab

- 6 Click the Installs tab and complete the fields on it as follows:

The screenshot shows the 'ServiceCenter - [Search Software Counter Records]' window with the 'Installs' tab selected. The 'Name' field contains 'All Norton Licenses'. Below the tabs, there are checkboxes for 'All Installation Models?' (unchecked) and 'Count Software Suite Components?' (checked). A table titled 'Installation Models' shows a single entry '531'. To the right, there are checkboxes for 'Count Removed or Unknown Installs?' (checked) and 'Count Non-Authorized Installs?' (checked). The status bar at the bottom indicates 'Ready' and 'Response 0.440 draw 0.100 insert software.counter.g(softwarecounter.search) [UP]'.

Figure 8-41: Software Counter Information form: Installs tab

- 7 Click Add. Notice that the form changes with the addition of the Results and Message Log tabs and the Compliance Check and Create Schedule Record buttons.
- 8 Click Compliance Check. Figure 8-42 shows the result.

The screenshot shows the 'ServiceCenter - [Software Counter: All Norton Licenses]' window with the 'Results' tab selected. The 'Name' field still contains 'All Norton Licenses'. Below the tabs, there are buttons for 'Compliance Check' and 'Create Schedule Record'. The 'No. of Rights' is 500 and 'Rights Counted' is 5. The 'Last Processed' date is 12/11/02 16:01:00. A table titled 'Non-Authorized Users' is empty. The status bar at the bottom indicates 'Ready' and 'Response 0.440 draw 0.100 insert software.counter.g(softwarecounter.search) [UP]'.

Figure 8-42: Software Counter Information form

Your organization is compliant for the Norton AntiVirus 7.5. The **No. of Rights** field indicates that the organization has 500 rights with its software license. The Compliance Check located five installations of the software. The organization still has 495 rights for this software.

Where to Find More Information

For information about asset management, see the *ServiceCenter Request Management Guide*. For information about modifying or deleting a record, or creating a contract, see the *ServiceCenter User's Guide*.

9 Service Level Management

CHAPTER

Service Level Agreements (SLAs) track performance and provide system feedback on service agreements between departments within a company. SLAs are integrated into the ServiceCenter suite of modules, but they may be implemented separately to monitor the quality of both external and internal service. This chapter provides a general definition of SLAs and how they are used in ServiceCenter and a general description of the SLA interface with other ServiceCenter modules and external sources.

Read this chapter for information about:

- *What Is a Service Level Agreement?* on page 260
- *SLM Concepts* on page 261
- *The SLM Module* on page 262
- *Status Progression* on page 267
- *Creating a Service Level Agreement* on page 269
- *SLA Maintenance Tasks* on page 279
- *Service Contracts* on page 319
- *Expense Lines* on page 329
- *Cost Assessment* on page 332
- *Entitlement Checking* on page 336
- *Viewing Contract Overruns* on page 339
- *Contract Wizard* on page 340

What Is a Service Level Agreement?

An SLA is an agreement between a service provider and a customer. An SLA can be internal, between the departments within an organization, or external, between an organization and a vendor. These agreements cover two important aspects of service:

- Availability of a specific resource within a specified time frame.
- Performance guarantees for service response times.

The Value of SLAs

SLAs manage performance tracking information and provide system feedback on service agreements between departments within a company. Use this information to quantify the level of service you receive both from within your organization and from service contracts with outside vendors and to determine if resources are available when you need them. It is important to know that when an outage occurs for a resource specified in a service agreement, the provider responds as promised.

Accumulating accurate service performance data manually and evaluating it properly over an extended period is not feasible for a large enterprise. Your organization must accumulate this data automatically to track service guarantees efficiently. You must detect the failure of a service guarantee to protect yourself from the economic consequences of lost productivity.

Using SLAs

You can use SLAs internally to track the service performance of an IT department within an organization. Service guarantees exist between IT and other departments in the organization to track object (e.g., devices or software) availability and response performance. For example, the IT department might guarantee that a development department server will be available 98% of the time and that 99% of the time IT will respond to an outage involving that device within one hour.

The SLA reflects these guarantees. The SLA also tracks compliance and show the potential economic impact of outages.

Most organizations apply SLAs in this manner:

- Focus on discrete measures of object performance, such as hardware availability.
- Add metrics for help desk performance, technician response time, and customer satisfaction.
- Assess economic impact on the enterprise resulting from SLA performance.
- Publish SLAs to the user community in an effort to increase end user satisfaction.

SLM Concepts

There are several key components in Service Level Management (SLM):

- Using clocks
- Natural progression
- SLA response phase

Read the following sections for more information.

Using Clocks

A clock is a ServiceCenter mechanism to keep track of time. In this context, clocks are used to keep track of how much time a ticket spent in an SLA response phase and how much time a ticket was in an intermediate state.

Clocks are stored in the `clocks` file and keep track of time as follows:

- In an SLA response phase, they have a clock type of `sla`. They have the same name as the phase they are tracking.
- In an Intermediate state, they have a clock type of `problem`. They have the same name as the intermediate state they are tracking.

Natural Progression

The natural progression is the path that an incident takes from the time you open it until the time you close it. This natural progression is defined in the Status Progression table of the `slacontrol` record. For more information, see *Status Progression* on page 267.

SLA Response Phase

The SLA response phase is the interval in the life of an incident that begins in one state and ends in another state. SLA response phases are defined on the Response Times tab of an SLA. An SLA response phase is one of the items that the SLM module uses to gather metrics. For example, the following table shows typical SLA response phases.

From	To
Open	Work in Progress
Open	Closed
Work in Progress	Resolved
Resolved	Closed

When defining a response phase the following rules apply:

- An SLA response must begin with a progression state, and it must end in a progression state that is farther in sequence.
- An SLA response phase may not begin or end in an intermediate state. Although an incident can go from a progression state to an intermediate state, these phases are not normally defined in the SLA because it does not make sense to collect metrics on them.

The SLM Module

The SLM module has a centralized repository of SLA information and it is fully integrated into the ServiceCenter suite of modules. The module runs automatically and continuously recalculates SLA performance.

ServiceCenter feeds availability and response metrics into the module and charts them graphically. ServiceCenter gathers outage information from sources such as incident tickets and change requests and compares the information with service guarantees to determine the status of the SLAs in the system.

The SLM module can also help prioritize incident resolution. For example, as a system administrator you can use the SLM module to escalate an Incident ticket inside ServiceCenter if the service guarantee is in jeopardy.

Interfacing with External Sources

SLM uses external event interfaces to external enterprise management sources to feed information about network status or technician performance into the SLM module, even if you have no other elements of the ServiceCenter suite installed at your site.

The SLA Configuration Record

The SLA configuration record displays control options for all the SLAs in your system. You should set up display preferences and processing options in this record before you use the Service Level Management module. You may edit the SLA configuration record at any time.

To access the SLA configuration record:

- 1 From the ServiceCenter home menu, click **Service Level Mgmt.** Figure 9-1 shows the Service Level Agreements tab.

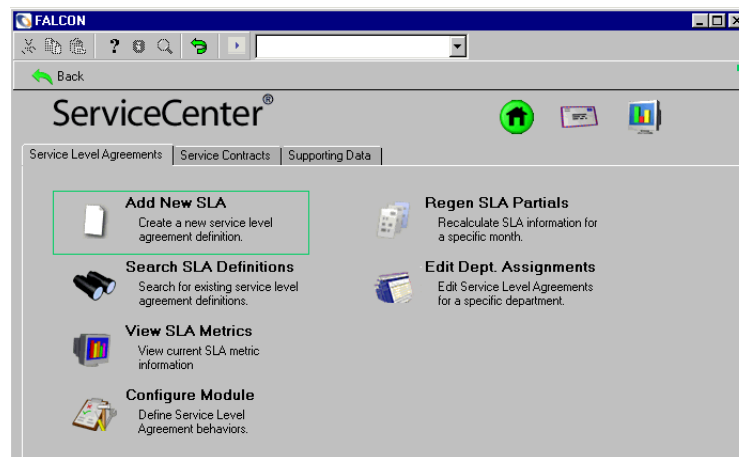


Figure 9-1: Service Level Management menu: Service Level Agreements tab

- 2 Click **Configure Module**. Figure 9-2 shows the SLA configuration record.

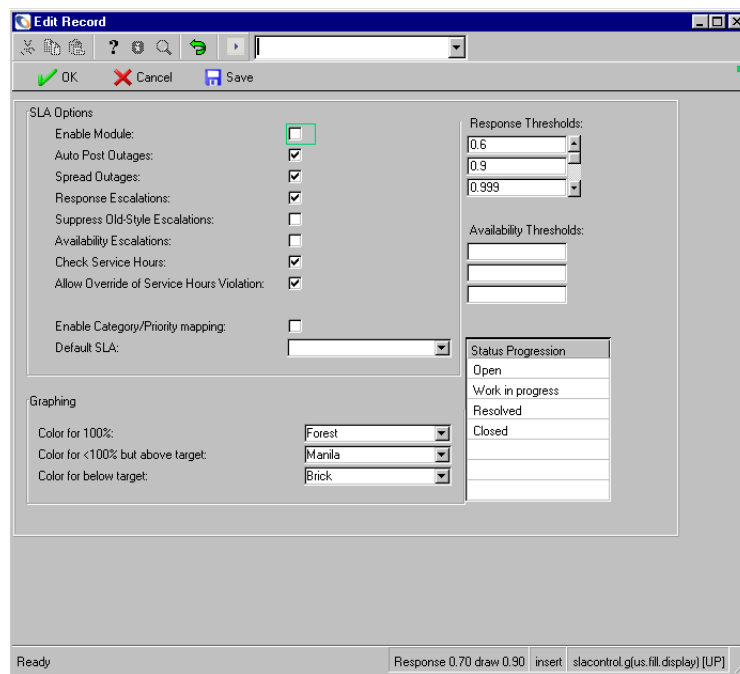


Figure 9-2: SLA configuration record

- 3 Select the desired configuration options. See these sections for a definition of each option.
 - *SLA Options* on page 265
 - *Graphing* on page 266
 - *Thresholds* on page 266
 - *Status Progression* on page 267.
- 4 Click **Save**. The status bar displays this message: **Record updated in the slacontrol file.**

Note: A single configuration record contains all control options for the SLM module.
- 5 Log out and then log in. Changes made to the SLA configuration record do not take effect until complete this step.

SLA Options

Select the following check boxes to activate the described option.

Check Box	Description
Enable Module	Enable the SLA configuration module. This selection also enables all the options selected in the SLA configuration record. You must log out and log back in for changes to this record to take effect.
Auto Post Outages	Use the open and close times of the related Incident ticket for the outage times. If you omit this option, the system prompts you for start and stop times for the outage when you open the Incident ticket.
Spread Outages	Automatically create outage records for any children of a device being reported for an outage.
Response Escalations	Escalate Incident tickets based on the percentage of allowable response time that has passed. The system uses the percentages defined in the Response Thresholds array to set Alert Stages. If the array is blank, the system uses default percentages. For more information, see Thresholds on page 266.
Suppress Old-Style Escalations	Disable the category-driven model for escalating Incident tickets.
Availability Escalations	Escalate Incident tickets based on the percentage of allowable downtime elapsed. The system uses the percentages defined in the Availability Thresholds array to set Alert Stages. If the array is blank, the system uses default percentages. For more information, see Thresholds on page 266.
Check Service Hours	Prevent users from opening Incident tickets outside of the service hours defined in the SLA. A dialog box advises the user that service is unavailable.
Allow Override of Service Hours Violation	Override the service hours limitations.
Enable Category/Priority Mapping	Whenever opening an Incident with a specific Department/Category/Priority, it is assigned a specific SLA.
Default SLA	The default SLA to use when opening Incident tickets when no specific SLA exists for the contact's department or the company.

Graphing

You can specify colors for your graphs from drop-down lists to show object performance percentages.

Field	Description
Color for 100%	Possible color choices are: Black, Red, Green, Blue, Gray, Light Gray, Dark Gray, Yellow, Cyan, Magenta, Navy, Forest, Purple, Teal, Brick, and Manila
Color for <100% but above target	Possible color choices are: Black, Red, Green, Blue, Gray, Light Gray, Dark Gray, Yellow, Cyan, Magenta, Navy, Forest, Purple, Teal, Brick, and Manila
Color for below target	Possible color choices are: Black, Red, Green, Blue, Gray, Light Gray, Dark Gray, Yellow, Cyan, Magenta, Navy, Forest, Purple, Teal, Brick, and Manila

Thresholds

You can specify threshold values for response and availability escalation.

Field	Description
Response Thresholds	<p>Determines the values for the Response Escalations option. Enter percentages in the array for setting Alert stages. For example, values set at 0.55, 0.75 & 0.85 escalate an Incident ticket in the following stages:</p> <ul style="list-style-type: none"> ■ Alert Stage I at 55% of the guaranteed response time ■ Alert Stage II at 75% of the guaranteed response time ■ Alert Stage III at 85% of the guaranteed response time
Availability Thresholds	<p>Determines the values for the Availability Escalations option. Enter percentages in the array for setting Alert stages. For example, values set at 0.55, 0.75 & 0.90 will escalate an Incident ticket in the following stages:</p> <ul style="list-style-type: none"> ■ Alert Stage I when 55% of the allowable downtime has elapsed ■ Alert Stage II when 75% of the allowable downtime has elapsed ■ Alert Stage III when 90% of the allowable downtime has elapsed

If you leave the threshold fields blank and select the **Response Escalations** and **Availability Escalations** options, the system uses these default:

- Alert Stage I at 50%
- Alert Stage II at 75%
- Alert Stage III at 90%

Status Progression

ServiceCenter includes two status types:

- Natural progression state
- Intermediate state

Natural Progression State

This state defines the natural progression or natural path that an incident may take from the time it is opened to the time it is closed. The natural progression goes from a lower progression sequence number to a higher progression sequence number. ServiceCenter ships with the following progression states.

Progression Sequence Number	Natural Progression State
1	Open
2	Work in Progress
3	Resolved
4	Closed

Given these progression states, an incident ticket naturally goes from Open, to Work in Progress, to Resolved, and then to the Closed state.

Intermediate States

This state, also known as a lateral progression state, refers to status that occurs outside of the natural progression that an incident takes during its lifetime. ServiceCenter ships with the following intermediate states:

- Pending customer
- Pending other
- Pending vendor

- Referred
- Reject
- Replaced problem
- Suspended

Rules for Natural Progression and Intermediate States

There are certain rules that govern the use of natural progression and intermediate states:

- A ticket may go from a natural progression to an intermediate state. When it returns to the natural progression cycle, it must return to a natural progression state that has the same or greater progression sequence number than it was before moving into the lateral progression state. The following table shows an example.

Action	State
Open incident	Open (a progression state)
Assign incident	Work in progress (a progression state)
Suspend the ticket for some reason.	Suspended (an intermediate state)

When work resumes and you are ready to move the ticket from a suspended state, the ticket state can be Work in Progress, Resolved, or Closed. The ticket cannot have an Open state because Open is a natural progression state that has a lower progression sequence number than Work in Progress, which is the natural progression state that the ticket was in before moving into the lateral progression state.

- You can define new states in the `pmstatus` file. If you define a new state and put it in the SLA progression table, it becomes a valid progression state. If you do not put the new state in the SLA progression table, it is an intermediate state.
- If you define a progression state, it must fall between the Open and Closed states. You cannot specify that the new state occurs before the Open state or after the Closed state.
- You can define a state only once in the Status Progression table.
- You may not put a ServiceCenter-defined intermediate state in the Status Progression table.

- You can define intermediate states as suspended states only by specifying that intermediate state in the Suspend Response Processing for these states field on the Misc. tab of the SLA record.

When an incident moves from a progression state to an intermediate state that is not a suspended state, the SLA Response Phase clocks continue to tick. However, when an incident moves from a progression state to an intermediate state that is a suspended state, the clock stops ticking during the time the incident is in the suspended state. It starts ticking again when the incident returns to a progression state or to an intermediate state that is not a suspended state.

Creating a Service Level Agreement

Each SLA record has three types of data.

Data type	Description
Descriptive	General description of the agreement
Availability	Specific terms of object availability (for example, schedule, downtime cost, and importance)
Response	Guaranteed response times

To create an SLA record:

- 1 From the ServiceCenter home menu, click the **Services** Tab and select **Service Level Mgmt.** Figure 9-3 shows the Service Level Agreements menu.

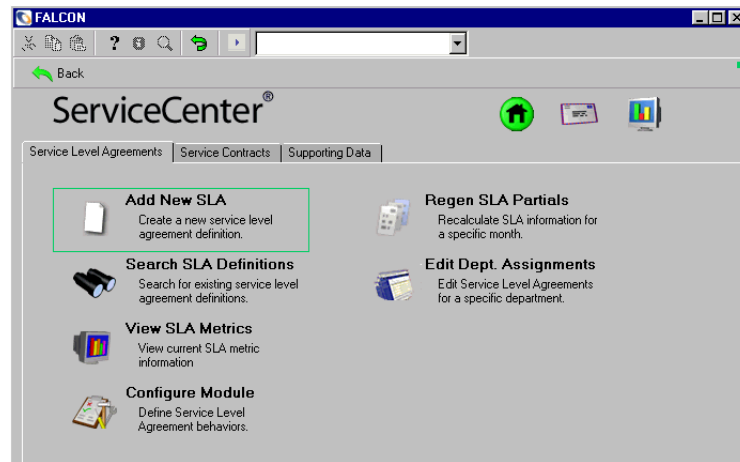


Figure 9-3: Service Level Agreements menu

- 2 Click **Add New SLA**. Figure 9-4 shows an SLA Record form.

 The screenshot shows a web browser window titled "ServiceCenter - [New Service Level Agreement]". The form has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Add, Find, and Fill. Below the toolbar, there are several input fields:

- Agreement ID:** A text input field.
- Expiration:** A date input field.
- Title:** A text input field.
- Service Hours:** A dropdown menu.
- Target:** A text input field.
- Dept Full Name:** A text input field.

 Below these fields, there are five tabs: "Description", "Availability", "Response Times", "Misc.", and "Attachments". The "Description" tab is active, showing a large text area for entering the description. The status bar at the bottom indicates "Ready" and "Response 0.521 draw 0.70 insert sla.edit.g(sla.edit.record) [UP]".

Figure 9-4: Blank SLA record form

- 3 Type values in the **Expiration**, **Title**, **Service Hours**, **Target**, and **Dept Full Name** fields. For more information, see *Each new SLA requires some header information.* on page 271.
- 4 Type a description of the SLA on the Description tab. For more information, see *Description Tab* on page 272.
- 5 Click the **Availability** tab. Specify the availability for the SLA. For more information, see *Availability Tab* on page 272.
- 6 Click the Response times tab. Type the response times for the SLA. For more information, see *Response Times Tab* on page 274.
- 7 Click the Misc. tab. Specify the Miscellaneous Guarantees for the SLA. For more information, see *Misc. Tab* on page 276.
- 8 Add any attachments to the SLA in the Attachments tab. For more information, see *Attachments Tab* on page 277.
- 9 Click **Add** to add the SLA definition to the database. The system assigns an Agreement ID number to the record and adds additional system tray buttons. Each new SLA requires some header information.

Field	Description
Agreement ID	Unique, system-generated identification number for your new agreement. This number is used internally by the system to track relationships between SLAs and their supporting data. The system assigns an Agreement ID number when the record is added to the database.
Expiration	Expiration date of this agreement.
Title	Unique title provided by the user. Be sure you give your SLA a title that adequately describes the nature of the agreement. The contents of this field is used in reports and elsewhere.
Service Hours	Calendar options in ServiceCenter. Select a shift from the drop-down list to define the service hours of the SLA. The system uses the value in this field to determine service rights of a caller on this SLA.
Target	Performance target of the SLA. The value is expressed as a percentage and is used by the system to determine if the SLA is meeting its performance goals.
Dept Full Name	Full name of the user's department, as defined in the Department form. This information is filled in automatically if it is included in the user's profile.

Description Tab

Use the blank space for a text description of the terms of your SLA agreement. Because this is the only place in the SLM module where this information appears, you should make this description as clear and precise as possible. Figure 9-5 shows the blank area on the Description tab.

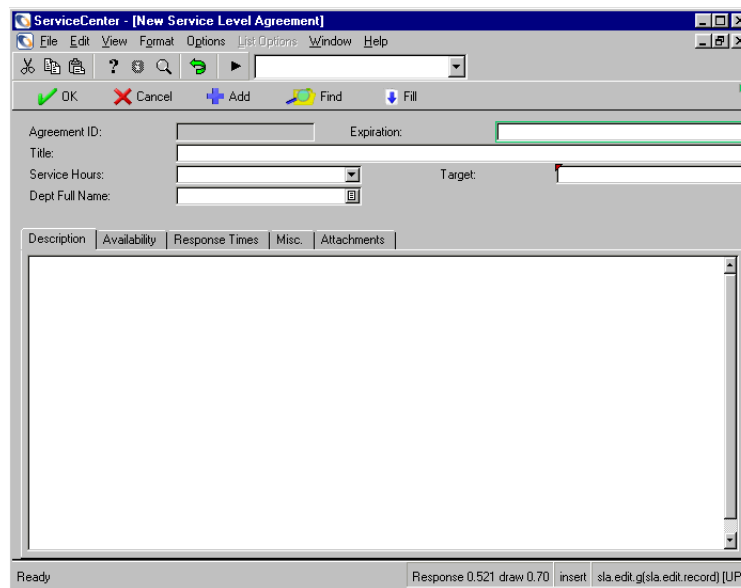


Figure 9-5: Description tab in an SLA record

Availability Tab

The Availability tab shows the guaranteed object availability for your SLA. This data is used by ServiceCenter to track such things as outage costs and the service calendar. Figure 9-6 on page 273 shows the Availability tab.

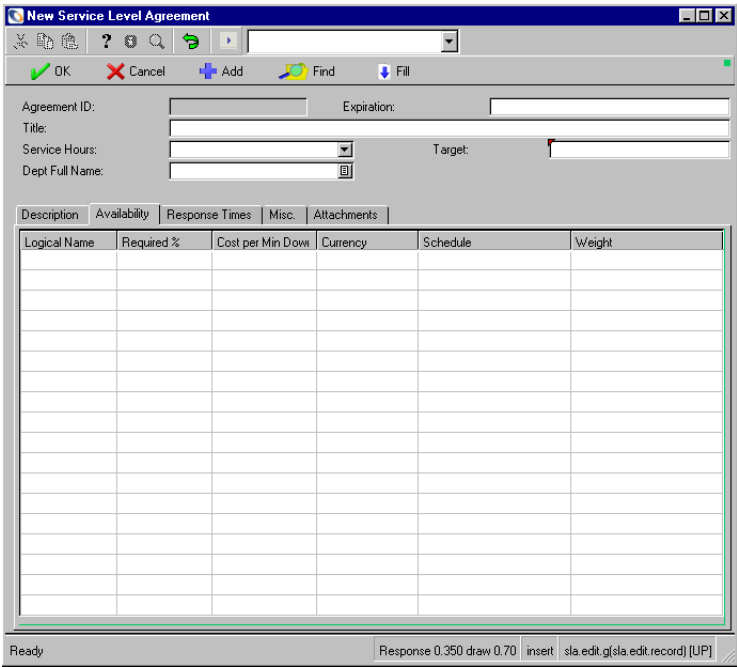


Figure 9-6: Availability tab in an SLA record

The following table identifies the columns on the Availability tab.

Field	Description
Logical Name	Name of the object whose availability is guaranteed by the SLA. This name must appear in the ServiceCenter inventory device file.
Required %	Target availability percentage of the object.
Cost Per Min Down	Cost of a minute of downtime for the object. The system analyzes this data to calculate costs of outages.
Currency	Currency on which this SLA is based. The value in this field is a three letter code from the currency file (for example, FRF for French Franc).

Field	Description
Schedule	Calendar options in ServiceCenter. You can select a predefined work shift from the drop-down list. If this field is left blank, the system assumes that 24x7 operation is required.
Weight	Value used by the system to calculate the relative importance of the object to the overall status of your SLA. The larger the number, the greater the impact of the object on the SLA. This value has no unit of measurement or scale limitations.

Response Times Tab

The Response Times tab shows the guaranteed response times for the objects in your SLA. ServiceCenter uses this data to track things such as service response times and the response calendar. Figure 9-7 shows the Response Times tab.

The screenshot shows a software window titled "New Service Level Agreement". It has a menu bar with icons for file operations and a toolbar with buttons for OK, Cancel, Add, Find, and Fill. Below the toolbar are input fields for Agreement ID, Title, Service Hours (a dropdown menu), Dept Full Name (with a selection icon), Expiration, and Target. A tabbed interface is present with tabs for Description, Availability, Response Times (which is selected), Misc., and Attachments. The "Response Times" tab contains a table with the following columns: Initial State, Final State, Name, Acceptable, Schedule, and Weight. The table is currently empty. At the bottom of the window, a status bar displays "Ready" and "Response 0.180 draw 0.71 insert sla.edit.g[sla.edit.record] [UP]".

Figure 9-7: Response Times tab in an SLA record

The following table describes the column headers on the Response Times tab.

Field	Description
Initial State	Initial Incident ticket states (for example, Open or Work in Progress, found in the drop-down menu). The system tracks and analyzes the SLAs of all tickets within the range of states defined in this field and in the Final State field. Note: Enter a value in this field only if the ServiceCenter Incident Management module is implemented in your system.
Final State	Final Incident ticket <i>states</i> (for example, Open or Work in Progress, found in the drop-down menu). The system tracks and analyzes the SLAs of all tickets within the range of states defined in this field and in the Initial State field. Note: Enter a value in this field only if the ServiceCenter Incident Management module is implemented in your system.
Name	Response name for the object. The name you give your response must be UNIQUE within this SLA (for example, Time to Repair), but the same name may appear in other SLAs. This name is used in reports and by external feeds to post response data into the system.
Acceptable	Target time for response of this object. You should use the format 00:00:00, when entering data in this field.
Schedule	Calendar options in ServiceCenter. You can select a predefined work shift from the drop-down list. If this field is left blank, the system assumes that 24x7 operation is required.
Weight	Value used by the system to calculate the relative importance of this response to the overall status of your SLA. The larger the number, the greater the impact of the response on the SLA. This value has no unit of measurement or scale limitations.

Misc. Tab

The Misc. tab displays information about additional guarantees that specifically concern the resolution of Incident tickets associated with this SLA. Figure 9-8 shows the Misc. tab.

The screenshot shows the 'ServiceCenter - [Edit SLA Record]' window. The 'Misc.' tab is active. Fields include: Agreement ID: 209, Title: SLA006, Service Hours: day shift, Dept Full Name: PRGN/Research & Developme, and Expiration: 12/31/02 00:00:00. The 'Misc.' tab contains a section for 'Tickets on this SLA must be resolved in:' with a value of 00:20:00, and 'Suspend Response Processing for these states:' with a dropdown menu showing 'Pending customer'.

Figure 9-8: Misc. tab in an SLA record

The following table describes the fields that appear on the Misc. tab.

Field	Description
Tickets on this SLA must be resolved in	Guaranteed time to resolution for any ticket affected by this SLA. Optional time limit for resolution of Incident tickets associated with this SLA. This guarantee covers the entire Incident cycle. You should use the format 00:00:00, when entering data in this field.

Field	Description
On this schedule	Work shift in which any ticket affected by this SLA must be resolved. Select a work shift from the drop-down list indicating when the associated Incident ticket must be resolved.
Suspend Response Processing for these states	<p>Suspends response time limits when the SLA is in this state. When an incident goes from a progression state to an intermediate state that is defined as a suspended state, the clock stops ticking during the time the incident is in the suspended state. It starts ticking again when the incident goes back to a progression state or to an intermediate state that is not defined as a suspended state.</p> <p>For example, response time spent waiting for a vendor to provide parts should not be charged to this SLA. In this case the state would be set at Pending vendor.</p> <p>Select a state (for example, Pending vendor) from the drop-down list. You can designate more than one state by using more than one field. Any delays encountered during these times will not be figured into the response calculations for the SLA.</p>

Attachments Tab

The Attachments tab uses an OLE container to store related attachments. Insert any document associated with this SLA into the Attachments tab. To view an attached document, double-click the button to open the item with the program that created it. Figure 9-9 on page 278 shows the Attachments tab.

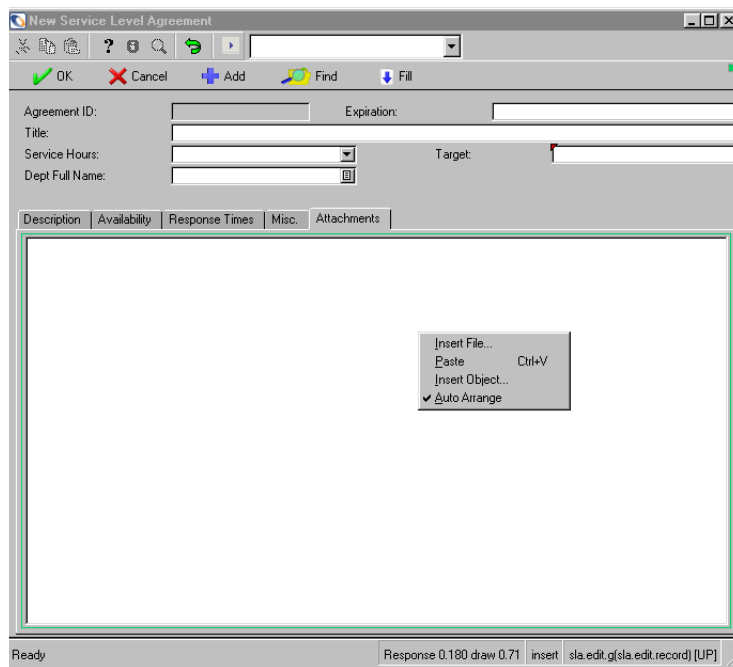


Figure 9-9: Attachments tab in an SLA record

Inserting Attachments

Use one of three methods to insert a file in the Attachments tab:

- Drag and drop an existing file into the Attachment tab.
- Insert an existing file
- Create a file to insert

To insert an existing file:

- 1 Right-click the Attachments tab.
- 2 Select **Insert File** from the shortcut menu.
- 3 Browse for the file you want to insert.
- 4 Do one of the following:
 - Double-click the file.
 - Select the file and click **Open** to insert the document. It is not necessary to save the record to save the changes. When you select the option, ServiceCenter inserts the document into the record permanently.

To create a file to insert:

- 1 Right-click the Attachments tab.
- 2 Select **Insert Object** from the shortcut menu.
- 3 Select **Create New** in the Insert Object dialog box.
- 4 Select an Object Type from the list.
- 5 Click **OK**. A new document appears in the program you selected.
- 6 Create a document to attach and save it. Your new document automatically attaches to the SLA record.

To delete a document from the Attachments tab:

- 1 Select the document you want to delete. A frame appears around the document.
- 2 Right-click the **Attachments** tab.
- 3 Select **Delete** from the shortcut menu. It is not necessary to save the record to save the changes. ServiceCenter removes the document from the record when you click Delete.

SLA Maintenance Tasks

There are common tasks associated with SLAs. You can perform any of the following SLA maintenance tasks:

- Edit an SLA. See *Editing an SLA Record* on page 280.
- Delete an SLA. See *Deleting an SLA Record* on page 281.
- Recalculate response time. See *Recalculating Outage Data* on page 282.
- Assign an SLA. See *Assigning an SLA to a Department* on page 283.
- Map category or Priority. See *Category and Priority Mapping* on page 285.

Editing an SLA Record

Follow these steps to edit an existing SLA record:

- 1 From the ServiceCenter home menu, click **Service Level Mgmt.** The Service Level Agreements menu shown in Figure 9-3 on page 270 appears.
- 2 Click **Search SLA Definitions.** Figure 9-10 shows the SLA search form.

Figure 9-10: SLA search form

- 3 Click **Search** or press **Enter** to display a list of all SLAs. If you have Records selected on the View menu, ServiceCenter displays the first record in the SLA record form, as shown in Figure 9-11 on page 281.

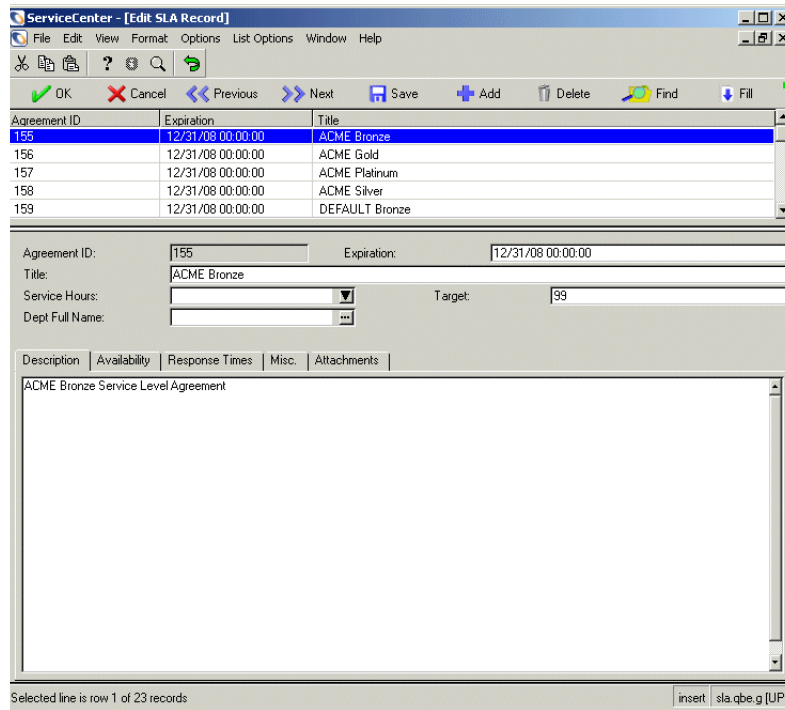


Figure 9-11: SLA record displaying a record list

- 4 Select the SLA you want to edit from the SLA Record list.
- 5 Edit the SLA record as required.
- 6 Click **Save**. The status bar displays a message that the record is updated in the sla file.

Deleting an SLA Record

Follow these steps to delete an existing SLA record:

- 1 From the ServiceCenter home menu, click **Inventory Management**.
- 2 Click **SLA Information**. The SLA Search form appears.

- 3 Do one of the following.
 - Find the SLA you want to delete. Type the SLA **Agreement ID** or **Title** and click **Search** or press **Enter**.
 - If you do not know the Agreement ID or Title, leave the form blank and click **Search** to perform a true query and retrieve a list of all current SLA records. From the displayed queue screen, select the record you want to delete.

The appropriate information appears in the SLA record form below the record list.

- 4 Click **Delete** to delete the SLA.
- 5 The status bar displays a message that prompts you to confirm your action. Click **Yes** to delete the record.

Recalculating Outage Data

The Regen SLA Partial function recalculates SLA outage records for a specified month and year.

To regenerate outage records:

- 1 From the ServiceCenter home menu, click **Service Level Mgmt.** The Service Level Agreements menu displays.
- 2 Click **Regen SLA Partial**. Figure 9-12 shows the Recalculate SLA Totals form.



Figure 9-12: Form for recalculating SLA totals

- 3 Type the month and year for the recalculation.
- 4 Click **Proceed** to recalculate outages for the time period specified.

- 5 When the Regen Completed prompt appears, click OK. You will return to the Service Level Agreements menu.



- 6 Click **View SLA Metrics** to display the results of the recalculation. For more information, see *Performance Views* on page 287.

Assigning an SLA to a Department

The SLA basic mapping feature assigns a default SLA to each department by using the ServiceCenter Department Data record. When first-level support personnel enter a caller ID into a report opened with another ServiceCenter module, the system identifies the caller's department and automatically assigns the default department SLA to the report. Basic mapping creates the default configuration for the SLM module.

Basic Mapping

To assign default department SLAs:

- 1 From the ServiceCenter home menu, click the **Toolkit** tab.



- 2 Click **Database Manager**. Figure 9-13 shows the blank Database Manager dialog box.

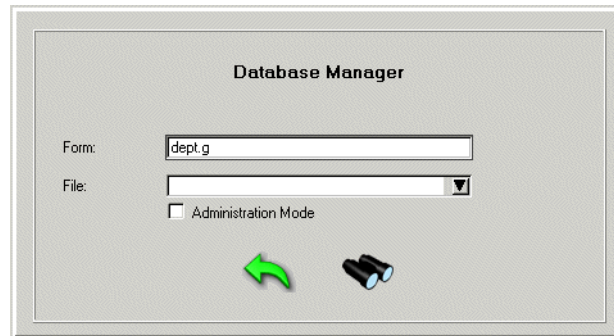


Figure 9-13: Database Manager dialog box

- 3 Type **dept.g** in the **Form** field of the Database Manager dialog box.



- 4 Click **Search** or press **Enter**.

- 5 Figure 9-14 shows a blank Department Data form. Click **Search** or press **Enter**.

Figure 9-14: Blank Department Data record

- 6 The first department record in the system displays accompanied by a record list of all the department records at the top if Records are enabled on the View menu, as shown in Figure 9-15. Otherwise, a record list appears. Select a record to view.

Dept	Dept Code	Company	Dept Full Name
ACME/Administration	1000	ACME	Administration
ACME/Asia Sales	Asia Sales	ACME	Asia Sales
ACME/Customer Supp	500000	ACME	Customer Support
ACME/Executive	1002	ACME	Executive

Figure 9-15: Department record and record list

- 7 Select the name of the department you want to view. Information for this department appears in the Department Data form.
- 8 Select the SLA you want to use as the department default from the drop-down list in the SLA field.
- 9 Do one of the following:
 - Click **Save** to update the record in the department file. The status bar displays this message: **Department record updated**.
 - Click **Add** if you are adding a new department. The status bar displays this message: **Department record added**.

Category and Priority Mapping

Category/Priority Mapping determines which SLA should be applied to a report, based on a combination of factors:

- Caller's department
- Call category
- Priority of the call

Category/Priority mapping features are controlled by the Configuration module. For more information, see [Recalculating Outage Data](#) on page 282. When the **Enable Category/Priority mapping** option is selected in the SLA configuration record, the system selects the appropriate SLA from the department assignments table.

There are two levels to this type of mapping:

- Priority Assignments
- Category Assignments

Assignments

This level of mapping defines SLAs based on both category and priority. When first-level support personnel enter a caller's ID into a record opened in another ServiceCenter module (for example, Service Management or Incident Management), the system identifies the caller's department and automatically assigns the default SLA defined for that priority level to the report.

To define category assignments for a department:



- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu appears.
- 2 Click **Edit Dept. Assignments**.

Figure 9-16 shows a dialog box with a drop-down list of SLA assignments.

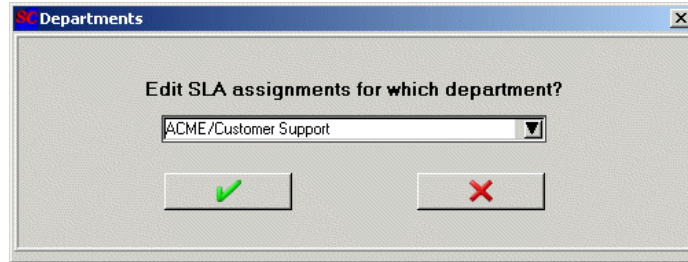


Figure 9-16: Edit Departments dialog box

- 3 To define an SLA, select the name of the department.
- 4 Click OK. Figure 9-17 shows the **SLA Assignments for Department** form that shows the default SLAs for the department by category and priority.

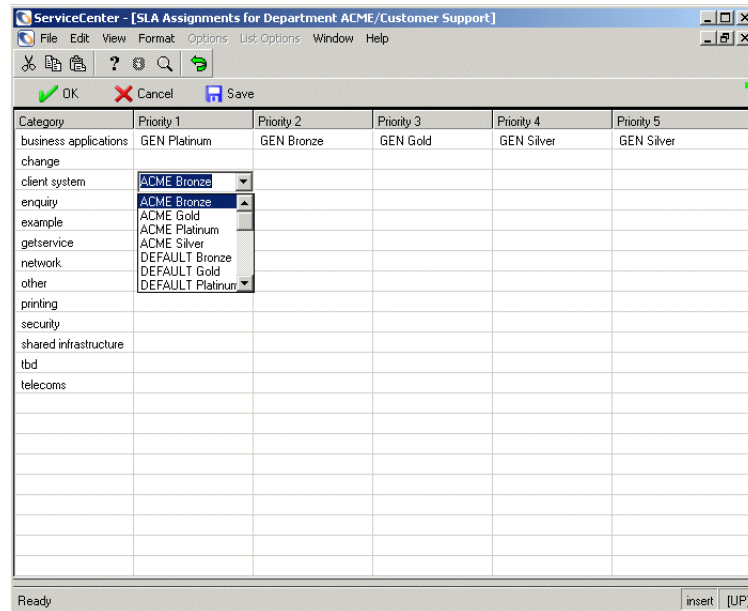


Figure 9-17: SLA assignments

- 5 Select the SLAs you want the system to use for particular combinations of categories and priorities from the drop-down lists in each cell.

If no SLA has been assigned to a category/priority, the system uses the default SLA for that priority. In the example above, call reports in the **client systems** category with a priority of 1 use the **ACME Bronze** SLA.

- 6 Click **Save**.

Performance Views

Service Level Management provides the user with a comprehensive view of SLA performance from an overall perspective to a focus on individual devices and response types. The performance analysis workflow chart shows the drill-down levels available in the SLA performance view. These measurement classifications are referred to as *metrics*. There are two types of metrics in Service Level Management:

- Availability Agreements guarantee the availability of a resource for a specified time. For more information, see [Availability Data](#) on page 288.
- Response Agreements guarantee response times for certain types of help desk requests. For more information, see [Response Time Data](#) on page 301.

Figure 9-18 on page 288 shows the performance workflow chart.

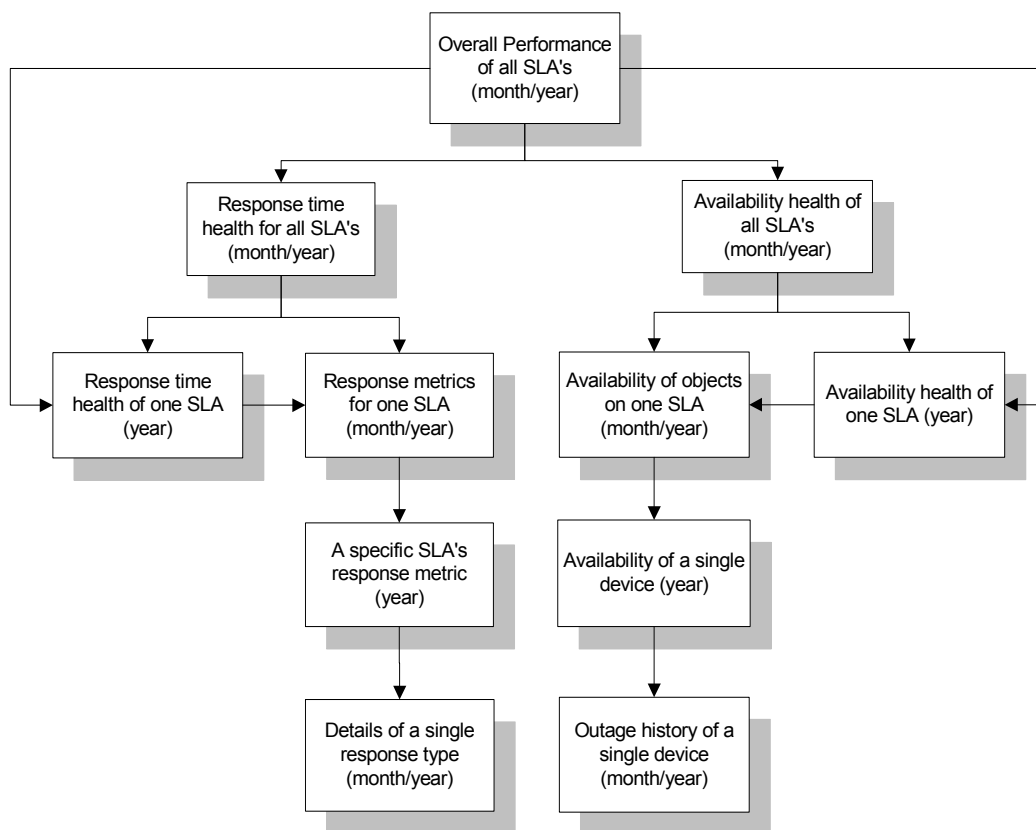


Figure 9-18: Performance analysis workflow

Availability Data

SLA availability data is used to track object availability (for example, a server or an application). The SLM module gathers the following information about objects in the system from agreement records:

- Target availability percentage
- Availability schedule
- Dollar cost for outages
- Importance of the object to the overall performance of the SLA

Accessing SLA Metrics

- 1 Click Service Level Mgmt. in the ServiceCenter home menu, as shown in Figure 9-19.

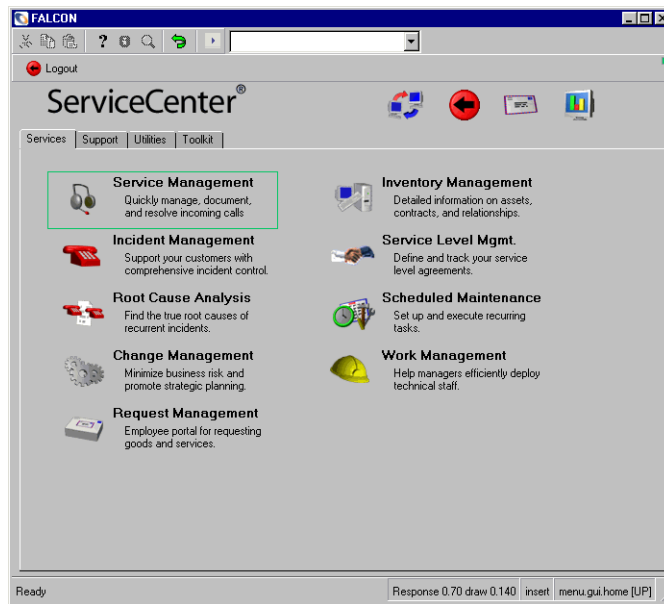


Figure 9-19: ServiceCenter home menu

Figure 9-20 shows the Service Level Agreements menu.

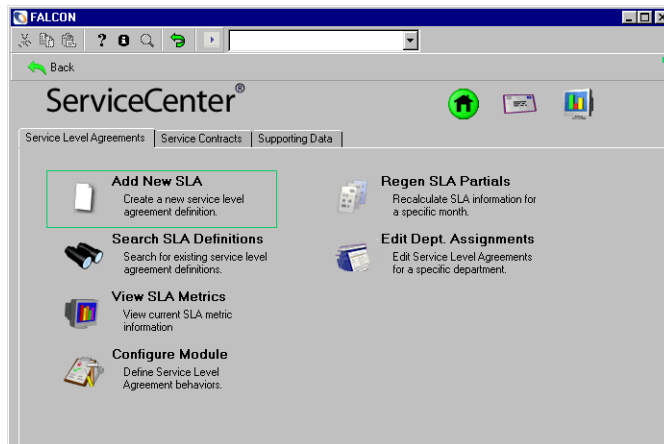


Figure 9-20: Service Level Agreements menu

2 Click View SLA Metrics.

Figure 9-21 shows the SLA Overall Performance form that displays the overall performance for SLAs in your system for the month selected.

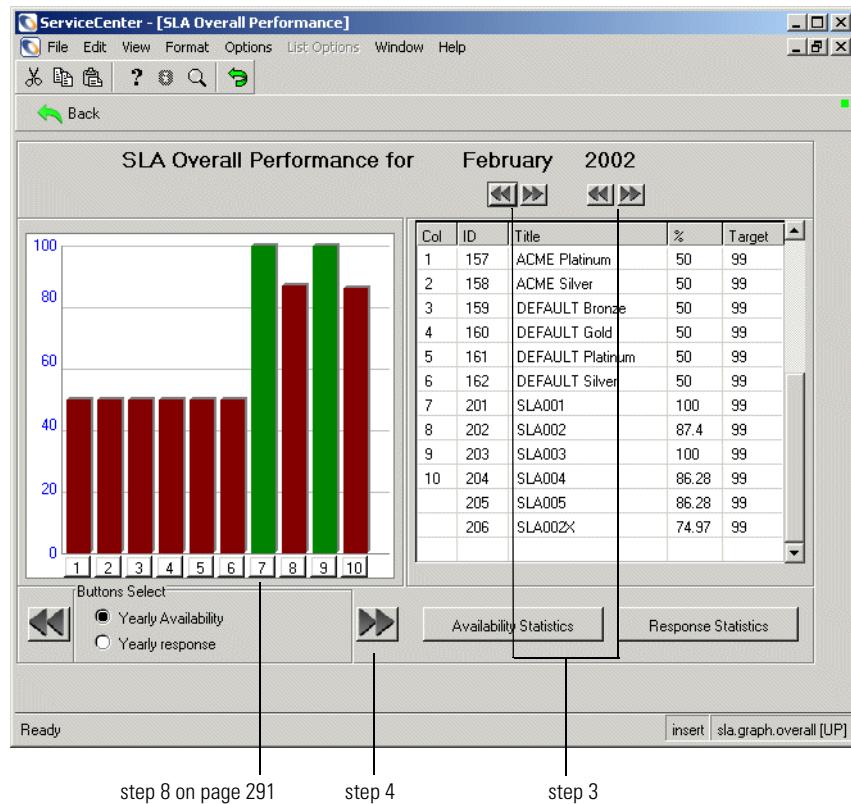


Figure 9-21: SLA overall performance

- 3 Use the directional buttons above the table to change the month or year.
- 4 Use the directional buttons beneath the chart to display additional entries within the table when more than 10 SLAs are listed. Each click of a directional button shifts button assignments 10 places up or down and displays the appropriate entries in the table.
- 5 Select the view by selecting the **Yearly Availability** or **Yearly Response** radio buttons beneath the color chart. For more information, see [Response Metric Performance for One Year](#) on page 309.
- 6 Click **Availability Statistics** to display the availability status of all your SLAs. Return by clicking **Back**.

- 7 Click **Response Statistics** to view the Response statistics. Return by clicking **Back**.
- 8 Click a numbered column button to display the availability status of a single SLA for one year.

Column Description

Col	Column numbers correspond to the numbers on the x-axis of the graph on the left-hand side of the screen.
ID	Unique identifier for an SLA.
Title	Description of the SLA
%	Overall performance of the SLA for the month. This is a pure average of the Availability performance percentage and the Response performance metric.
Target	This is the target percentage specified on the SLA.

Availability status of all SLAs

The availability performance characteristics described in this section are for all the SLAs in your system. The table compares actual performance levels with the target performance guaranteed by the SLA. The color chart displays the same performance data as that given in the table, but in a visual format. The chart also provides access buttons for moving to the next level. For more information, see [Recalculating Outage Data](#) on page 282.

To access SLA availability performance information:

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu appears.



- 2 Click **View SLA Metrics**. The SLA Overall Performance form appears.
- 3 Click **Availability Statistics**.

Figure 9-22 shows the SLA Availability Performance form, which displays the availability performance of all SLAs in your system.

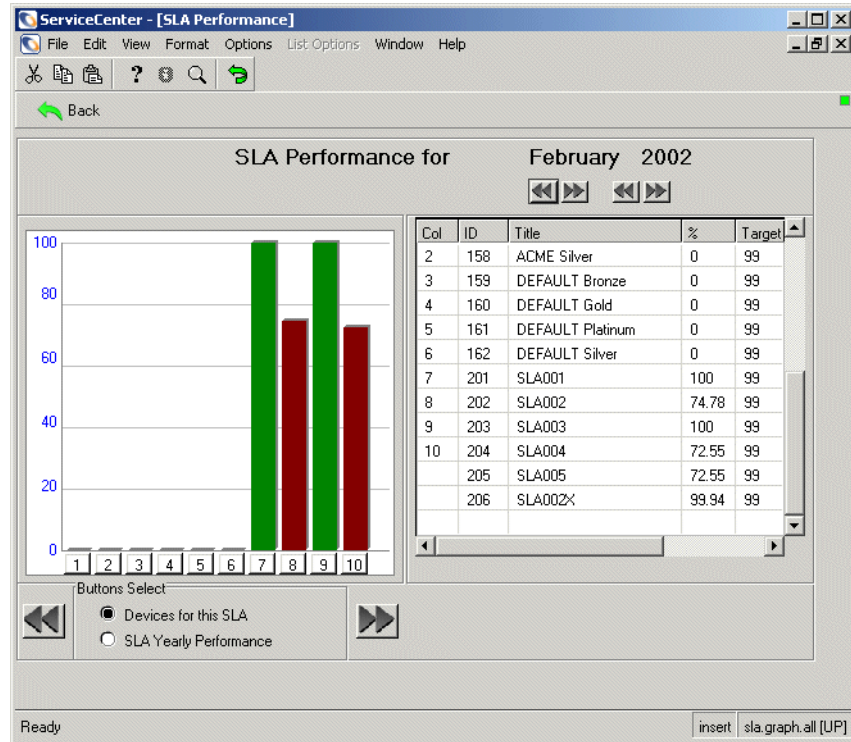


Figure 9-22: SLA availability performance form

The following table describes the buttons on the SLA Performance form.

Button	Action
Devices for this SLA	Select this option to display the devices for a single SLA. Click a numbered column button beneath the column corresponding to the SLA you want to view. An SLA Availability Performance form appears. This form provides the object (device) availability for the corresponding SLA listed in the table in the SLA Overall Performance form.
SLA Yearly Performance	Select this option to display the yearly performance for a single SLA. Click a numbered column button beneath the column corresponding to the SLA you want to view. A form displaying the yearly performance information for a single SLA appears.

Availability status of a single SLA

The availability performance characteristics described in this section are for individual SLAs in your system. The table lists actual performance levels achieved for a single SLA in each month of a given year. The color chart displays the same performance data as that given in the table, but in a visual format. The chart also provides access buttons for displaying performance data for a single object (device or application) in an SLA. For more information, see *Recalculating Outage Data* on page 282.

To access the yearly performance information for a single SLA:

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu appears.
- 2 Click **View SLA Metrics**. The SLA Overall Performance form appears.
- 3 Select the **Yearly Availability** option beneath the chart.
- 4 Do one of the following:
 - Click a numbered column button. Yearly performance information for the SLA selected from the table in the SLA Overall Performance form appears.
 - Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu appears.
- 5 Click **View SLA Metrics** in the Service Level Agreements menu. The SLA Overall Performance form appears.
- 6 Click the **Availability Statistics** button. The SLA Availability Performance form appears.
- 7 Select the **SLA Yearly Performance** option beneath the chart.
- 8 Click a numbered column button.

Figure 9-23 shows the yearly performance information for the SLA selected from the table in the SLA Overall Performance form.

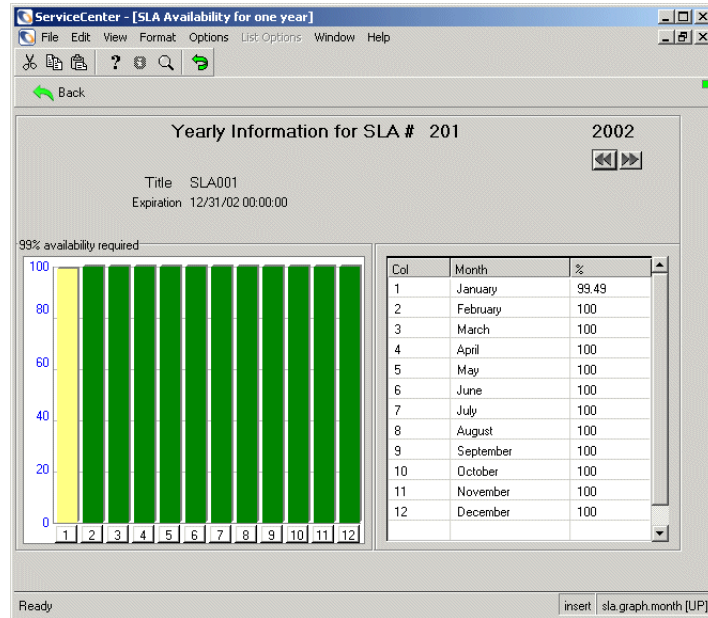


Figure 9-23: Yearly performance information for a single SLA

The following table describes the fields on the Yearly Information form.

Field	Description
<%> Availability Required	The label on the structure around the color chart indicates the general availability of the SLA as guaranteed in the agreement.
Col	The numbers, representing months, on the x-axis of the graph on the left-hand side of the screen

Field	Description
Month	Months of the year indicated on the right side of the form.
%	<p>The weighted average of the uptime percentage for the month for all devices covered in the SLA. The derivation of this figure is as follows:</p> $((Dn * DnW) + \dots (Dn * DnW)) / (DnW + \dots DnW)$ <p>where</p> <p>Dn is the uptime percentage of Device n for the month</p> <p>DnW is the weight assigned to Device n (specified on the Availability tab of the SLA)</p> <p>This formula can also be stated as follows:</p> <p>(the sum of (the uptime percentage*its corresponding weight) for all devices in the SLA) / (the sum of all the weights)</p> <p>Note: The total available time for a month for a device depends upon the Calendar schedule that the device is on. (This is specified in the Availability tab of the SLA.) This is taken into consideration when calculating the availability percentage. The uptime for a device would be:</p> $((\text{total available time for the month}) - (\text{total time device was down for the month})) / (\text{total available time for the month})$

Button selection

To view the availability of objects in a single SLA, click the numbered column button in the chart that corresponds to the desired month in the table.

Availability of Objects in a Single SLA

The availability performance characteristics described in this section are for all objects (devices) in a single SLA. The table in the **Device Availability for a SLA** compares actual performance with the target performance guaranteed by the agreement. The color chart displays the same performance data in a visual format as that shown in the table. The chart also provides access buttons for displaying outage histories for each device listed. For more information, see [Recalculating Outage Data](#) on page 282.

Method 1: Access performance information for all devices in a single SLA

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu appears.

2 Click View SLA Metrics.

The SLA Overall Performance form displays. Select the **Yearly Availability** option beneath the chart.

3 Click a numbered column button. The yearly performance of the selected SLA appears, corresponding to the SLA listed in the table in the SLA Overall Performance form.**4 Click a numbered column button.** Performance information for all devices in a single SLA appears.**Method 2: Access performance information for all devices in a single SLA****1 Click Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu appears.**2 Click View SLA Metrics** in the Service Level Agreements menu. The SLA Overall Performance form appears.**3 Click Availability Statistics.** The SLA Availability Performance form appears.**4 Select the Yearly Performance** option beneath the chart.**5 Click a numbered column button.** The yearly performance of the selected SLA appears, corresponding to the SLA listed in the table in the SLA Overall Performance form.**6 Click a numbered column button.**

Figure 9-24 shows performance information for all devices in a single SLA.

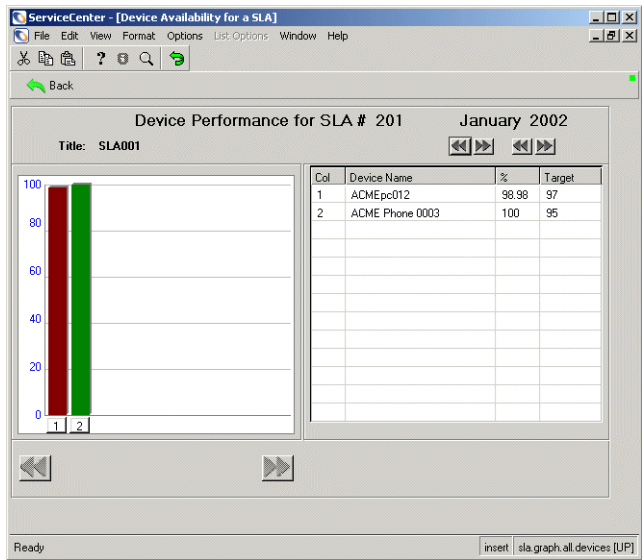


Figure 9-24: Performance information for devices in a single SLA

The following table describes the fields on the Device Performance form.

Field	Description
Col	Column numbers correspond to the numbers on the x-axis of the graph on the left-hand side of the screen.
Device Name	Logical names of the device.
%	<p>The uptime percentage of the device for the month. The derivation of this figure is:</p> <p>((total available time for the month) - (total time device was down for the month)) / (total available time for the month)</p> <p>Note: The total available time of a device for a month depends upon the Calendar schedule that the device is on. (See the Availability tab of the SLA record.)</p>
Target	The targeted uptime percentage for the device. This is specified on the Required % field on the Availability tab of the SLA record.

Button selection

To view the yearly performance of a single object (device or application), click the numbered column button that corresponds to the object listed in the table.

Availability of a Single Device

The availability performance characteristics described in this section are for a single device in an SLA. The table shown in the form lists actual performance levels achieved for each month of a given year. The color chart displays the same performance data in a visual format and provides access buttons for displaying performance data for a single device (device or application). For more information, see *User Profiles* on page 21.

Access the availability performance information for a single device in an SLA from the **Device Availability for a SLA** form shown in Figure 9-24 on page 297. For more information, see *Availability of Objects in a Single SLA* on page 295.

- Click a numbered column button in the chart on the left side. Figure 9-25 shows a form with the availability information for the selected device for one year.

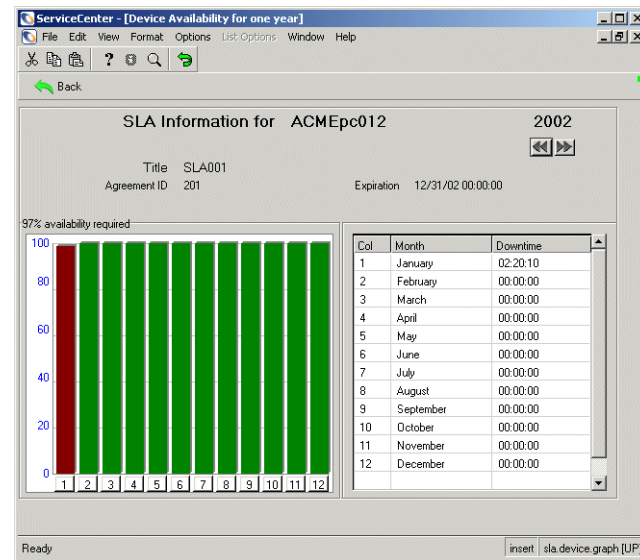


Figure 9-25: Performance information for a single device

The following table describes the fields on the SLA Information form.

Field	Description
<%> Availability Required	The label on the structure around the chart indicates the general availability of the SLA as guaranteed in the agreement.
Col	Column numbers correspond to the numbers on the x-axis of the graph on the left-hand side of the screen.
Month	Months of the year that is indicated on the right-hand side of the form.
Downtime	Total amount of time the device was down for the month.

Button selection

To view the outage history of the current object for a month, click the numbered column button that corresponds with the month desired.

Outage History of a Single Object

The availability data in this section provides the outage history for a single object (device) in an SLA.

Access the outage history of an object from the **Device Availability for One Year** form shown in Figure 9-25 on page 298. For more information, see [Availability of a Single Device](#) on page 298.

- Click a numbered column button in the chart. ServiceCenter displays a form showing the outage history of the device, if a history exists. If the device has no outage history, the status bar displays this message: **No records found for query:....** Figure 9-26 on page 300 shows the outage history of a device.

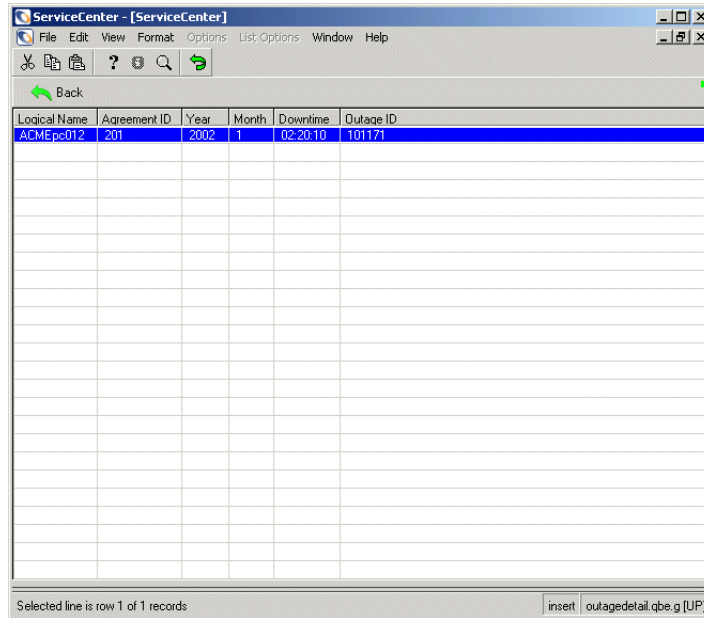


Figure 9-26: Outage history of a single device

The following table describes the fields on the outage history form.

Field	Description
Logical Name	Name of the device as it appears in the device file.
Agreement ID	Unique number identifying the record for this SLA.
Year	Year of the outage (see Figure 9-25 on page 298).
Month	Month of the outage (see Figure 9-25 on page 298).
Downtime	Total downtime that the outage record covers.
Outage ID	Unique ID of the outage record. (It is possible that the device could be down multiple times during the month, in which case, multiple outage records display.)

Accessing an incident ticket

To display the incident ticket that describes a selected outage, double-click an entry in the table, or select an entry and press **Enter**. Figure 9-27 shows an incident ticket with a reported outage.

The screenshot shows the 'ServiceCenter - [Update Incident Number IM10001]' window. The 'Ticket Status' is 'Closed'. The 'Incident Title' is 'Test SLA001'. The 'Incident Details' tab is active, showing fields for Alert Status (closed), Category (client system), Subcategory (hardware), Product Type (desktop), Problem Type (hard disk), Manufacturer (Unknown), Class (UNKNOWN), Contact Time, Elapsed Time, Contract (ACME US), Company (ACME), and Contact (BROWN, NICHOLAS). The 'Owner' is 'esoriano'. The 'Primary Asgn Group' is 'HELPDESK', 'Assignee Name' is 'HELPDESK 1', and 'Second Asgn Group' is 'Field Eng.'. The 'Hot Ticket' checkbox is unchecked. The 'Severity' is '4 - Low', 'User Priority' is empty, 'Site Category' is 'B - Major Site', 'Cause Code' is 'Authentication Failure', and 'Site' is empty. The 'Phone / extension' is '(770) 954-4588 / 243'. The 'Incident Description' field contains 'Test SLA001'. The status bar at the bottom shows 'Ready' and a command line 'insert | problem.template.close.g [UP]'.

Figure 9-27: Incident ticket describing an outage



Note: This is the end of the availability data flow. Click **Back** to return to the previous screen in the flow, or use the **Return** button to return to the Service Level Agreements menu.

Response Time Data

SLA response time data is used to track guarantees of response time in the case of an outage. The SLM module gathers the following information about response times in the system from agreement records:

- Tracking from specific Incident ticket states
- Target response time
- Calendar (work shift) affected by the guarantee
- Importance of the response time to the SLAs overall performance

Response time status of Service Level Agreements

The response time performance characteristics described in this section are for all the SLAs in your system. The table in the **SLA Response Time Performance** form compares actual performance with the target performance guaranteed by the agreement. The color chart displays the same performance data as that given in the table, but in a visual format. The chart also provides access buttons for moving to the next level. for more information, see [Recalculating Outage Data](#) on page 282.

To access the response time performance information for all SLAs:

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu appears.
- 2 Click **View SLA Metrics.**
- 3 The SLA Overall Performance form shows the overall performance for SLAs in your system for the month selected, as shown in Figure 9-21 on page 290.
- 4 Select the **Yearly Response** option beneath the chart.
- 5 Click the **Response Statistics** button to display the response time status of all your SLAs, as shown in Figure 9-28.

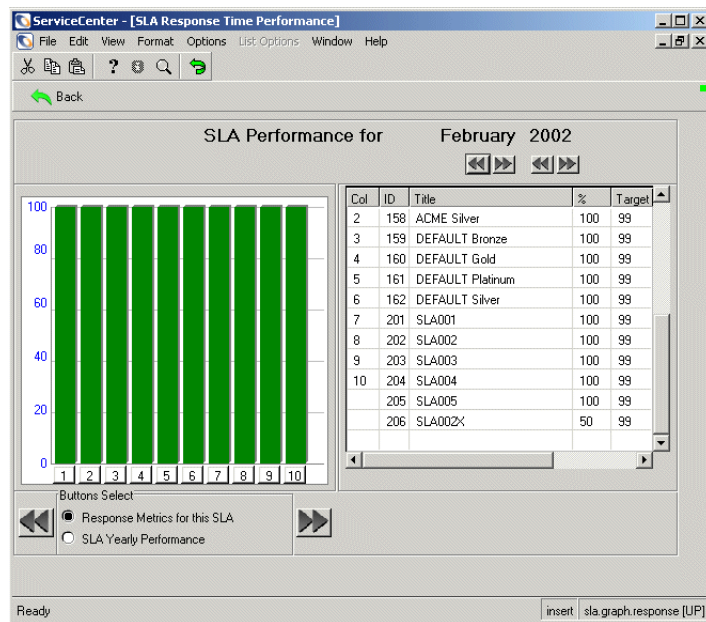


Figure 9-28: Response time status for all SLAs

The following table describes the fields on the SLA Performance form.

Field	Description
Col	Column numbers correspond to the numbers on the x-axis of the graph on the left-hand side of the screen.
ID	Unique identification numbers assigned by the system to the SLA records when they were created.
Title	Title given to the SLAs when they were created, for example, Development & IT.
%	Actual performance percentages of the response times.
Target	Performance percentages of response times, guaranteed in the agreement.

The following table describes the buttons on the Device Performance form.

Button	Action
Response Metrics for this SLA	When this view is selected, the numbered column buttons display the response metrics of a single SLA.
SLA Yearly Performance	When this view is selected, the numbered column buttons display the yearly response time performance of a single SLA.

Response time status for a single SLA

The response time performance characteristics described in this section are for each month in one year for a single SLA. The table in the **SLA Response Time Performance for One Year** form displays actual performance percentages for each month. The color chart displays the same performance data in a visual format and provides access buttons for displaying the response metrics for a single SLA.

The access point is the **SLA Overall Performance** form shown in Figure 9-21 on page 290. For more information, see [Accessing SLA Metrics](#) on page 289.

Method 1: Access yearly response time performance for a single SLA

- 1 Select the **Yearly Response** option beneath the chart in the **SLA Overall Performance** form.
- 2 Click a numbered column button. Yearly performance information for the SLA selected from the table in the **SLA Overall Performance** form displays.

Method 2: Access yearly response time performance for a single SLA from the SLA Overall Performance form

- 1 Access the **SLA Overall Performance** form.
- 2 Click **Response Statistics** to display the response time status of all your SLAs.
- 3 Select the **SLA Yearly Performance** option.
- 4 Click a numbered column button to display the response time status of a single SLA, as shown in Figure 9-29.

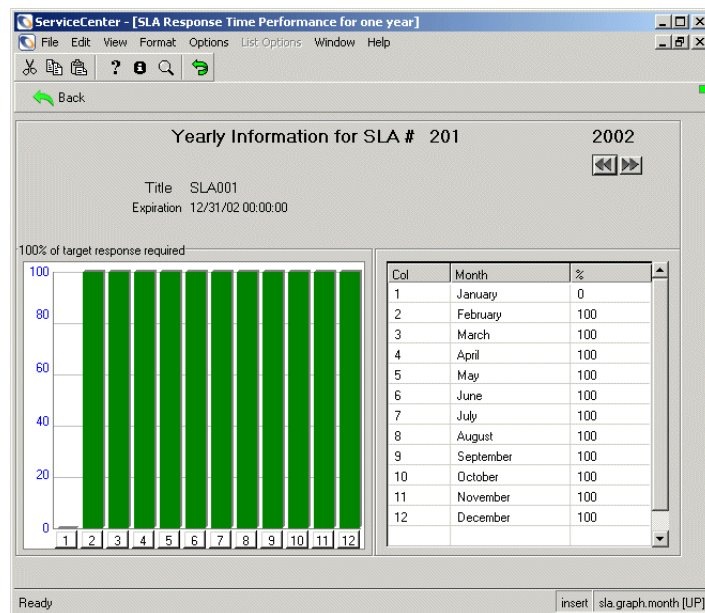


Figure 9-29: Yearly response time performance for a single SLA

The following table describes the fields on the SLA Performance form.

Field	Description
<%> of target response required	The label on the structure around the color chart indicates the target response required of the SLA as guaranteed in the agreement. In this example, the availability percentage is 100%.
Col	Column numbers correspond to the numbers on the x-axis of the graph on the left-hand side of the screen.
Month	Months of the year that is indicated on the upper right-hand side of the form.
%	<p>The percentages of responses that were met. On the Response Times tab of an SLA, the user can define a named response phase of the life cycle of an incident ticket. For example, an SLA could have the following two named phases defined:</p> <p>Open-to-WIP — Acceptable response time is 01:00:00 (one hour) which is the time elapsed between when the incident is opened until to it is assigned to someone.</p> <p>WIP-to-Resolved — Acceptable response time: 02:00:00 (two hours)</p> <p>Assume that an incident ticket is opened using this SLA and the first named response phase (Open-to-WIP) takes MORE than the acceptable one hour to complete.</p> <p>Once the ticket is assigned, the second named response phase (WIP-to-Resolved) takes LESS THAN or equal to the acceptable two hours to complete.</p> <p>The response percent for this SLA would be 50% since one named response phase failed to complete in the acceptable timeframe and the other was completed within the acceptable timeframe.</p> <p>This percentage can be expressed as:</p> $(\text{number of times in the month a named response phase of the SLA was responded to within the allotted time.}) / ((\text{number of named response phased defined in the SLA}) * (\text{number of incident tickets against the SLA in a month}))$ <p>This formula reflects what percentage of ALL the named response phases defined for the SLA were responded to within the allotted time.</p>

Button selection

To view response metrics for a single SLA for 1 year, follow steps 1 - 6 in the previous section. Clicking on a numbered button beneath a column in the chart in the **Response Metrics for a SLA** form will display the metrics for the corresponding month.

Response Metrics for a Single SLA

The response time performance characteristics described in this section are for all named responses in a single SLA. The table displays actual performance percentages. The color chart displays the same performance data in a visual format and provides access buttons for displaying response metrics for an entire year.

To access the response metrics for a single SLA:

Method 1

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu displays.
- 2 Click **View SLA Metrics**.
- 3 The SLA Overall Performance form appears, displaying the overall performance for SLAs in your system for the month selected.
- 4 Click **Response Statistics**. The response time status of all your SLAs appears.
- 5 Select the **Response Metrics for this SLA** option.
- 6 Click a column number button.
- 7 The response metrics for a single SLA appear.

To access the response metrics for a single SLA

Method 2:

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Agreements menu displays.
- 2 Click **View SLA Metrics**.
- 3 The SLA Overall Performance form appears, displaying the overall performance for SLAs in your system for the month selected.
- 4 Select the **Yearly response** option.
- 5 Click the column number button for the SLA whose response you want to display. The yearly response time performance of a single SLA appears.
- 6 Click a column number button to display the response metrics for a single month. Figure 9-30 shows the response performance for an SLA.

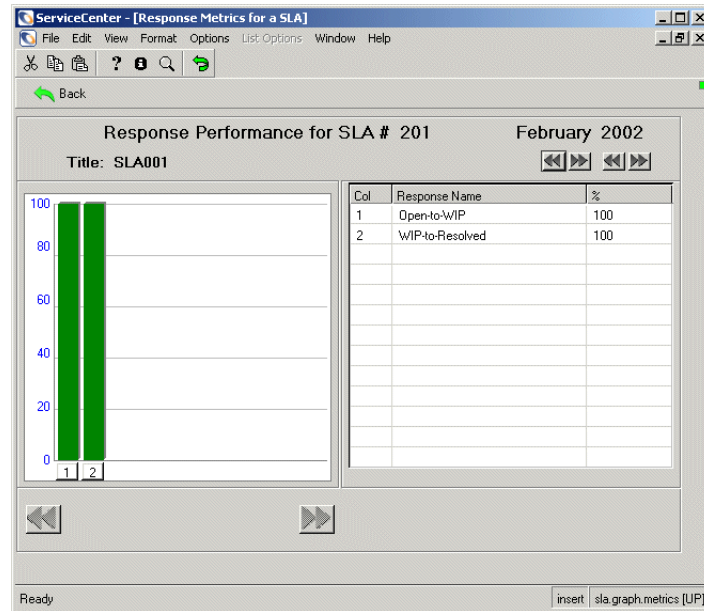


Figure 9-30: Response metrics for a single SLA

The following table describes the fields on the Response Performance form.

Field	Description
Col	Column numbers correspond to the numbers on the x-axis of the graph on the left-hand side of the screen.
Response Name	Name of the named response phase.
%	The percentage that the named response phase was responded to during the month within the allotted time. $\frac{\text{(number of times during the month the named response phase of the SLA was responded to within the allotted time)}}{\text{(number of Incident tickets against the SLA during the month)}}$

Button selection

To view response metrics for a single SLA for 1 year, click a numbered button beneath a column in the chart in the **Response Metric Performance for a SLA** form.

Single SLA Response Metrics for One Year

The response time data described in this section are actual response times for individual response metrics. The table in Figure 9-31 displays actual performance percentages. The color chart provides access buttons for displaying the details of a single response type. For more information, see [Details of a Single Response Type](#) on page 309.

Click a numbered button beneath a column in the chart in the **Response Metrics for a SLA** form, corresponding to a particular response. For example, click WIP-to-Resolved and Figure 9-31 shows the result. For more information, see [Response Metrics for a Single SLA](#) on page 306.

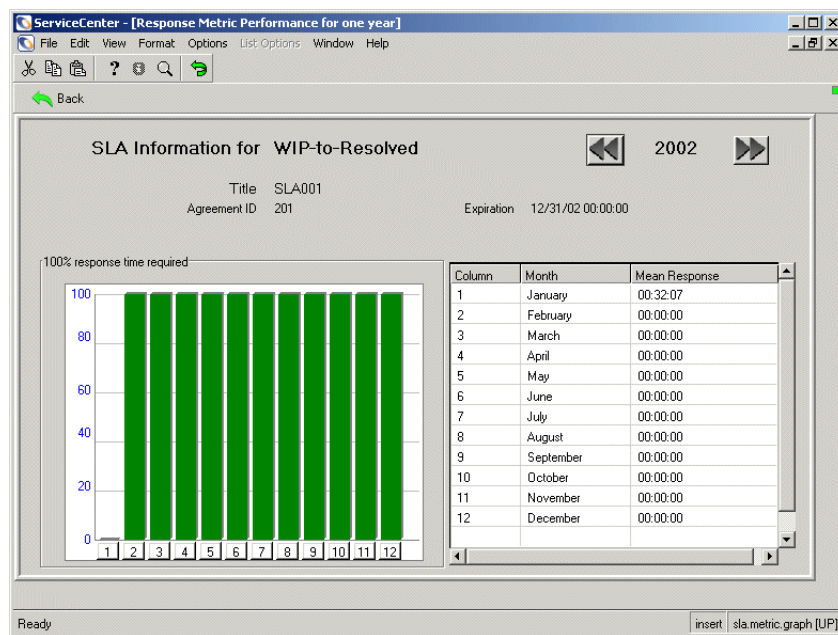


Figure 9-31: Response metric performance for one year

The following table describes the fields on the SLA Information form.

Field	Description
Col	Column numbers correspond to the numbers on the x-axis of the graph on the left-hand side of the screen.

The following table describes the fields on the Response Metrics form.

Field	Description
Response Name	Unique names identifying the response types. Response types must be unique within a particular SLA, but can be used for other SLAs.
Agreement ID	Unique identification numbers of the SLA in which the response type appears.
Year	Year in which the response type occurs.
Month	Month in which the response type occurs.
Percentage Hit	The percentage that the named response phase was responded to during the month within the allotted time. $\frac{\text{(number of times during the month the named response phase of the SLA was responded to within the allotted time)}}{\text{(number of Incident tickets against the SLA during the month)}}$
Mean	Average response time for this response type. The system derives this value by adding all the response times together and dividing the sum by the total number of responses.
Median	Median response time for this response type. The system derives this value by dividing the sum of the highest and lowest response times by 2.
Deviation	Standard deviation from the response time for that response type. This value helps you isolate chronically slow response types.



Note: This is the end of the response time flow. Click **Back** to return to the previous form in the flow, or click the **Return** button to return to the Service Level Agreements menu.

Service Level Contracts

The Contract Management module integrates information and tracking into the enterprise Service Desk. Unlike Service Level Agreements (SLAs), which describe *how* services in a contract are to be rendered, service contracts are financial agreements that define the services to be provided and the financial implications of using those services.

Features of Contract Management

On-Line Contract Storage

Contracts can be stored on-line in the ServiceCenter repository in a structured format for automated analysis, or as the original contract document.

Contract Determination Wizard

Contract Management includes links to Incident Management and Service Management that allow a first level technician single-button access to a contract determination wizard. The wizard then guides the technician to the appropriate service contract and service level for that specific service event. Contract Management can then determine when budgeted thresholds are exceeded for a specific contract. These thresholds can be either limits on numbers of calls or incidents, or thresholds on the cost of services offered under a contract.

Charge back

Contract Management allows charge back of costs, meaning the customer can be charged back the costs incurred while working with incidents, handling calls, or implementing changes to a specific service contract.

Contract Tracking

Contract Management ties discrete incidents and calls to service contracts. It provides up-to-date information about the state of each contract, including its budgeted allocations and the actual number of calls and Incidents applied against each contract.

Time and Materials

The existing Service, Incident, and Change Management modules now associate service contracts with time and materials expended. This feature makes it possible to compute the real cost of handling each incident and call, as well as to calculate the cost of managing each service contract.

Setup

Before you begin to use Contract Management, you must complete the following steps:

- *Configuration*.
- *Currency Conversion* on page 314.
- *Currency Definitions* on page 314.
- *Part Usage Detail* on page 315
- *Labor Performed Detail* on page 317

Configuration

Specify those contract elements you want the system to calculate, select a base currency for all your contracts, or switch off the automatic processing of contract specifics in the configuration record.

To configure the Contract Management module:

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Management menu appears.

- 2 Click the Service Contracts tab shown in Figure 9-33.

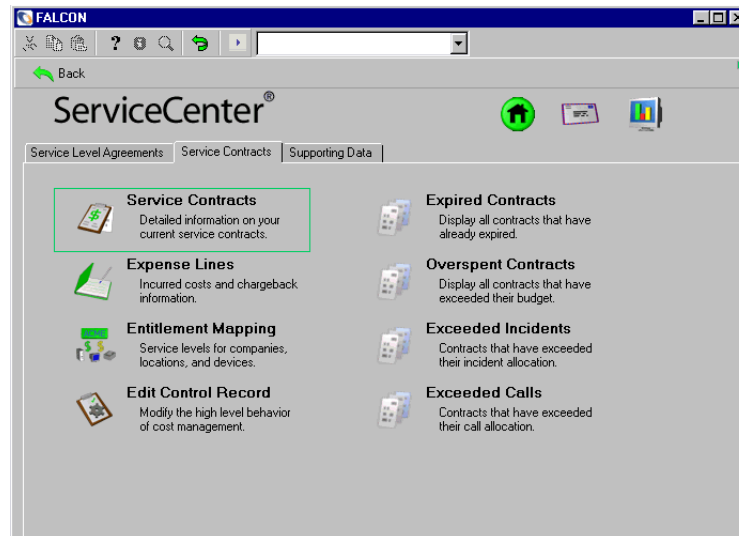


Figure 9-33: Service Level Management menu: Service Contracts tab

- 3 Click Edit Control Record.

Figure 9-34 shows the Contract Management configuration record.

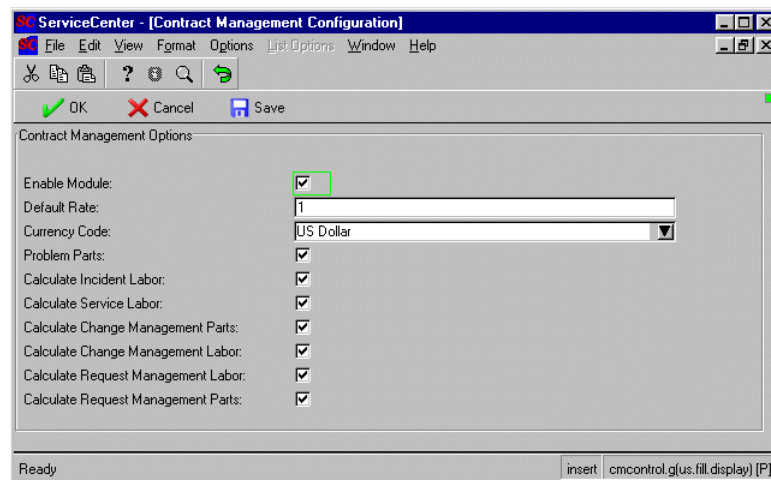


Figure 9-34: Contract Management options

Click **Save** to save any changes to the configuration record. The following table describes the fields in the Contract Management configuration record.

Field	Description
Enable Module	Select this check box to enable the Contract Management data collection processes.
Default Rate	Enter the default labor rate for the module.
Currency Code	The value in this field sets the currency code for Contract Management. Currency conversions for all contracts in the database are based on this code.
Problem Parts	Select this check box to calculate the cost of parts from the Parts & Labor tab in an incident ticket.
Calculate Incident Labor	Select this check box to calculate the cost of labor from the Parts & Labor tab in an incident ticket.
Calculate Service Labor	Select this check box to calculate the cost of labor from the Time Spent Working on Call field in a call report.
Calculate Change Management Parts	Select this check box to calculate the cost of parts from the Parts & Labor tab in a change request.
Calculate Change Management Labor	Select this check box to calculate the cost of labor from the Parts & Labor tab in a change request.
Calculate Request Management Labor	Select this check box to calculate the cost of labor from the Parts & Labor tab in a change request.
Calculate Request Management Parts	Select this check box to calculate the cost of parts from the Parts & Labor tab in a change request.

Currency Conversion

Contract Management provides a currency conversion utility that automatically converts 166 national currencies, depending upon exchange rates at the time the contract is granted. Daily exchange rates can be entered into the system, ensuring accurate rate conversions. For more information, see [Currency Conversion Utility](#) on page 215.

Currency Definitions

Currency definition records define currency codes for each of the international currencies entered in the system and establish whether or not an individual currency has European Union Currency (EUR) as its root. For more information, see [Currency Definitions](#) on page 217.

Part Usage Detail

Part Usage Detail records define the details of used parts, including device type, part number, model number, location where asset is being used, and so forth.

To view a used parts record:

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Click the **Supporting Data** tab.
- 3 Click **Part Usage Detail**.

Figure 9-35 shows a blank Part Used form.

The screenshot shows a web application window titled "ServiceCenter - [cmparts]". The menu bar includes File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu is a toolbar with icons for Back, Add, and Search. The main content area is titled "Parts Used -- Detail" and contains a list of labels on the left and corresponding input fields on the right. The labels are: ID, Reference File, Reference Key, Part Number, Quantity Used, Contact, Department, Company, Location, Asset, Model, Device Type, and Vendor. The input field for "ID" is highlighted with a green border. At the bottom of the window, the status bar displays "Ready" on the left and "insert cmparts.g(db.search) [P]" on the right.

Figure 9-35: Used Parts — Detail Record Search Form

- 4 Do one of the following:
 - Enter the name used part or other search criteria and click **Search** or press **Enter**.
 - Leave all fields blank and click **Search** to perform a *true* query and retrieve a list of all used parts records.

Figure 9-36 shows the requested record, or a QBE list of records appears where you can select a record to view or modify.

id	reference.file	asset
123	problem	
124	problem	
125	problem	
126	problem	

1/32+

Parts Used -- Detail

ID: 123
 Reference File: problem
 Reference Key: FM1001
 Part Number: 434
 Quantity Used: 1
 GL Number:
 Contact:
 Department:
 Company:
 Location:
 Asset:
 Model:
 Device Type:
 Vendor:

Ready Response 0.100 draw 0.190 insert cmparts.qbe.g [UP]

Figure 9-36: Used Parts Detail Definition record

- 5 You can add, edit, or delete part usage details in this form. The following table shows the fields on the Parts Used form.

Field	Description
ID	Unique serial number for this device type.
Reference File	The file accessed to reference this information, such as the problem file.
Reference Key	Event triggering a response. For example, an incident ticket number within the problem file.
Part Number	A unique part number used to define this model.
Quantity Used	The number of assets being used.
Contact	Individual in the contacts file associated with this device or primary asset.
Department	The department associated with this device or primary asset.
Company	The company associated with this device or primary asset.

Field	Description
Location	The location within a company associated with this device or primary asset.
Asset	Asset that this used parts record is defining.
Model	Model of this device or primary asset.
Device Type	Type of device this asset represents.
Vendor	Provides services for this component.

Labor Performed Detail

The Labor Performed Detail definition records define the details of where and how labor was performed on components for service records and billing purposes.

- 1 Click **Service Level Mgmt** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Select the **Supporting Data** tab.
- 3 Click **Labor Performed Detail**. Figure 9-37 shows a blank Labor Performed form.

The screenshot shows a web application window titled "ServiceCenter - [cmlabor]". The menu bar includes File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu bar is a toolbar with icons for Back, Add, and Search. The main content area is titled "Labor Performed -- Detail" and contains a list of labels with corresponding input fields: ID, Reference File, Reference Key, Technician, Hours Worked, Date Worked, Contact, Department, Company, Location, Asset, Model, Device Type, and Vendor. The ID input field is highlighted with a green border. At the bottom of the window, there is a status bar that says "Ready" and a small text area containing "insert cmlabor.g(db.search) [P]".

Figure 9-37: Labor Performed Detail Record Search form

- 4 Do one of the following:
 - Enter the applicable search criteria and click **Search** or press **Enter**.
 - Leave all fields blank and click **Search** to perform a *true* query and retrieve a list of all labor performed (detail definition records).

Figure 9-38 shows the requested record, or a QBE list of records where you can select a record, to view or modify.

The screenshot shows the ServiceCenter application window titled "ServiceCenter - [cmlabor 34]". The menu bar includes File, Edit, View, Format, Options, List Options, Window, and Help. The toolbar contains icons for Cut, Copy, Paste, Find, and other standard functions. Below the toolbar is a row of buttons: OK, Cancel, Previous, Next, Add, Save, and Delete. The main area is divided into two sections. The top section is a table with two columns: "id" and "reference.file". The table contains the following data:

id	reference.file
34	incidents
35	incidents
76	incidents
77	incidents
103	problem

The bottom section is titled "Labor Performed -- Detail" and contains a form with the following fields and values:

ID:	34
Reference File:	incidents
Reference Key:	CALL1020
Technician:	bob.helpdesk
Hours Worked:	0.024444
Date Worked:	02/08/99 12:50:24
Contact:	
Department:	
Company:	
Location:	
Asset:	
Model:	
Device Type:	
Vendor:	

At the bottom of the form, it says "Selected line is row 1 of 32 records retrieved" and "insert cmlabor.g(db.view) [P]".

Figure 9-38: Labor Performed Detail Definition record

- 5 You can add, edit, or delete definitions in this form. The following table shows the fields on the Labor Performed form.

Field	Description
ID	Unique serial number for this device type.
Reference File	The file accessed to reference this information, such as the problem file.
Reference Key	Event triggering a response. For example, an incident ticket number within the problem file.

Field	Description
Technician	Technician assigned to service this device or primary asset.
Hours Worked	Number of hours spent servicing this device or primary asset.
Date Worked	Date services rendered on this device or primary asset.
Contact	Individual in the contacts file associated with this device or primary asset.
Department	The department associated with this device or primary asset.
Company	The company associated with this device or primary asset.
Location	The location within a company associated with this device or primary asset.
Asset	Asset that required repairs.
Model	Model of this device or primary asset.
Device Type	Type of device this asset represents.
Vendor	Provides services for this component.
GL Number	

Service Contracts

ServiceCenter stores contract information inside its repository in two forms:

- Detailed format designed for automated analysis.
- Entire contract in its original form.

Service contracts are the principal records for Contract Management. Contract information displays here to determine what services have been used and what services remain. You can create, edit, or delete contracts in this form.

Accessing a Contract

To access an existing contract:

- 1 Click **Service Level Mgmt** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Click the **Service Contracts** tab.
- 3 Click **Service Contracts**.

Figure 9-39 shows a blank contract search form.

The screenshot shows a window titled "ServiceCenter - [servicecontract]". The menu bar includes File, Edit, View, Format, Options, List Options, Window, and Help. The toolbar contains icons for Back, Add, Search, Find, and Fill. Below the toolbar, there are input fields for "Contract ID:" and "Reference Name:". A tabbed interface is visible with tabs for General Information, Details, Rules, Named Users, Comments, Attachments, and Additional Services. The "General Information" tab is active, displaying various fields with dropdown menus: Start Date, End Date, Provider Company, Cost Center, Technical Account Manager, TAM Phone number, Escalation Contact, Escalation Phone number, Client Company, Client Contact, Duty Calendar, Alert when not updated for, Call time limit, and Warning time alert. A "Line Items" button is located below the Client Contact field. The status bar at the bottom shows "Ready" and "insert servicecontract.q(db.search) [P]".

Figure 9-39: Blank Service Contract Search form

- 4 Click **Search** or press **Enter** to perform a *true* query and retrieve a list of all current contract records. A contract record list appears, listing all contracts in your system.
- 5 Select a record to view and modify by double-clicking on the Name in the Contract ID.

Figure 9-40 shows the appropriate information in the contract form.

Contract ID	Reference Name	Start Date	End Date
15	General Support	01/01/99 00:00:00	01/01/02 00:00:00
17	GEN International	01/01/99 00:00:00	01/31/03 00:00:00
18	GENERICOM GEN	01/01/99 00:00:00	01/01/02 00:00:00
19	ACME INTERNATIONAL	01/01/99 00:00:00	01/01/02 00:00:00

Contract ID: 15
Reference Name: General Support

General Information | Details | Rules | Named Users | Comments | Attachments | Additional Services

Start Date: 01/01/99 00:00:00
End Date: 01/01/02 00:00:00
Provider Company: PRGN
Cost Center:
Technical Account Manager: FALCON
TAM Phone number:
Escalation Contact:
Escalation Phone number:
Client Company: PRGN
Client Contact: TRASK
Line Items
Duty Calendar:
Alert when not updated for:
Call time limit:
Warning time alert:

Selected line is row 1 of 7 records | insert | servicecontract.qbe.g [P]

Figure 9-40: Service Contract search results

Header Fields

Contract ID is the number provided by the system as the unique identifier for this contract.

Reference Name (*required*) is an alternate unique identifier. Generally, this is the client company's contract number.

General Information tab

The following table shows the fields on the General Information tab.

Field	Description
Start Date	Date when the contracted services begin.
End Date	Date when the contract expires.

Field	Description
Provider Company	Name of the client company. The name in this field references a System Wide Company Record in the ServiceCenter company file.
Cost Center	Cost center for the contract.
Technical Account Manager	Technical account manager for the contract.
TAM Phone number	Technical account manager's phone number
Escalation Contact	Who to contact in case of an escalation on the contract.
Escalation Phone number	Who to contact in case of an escalation on the contract.
Client Company	Name of the company contracting for the services. The name in this field references a System Wide Company Record in the ServiceCenter company file.
Client Contact	Name of the contact inside the client company who can answer questions about the contract.
Duty Calendar	What calendar the contract uses (see ServiceCenter calendars).
Alert when not updated for	Reserved for a future release.
Call time limit	Reserved for a future release.
Warning time alert	Reserved for a future release.

Details tab

Figure 9-41 shows the Details tab.

Field	Value
Budgeted Amount	50000
Budgeted Currency	US Dollar
Root Budget Amount	50000
Root Currency	US Dollar
Spent To Date	3391.194444
Budget Grant Date	01/01/99 00:00:00
Contracted Incidents	1000
Used Incidents	183
Contracted Calls	2000
Used Calls	2

Figure 9-41: Details tab

The following table shows the fields on the Details tab.

Field	Description
Budgeted Amount	Maximum amount of money that is budgeted for the services defined in the contract.
Budgeted Currency	International currency in which the Budgeted Amount is expressed (for example, French Franc).
Root Budget Amount	Budgeted amount translated into the system's root currency. This quantity is automatically calculated.
Root Currency	System's root currency.
Spent to Date	Total amount of money spent to date servicing this contract.
Budget Grant Date	Date on which the budget was granted. The system bases all currency conversions regarding this contract on this date.
Contracted Incidents	Total number of incidents budgeted for this contract.
Used Incidents	Total number of Incidents opened to date against this contract.
Contracted Calls	Total number of calls budgeted for this contract.
Used Calls	Total number of calls opened to date against this contract.

Rules tab

The choices on the Rules tab, shown in Figure 9-42, define the course of action a customer service technician should take when the terms of a service contract are exceeded.

The screenshot shows a software interface with a tabbed menu at the top: General Information, Details, Rules (selected), Named Users, Comments, Attachments, and Additional Services. Below the tabs are four sections, each with a title and three radio button options:

- When a caller exceeds his purchased calls we should:**
 - ☒ Ignore It
 - ☐ Warn the User
 - ☐ Refuse Service
- When a caller exceeds his purchased incidents we should:**
 - ☐ Ignore It
 - ☒ Warn the User
 - ☐ Refuse Service
- When a caller exceeds his purchased service reviews we should:**
 - ☐ Ignore It
 - ☐ Warn the User
 - ☐ Refuse Service
- When a caller exceeds his purchased site visits we should:**
 - ☐ Ignore It
 - ☐ Warn the User
 - ☐ Refuse Service

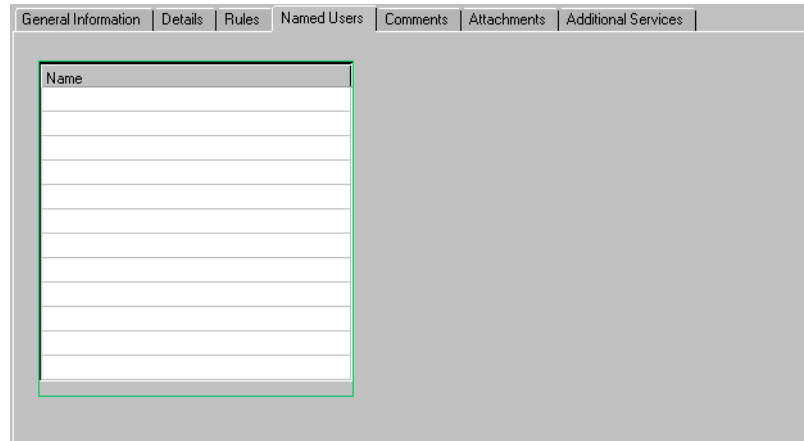
Figure 9-42: Rules tab

When a caller exceeds the purchased calls, incidents, service reviews, or site visits, click:

- **Ignore it** if you want the technician to service calls or incidents that exceed the limit for this contract.
- **Warn the User** if you want the technician to warn the user when calls or incidents exceeds the limit for this contract.
- **Refuse Service** if you want the technician to refuse service for calls or incidents that exceed the limit for this contract.

Named Users tab

In the Named Users dialog box, enter the customer contact names for the contract who are entitled to update or request service against the contract. Contacts entered on this tab must exist in the **Contacts** record. Figure 9-43 on page 325 shows the Named Users tab.

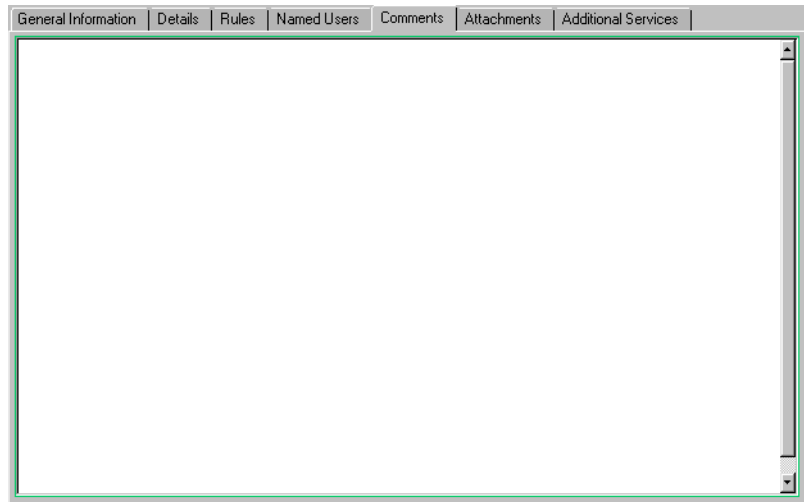


The screenshot shows a software interface with a tabbed menu at the top. The tabs are: General Information, Details, Rules, Named Users (which is the active tab), Comments, Attachments, and Additional Services. The main content area of the 'Named Users' tab contains a table with a single header row labeled 'Name' and several empty rows below it, suggesting a list of users to be managed.

Figure 9-43: Named Users tab

Comments tab

Enter notes, cautions or special conditions regarding this contract on the Comments tab shown in Figure 9-44. This text does not display anywhere else in the system.



The screenshot shows the same software interface as Figure 9-43, but with the 'Comments' tab selected. The main content area is a large, empty text box with a vertical scrollbar on the right side, intended for entering notes or special conditions.

Figure 9-44: Comments tab

Attachments tab

Attach any documents pertaining to this contract in this tab, including the actual contract itself. Contract Management recognizes a wide range of document formats. There are two options for attaching documents to a service contract:

- **Pop-up menu:** Right-click in the **Attachments** tab and select Insert from the shortcut menu.
- **Drag and drop:** Drag documents from a file folder directly into the **Attachments** tab.

Figure 9-45 shows the Attachments tab.



Figure 9-45: Attachments tab

For more information, see the *ServiceCenter System Administrator's Guide*.

Additional Services tab

Figure 9-46 shows the Additional Services tab.

Figure 9-46: Additional Services tab

The following table shows the fields on the Additional Services tab.

Field	Description
Contracted Service Reviews	Enter the number of Service Reviews to which the customer is entitled.
Used Service Reviews	Number of remaining Service Reviews the customer is entitled to. This number is updated automatically from the Incident Record.
Contracted Site Visits	Enter the number of Site visits to which the customer is entitled.
Used Site Visits	Number of remaining Site Visits the customer is entitled to. This number is updated automatically from the Incident Record.

Creating a Contract

To create a new contract in Contract Management:

- 1 Click **Service Level Mgmt** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Click the **Service Contracts** tab.
- 3 Click **Service Contracts**. A blank contract form appears.
- 4 Fill in the tabs with the appropriate data.
- 5 Click **Add** to add the record to the file.



The status bar displays this message: **Record added to the servicecontract file.**

Editing a Service Contract

To edit a service contract:

- 1 Click **Service Level Mgmt** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Click the **Service Contracts** tab.
- 3 Click **Service Contracts**. A blank service contract search form appears.
- 4 Do one of the following:
 - Type search criteria. Click **Search** or press **Enter**.
 - Leave the fields blank and click **Search** to perform a *true* query and retrieve a list of all current service contract records. Select a record to view and modify.
- 5 Edit the record as needed.
- 6 Click **Save** to save the changes. The status bar displays this message: **Record updated in the servicecontract file.**
- 7 Click **OK** to exit the servicecontract file.

Deleting a Service Contract

To delete a service contract:

- 1 Click **Service Level Mgmt** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Click the **Service Contracts** tab.
- 3 Click **Service Contracts**. A blank service contract search form appears.
- 4 Do one of the following:
 - Type a name in the **Reference Name** field or click **Browse** to select search criteria.
 - Leave the fields blank and click **Search** to perform a *true* query and retrieve a list of all current service contract records. Select a record to delete.The requested record appears.
- 5 Click **Delete**. A message prompts you to confirm the action.
- 6 Click **Yes** to delete the contract record. The status bar displays this message: **Record deleted from the servicecontract file.**
- 7 Click **OK** to exit the servicecontract file.

Expense Lines

An *expense line* record is an itemized accounting of expenses incurred by the provider while servicing a contract. Expense lines are generated by the system as services are rendered and automatically calculate the money spent for each part or service in the currency of the contract. Figure 9-47 shows an expense line record.

The screenshot displays the ServiceCenter application window titled "ServiceCenter - [expline: 799]". It features a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Previous, Next, Add, Save, Delete, Find, and Fill. Below the toolbar is a table listing expense lines. The table has columns for ID, Date Cut, State, Currency Code, and Amount. The first row (ID 799) is highlighted. Below the table is a section titled "Expense Line Information" containing two columns of input fields. The left column contains fields for ID, Date Cut, Date Processed, State, Currency Code, Amount, Service Contract ID, Asset Contract ID, Source File, Source Key, Root Currency, Root Amount, Type, Micro-State, Cost Center, and Budget Center. The right column contains fields for Bill To, Bill Type, GL Number, Payment Type, Contact, Department, Company, Location, Asset, Model, Device Type, Vendor, and Associated Data. The status bar at the bottom shows "Ready" and "Response 0.130 draw 0.191 insert expline.g[db.vie]".

ID	Date Cut	State	Currency Code	Amount
799	08/26/02 16:20:42	closed	USD	0
800	08/26/02 16:32:14	closed	USD	0
801	08/27/02 08:42:12	closed	USD	0
802	08/27/02 08:45:08	closed	USD	0
803	08/29/02 10:24:10	closed	USD	0.305
804	08/29/02 10:27:28	closed	USD	0.513

Expense Line Information

ID:	799	Bill To:	
Date Cut:	08/26/02 16:20:42	Bill Type:	
Date Processed:	08/26/02 16:27:52	GL Number:	
State:	closed	Payment Type:	
Currency Code:	USD	Contact:	BROWN, NICHOLAS
Amount:	0	Department:	Administration
Service Contract ID:		Company:	ACME
Asset Contract ID:		Location:	ACME HQ
Source File:	probsummary	Asset:	ACMEpc012
Source Key:	IM1002	Model:	510CDT
Root Currency:	USD	Device Type:	
Root Amount:	\$ 0.00	Vendor:	AT&T Systems
Type:	labor	Associated Data:	219
Micro-State:			
Cost Center:			
Budget Center:			

Ready Response 0.130 draw 0.191 insert expline.g[db.vie]

Figure 9-47: Expense Line record

The following table describes the fields in the Expense Line Information form.

Field	Description
ID	The unique identifier assigned by the system to the expense line record.
Date Cut	Date the expense line record was created.
Date Processed	Date the expense line record was updated.

Field	Description
State	<p>Exchange rate processing status of the record.</p> <ul style="list-style-type: none"> ■ closed — indicates that the exchange rate has been locked in and the value computed exactly. ■ ready — indicates that the record is waiting to be processed. ■ pending — indicates that the record is waiting for the exchange rate to be entered in the system.
Currency Code	The value in this field sets the currency code for Contract Management. Currency conversions for all contracts in the database are based on this code.
Amount	Amount spent by the provider in the contract currency.
ServiceContract ID	Number provided by the system as the unique identifier for this contract.
Asset Contract ID	Number provided by the system as the unique identifier for this contract.
Source File	Name of the file from which the type of expenditure is calculated (for example, outage , operator , model).
Source Key	Unique identifier of the record in the file generating the expense line. For example, CALL1021 (Service Management) and IM10011 (Incident Management).
Root Currency	Root currency for the ServiceCenter system.
Root Amount	Equivalent sum, in root currency, of the amount entered in the Amount field.
Type	<p>Type of expenditure involved.</p> <ul style="list-style-type: none"> ■ Parts — used to compute the cost of parts used in servicing a contract, the system searches in the model file. ■ Labor — used to compute the cost of labor involved in servicing a contract, the system searches in the operator file for the technician's hourly rate. ■ Outage — used to compute the cost resulting from outages, the system searches at the service level agreement (SLA) for the device in question. ■ Handling — used to compute the cost resulting from handling a customer call, the system searches at the Service Management call report. ■ Other — area is available for user tailoring. Creating your own expenditure type is an advanced procedure.
Micro-State	Used for system processing.

Field	Description
Cost Center	Cost center for the expense line.
Budget Center	The budget center (profit center) the expense line is associated with.
Bill To	A person or department.
Bill Type	Whether the bill to value contains a person or department.
GL Number	Global Ledger number.
Payment Type	Depend on the nature of the expense. For example, contract payments include the following payment types: buyout, renewal, purchase.
Contact	Individual in the contacts file associated with this expense line.
Department	The department associated with this expense line.
Company	The company associated with this expense line.
Location	The location within a company associated with this expense line.
Asset	Asset to which this expense line refers.
Model	Model of this device or primary asset.
Device Type	Type of device this asset represents.
Vendor	Provides services for this component.
Associated Data	User comments field for such things as the device involved.

Accessing Expense Line Records

To open an expense line record:

- 1 Click **Service Level Mgmt** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Click the **Service Contracts** tab.

- 3 Click **Expense Lines** in the Service Contracts menu. Figure 9-48 shows a blank expense line record.

Figure 9-48: Expense Line Search form

- 4 Do one of the following:
 - Type search criteria in a field and click **Search** or press **Enter**.
 - Leave the fields blank and click **Search** to perform a *true* query and retrieve a list of all current service contract records. Select a record to view.

The QBE record list displays all the expense line records in the system.

Cost Assessment

Each time a client company provides a service to a customer, real cost is incurred from three sources:

- The cost of interacting with the customer. This can be evaluated as the time spent by first level technicians handling the customer's call, multiplied by the hourly wage of the technician.
- The cost of labor associated with actually fixing an incident. As one or more technicians actually work on an incident, their time is multiplied by their hourly rate to determine the cost.
- The cost of any parts used in the repair process.

Handle Time

The time spent receiving and handling a request for service costs a provider money. A ten-minute phone conversation with the customer, however insignificant it may seem, represents an expense that should be charged back to the customer. A large number of these brief calls consumes a significant amount of a provider's resources.

Contract Management is integrated with ServiceCenter's Service Management module. As calls are received, the Service Management module automatically determines the time that was spent handling the calls. In Service Management, accounting for handle time begins when a call report starts and terminates when the help desk technician ends the call. These handle times are multiplied by the handling technician's bill rate and recorded as expense lines against the relevant service contract.

Labor

As an incident ticket or change request is managed, more than one person may work on the issue. A given technician may work on the issue more than once over a period of days or weeks. Contract Management integrates with the ServiceCenter Incident, Change, and Request Management modules to allow technicians to record the hours they spent working on a change request, incident ticket, or request management quote.

As the technicians record their labor in the incident ticket, line item, or change request, the system automatically translates this information into expense lines that tie back to Incident, Request, and Change.

Figure 9-49 shows the Parts & Labor tab for an expense line record.

Update Incident Number IM1078

OK Cancel Previous Next Save Undo Close Find Fill Clocks

ID	Open Time	Update Time	Alert Status	Category	Title
IM1075	12/29/00 16:2	03/08/01 16:12:19	alert stage 3	client system	Bootup of host workstation doesn't show tape drive as a scs
IM1076	12/29/00 16:2	03/08/01 16:12:25	alert stage 3	client system	Workstation is down and won't boot at all. Monitor is dead ar
IM1077	12/29/00 16:3	03/08/01 16:12:45	alert stage 3	enquiry	Wants to know how to set up a daisy chain of tape drives, C
IM1078	12/29/00 16:3	03/08/01 16:12:51	alert stage 3	client system	Monitor is getting more and more dim, and sometimes loses c
IM1079	12/29/00 16:3	03/08/01 16:12:31	alert stage 3	client system	Can't get the controller to recognize a 3rd party external disk

IM1078 Ticket Status: Open Incident Ticket

Incident Title: Monitor is getting more and more dim, and sometimes loses color entirely.

Change C2 - Prompt

OK Cancel Prev Next Save Close Find Fill Clocks

Number	Category	Priority	Phase	Asset	Start	End	Title
C14	RFC - Adv	3	2 plan		05/09/0	05/10	02/21/02 23:24:19 (FALCON);
C15	RFC	3	Assessme	AdamPC	06/17/0	06/17	Replace sound card on demo machine.
C16	MAC	4	Approval		05/13/0	05/15	Add a new printer to the network.
C2	Application	2	Design		05/01/0	05/02	Duplicate records exist in the database.
C3	Hardware	4	HW Spec		04/12/0	04/12	Install new pc

Change No.: C2 Planned Start: 05/01/02 08:00:00

Category: Application Planned End: 05/02/02 17:00:00

Phase: Design Status: initial

Alert Stage: Approval Status: pending

General Product Description Resolution Work Around Approvals **Parts & Labor** Attachments Related

Service Contract:

Date	Part Number	Quantity Used
		Change
		Request

Date	Technician	Hours Worked	Service Contract

Selected line is row 9 of 16 records Response 0.220 draw 0.320 insert cm3r.application.g[cm.view.display] [UP]

Figure 9-49: Parts & Labor tab

Parts

Contract Management is integrated with ServiceCenter's Incident, Request, and Change Management modules to allow technicians to record any parts they use to resolve the issue. As these parts are recorded, ServiceCenter takes the following action:

- Expense lines are created against the relevant contract.
- Quantities of these parts in stock are adjusted accordingly.

The system automatically tracks the number of parts in stock and, through Request Management, places replacement parts orders when quantities in stock dip below a user definable threshold.

Itemizing Costs

Contract Management allows you to itemize the cost of fixing a particular incident. Detailed cost data helps the user make informed decisions by answering such questions as:

- What type of incidents are the most expensive to fix?
- What percentage of your costs are parts?
- What percentage of your costs are labor?

To display a cost table and an expense line record:

- 1 Open an existing incident ticket.
- 2 Choose **Options > Show Costs**. Figure 9-50 shows a cost table for the incident ticket.

Type:	Cost:
Parts	\$ 0
Labor	\$ 0
Outage	\$ 0
Other	\$ 0
Call Handling	\$ 21.722222

Figure 9-50: Costs associated with an incident

- Click a button (**Parts**, **Labor**, and so on) to the right of the table to display the expense line records related to that incident. For example, click **Handling** and the window shown in Figure 9-51 appears.

The screenshot shows the ServiceCenter - [Database] window. At the top is a menu bar with File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu bar is a toolbar with icons for OK, Cancel, Save, Add, Delete, Find, and Fill. A table with 7 columns (ID, Date Cut, State, Currency Cod, Amount, Contract ID, Type) is displayed. The first row is highlighted in blue and contains the values: 345, 01/02/01 14:13, closed, USD, 21.722222, , labor. Below the table is a tab labeled 'Expense Line'. The 'Expense Line' tab contains a form with two columns of fields. The left column contains: ID (345), Date Cut (01/02/01 14:13:23), Date Processed (01/02/01 14:13:23), State (closed), Currency Code (USD), Amount (21.722222), Contract ID (), Source File (incidents), Source Key (CALL1013), Root Currency (USD), Root Amount (21.722222), Type (labor), and Micro-State (). The right column contains: Bill To (), Bill Type (), GL Number (), Contact (), Department (), Company (), Location (), Asset (), Model (), Device Type (), Vendor (), and Associated Data (137). At the bottom of the window, a status bar shows 'Selected line is row 1 of 1 records' and a button labeled 'insert' followed by the text 'expline.gl(QBE.display.gui) [P]'.

ID	Date Cut	State	Currency Cod	Amount	Contract ID	Type
345	01/02/01 14:13	closed	USD	21.722222		labor

Expense Line

ID: 345
 Date Cut: 01/02/01 14:13:23
 Date Processed: 01/02/01 14:13:23
 State: closed
 Currency Code: USD
 Amount: 21.722222
 Contract ID:
 Source File: incidents
 Source Key: CALL1013
 Root Currency: USD
 Root Amount: 21.722222
 Type: labor
 Micro-State:

Bill To:
 Bill Type:
 GL Number:
 Contact:
 Department:
 Company:
 Location:
 Asset:
 Model:
 Device Type:
 Vendor:
 Associated Data: 137

Selected line is row 1 of 1 records

insert expline.gl(QBE.display.gui) [P]

Figure 9-51: Expense Line record for Handling

Entitlement Checking

When a customer contacts a client company and requests service, it is important to determine whether or not that user is entitled to additional service; if the contract provides for five service calls, and the user has already reached that limit, service may be denied.

Because the precise nature of language and rules varies from contract to contract, the process of determining what contract applies at a given time is complex and difficult to generalize. Contract Management solves this difficulty with a sophisticated rule-processing engine that allows customers

to write their own wizard scripts. Technicians are guided by the script through a custom set of questions and answers before eventually determining a particular caller's contract information. This rule engine is linked to ServiceCenter's Incident and Service Management modules.

The object of any entitlement determination sequence is to identify both a contract and a service level agreement (SLA) that apply to the current situation. Once that information is located, the system automatically checks to see whether the referenced contract permits service at this time. Has the user exceeded the call budget? Has the contracted number of incidents been used? All this can be checked automatically.

That information is then linked to the incident ticket, call report, or change request document. The Contract Management module can then use the service information for other purposes.

Entitlement Record

The entitlement record connects a device to a service level agreement (SLA) and a contract. ServiceCenter automatically checks the entitlement record when a call is opened to determine if the device entered is entitled to service.

To access an entitlement record:

- 1 Click **Service Level Mgmt.** in the ServiceCenter home menu. The Service Level Management menu appears.
- 2 Click the **Service Contracts** tab.
- 3 Click **Entitlement Mapping** in the Service Contracts menu. A blank entitlement record appears.
- 4 Do one of the following:
 - Type search criteria in a field or select values from the drop-down lists.
 - Leave the fields blank and click **Search** or press **Enter** to perform a *true* query and retrieve a list of all current entitlement mapping records.

Figure 9-52 shows an entitlement record selected from a list of QBE records.

ID	Company	Location	Service Type	Device Type	Logical Name	SLA ID	Contract ID
1	PRGN					151	21
2	PRGN	Houston				152	15
3	PRGN	Houston				154	21
4	GENERICOM					103	18

1/12

Company: PRGN
 Location:
 Service Type:
 Device Type:
 Logical Name:
 SLA ID: PRGN Platinum
 Contract ID: PRGN VIP SERVICE

Ready Response 0.60 draw 0.231 insert servicecent.qbe.g [UP]

Figure 9-52: Entitlement Record

The following table describes the fields in the Entitlement record.

Field	Description
ID	The system assigns an ID number to each entitlement record automatically when the record is created.
Company	Select the name of the company receiving the service from the drop-down list.
Location	Click Browse to enter the location (from the location file) for the company you selected in the previous field.
Service Type	Select the type of service (Service and Incident Management category) specified in the contract.
Device Type	Contains the generic name of the type of device covered by the service contract (for example, pc).
Logical Name	Contains the unique name of the particular device covered by the service contract. (for example, pc002).

Field	Description
SLA ID	Select the service level agreement (SLA) involved in the servicing of this contract.
Contract ID	Select the unique ID of this contract from the drop-down list. This value matches the Contract ID in the contract record.

Viewing Contract Overruns

Options on the Service Contracts menu allow you to view contracts that have reached certain limits. The system lists the contracts meeting each of the search parameters defined below in a standard contract record. You may add, edit, or delete contracts in this mode. The following table describes the types of contract overruns.

Option	Description
Expired Contracts	Displays all contracts in the system whose time limit for service has expired.
Overspent Contracts	Displays all contracts in the system whose budget has been exceeded, regardless of where the money has been spent (that is, calls or Incidents).
Exceeded Incidents	Displays all contracts in the system that have exceeded their Incident allocation limit.
Exceeded Calls	Displays all contracts in the system that have exceeded their call allocation limit.

Figure 9-53 on page 340 shows a record for a contract overrun.

Contract ID	Reference Name	Start Date	End Date
18	GENERICOM GEN	01/01/99 00:00:00	01/01/02 00:00:00
20	ACME US	01/01/99 00:00:00	01/01/02 00:00:00

Contract ID: 18
Reference Name: GENERICOM GEN

General Information | Details | Rules | Named Users | Comments | Attachments | Additional Services

Start Date: 01/01/99 00:00:00
End Date: 01/01/02 00:00:00
Provider Company: PRGN
Cost Center:
Technical Account Manager: FALCON
TAM Phone number:
Escalation Contact:
Escalation Phone number:
Client Company: GENERICOM
Client Contact: GALLAWAY, SUSAN
Line Items
Duty Calendar:
Alert when not updated for:
Call time limit:
Warning time alert:

Selected line is row 1 of 2 records insert servicecontract.qbe.g [P]

Figure 9-53: Record for an Overspent Contract

Contract Wizard

Different devices, or objects, may have different contracts associated with them, even from the same provider. The Contract Management module contains a *contract wizard* designed to associate a new call with the proper contract and SLA (service level agreement). The contract wizard fills the SLA and Contract fields of the call report and establishes the link to a specific contract. Any service provided to the customer as a result of this call is automatically calculated and charged back against the correct contract. This tool greatly increases the accuracy of the accounting process.

To use the contract wizard:

- 1 Click **Service Management** in the ServiceCenter home menu. The Service Management menu appears.

- 2 Click **Take New Calls**. A new call report form appears.
- 3 Choose **Options > Get Contract**, as shown in Figure 9-54.

ServiceCenter - New Call

File Edit View Format Options List Options Help

Find Solution
SM Call List
Notify
Add/Edit Contact
Get Contract

00:02:46 Call Detail

Call ID: CALL0007

Contact Name: [Text Field]
Full Name: [Text Field]
Email: [Text Field]
Payroll No.: [Text Field]
Corp Struct/Div.: [Text Field]
Phone: [Text Field] Ext.: [Text Field]
Fax: [Text Field]

Status: Open - Idle
Owner: FALCON
Category: [Text Field]
Subcategory: [Text Field]
Product Type: [Text Field]
Problem Type: [Text Field]
Assignment: [Text Field]
Severity: [Text Field]

Reported By different from Contact Name ☐

Location: [Text Field]
Room/Floor Ref.: [Text Field]
Cost Center: [Text Field] ☐ Critical User

User Type: [Text Field]
Company: [Text Field]

Description: [Text Area]

Site Category: [Text Field]
Projected SLA: [Text Field]
Entitlement: [Text Field]

Notify By: [Text Field]
GL Number: [Text Field]
Bill To: [Text Field]

Asset ID: [Text Field]
Type: [Text Field]
Model: [Text Field]
Cause Code: [Text Field]

☐ Total Loss of Service
☐ Failed Entitlement

☐ Dept ☐ Contact

☐ Critical Asset

You have chosen to have multiple companies available.

Ready Response 0.251 draw 0.90 insert cc.inquick_g(cc.first) [UP]

Figure 9-54: New Call report

- 4 Figure 9-55 shows the first prompt of the contract wizard.

SC Contract Wizard

Contract Wizard

What company is the contact calling for?

Company: [Dropdown Menu]

<< >>

Figure 9-55: Selecting a company

5 Do one of the following:

- Select a client company from the drop-down list in the **Company** field.
- Click **Back** or **Next** to exit the contract wizard.



For this example, select a company name from the drop-down list in the **Company** field.

6 Click **Next** to go to the location prompt, or click **Back** to return to the previous prompt.

Note: You can click **Back** any time to return to the previous prompt.

7 Select the client location from the drop-down list in the **Location** field.

8 Click **Next** to go to the service type prompt, or click **Back** to return to the previous prompt.

9 Select the type of service required from the drop-down list in the **Service Type** field.

10 Click **Next** to go to the type of device prompt, or click **Back** to return to the previous prompt.

11 Select the type of device involved from the drop-down list in the **Device Type** field.

12 Click **Next** to go to the specific device prompt, or click **Back** to return to the previous prompt.

13 Select the specific device involved from the drop-down list in the **Logical Name** field.

14 Click **Next** to return to the call report or click **Back** to return to the previous prompt.

10 Change Management

CHAPTER

ServiceCenter's Change Management module is the process for requesting and approving changes in your infrastructure. Changes, as opposed to Service requests, generally affect shared equipment or multiple users. Change Management automates the approval process, eliminating the need for continuous memos, e-mails, and phone calls. However, within this process, approvers must still manually approve each change. This chapter describes the administration of ServiceCenter's Change Management module. For more information, see the *ServiceCenter User's Guide*.

Read this chapter for information about:

- *Relationship to Service Management* on page 346
- *Components of Change* on page 348
- *Workflow* on page 348
- *Security and Access Control* on page 352
- *Using Change Management* on page 354
- *Managing Categories and Phases* on page 370
- *Change and Task Phases* on page 384
- *Change Records* on page 409
- *Tasks* on page 425
- *Approvals* on page 435
- *Risk Calculation* on page 446
- *Events, Alerts, and Messages* on page 450

Relationship to Service Management

Service Management has relationship models that define different methods that can be used to control the relationships between records inside ServiceCenter. For more information, see [Service Management Record Relationship Models](#) on page 46.

Glossary

The following table lists terms used in Change Management.

Term	Definition
Alerts	A series of checkpoints taken against a change or task to ensure that required work activities occur within specified time frames.
Approvals	A list of groups or operators who must acknowledge or accept the risk, cost, and so on associated with the implementation of a change or task. Once the approval requirements are set up, approvals give controlling authorities the ability to stop work and to control when certain work activities can proceed. Approvers manually approve changes before tasks are assigned.
Approval sequence	Order in which approval requirements are made active. The process first makes the lowest sequence numbers available for approval activity. Once these are approved, the next highest number is made available. Groups with the same sequence number can approve in any order.
Category	Major logical classification of change requests and tasks. The category determines the data to be collected for a particular change or task. ServiceCenter includes a series of default categories, or administrators can create new categories.
Changes	Changes are the records submitted seeking the change. The change has a life cycle containing approvals, alerts, tasks, phases, and closure. Changes are based on categories.
Change number	Unique ID assigned to a change when it is submitted.
Change owners	Required to give a technical approval for the phase to proceed.

Term	Definition
Change sponsors	Required to authorize the change from the customer business perspective. If a Change Sponsor does not have access to ServiceCenter, Change Administrators (CAs) are responsible for ensuring that authorization is obtained from the Change Sponsor. CAs must approve the RFC on behalf of the Change Sponsor on the ServiceCenter system.
Event	The occurrence of a specific detectable action or condition; such as the opening of a change or task, an approval, an update, and so on.
Group	One or more operators assigned to a common area of responsibility. Typically, each group reflects a business or technical area (or department).
Initiator	Person who starts the process of a Request for Change.
Phase	An administrative step within the change or task that is needed to complete the work. A phase determines how forms are viewed by the users, approval requirements, and the intervals at which alerts are sent. Phases are sequential, repeatable steps characteristic of a Change category. You can approve or close a phase. When you take an action on a phase, you can move to the next phase. When a task or Change has no more phases, that task or Change can be closed.
Profile	The security record that defines which options and authorities are available to the operator or group using the profile.
Projected data	Data copied from fields in a model record to identically named fields in the newly opened Request record (source).
Task	<p>Work processes necessary to complete the change and related to the Change. For example, the tasks involved in replacing a hard drive with a larger model might include: ordering the new drive, backing up the old drive, and installing the new drive.</p> <p>Tasks must belong to a Change. Task start and end dates, if specified, must fall within the start and end dates of the parent change. Tasks, themselves, can be broken into phases, if that level of discrimination is necessary.</p> <p>Tasks are classified by categories.</p>
Task number	A unique ID assigned to a task.

Components of Change

The Change process allows needed work to be accomplished. Improvements and maintenance are initiated by requests made by users and managers across the system. Requests are implemented in the following manner:

- A technician creates a *change record* and assigns a *change category* to the record. The category is a classification of the change requested (for example, hardware).
- ServiceCenter assigns a predefined *change phase* to the change, based on the category the technician selected. The phase selected determines such things as which forms are displayed, how the request is reviewed, and which general system options are available during that phase.
- If the initial change phase requires it, *approvals* must be given before that phase can be closed.
- Closed change phases automatically advance to the next phase in a predetermined sequence, unless the change has only one phase.
- If a change phase requires several steps to accomplish, it may be necessary to create one or more *tasks*.
- When you create a task, the system displays a prompt for a *task category*.
- A predetermined *task phase* for the selected category is assigned to the task.
- Closed task phases automatically advance to the next phase in a predetermined sequence. All task phases must be closed before the change request can be advanced to the next change phase.

Note: Although the functionality exists to create long sequences of task phases, such detail is seldom needed to resolve a change project. It is usually sufficient to resolve a change phase with a single task phase per task.

Workflow

Change Management allows the user to request a change to software, hardware, network connections, and facilities quickly and easily. ServiceCenter leads you through the process by prompting you for required information, and adding information through the Fill process. Figure 10-1 on page 350 shows a flowchart of the change process, using the example of requesting a new hard drive for a server.

Note: The workflow can be changed by modifying ServiceCenter scripts to meet your business process flow.

To begin the change process, you submit a *request for change*. This is similar to opening an incident ticket.

For example: You are responsible for supporting an application that runs on a server. You discover the hard drive in your Application server is not large enough to support expected growth.

To submit a change:

- 1 You *open* a change from Change Management. In submitting (opening) a change, you are the *requestor*. In this example, you would request the larger hard drive.
- 2 After you submit your change, *approval groups* are notified. In this example, the change is sent to your manager.
- 3 Your manager *reviews* the change.
- 4 A *decision* is made on the change. Your manager either:
 - a *Approves* the change. The change process then moves to step 5.
 - b *Denies* the change. The change process then moves to step 9 to notify the user who opened the change.
- 5 The process moves to the next change phase, which is notifying the personnel who can implement the change. In this example, the *IT department* is notified of the change.
- 6 In this phase, a task is created. In this example, the IT manager notifies the appropriate *technician* of the change.
- 7 The actual work to complete the change becomes a task phase. The technician installs the hard drive.
- 8 The technician closes the task phase.
- 9 You, as the requestor, are notified.
- 10 The change phase is closed.

Note: Instructions for opening and approving changes are provided later in this chapter.

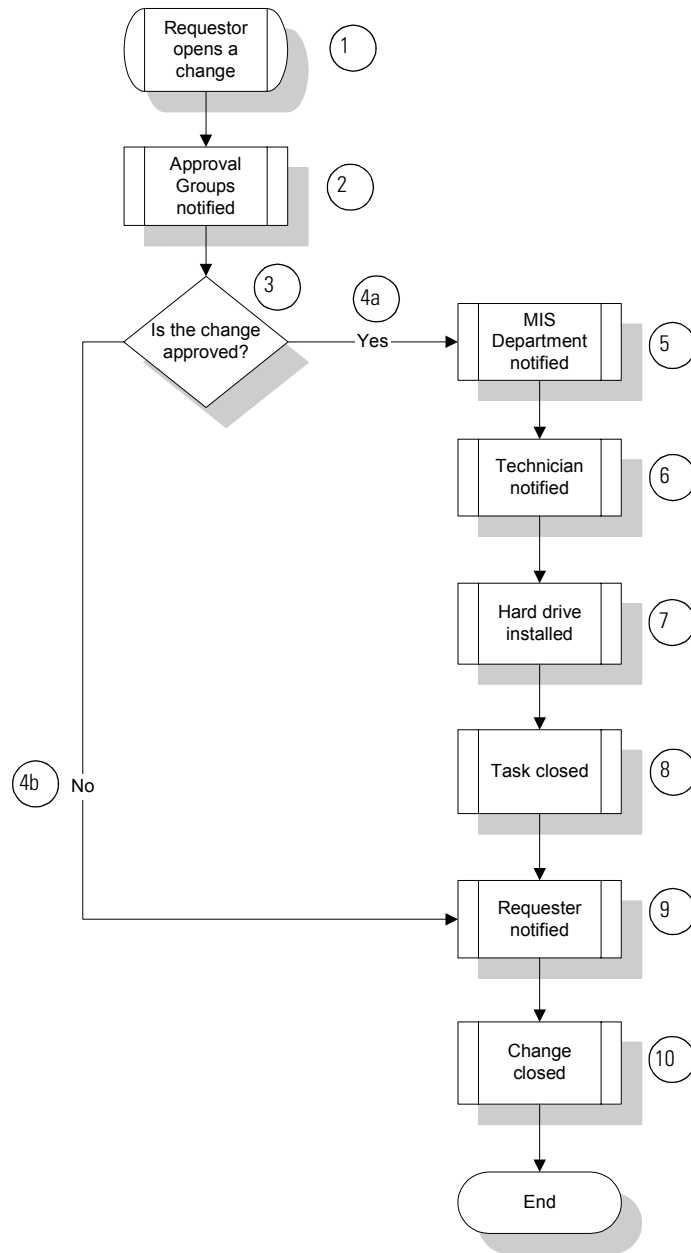


Figure 10-1: Change Management Flow

A denial does not necessarily mean the end of a change. Figure 10-2 shows alternate flowchart of the change process.

To submit a change (alternate example):

- 1 You, as the *requestor*, submit a change.
- 2 After you submit a change, notifications are sent to the appropriate personnel (*approval groups*) via e-mail, internal mail, or paging. Notifications can be sent at any time during the approval process.
Change Management also sets an alert schedule. The ServiceCenter administrator determines who receives change requests and when alerts are issued.
- 3 Approval groups review the change request. A change request can be reviewed after an approval is issued. Change Management contains a list of authorized approvers.

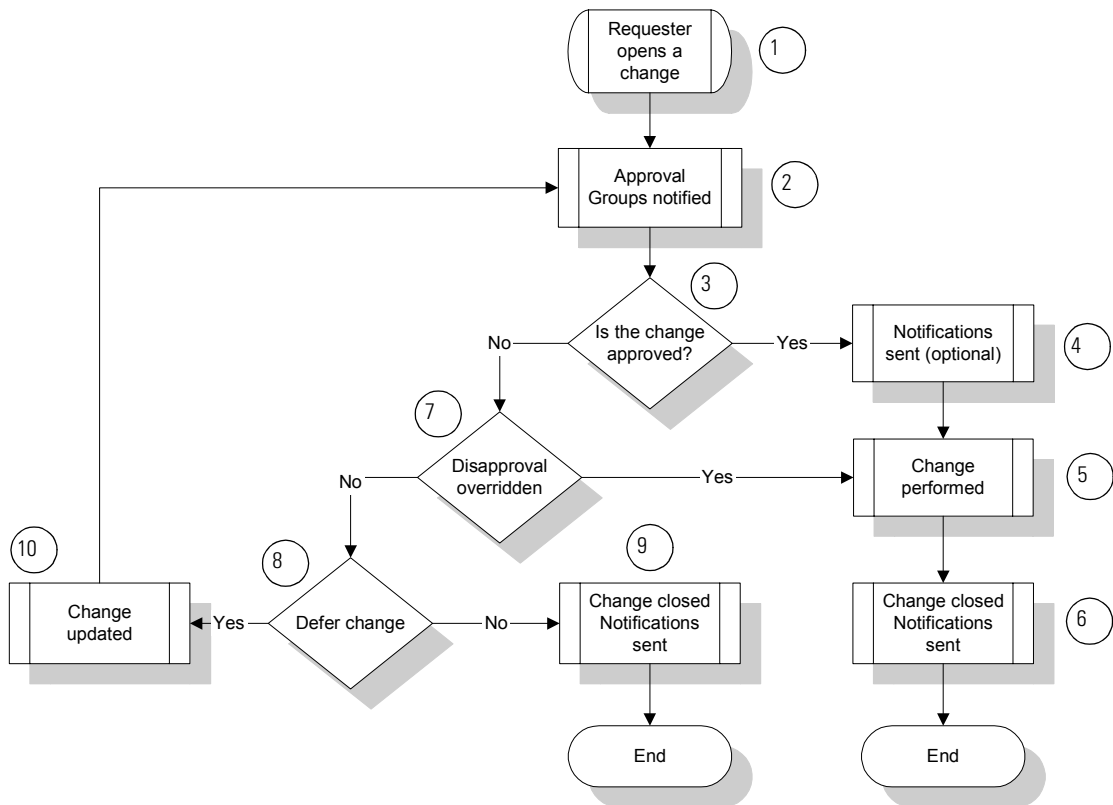


Figure 10-2: Alternate Change Management Flow

If the change is Approved:

- 1 A notification can be sent to the personnel involved, for example, the requestor and those implementing the change.
- 2 The change is performed and notifications are sent. This actual work to complete the change can be broken down into tasks and phases. For more information, see *Change and Task Phases* on page 384.
- 3 The change request is closed.

If the change is Denied:

- 1 The denial can be overridden, which takes the change back to step 5.
- 2 A decision is made whether or not to postpone (defer) the change.
- 3 If the change is *not* deferred, the change is closed and the requestor and other appropriate personnel are notified.
- 4 If the change is deferred, the change request is updated and is automatically resubmitted to the approval process at step 2.

Security and Access Control

Access procedures to Change Management functions are controlled in the following order:

- 1 The user's operator record is selected for capability words to determine which, if any, of the functional areas within Change Management the user can access.
- 2 If the user has the right capability word(s) to get into the Change Management functional areas, the system searches for:
 - a The user's Change Management *Profile record*, based on the *User Role* selected in the user's operator record.
 - b If the application profile record for the operator is blank, the system checks the *environment* record to determine if the operator can use the DEFAULT profile record for the specific Area. If no DEFAULT profile exists for the specific Area, the system searches for the DEFAULT profile for All Areas.
- 3 Once the user enters Change Management, capabilities are established using either the User Role profile record or the DEFAULT profile record.

- 4 Depending upon the conditions set up in the *phase* definition record, a user might not be allowed to update a change or task, even if granted the general capability to do so in the User Role profile record. Figure 10-3 shows the order of execution.

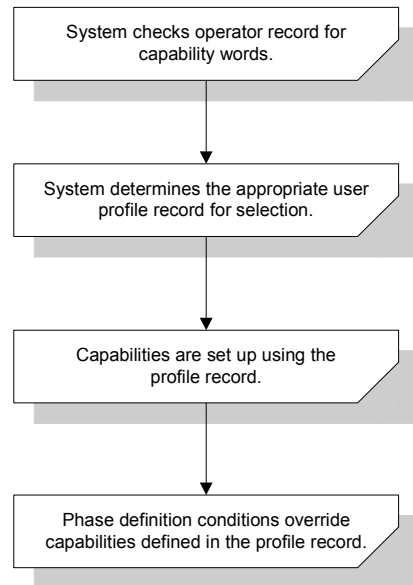


Figure 10-3: Execution Order of Change Management Access Control

Capability Words

Before you can add a profile to a Change Management user, that user must have an operator record. A user's Change Management abilities are set in the Execute Capabilities array of the operator record.

These capability words are used to set a user's access:

- **SysAdmin** — access to all user and administrative functions, as well as the rest of ServiceCenter. Access to all CM (Change Management) modules for administration and user functions is available regardless of the Change or Task profile that is set in the user's operator record.
- **CM3Admin** — allows access to all CM (Change Management) modules for administration and user functions regardless of the Change or Task profile that is set in the user's operator record. CM3Admin is not required for SysAdmin.

- **change request** — allows access to Change Management changes.
- **change task** — allows access to Change Management tasks.

Note: The CM profile only adjusts CM security access for users with CM3Admin capability. SysAdmin and CM3Admin capabilities both grant complete access to all ICM functionality.

The capability words control which options are available in the profile record. The operator record overrides the profile record. If the user does not have a capability word in the operator record, that option cannot be used, even if the option is selected in the profile. For a complete list of capability words, see the *ServiceCenter System Administrator's Guide*.

Using Change Management

You can access Change Management for administrative purposes from the Change Management section of the ServiceCenter home menu, or from the Central Administration Utilities.

The Central Administration Utilities allow a system administrator to access the operator's record for user and contact information, application profile privileges, and the Mandanten utility. This allows the administrator to control and access several users or a group's access from one central location, rather than having to control access from within each module or utility.

To administer *User Role Profiles* from the Central Administration Utility, see the *System Administrator's Guide*.

To modify the operator record of an existing user to provide Change Management capability:

- 1 Select the **Utilities** tab in the ServiceCenter home menu shown in Figure 10-4.

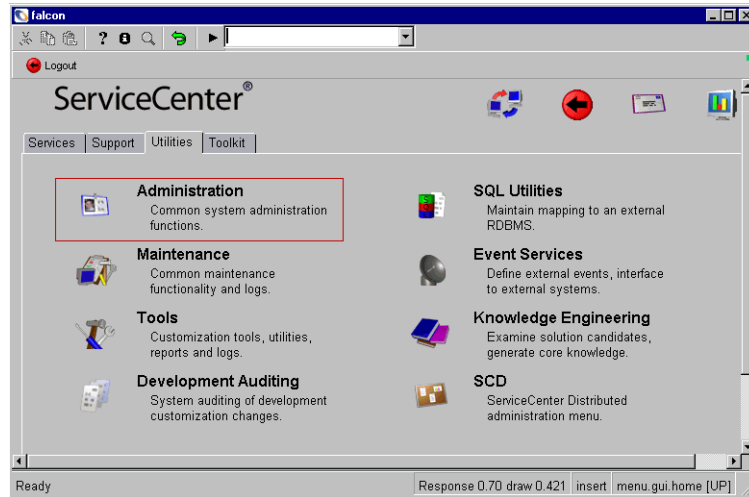


Figure 10-4: ServiceCenter home menu: Utilities tab

- 2 Click **Administration**. Figure 10-5 shows the The Administration menu.

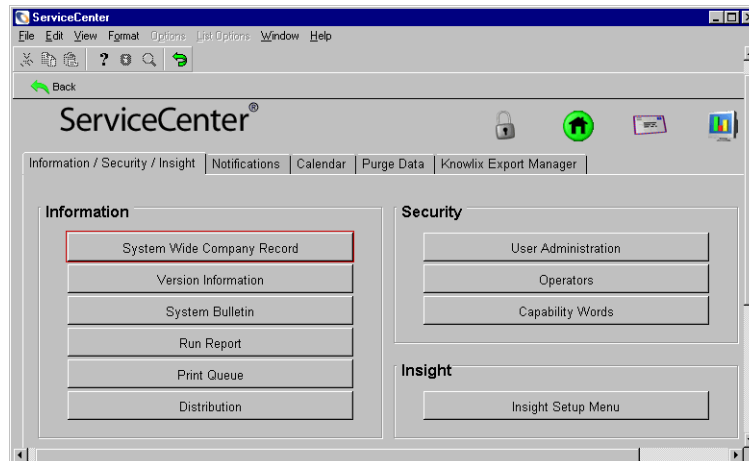


Figure 10-5: Administration menu: Information/Security/Insight tab

- 3 Click **Operators** in the Security structure. A blank operator record appears.

- 4 Type the ServiceCenter Login name for the user operator record to be modified.
- 5 Click **Search** to access the user's operator record. Figure 10-6 shows the Operator record.

The screenshot shows a window titled "Search Operator Records" with a toolbar containing icons for Cut, Copy, Paste, Help, Find, and a search button. Below the toolbar is a tabbed interface with the "Operator Record" tab selected. The tabs include General, Security, Login/Contact Profiles, Startup, Notification, Security Groups, and Billing Information. The "General" tab contains several sections:

- General Information:** Login Name (text field), Language (dropdown), Full Name (text field), and Default Company (dropdown).
- Date Information:** Time Zone (text field) and Format (dropdown).
- Time Limits:** Database (text field), Asset Mgmt (text field), and Change Mgmt (text field).
- Application Profile:** A list of profiles with checkboxes: User Role, Service Profile, Incident Profile, Root Cause Profile, Inventory Profile, Contract Profile, Change Profiles, and Request Profiles.

 The status bar at the bottom displays "Ready", "Response 0.230 draw 0.311", and "insert operator.g(operator.search) [UP]".

Figure 10-6: Operator Record: General tab

For more information, see the *System Administrator's Guide*.

- 6 Select the **Startup** tab. Add the desired Change Management capabilities to the Execute Capabilities array.
- 7 Click **Save** or press F2. The status bar displays this message: User profile record updated.

Environment

Change Management contains an environment record that defines options that affect functionality of the Change Management module for all Change Management users. This configuration is accomplished in *two* Change Management environment records, for *Changes* and *Tasks*. Each record has the same options. Two records are needed, because user profiles are defined as either change profiles or task profiles in the **Area** field. For more information, see [Security Profiles](#) on page 358.

To set up the Change Management environment using the Central Administration Utilities, see the *System Administrator's Guide*.

To set up the Change Management environment:

- 1 Click **Change Management** in the ServiceCenter home menu.
The Change Management menu appears.
- 2 Select the **Changes** or **Tasks** tab.
- 3 Click **Change Environment** or **Task Environment**. Figure 10-7 shows the Change Management application environment record.

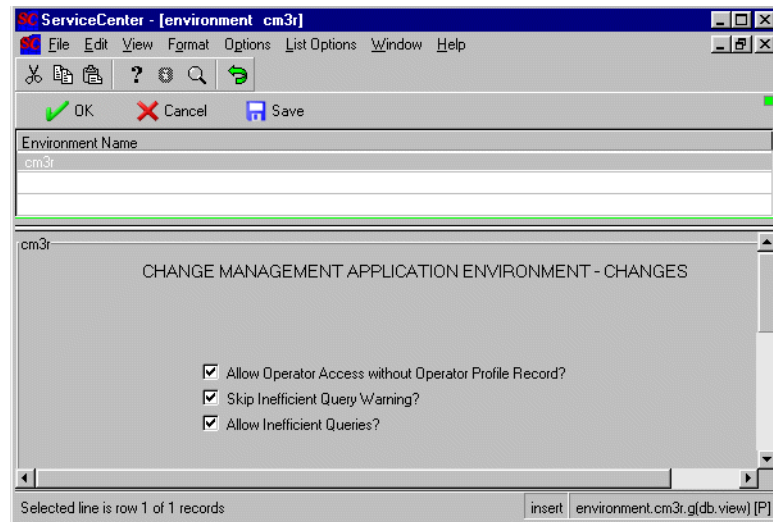


Figure 10-7: Change Management Application Environment record

- 4 Select the fields representing the parameters you want to apply to your Change Management system.

- **Allow Operator Access without Operator Profile Record?** — permits users without an Operator Profile for Change Management to access the module using the DEFAULT profile.
 - **Skip Inefficient Query Warning?** — disables message, warning users that a non-keyed query will be slow. Setting to *true* (selected) overrides the setting in the **Allow Inefficient Queries?** option.
 - **Allow Inefficient Queries?** — allows the user to execute an incomplete or partially-keyed query. This option is overridden when **Skip Inefficient Query Warning?** set to *true*.
- 5 Click **Save** or press F2 to save any changes to the record.
- The status bar displays this message: **Environment record updated.**

Security Profiles

Change Management security profiles define the abilities of Change Management users. Multiple users can share one profile. A user can have multiple profiles, for Tasks and Changes.

When a user accesses Change Management, ServiceCenter checks for the profile found in the operator record for Change Management. First the operator profile records are selected for that user and area, then the records are selected.

Profile records can work in conjunction with Message Group Definition records. For more information, see [Message Group Definition Record](#) on page 366.

Note: When configuring a large system with many operators, you can add multiple members to a group security type of profile based on the User Role. This reduces the number of duplicate operator security profiles necessary to fulfill the same function.

As a system administrator, you can add, modify, or delete profiles. For more information, see the *ServiceCenter System Administrator's Guide*.

To access profile records:

- 1 Click **Change Management** in the ServiceCenter home menu. The Change Management menu appears.
- 2 Select the **Maintenance** tab in the Change Management menu.
- 3 Click **Profiles**. Figure 10-8 shows a blank Security Profile form.

The screenshot shows a window titled "ServiceCenter - [User Change Profile]". It has a menu bar with File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu bar is a toolbar with icons for Back, Add, Search, Find, and Fill. The main area is titled "CM Security Profile" and has a "Profile Name" field. There are four tabs: Basic, Approval/Print, Query, and Category. The "Basic" tab is selected. Under "Basic Options", there are two columns of checkboxes: Alerts, Calculate Risk, Close, Change Category, Change Phase, Copy and Open, Count Records, Open, Reopen, Expand Array, Fill, Find, I/R Query, List Pages, Notify, Save, (closed) Save, Profile Area (dropdown), Review, Search Duplicates, Show Parent, Tasks, Validity Lookup, and Views. At the bottom, there are fields for Change Manage Format, Task Manage Format, Initial Change Inbox, Initial Task Inbox, Approval Groups, Review Groups, and Manager Group. The status bar at the bottom shows "Ready" and "insert cm3profile.gl(profile.search) [P]".

Figure 10-8: CM Security Profile form

- 4 Click **Search** to perform a *true* query and retrieve a list of all current profile records. Figure 10-9 shows a QBE list of profile records.

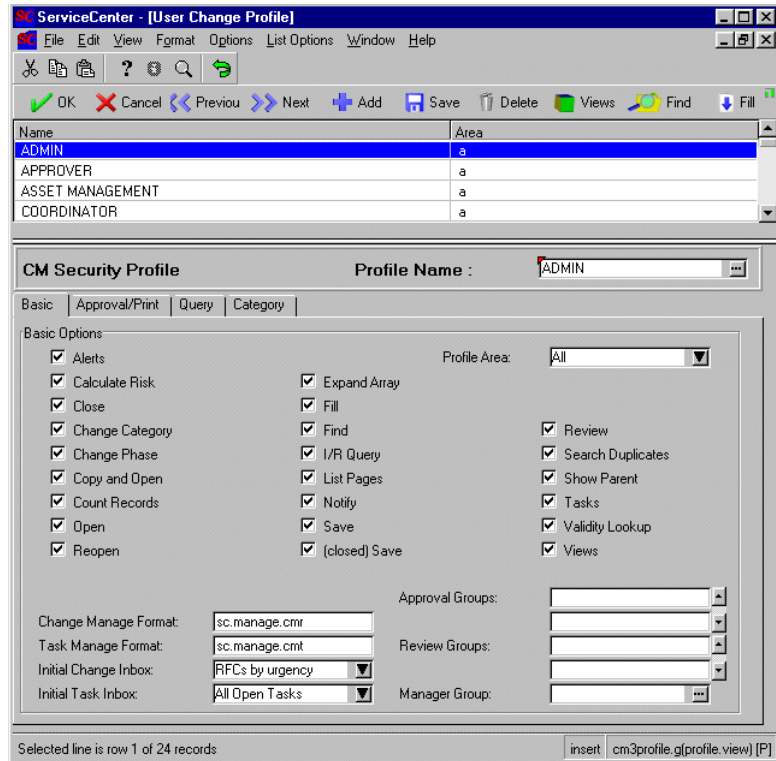


Figure 10-9: CM Security Profile with a record list

- 5 Select a profile from the record list. The appropriate profile information displays.

Header field

Change Management Profile fields are grouped in tabs to define the Change Management user. Required fields are noted.

Field	Description
Oper/Group Name (required)	Name of the user or group that is defined by this profile. The Fill function can be used on this field, or you can enter a new name.

Basic tab

The following table describes fields on the Basic tab.

Field	Description
Profile Area (<i>required</i>)	Area of Change Management that applies to the user: Changes, Tasks or All.
Alerts	Allows the users to check the alert status for a change or task record.
Calculate Risk	Enables the manual execution of risk calculation. If selected, the Calculate Risk option displays in the Options menu of a change request.
Close	Allows the user to close the currently opened task or change. All tasks must be completed to close a change.
Change Category	Allows the user to change task or change categories while in the update mode.
Change Phase	Allows the user to change the task's or change's phase while in the update mode.
Copy and Open	Allows the user to copy information in the current change or task record and open a new record containing the same information. If the record has associated tasks, ServiceCenter prompts you to copy the tasks with the change or task record. If you choose to copy the tasks, ServiceCenter creates a new task for each original task. The new record can then be modified and added. For more information, see the <i>ServiceCenter User's Guide</i> .
Count Records	Allows the user to count the number of records in a QBE list.
Open	Allows a user to open a new change or change task.
Reopen	Allows a user to reopen a closed change or change task.
Expand Array	Allows the user to add a field to, or easily edit, an array. The array appears in a separate window, allowing you to avoid the need to scroll through the array to do your editing.
Fill	Allows the user to use ServiceCenter's Fill function.
Find	Allows the user to use ServiceCenter's Find function.
I/R Query	Allows the user to access ServiceCenter's IR Expert application and run a query against a specified file.
List Pages	Allows the user to access all the pages in a task or change record.

Field	Description
Notify	Allows the user to access the <i>mail.notify</i> form, containing a message window and the record. A user can attach a message to the record and send the record to someone else via standard e-mail, SCmail, or fax. Using ServiceCenter for e-mail, faxing, and paging is discussed in the Event Services documentation.
Save	Allows the user to save updates to a task or change record.
(closed) Save	Allows the user to save updates in a closed record.
Review	Allows a user to review change tasks or changes.
Search Duplicates	Allows the user to query the Change Management database for duplicate changes. If you place your cursor in the field of a record and select Search Duplicates, a QBE list of records displays that contains the same values as the field in which the cursor was placed. When a you access this option, a message asks which change status should be searched: <ul style="list-style-type: none"> ■ Active — currently open changes. ■ Inactive — closed changes. ■ Deferred — changes that have been deferred. ■ All — search all changes in the database.
Show Parent	Allows the user to locate the parent change for a task.
Tasks	Allows the user to access the Task functionality of Change Management.
Validity Lookup	Allows the user to check a selected field against the ServiceCenter validity tables.
Views	Allows the user to access the Views function in the task and change records.
Change Manage Format	Name of the form you want to open as the default change queue form.
Task Manage Format	Name of the form you want displayed as the default task queue form.
Initial Change Inbox	Inbox (records) that display initially in the change queue.
Initial Task Inbox	Inbox (records) that will display initially in the task queue.
Approval Groups	Members of the approval groups have approval authority. Members in this group should be added to each Message group's Approvers array, so they can receive notification when requests are awaiting their approval.

Field	Description
Review Groups	Members of the review groups are the personnel who can examine the tasks and phases of a change, but do not have approval authority. Members in this group should be added to each Message group's Reviewers array, so they can receive notification when requests are awaiting their review as part of the approval process.
Manager Group	Members of the manager group are a necessary part of the process to manage the requests for change for a user or a group of users.

Approval/Print tab

Figure 10-10 shows the Approval/Print tab.

The screenshot shows a software interface with four tabs: Basic, Approval/Print, Query, and Category. The 'Approval/Print' tab is active. Below the tabs, there are two sections: 'Approval Options' and 'Print Options'. In the 'Approval Options' section, there are three checkboxes: 'Approvals' (checked), 'Override' (checked), and 'Mass Approve' (unchecked). In the 'Print Options' section, there are two checkboxes: 'Print' (checked) and 'Print List' (checked).

Figure 10-10: Security Profile record: Approval/Print tab

Approval Options

The following table describes options on the Approval/Print tab.

Option	Description
Approvals	Allows the user to approve tasks or changes.
Mass Approve	Allows the user to approve all current tasks or changes in that user's approval queue. If this check box is selected, the Mass Approve option displays in the List Options menu of tasks and changes.
Override	Allows you the approval authority to override a prior approval action, whether approved, denied, or retracted.

Print Options

The following table describes options on the Approval/Print tab.

Option	Description
Print	Allows this profile to print individual change requests. If this check box is selected, Print displays in the Options menu of a change request.
Print List	Allows this profile to print a Change Management QBE list. If this check box is selected, Print List displays in the List Options menu of a change request record list.

Query tab

Figure 10-11 shows the Query tab.

The screenshot shows the 'Query Options' dialog box. It has four tabs: 'Basic', 'Approval/Print', 'Query' (selected), and 'Category'. Under the 'Query' tab, there are two columns of checkboxes. The first column contains 'Active' (checked), 'Expert Search' (checked), 'All' (checked), and 'Clear' (checked). The second column contains 'Deferred' (checked), 'Inactive' (checked), 'Inefficient Query' (checked), and 'Mod Time Limit' (checked). The third column contains 'Restore' (checked) and 'Skip Warning' (checked). At the bottom, there are four fields: 'Append Query:' (empty), 'Time Limit:' (00:00:10), 'Initial Format:' (cm3r.search), and 'QBE Format:' (empty). Each of the last three fields has a dropdown arrow on the right.

Figure 10-11: Security Profile Record: Query tab

Query Options

Note: The Active, All, Deferred, and Inactive options define what type of changes and/or tasks a user can look up. At *least* one of these options must be checked, or the profile record cannot be saved.

Option	Description
Active	Allows users of this profile to query for active task and change records.
Expert Search	Allows users of this profile to run an advanced search, where the query parameters can be modified. If this is selected, Expert Search displays in the Options menu of the Change Management search forms.

Option	Description
All	Allows users of this profile to query all task and change records.
Clear	Allows users of this profile to remove data from all fields in a form.
Deferred	Allows users of this profile to query for deferred tasks and changes.
Inactive	Allows users of this profile to query for inactive tasks and changes.
Inefficient Query	Allows users of this profile to run an incomplete (inefficient) query. This setting is overridden when Skip Warning set to true.
Mod Time Limit	Allows users of this profile to modify a query's time limit.
Restore	Allows you to return the fields in the form to the previous values. Only available in the initial form where you enter data.
Skip Warning	Sets ServiceCenter to avoid inefficient query warnings in Change Management for users of this profile. Setting to <i>true</i> (selected) overrides the setting in Inefficient Query.
Append Query	Expression that the system will append to all queries executed by users of this profile.
Time Limit	Sets the amount of time a query runs for this profile before a message that no matching records were found appears.
Initial Format	Sets the form used for the query (search) form used when this profile is in effect.
QBE Format	Sets the form (format) used for this profile to display a QBE list.

Category tab

Figure 10-12 shows the Category tab.

The screenshot shows a software window titled 'Security Profile Record: Category tab'. At the top, there are four tabs: 'Basic', 'Approval/Print', 'Query', and 'Category'. The 'Category' tab is selected. The main area is divided into two sections. The top section, 'Category Restrictions', contains three labels: 'Default Change Category:', 'Default Task Category:', and 'Allowed Categories:'. Each label is followed by a text input field. The 'Default Change Category' field is highlighted with a green border. The 'Allowed Categories' field is a multi-line text area. The bottom section, 'Statements', contains a list box with several empty rows for text entry.

Figure 10-12: Security Profile Record: Category tab

The following table describes restrictions that you can set on the Category tab.

Restriction	Description
Default Change Category	This field only displays if the profile area is “c” or “a.” Sets the default Change Management Request category for the user(s) defined in this profile.
Default Task Category	This field only displays if the profile area is “t” or “a.” Sets the default Change Management Task category for the user(s) defined in this profile.
Allowed Categories	Names the categories that can be used in a change request. The records of categories are displayed in this list and are the only category records that can be opened to users of this profile. Note: You can still view other categories.
Statements	Allows you to enter statements to further restrict this profile’s capabilities.

Message Group Definition Record

ServiceCenter Change Management uses Message groups to identify the members of a work group, also known as a Message group. Message groups include two kinds of members:

- Members who receive work messages sent to the group. Typically these include event and alert messages. For example, notifying members of the progress of requests and tasks that their group is responsible for managing or working. Members automatically act as reviewers.
- Approvers are group members authorized to approve requests for this group. They typically receive notifications when a request is awaiting their approval.

Approvers are not automatically reviewers. If any approvers need to receive ALL of the group's notifications, whether related to work activities or to approvals, you should add them to both this group's Members and Approvers lists.

The Message group definition record stores the individual login IDs of the group’s members and approvers who will receive notification and messages during a change project.

To create a Message group definition record:

- 1 Select the **Maintenance** tab in the Change Management menu.
- 2 Click **Groups**. A blank Groups Definition form appears.
- 3 Do one of the following:
 - You can create a new message group.
 - Click **Search** to perform a *true* query and retrieve a list of all the message group records. Select a record to copy. If you copy an existing record, be sure to **Add** the new record to create it, rather than edit the existing selected record. Figure 10-13 shows a QBE list of records.

The screenshot shows the ServiceCenter - [Change Groups] window. At the top is a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Previous, Next, Add, Save, Delete, Find, and Fill. Below the toolbar is a table with three columns: Name, Area, and Description.

Name	Area	Description
ADMIN	a	Change Administrators
ASSET MANAGEMENT	a	Asset Managers
COORDINATOR	a	Change Managers
EMERGENCY GROUP	a	EMERGENCY GROUP

Below the table is a section titled "CHANGE MANAGEMENT GROUPS DEFINITION". It contains several fields:

- Group Name: ADMIN
- Area: All
- Description: Change Administrators
- Manager: FALCON
- Calendar: (empty)
- Company: PRGN
- Company: GENERICOM
- Company: DEFAULT
- Company: (empty)
- Company: (empty)

At the bottom, there are two lists: "Members" and "Approvers".

Members	Approvers
CA 1	CA 1
CA 2	CA 2
CA 3	CA 3

At the bottom of the window, it says "Selected line is row 1 of 19 records" and "insert: cm3groups.gl(group.view) [US]"

Figure 10-13: Messaging Rights for Members (Reviewers) and Approvers

4 Populate the fields with the following values.

Field	Description
Group Name (<i>required</i>)	Name of the group, usually indicative of the department to which it refers. This name must be unique with each Area.
Area	Change Management functions available to this group. Valid values are: Changes, Tasks, and All.
Description	Description of the group.
Manager	The name of the person who will be managing the group.
Calendar	Shift calendar defining the working hours of this group. This value is used in alerts processing.
Company	Company the group belongs to.
Members	Login IDs of the group members who will receive alert and event messages for this group and messages sent to this group's reviewers. Members are added to this list through the profile record. Select Options > Rebuild Group to update this Members list to include any profile record group additions or changes made in the profile record.
Approvers	Login IDs of this group's authorized approvers who will receive messages sent to this group's approvers. Approvers are added to this list through the profile record. Select Options > Rebuild Group to update this Approvers list to include any profile record group additions or changes made in the profile record.



- 5 Click **Add** to add the new record to the file. The status bar displays this message: **cm3groups record added**.

Options Menu — Blank Record

The options menus for all blank Message group definition records located in the Maintenance tab of the Change Management menu contain the same options.

Option	Description
Clear	Clears the data entered in the form.
Restore	Returns the fields in the form to the previous values. Only available in the initial form where you enter data.
Advanced Search	Displays a list of possible search parameters. If a partial or non-keyed query is entered, a time limit window appears to allow you to set a time limit for a query. This time is entered in the hh:mm:ss format.
IR Query	Accesses ServiceCenter's IR Expert application.
Export/Unload	Allows you to export this record into a file for importing into a spreadsheet, or unload this data set for loading into another ServiceCenter system.
Validity Lookup	Checks the data in the current field against the ServiceCenter validity table for that field.
Reset	Deletes <i>all</i> records in the current file.
	Warning: Do not use the Reset option unless you want to rebuild all the records in the current file.
Regen	Regenerates the indices for the current file.
Open Inbox	Allows the user to select a predefined query (inbox) to search the file.
Expand Array	Allows you to add a field to an array. A separate window appears to allow you to enter data.

Options Menu — Active Record

The options menus for active Message group definition records located in the Maintenance tab of the Change Management menu contains the following option.

Option	Description
Rebuild Group	<p>Updates the Message Group definitions to match the Members (reviewers) and Approver Groups data from all Change Management profile definitions (cm3profiles). This option displays for Message groups only.</p> <ul style="list-style-type: none"> ■ For any profile that includes this Message Group in the Member (reviewer) Groups array, it adds the operator or group name to the Message Group's Members (reviewers) array. ■ For any profile that includes this Message Group in the Approval Groups array, it adds the operator or group name to the Message Group's Approvers array.

Managing Categories and Phases

Categories are used to classify changes and tasks. Categories are also used to define the phases of a change. These phases are defined within the category. The phase determines which form is used with a record, along with behaviors such as approvals, edits, and so on. As a ServiceCenter administrator, you can utilize the default categories shipped with the product, or create new categories to match your enterprise.

Changes and tasks each have their own categories. A category must have at least one phase. A phase is a step in the life-cycle of a task or change. A task is the work necessary to complete a change phase.

See Figure 10-17 on page 375 for a description of how categories and phases operate in Change Management. Notice that you cannot create *Change Phase 2* until you close all tasks in *Change Phase 1*.

When you open a new change for the first time in a session, ServiceCenter asks you for the *Change profile* you want to use for this change session. You are then prompted to select a *change category*.

Within each change category, a *change phase* or group of phases is defined. The change phases can be broken down into tasks. A change phase can have one task, multiple tasks or no tasks. These tasks are defined by their respective categories. Each task category can have a phase or a group of phases.

Each change and task category and phase has a definition record. The rest of this section describes how to access, create, change, delete, and use category and phase definitions. Changes and tasks have nearly identical category and phase definition records. A few differences do exist, however, so this guide discusses each one separately.

Change Categories

Whenever you attempt to open a new change, Change Management asks you for a category. The form displayed is dependent upon which category you select. For more information, see the *ServiceCenter User's Guide*.

Category	Description
Application	Manages production application changes.
HW Server	Manages HW Server changes.
Hardware	Manages Hardware changes.
MAC	Manages general Moves, Adds and Changes.
RFC	Request for Change.
RFC - Advanced	Manages the operational risks and costs of system wide changes, such as moving personnel, assets, and systems of a single business unit or multiple business units.
Security	Manages changes in Security profiles and user accounts.

Figure 10-14 shows Change Category records.

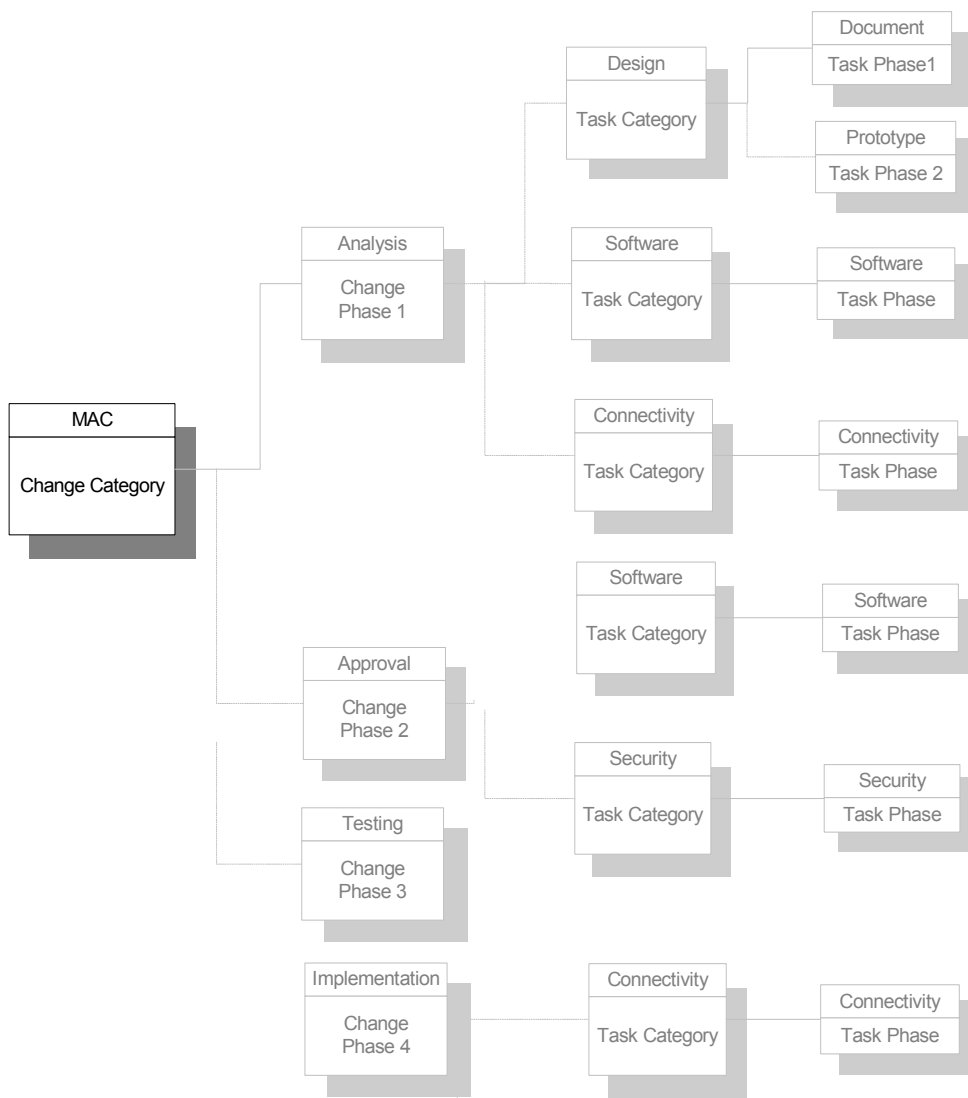


Figure 10-14: Change Category records

To access the change category records:

- 1 Click **Change Management** in the ServiceCenter home menu.
The Change Management menu appears.
- 2 Click **Change Categories**. A blank change category record appears.

- 3 Click **Search** or press **Enter** to perform a true query and retrieve a list of all current change category records. Figure 10-15 shows a QBE list of all change categories in the system.

Category	Description
Application	Production Application Changes
HW server	Hardware Server
Hardware	Hardware Move/Add/Change
MAC	General Purpose Move/Add/Change
RFC	Request For Change
RFC - Advanced	Advanced Request for Change
Security	Request Chg/Add/Del of User Accts

Selected line is row 1 of 7 records insert cm3rcategory.qbe.g(cm3.category.maint.qbe) [P]

Figure 10-15: QBE List of Change Categories

- 4 Double-click a category in the list. Figure 10-16 shows the selected record.

ServiceCenter - [Edit Category Record]

OK Cancel Previous Next Add Delete Save

Category Name: RFC

Category Description: Request For Change

Company: PRGN

Availability: true

Assign Number?: ☒

Change Phases

- Assessment
- Building
- RFC Testing
- RFC Implementation

Ready insert cm3rcategory.g [P]

Figure 10-16: Change Category record

Change Category Record Fields

The following table describes fields in the Change Category record.

Field	Description
Category Name	Unique name assigned to the category record.
Category Description	Brief description of this category.
Company	Indicates that a category can be used by the company entered. One help desk may be used for multiple companies. Indicate which company uses a category with this option. (This option can be set up to be used with Format Control or validity to enforce the use of a category by only certain companies.)
Availability	Conditional field specifying if a user is allowed access to this category. This field can be set to <i>true</i> or <i>false</i> or a condition the user must meet to have access. Users with SysAdmin or CM3Admin capabilities will have access to the category regardless of the condition specified in this field.
Assign Number?	Indicates when Change Management assigns a unique ID to a change. Selecting the box for this field (a <i>true</i> setting) indicates the unique ID is assigned before the change is opened. Default is <i>false</i> , if <i>NULL</i> . Note: When modifying the RFC - Advanced category, this field must be checked (<i>true</i>), so that a number is immediately assigned to a change. If this field is left unchecked (<i>false</i>), the change will not open.
Change Phases	Lists the phases through which this change must go. For more information, see Change and Task Phases on page 384.

Task Categories

Whenever you attempt to open a new change task, a message asks you to select a category. The change task form displayed is dependent on which category you select.

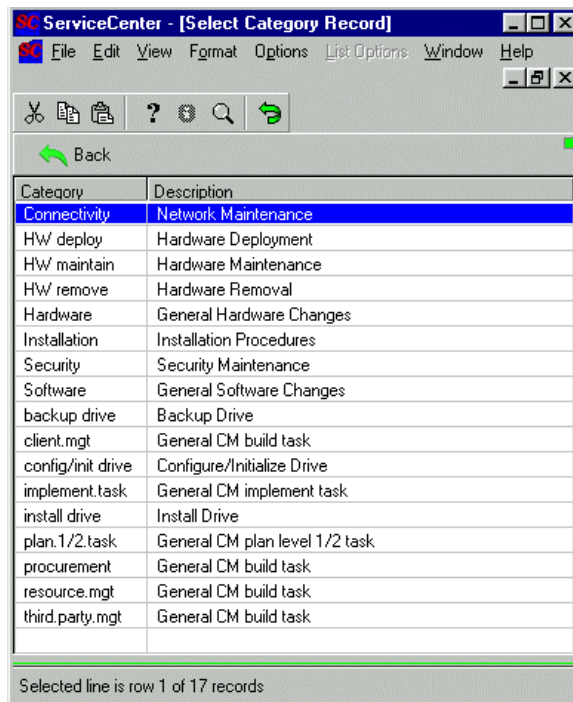
Figure 10-17 shows Change Category tasks.



Figure 10-17: Change Category tasks

To access the task category records:

- 1 Click **Change Management** in the ServiceCenter home menu.
The Change Management menu appears.
- 2 Select the **Tasks** tab.
- 3 Click **Task Categories**. A blank task category record appears.
- 4 Click **Search** or press **Enter** to perform a *true* query and retrieve a list of all current task category records. Figure 10-18 shows a QBE list of task categories.



The screenshot shows a window titled "ServiceCenter - [Select Category Record]". It has a menu bar with File, Edit, View, Format, Options, List Options, Window, and Help. Below the menu bar is a toolbar with icons for cut, copy, paste, help, search, and refresh. A "Back" button with a left arrow is also present. The main area contains a table with two columns: "Category" and "Description". The "Connectivity" category is highlighted in blue. Below the table, a status bar indicates "Selected line is row 1 of 17 records".

Category	Description
Connectivity	Network Maintenance
HW deploy	Hardware Deployment
HW maintain	Hardware Maintenance
HW remove	Hardware Removal
Hardware	General Hardware Changes
Installation	Installation Procedures
Security	Security Maintenance
Software	General Software Changes
backup drive	Backup Drive
client.mgt	General CM build task
config/init drive	Configure/Initialize Drive
implement.task	General CM implement task
install drive	Install Drive
plan.1/2.task	General CM plan level 1/2 task
procurement	General CM build task
resource.mgt	General CM build task
third.party.mgt	General CM build task

Figure 10-18: Task Categories in the Base ServiceCenter System

- 5 Double-click a category from the list to select it. Figure 10-19 shows a task category record.

Figure 10-19: Task Category Record

The following table describes the fields on the Task Category record.

Field	Description
Company	Indicates which company uses a category with this option. (This option can be set up to be used with Format Control or validity to enforce the use of a category by only certain companies.)
Category Name	Unique name assigned to the category record.
Category Description	Brief description of this category.
Availability	Conditional field specifying if a user is allowed access to this category. This field can be set to true or false or a condition evaluating to true.

Field	Description
Assign Number?	Indicates when Change Management assigns a unique ID to a task. Checking the box for this field (a <i>true</i> setting) indicates the unique ID is assigned before the task is opened. Note: When modifying the RFC - Advanced category, this field must be checked (<i>true</i>), so that a number is immediately assigned to a task. If this field is left unchecked (<i>false</i>), the task will not open.
Task Phases	Lists the phases through which this task must go. Phases are discussed later in this section.
Available Change Phases	Lists the change phases that can access this task. Remember: change phases contain tasks.

Creating a Category

As a ServiceCenter administrator, you may need to create new change or task categories to customize the system for your enterprise. These records can be created by either copying and modifying an existing record, or by creating a new record from scratch. ServiceCenter is shipped with a series of task category records you can use or modify. The simplest way to create a new change or task category is to copy an existing record.

To create a new category from an existing record:

- 1 Click **Change Categories** or **Task Categories** in the respective Changes or Tasks tab in the Change Management menu.
A blank category record appears.
- 2 Click **Search** to perform a true query and retrieve a list of all current category records. A QBE list of existing categories appears. See the sample change and task category lists shown in Figure 10-15 on page 373 and Figure 10-18 on page 376.
- 3 Double-click a category record you want to copy in the QBE list.
- 4 Replace the name in the **Category Name** field with the name of your new category.
- 5 Modify any fields that need to be changed for the new category and list the appropriate phases. You may select existing phases from the drop-down lists, or enter new phases you want to create for the new category. At least one phase must be entered in the **Phases** array to create a category.



- 6 Click **Add** or press F1 to create the new category record.
 - If all the phases listed have a record, the status bar displays this message: **Creation of Change Category *new name* is complete.**
 - If the phase you have listed does not exist, the system prompts you to create a new phase record.
- 7 Click **Yes** to open a new phase record for the phase you have listed. For more information, see *Creating a Phase* on page 400.
- 8 Click **OK** when you have finished editing the fields of the phase record. The status bar displays this message: **Phase *name* Phase Definition added.**



- 9 Click **Continue** to return to the category record. The status bar displays this message: **Creation of Change/Task Category *category name* is complete.**

Creating Related Records

The creation of a new change or task category also involves the creation of a number of other ServiceCenter elements. Some or all of the following additions may be necessary for your category to function fully:

Build a New Form

If you create a new category, you can build forms to reflect the different data requirements of the new category. These forms are related to the phases of the category. For detailed instructions on building forms refer to *System Tailoring Guide, Volume 1*.

Important: The primary form used to view and modify any change or task is in the phase definition record, found in Scripts/Views tab, View window, Default field.

Add New Fields to the Database Dictionary

Any new fields you have created in any subform or new tabbed category forms must be added to the database dictionary. Since data files for Change Management are made up of structures, new fields must be added to the correct structure. For detailed instructions on editing the Database Dictionary, refer to the *System Tailoring Guide, Volume 1*.

Important: Add new category-specific data fields to the **middle** structure of the dbdict.

Create Necessary Link Records

Link records bring related data from a supporting file into your change or task record. The name of the link record should match the name of the category-specific or phase-specific form you built. Add any field from your new form to the link record if you want that field to display linked data. For detailed instructions on creating link records, see *System Tailoring Guide, Volume 2*.

Create Necessary Format Control

Format Control is used to control either the presentation of the data on the form or how the data is stored in the file. For detailed instructions on creating Format Control records, refer to *System Tailoring Guide, Volume 1*.

Format Control in Change Management is applied differently than in other modules in ServiceCenter. Change Management allows you to define the following types of Format Control records:

- **Master:** The *master* Format Control record allows you to define the Format Control statements that apply to *all* change request phases. The name of the master Format Control record for changes is *cm3r* (*cm3t* for tasks). The options on this record are executed during all change and task processing except for approval and background processing. The master Format Control record is processed *before* the detail Format Control record.
- **Detail:** To enforce processing rules that are unique to a phase, define a Format Control record that has the same name as the *default* view of that phase.

Change Management processes master and detail Format Control as follows:

- The **add options** are processed at open time by clicking **Open**.
- The **update options** are processed at update time by clicking **Update** or **Reopen**.
- The **delete options** are processed at close time by clicking **Close**.
- The **display options** are processed before a record appears.

The Format Control functions for a particular option (**add**, **update**, **delete** or **display**) are executed *after* the process is invoked but *before* the record is permanently updated. For example, the **add options** are executed *after* the user clicks **Open New Change** in the Change Management menu but *before* the user clicks Save to add the change to the database. The **display options** are executed *after* a record has been selected from the QBE list but *before* the record is actually displayed.

You can execute both a *master* Format Control and a *detail* Format Control for each change or task process. If any of the Format Control functions fail for any reason, the user is always returned to the previously displayed screen with the appropriate error messages.

Set up Approval/Member (Reviewer) Groups

Certain change and task phases require approvals before the process can move ahead to the next phase. If they don't already exist, you must create the necessary approval and member groups for each phase named in your new category. For detailed instructions on creating approval groups, refer to the sections on *Group profiles* and *Group definition records*.

Define the Alerts

Associate any alert conditions with the phase definitions for the category you have created. Event records determine who receives notification messages about an alert condition.

Create Necessary Scripts

Create any scripts you want to execute during the change process. Scripts defined for the Open, Close, Reopen, or Update process are executed prior to starting the process. Script definitions are optional.

Note: Creating new categories in Change Management is considered an advanced tailoring option.

Updating a Category Record

Follow these steps to update an existing category.

- 1 Click **Categories** in the Changes or Tasks tab in the Change Management menu. A blank category record appears.
- 2 Access the existing category record you want to modify. Do one of the following:
 - Enter the name of the category in the **Category Name** field and click **Search**.
 - Leave all the fields blank and click **Search** to perform a true query and retrieve a list of all current category records. Select the desired category from the QBE list displayed.
- 3 Modify any fields that need to be changed for the category. If you modify or add any phase names that are not already defined, a message prompts you to create a new phase record.

- 4 Click **Save** or press F2 to update the category record. The status bar displays this message: *category name* Category Definition updated.

Deleting a Category Record

To delete obsolete or unwanted category records:

- 1 Click **Categories** in the Changes or Tasks tab in the Change Management menu.

A blank category record appears.

- 2 Access the existing category record you want to modify. Do one of the following:
 - Enter the name of the category in the **Category Name** field and click **Search**.
 - Leave all the fields blank and click **Search** to perform a true query and retrieve a list of all current category records. Select the desired category from the QBE list displayed.
- 3 Click **Delete** or press F4. Figure 10-20 shows new Delete buttons.

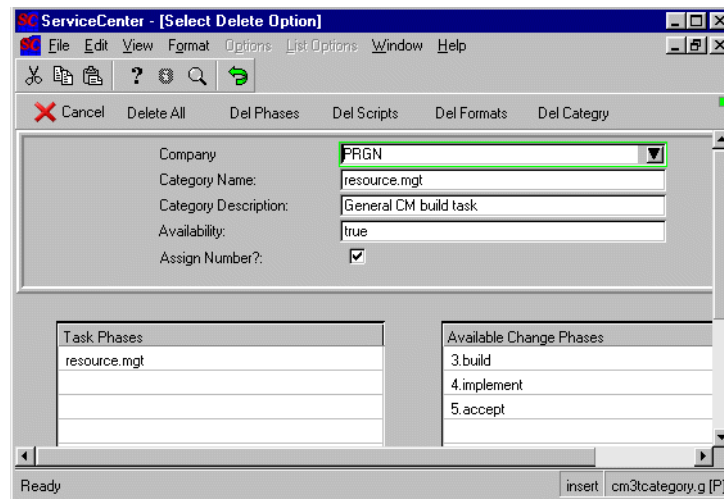


Figure 10-20: Delete Option Buttons

- 4 Click **Del Category** or press F7 to delete the record. A delete form appears. The name of the category to be deleted displays in the **Category** field at the top of the form, as shown in Figure 10-21.

Figure 10-21: Category Delete form

Important: Ensure you know which elements of this category you want to delete before proceeding. Clicking on the other delete options deletes the associated records for the phases, forms, scripts, and so on, for that category.

- 5 Click **Delete** or press F1. The system exits to the Category QBE form. The status bar displays this message: **All specified items have been deleted.**
- 6 Click **Back** or press F3 to display a blank category record.

Printing a Category Record

To print a category record:

- 1 Click **Categories** in the Changes or Tasks tab in the Change Management menu. A blank category record appears.
- 2 Access the existing category record you want to modify. Do one of the following:
 - Enter the name of the category in the **Category Name** field and click **Search**.
 - Leave all the fields blank and click **Search** to perform a true query and retrieve a list of all current category records. Select the desired category from the QBE list displayed.
- 3 Select **Print** from the **Options** menu. The status bar displays a message that the category is scheduled to be printed and specifies the date and time of day this will occur.

Change and Task Phases

If you are creating a new change or task category, you are required to enter at least one phase. ServiceCenter is shipped with a series of predefined phases, but you can also add new phases. If you enter a phase that does not exist, ServiceCenter displays a message that asks you to create this phase. As mentioned earlier in this chapter, a phase is an administrative step within the change.

Figure 10-22 shows the Change Phases.

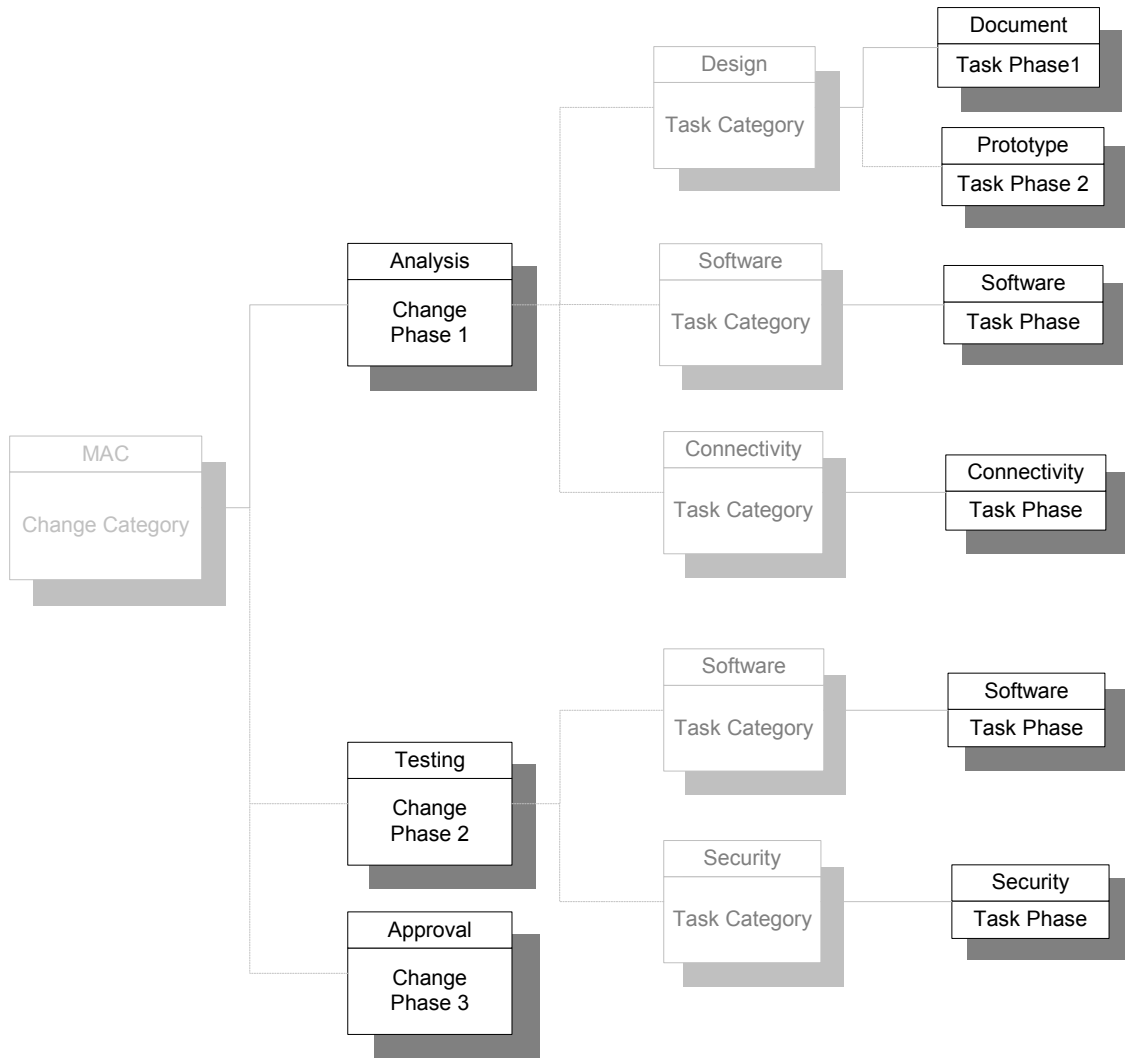


Figure 10-22: Components of a Change — Phases

Accessing Phase Records

Existing change and task phase records are accessed with the same procedures. You may access phase records from two points:

- **Phase in the Change Management menu**
- **Category record.** Use the Find Phase or Search Phase option.

Change Menu

The following example uses the procedure for accessing a change phase record.

To open a phase record:

- 1 Click **Change Management** in the ServiceCenter home menu.
- 2 Select the **Changes** tab.
- 3 Click **Change Phases**. Figure 10-23 shows the blank change phase record.

The screenshot shows a software window titled "ServiceCenter - [Enter QBE Search Criteria]". The window has a menu bar with "File", "Edit", "View", "Format", "Options", "List Options", "Window", and "Help". Below the menu bar is a toolbar with icons for "Back", "New", and "Search". The main area of the window is divided into several sections:

- Change Phase:** A text input field.
- Description:** A text input field.
- OpenID (true) or Full Name (false):** A text input field.
- Require a Start/End Date?:** A checkbox.
- Definition** tab: This tab is selected. It contains:
 - Risk:**
 - Maximum:** A text input field.
 - Calculation:** A text input field.
 - History:**
 - Pages:** A text input field.
 - Audit Records:** A text input field.
 - Controls:**
 - Update:** A text input field.
 - Approval:** A text input field.
 - Close:** A text input field.
 - Message:** A text input field.

The status bar at the bottom of the window shows "Ready" and "insert cm3rcatphase.main.g [P]".

Figure 10-23: Change Phase Record — Searching for an Existing Phase

- 4 Do one of the following:
 - Enter a phase name in the **Change Phase** field and click **Search** or press **Enter**.
 - Leave the fields blank and click **Search** to perform a *true* query and retrieve a list of all current change phase records. Select a record to view and modify by double-clicking on the selected record.

Category Record — Find Phase Option

To open a phase record from a category record with the **Find Phase** option:

- 1 Click **Change Management** in the ServiceCenter home menu.
- 2 Select the **Changes** tab.
- 3 Click **Change Categories**. A blank category record appears.
- 4 Do one of the following:
 - Enter a category name in the **Category Name** field and click **Search** or press **Enter**.
 - Leave the fields blank and click **Search** to perform a *true* query and retrieve a list of all current change category records.

Figure 10-24 shows a QBE list of existing change category records.

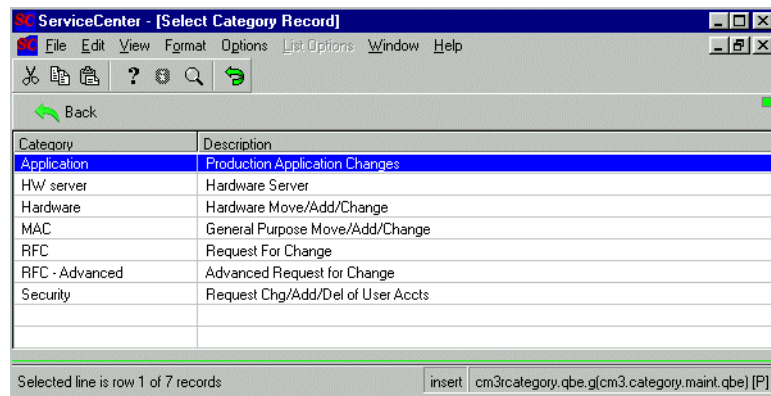


Figure 10-24: Selecting a Change category

- 5 Select a change category from the QBE list of records. Figure 10-25 on page 388 shows the selected change category record.

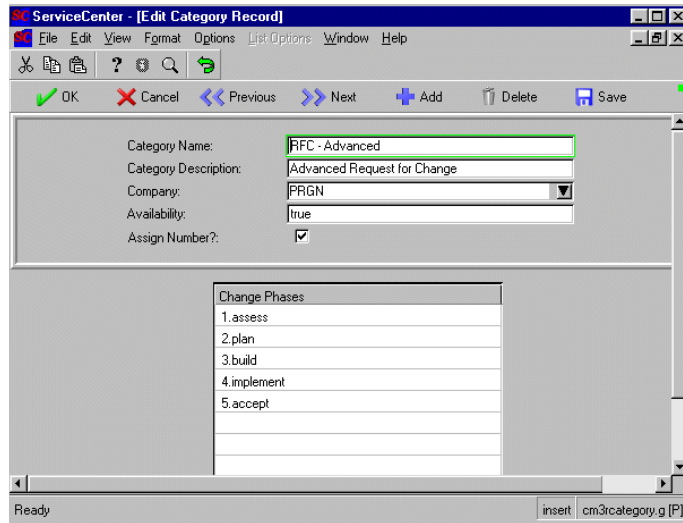


Figure 10-25: Accessing Phases from the Category Record

- 6 Select a phase name in the Change Phases array of the category record.
- 7 Select Find Phase from the Options menu. Figure 10-26 shows the selected phase record.

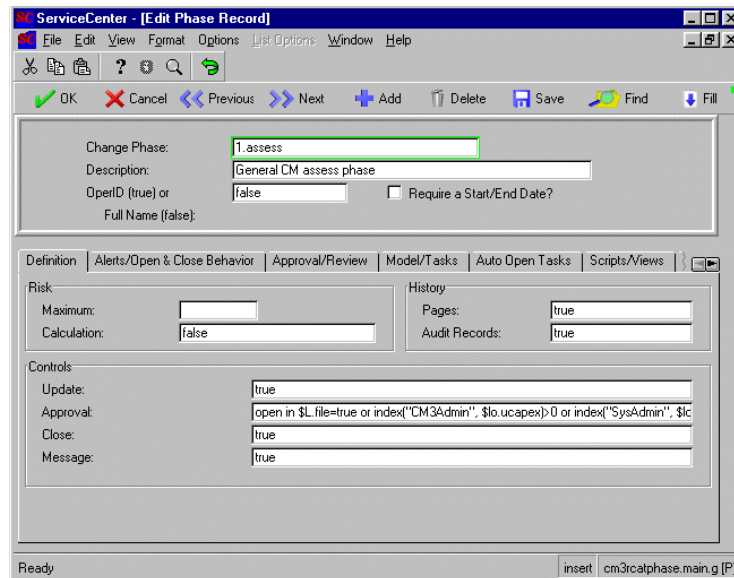


Figure 10-26: Existing Phase Record

Category Record — Search Phase Option

Follow these steps to open a phase record from a category record with the Search Phase option.

- 1 Click **Change Management** in the ServiceCenter home menu.
- 2 Select the **Changes** tab.
- 3 Click **Change Categories**.
A blank category record appears.
- 4 Do one of the following:
 - Enter a category name in the **Category Name** field and click **Search** or press **Enter**.
 - Leave the fields blank and click **Search** to perform a *true* query and retrieve a list of all current change category records.
 A QBE list of existing change category records appears, as shown in Figure 10-24 on page 387.
- 5 Select a change category record from the QBE list. The selected change category record appears, as shown in Figure 10-25 on page 388.
- 6 Select **Search Phase** from the Options menu. Figure 10-27 shows a blank change or task phase record.

Figure 10-27: Change category - searching for a Change phase

- 7 Do one of the following:
 - Enter a phase name in the **Change Phase** field and click **Search** or press **Enter**.
 - Click **Search** or press **Enter** in the blank phase record form and select the desired record from the QBE list displayed.

Phase Record Fields

Change and task phase records contain field names that are appropriate to the function of the record (change or task). Like categories, there are some differences between the change and task. Not all fields are required. The required fields are noted in the following definitions. Figure 10-28 shows the Definition tab.

The screenshot shows the 'ServiceCenter - [Edit Phase Record]' window with the 'Definition' tab selected. The window has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Previous, Next, Add, Delete, Save, Find, and Fill. The main form contains the following fields:

- Change Phase:** 1. assess
- Description:** General CM assess phase
- OpenID (true) or Full Name (false):** false
- Require a Start/End Date?** ☐
- Risk:**
 - Maximum:**
 - Calculation:** false
- History:**
 - Pages:** true
 - Audit Records:** true
- Controls:**
 - Update:** true
 - Approval:** open in \$L.file=true or index("CM3Admin", \$lo.ucapex)>0 or index("SysAdmin", \$lc
 - Close:** true
 - Message:** true

The status bar at the bottom shows 'Ready' and 'insert cm3rcatphase.main.g [P]'.

Figure 10-28: Phase Record — Definition tab

The following table describes the fields on the Definition tab.

Field	Description
Change/Task Phase (<i>required</i>)	A unique name identifying the phase.
Description	Provides general information or comments about the phase.
OperID (true) or Full Name (false)	Logical field that indicates whether the operator's user ID (true) or the operator's full name (false) is used to track activity in this change phase.
Require a Start/End Date?	Logical field that controls whether or not a change request requires a start and end date. When selected (<i>true</i>), requires a valid value in the Planned Start and Planned End fields.

Definition tab

The Definition tab shown in Figure 10-28 on page 390 displays three areas containing the following fields. The following table describes the fields in the Risk area.

Field	Description
Maximum	Highest risk value allowed in this phase. The risk scale ranges from 0 (no risk) to a user specified maximum (high risk).
Calculation	Logical field that indicates if the risk assessment is automatically calculated when there is a change or update in this phase.

The following table describes the fields in the History area.

Field	Description
Pages	If selected (<i>true</i>), stores a copy of the entire record each time it is updated.
Audit Records	If selected (<i>true</i>), calls the ServiceCenter auditing system.

The following table describes the fields in the Controls area.

Field	Description
Update	Logical field that defines the conditions under which a phase can be updated.
Approval	Logical field that defines the conditions under which a phase can be approved.
Close	<p>Logical field that defines the conditions under which a phase can be closed. For example, you can change this field to set up the close control criteria. You can replace <code>true</code> with:</p> <p>approval.status in \$L.file="approved"</p> <p>This statement requires this phase to be approved before it can be closed, in order to move to the next phase or to close the change or task if there are no more phases.</p> <p>Note: The current file variable for a change is <code>\$L.file</code>. The current file variable for tasks is not <code>\$L.file</code> (for this reason). However, in the task definition records, the task variable is <code>\$L.file</code> and its parent change is <code>\$L.parent</code>. <code>\$L.file</code> is the variable commonly used to reference records in the document engine.</p>
Message	Logical field that indicates if messages are sent during the processes of this phase, including open, update, close, approve, deny, retract, and reopen.

Alerts/Open & Close Behavior tab

Figure 10-29 shows the Alerts tab.

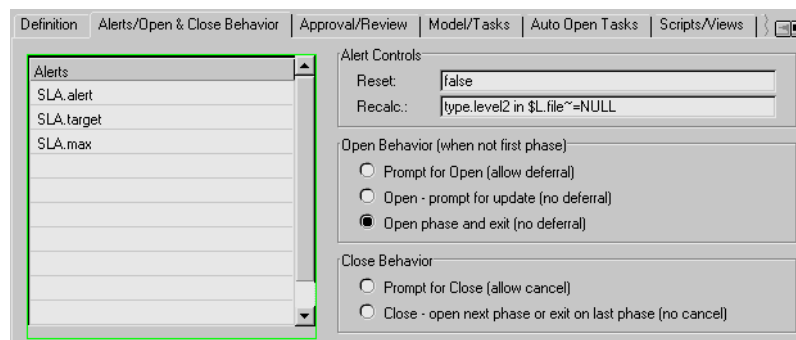


Figure 10-29: Phase Definition Record — Alerts/Open & Close Behavior tab

The following table describes the Alerts/Open & Close Behavior tab.

Field	Description
Alerts	Alerts and messages available for this phase. You can enter as many alerts or messages as you need. For more information, see Events, Alerts, and Messages on page 450.

The following table describes the fields in the Alert Controls area.

Field	Description
Reset	Logical field defining conditions under which alert processing is reset (restarted) during an update.
Recalc	During an update, causes alert names defined in this phase to be rechecked for appropriateness if this field evaluates to <i>true</i> .

Note: These options determine how to open this phase, if it follows other phases in sequence.

The following table describes the fields in the Open Behavior (When Not First Phase) Area.

Field	Description
Prompt for Open (allow deferral)	prompts user to open this next phase in a sequence of phases. If the user does not open the subsequent phase, the phase is put into a <i>deferred</i> status.
Open - prompt for update (no deferral)	automatically starts the next phase in a sequence of phases and displays it in update mode.
Open phase and exit (no deferral)	automatically starts the next phase in a sequence and returns the user to the previous window (for example, search window, menu, and so on).

The following table describes the fields in the Close Behavior area.

Field	Description
Prompt for Close (allow cancel)	When the user chooses to close a change or task, a record with the close view format displays and allows the user to cancel out of the close process.
Close - open next phase or exit on last phase (no cancel)	When the user chooses to close a change or task, there is no close confirmation screen and the next phase is automatically opened (if there is another phase). The user is allowed to exit without canceling.

Approval/Review tab

The Approval/Review tab contains the approval fields for the phase record, in which you can reset and recalculate approval definitions. Reviewer requirements can also be configured for a phase, allowing you to define the Reviewer list. Figure 10-30 shows the Approval/Review tab.

Figure 10-30: Phase Definition Record — Approval/Review tab

The following table describes the fields in the Approval Requirements area.

Field	Description
Approvals	A list of groups or operators who must acknowledge or accept the risk, cost, and so on associated with the implementation of a change request or task. Approvals give controlling authorities the ability to stop work and to control when certain work activities can proceed.

Field	Description
Reset Approvals	Resets all approvals for this phase and reevaluates the conditions on all possible Approval Definitions.
Recalc Approvals	Recalculates the Approval Definitions for all current approvals.

For more information, see the *ServiceCenter User's Guide*.

The following table describes the fields in the Reviewer Requirements area.

Field	Description
Group/Operator	Lists the individual or group profiles of those who will be notified to review this phase. Both individual and group names must match an existing Change Management profile record (cm3profiles) with Review privileges. Reviewers receive an optional, courtesy notification after a phase is approved. Their review is for their own benefit only; they cannot deny an approved request or task.
Condition	Sets the conditions under which a group or user will receive review notification for a change or task phase. The condition field is boolean. The reviewing requirement is added to the phase when the expression in the field evaluates to <i>true</i> . The condition is <i>false</i> by default.

Model/Tasks tab

The Model/Tasks tab in a change phase allows you to copy task, change, and phase information from an existing change (*model*) into a new change. Figure 10-31 shows the Model/Tasks tab.

Figure 10-31: Phase Definition Record — Model/Tasks tab

There are three structures in this tab containing the following fields:

You can designate an existing change record as a template used to pre-fill specified fields whenever you open a new change request of this type. The fields in this area identify the model change and fields to copy.

Field	Description
Number	Unique ID of the existing change record to use as a template.
Link	Link record to use when this change is copied. This record identifies which fields to copy. When data is linked, you can move data from one model field to a different change request field.

The following table describes the fields in the Link to User for Copy/Open area.

Field	Description
Link	Link record to use to copy information into the current record. The Copy/Open link is used to specify which fields are copied into the current record when creating a new change with the copy/open approach.

The following table describes the fields in the When Last Task is Closed area.

Field	Description
Change status to	Allows the status to be changed to the status entry indicated when the last task has been closed. If this check box is selected, indicate the new status. The <i>Change status to</i> option displays in the Options menu of tasks and changes.
Close this phase	Allows the phase to be closed when the last task has been closed. If this check box is selected, the <i>Close this phase</i> option displays in the Options menu of tasks and changes.

Auto Open Tasks tab

Figure 10-32 shows the Auto Open Tasks tab.

Category	Condition	Background Open?

Array Field in Source Change:	<input type="text"/>	Task Category:	<input type="text"/>
Scalar Field in Target Tasks:	<input type="text"/>	Open in Background?:	<input type="text"/>

Figure 10-32: Phase Definition Record — Auto Open Tasks tab

The following table describes the fields in the Automatically Open Tasks (Standard) area.

Field	Description
Category	The task category to be used.
Condition	Logical expression determining whether or not a task starts automatically. When the phase is opened, the user is presented with each task that evaluates to true. The condition is false by default.
Background Open?	Logical field that determines whether or not the user is prompted when opening a task. A value of <i>false</i> (blank) enables you to open or cancel the task. A value of <i>true</i> starts the task automatically. In both cases, a message appears.

Define those entries in an array field for which individual tasks should be created. For example, your change form may contain an array called Locations Affected in which several locations are entered. Use the controls in the Auto Open Tasks tab to create a separate task for each of the locations listed in the array.

Field	Description
Array Field in Source Change	The array field in the change record. For every entry in this array, the system creates one task.
Task Category	Task category to be assigned to all tasks opened.

Field	Description
Scalar Field in Target Task	Scalar field in the task record that is populated with the value from the Array Field in Source Change field for this task. Continuing our example, you can populate the location field with each new change task.
Open in Background?	Logical field that determines if the tasks are automatically opened in the background. If this field evaluates to <i>false</i> , the user is presented with and has to save each task. The background value is <i>false</i> by default.

Scripts/Views tab

Change Management allows you to select the ServiceCenter scripts that are run at various phase milestones of a change or task. Scripting allows you to alter the flow of a ServiceCenter process without changing the code in which it was written. For more information, see the *ServiceCenter System Tailoring Guide*. You must also name the forms used by the phase in the Views structure.

Figure 10-33 shows the Scripts/View tab.

The screenshot shows the 'Scripts/Views' tab in a software interface. The 'Scripts' section contains four rows: 'Open', 'Update', 'Close', and 'Reopen'. Each row has a dropdown menu. The 'Open' dropdown is currently set to 'cm3r.company'. To the right of these dropdowns is a 'Condition' field with the text 'company in \$.file=NULL or subcategory in \$.file=NULL'. Below the Scripts section is the 'Views' section, which has two fields: 'Default' and 'Close'. Both fields are set to 'cm3r.assess.default' and 'cm3r.assess.close' respectively.

Figure 10-33: Phase Definition Record — Scripts/Views tab

The following table describes the fields in the Scripts area.

Field	Description
Open	A script you want executed when this phase change or task is opened.
Update	A script you want executed when this phase change or task is updated.

Field	Description
Close	A script you want executed when this phase change or task is closed.
Reopen	A script you want executed when this phase change or task is reopened.
Condition	Logical statements that trigger the script when the statement evaluates to <i>true</i> . You also can simply enter <i>true</i> in the field. The condition is <i>false</i> by default.

For more information, see [Tasks](#) on page 425, [Change Records](#) on page 409, and see the *ServiceCenter User's Guide*.

The following table describes the fields in the Views area.

Field	Description
Default	Name of the form you want Change Management to display for this phase as a default.
Close	Name of the form you want Change Management to display when this phase is closed.
Print	Name of the form you want Change Management to use when printing this phase record.

The Default and Approvals form names also identify the detail and approvals Format Control records, respectively, used for this phase. For more information, see [Create Necessary Format Control](#) on page 380.

Reports tab

The Reports tab defines the reports used when a change or task report is run in this phase. Figure 10-34 shows the Reports tab.

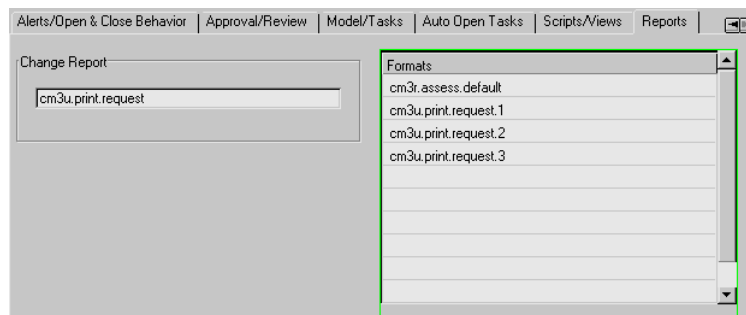


Figure 10-34: Phase Definition Record — Reports tab

The following table describes the fields on the Reports tab.

Field	Description
Change Report	Select the report to be run during this phase definition.
Formats	Select the formats to be used when this report is run.

Creating a Phase

Phases are defined in a phase definition record. The **COMPANY MASTER** record is the default phase record. This record allows you to define the defaults that are used when a new phase is created.

To create a new phase using the COMPANY MASTER phase definition record as a template:

- 1 Click **Change Categories** in the Change Management menu. A blank Category record appears. This process works the same for change or task categories.
- 2 Click **Search** to perform a true query and retrieve a list of all current change category records. A QBE list of existing category records appears, as shown in Figure 10-24 on page 387.
- 3 Select a category from the QBE list. Figure 10-35 on page 401 shows the example using the RFC - Advanced change category.

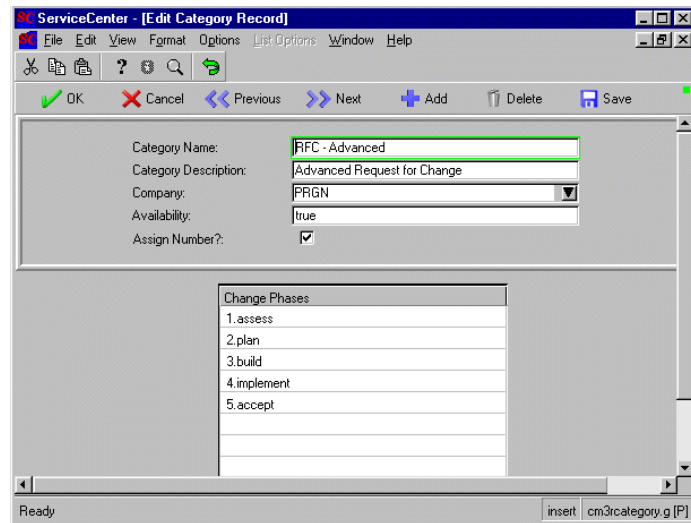


Figure 10-35: New Phase Added to a Category Record

- 4 Type the name of the new phase in the **Change Phases** array. If you are adding an existing phase to the category, insert your cursor in the next blank line and click the drop-down arrow. For this exercise, select the **COMPANY MASTER** default record, as shown in Figure 10-36.

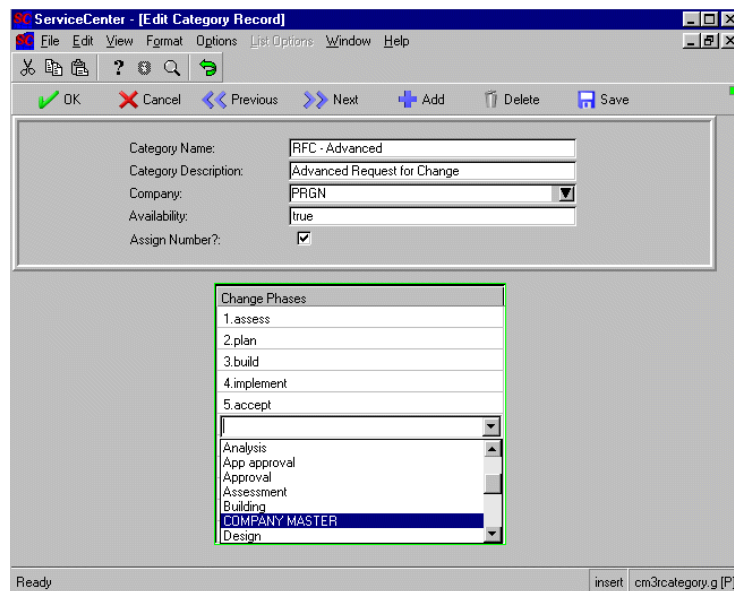


Figure 10-36: Selecting the COMPANY MASTER Change Phase

- Position your cursor on the new phase, and select **Find Phase** from the Options menu, as shown in Figure 10-37.

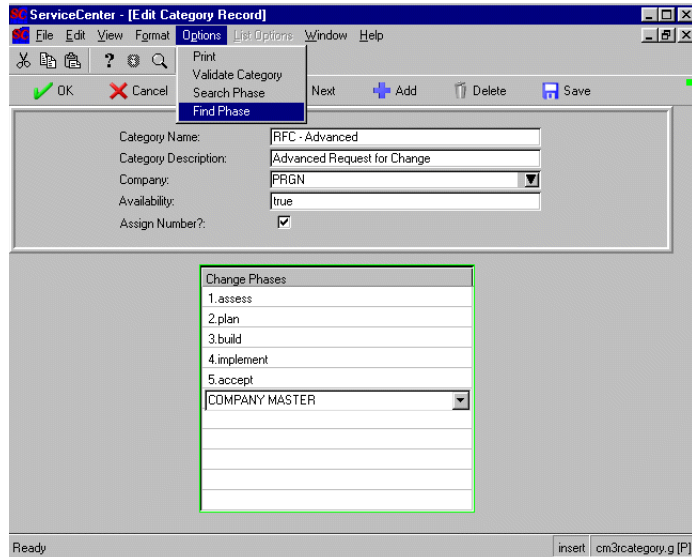


Figure 10-37: Finding a phase within the COMPANY MASTER category record

- Click **Find Phase** to create a new phase definition record based on the COMPANY MASTER default record, as shown in Figure 10-38.

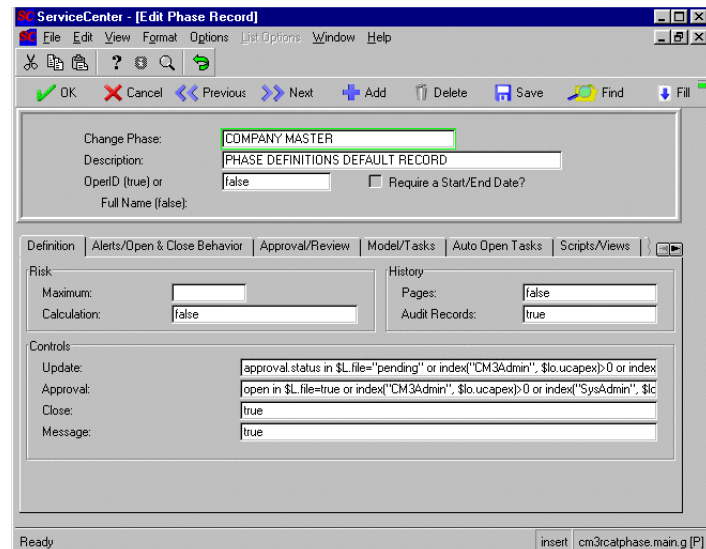


Figure 10-38: New Phase Record Based on Default

- 7 Enter a name for the new change phase in the **Change Phase** field.
- 8 Enter a description for the new phase in the **Description** field.
- 9 Click **Add**, to add the new phase definition record and to *not* change the existing COMPANY MASTER definition record in error.

The status bar displays this message: *phase name* Phase Definition added.

Alternately, you can click **Cancel** to return to the category record.

For this exercise, create TESTING PHASE with a description of TESTING NEW CHANGE PHASE RECORD.

- 10 Modify the fields in the other tabs to match the values you want for the new phase. For more information, see [Phase Record Fields](#) on page 390.
- 11 Click **OK** to return to the category record shown in Figure 10-39.

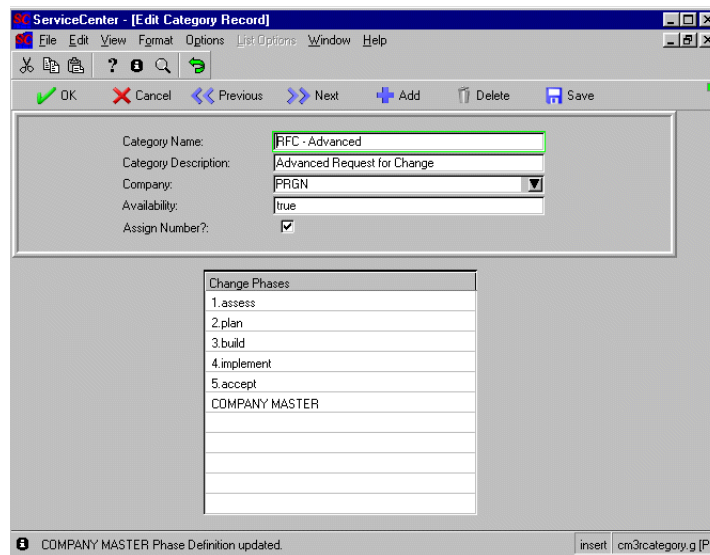


Figure 10-39: Updating the category record with a new change phase definition

- 12 Insert your cursor in the COMPANY MASTER line in the **Change Phases** array. Press **Backspace** to blank out this line, taking the COMPANY MASTER change phase line out of the array.
- 13 Click **OK** to save the change to the RFC - Advanced category to include the new change phase record you just created. The QBE list of change category records list appears.

- 14 To make this change phase record available in the RFC - Advanced category Change Phases array, log off ServiceCenter and then log back on to update your global variables. Otherwise, the new change phase record is not available to the RFC - Advanced category record until you do this.
- 15 Select **Change Management** from the ServiceCenter home menu.
- 16 Click **Change Categories** in the Change Management menu. A blank category record appears.
- 17 Click **Search** to perform a true query and retrieve a list of all current change category records. A QBE list of existing category records appears, as shown in Figure 10-24 on page 387.
- 18 Double-click **RFC - Advanced** in the QBE list of category records.
- 19 Insert your cursor in the next blank line of the **Change Phases** array. Do one of the following:
 - Enter the name of the new change phase record you just created (TESTING PHASE) in the **Change Phases** array.
 - Click the drop-down list of the change phase records available to the RFC - Advanced change category, as shown in Figure 10-40.

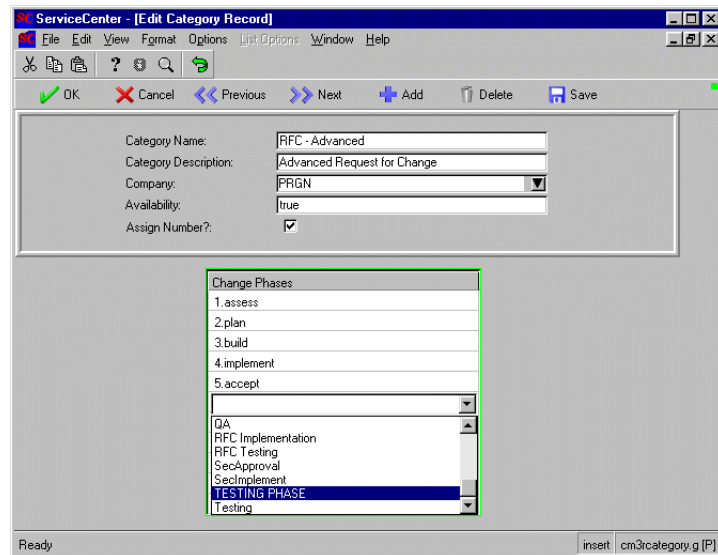


Figure 10-40: Selecting the new change phase record from the QBE list

- 20 Select the new TESTING PHASE change phase record to add it to your Change Phases array.

- 21 Click **OK** to update the RFC - Advanced category record. The TESTING PHASE change phase record is now part of the RFC - Advanced category record.

Validate the Phase

After you have created a new phase, you need to validate the phase to ensure that all forms, or *views*, created for use with the new phase are properly referenced.

To validate the new phase record, do one of the following:

- Open the new change or task phase record you created and click **Validate Phase** in the Options menu.
- Open the category record for which the new change or task phase was created and validate the category. When you choose to validate the category, all the phases within the category are also validated.

For this example, we will validate the new TESTING PHASE change phase record created in *Creating a Phase* on page 400.

To validate a new change phase record:

- 1 Click **Change Phases** in the Change Management menu. A blank change phase record appears.

- 2 Click **Search** to perform a true query and retrieve a list of all current change phase records. A QBE list of existing change phase records appears, as shown in Figure 10-41.

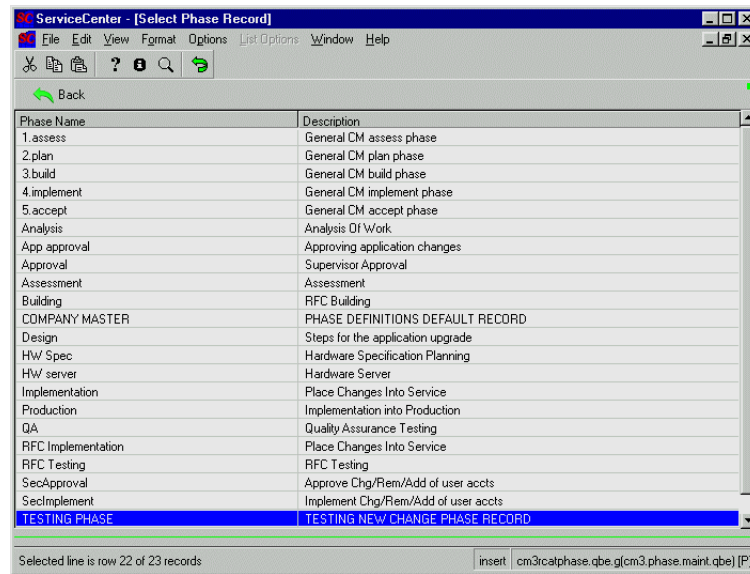


Figure 10-41: Selecting a Change Phase record

- 3 Double-click **TESTING PHASE** in the QBE list of change phase records.
 - 4 Select **Validate Phase** from the Options menu of the phase record. The status bar displays this message: **Validation of Phase *phase name* is complete.** If you have not created a new form for your phase, a message that the form does not exist appears.
 - 5 Click **OK**. A message asks if you want to create the missing form.
 - 6 Click **Yes** to open a blank canvas in Forms Designer. For more information, see the *System Tailoring Guide, Volume 1*.
- Note:** You can copy an existing form or copy and paste portions of existing forms.
- 7 Click **OK** in Forms Designer when you have completed the form. The system exits to the phase record you have created. The status bar displays this message: **Validation of Phase *phase name* is complete.**

Change and Task Phase Functionality

This section describes the common functionality between change and task phases records. This functionality includes adding, updating, printing, and deleting phase records. For more information, see [Creating a Phase](#) on page 400, and [Approvals](#) on page 435.

To update a phase record:

- 1 Access an existing change or task phase record using one of the procedures described in [Accessing Phase Records](#) on page 386.
- 2 Modify any fields you want to update.
- 3 Click **Save** or press F2 to update the phase record. The status bar displays this message: *phase name* Phase Definition updated.

To print an existing phase record:

- 1 Access an existing change or task phase record using one of the procedures described in [Accessing Phase Records](#) on page 386.
- 2 Select **Print** from the Options menu. The status bar displays this message: Report CM3 Task Category Print scheduled to run at *mm/dd/yy hh:mm:ss*. The default ServiceCenter server printer prints the record.

To delete an existing phase record:

- 1 Access an existing change or task phase record, using one of the procedures described in [Accessing Phase Records](#) on page 386.
- 2 Click **Delete** or press F4. The system tray buttons are changed, and the record switches to the browse (read only) mode.

Important: In order to delete a phase record, you must first remove its name from each category phase list in which it displays.

Figure 10-42 shows the delete confirmation.

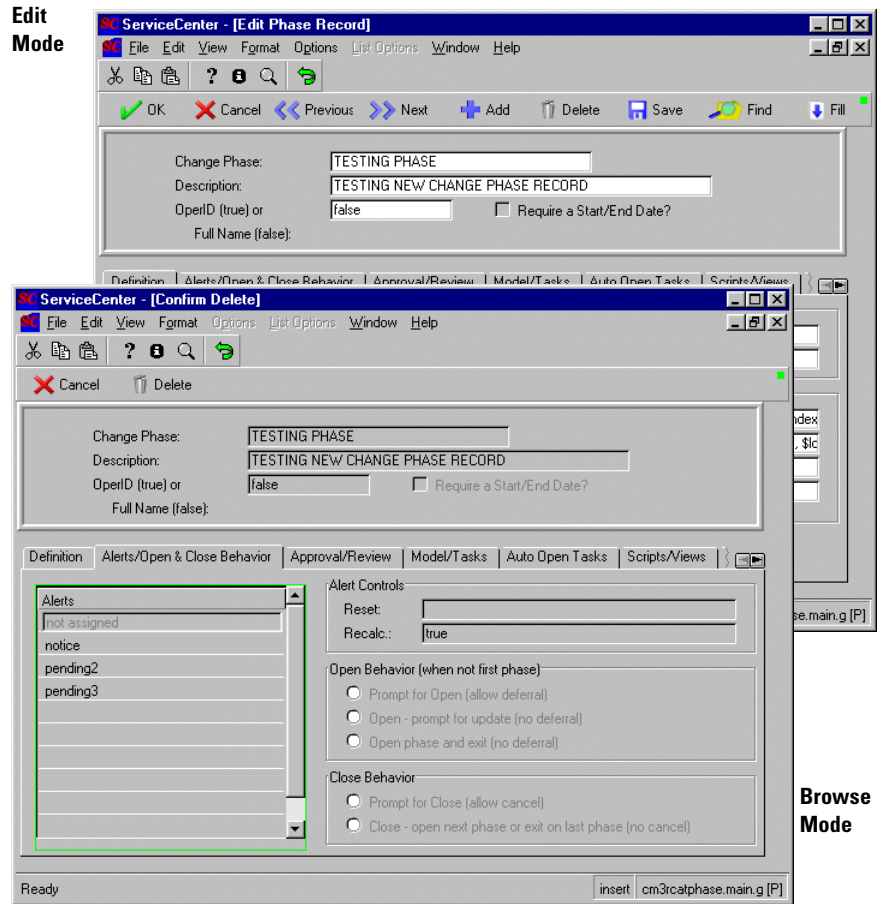


Figure 10-42: Deleting a Phase Record

- 3 Click Delete or press F4.
 - a If you have accessed the phase from a category record, the system exits to that record. The status bar displays this message: *phase name* Phase Definition deleted.
 - b If you have accessed the phase from clicking Phases in the Changes or Tasks tab, the system exits to the QBE list of phases. The status bar displays this message: *phase name* Phase Definition deleted.

A change category confirmation form appears, listing the phase and the phase's associated category, formats, and scripts.

Warning: When deleting a category, any item listed in the deleted form is deleted (that is, any formats or scripts).

Change Records

Refer to the *User's Guide* to learn how to open a new change request.

Searching for an Existing Change

ServiceCenter is shipped with sample changes for you to use while you are learning the system. You can access an existing change record from the Change Management menu using the Search form or Change queue

Search Form

To search for a change record:

- 1 Click **Change Management** in the ServiceCenter home menu.
The Change Management menu appears.
- 2 Click **Search Changes** in the Change Management menu.

Figure 10-43 shows the Change Management search form.

Figure 10-43: Change Management Search Form

- 3 To search for a change record, do one of the following:
 - Perform a *true* query. Leave all the fields blank and click **Search** or press **Enter**. A QBE list of all current change records appears.
 - Type search criteria in one or more of the fields in the Basic Search tab shown in Figure 10-43. Click **Search** or press **Enter**. A QBE list of all current change records that meet the selected criteria appears.

- Click the **Advanced Search** tab shown in Figure 10-44. The date and time information is optional. Enter the **After** and **Before** dates and times the change was opened or updated. The default format is *mm/dd/yyyy hh:mm:ss*. If a time is not entered, the default is *00:00:00*.

The screenshot shows the 'ServiceCenter - [Display Which Changes?]' application window. The 'Advanced Search' tab is selected, displaying a form with three groups of input fields for date and time ranges. Each group consists of an 'After' field and a 'Before' field. The first group is for 'Starting' and 'Ending', the second for 'Closed', and the third for 'Created'. The status bar at the bottom indicates the application is 'Ready' and shows a command line: 'insert cm3t.search.gl(cm.search.display) [P]'.

Figure 10-44: Advanced Search form

Note: The date and time format can be set in the System Wide Company Record or in individual operator records. Therefore, the date and time format you use may vary from the default described here.

IR Query

Figure 10-45 shows the IR Query form.

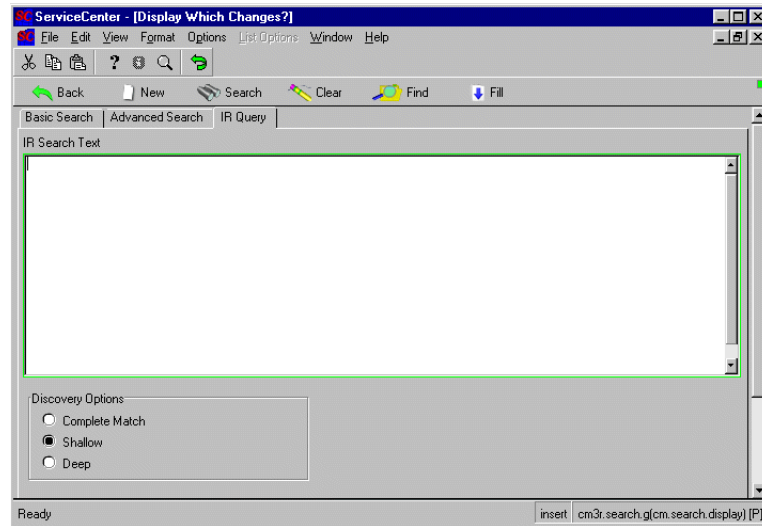


Figure 10-45: The IR Query tab

The following table describes the fields on the IR Query tab.

Field	Description
IR Search Text	Access ServiceCenter's IR Expert application, an intelligent, concept-based information retrieval engine that searches the ServiceCenter database for similar or related information, based on a simple, natural language query. Enter a plain text query in the blank text box. ServiceCenter adds the plain text to the search parameters.
Discovery Options	<ul style="list-style-type: none"> ■ Complete Match — system searches for an absolute match to the text you have typed. ■ Shallow — system uses narrow parameters and returns fewer records than with a deep search. ■ Deep — systems performs a broad search. This is a good option if a shallow search does not return the desired records.

Figure 10-46 shows a change record list that displays the first record.

The screenshot shows the 'ServiceCenter - [Change C1 - Prompt]' window. At the top is a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Save, Close, Find, Fill, and Clocks. Below the toolbar is a table with columns: Number, Category, Priority, Phase, Asset, Start, End, Title. The first row is highlighted in blue and contains the following data:

Number	Category	Priority	Phase	Asset	Start	End	Title
C1	RFC - Advanced	3	1. assess				

Below the table is a section for 'Change Number: C1' with fields for 'Category: RFC - Advanced', 'Phase: 1. assess', 'Ext. Project Ref.', 'Planned Start', and 'Planned End'. Below this is a tabbed interface with tabs for 'General', 'Description', 'Contact', 'Assets', 'Attachments', and 'Related Records'. The 'General' tab is active, showing fields for 'Coordinator' (Name: Joe User, Department: customer service, Phone: , RFC Cost Center:) and 'Assigned To' (Name: BOB.HELPSK, Department: LAN SUPPORT, Phone: 619-481-5000). Below these are 'General' and 'SLA' sections. The 'General' section has fields for 'Impact: 2 - Business Change', 'Priority: 3 - Normal Change', 'Status: initial', 'Approval Status: approved', and 'Alert Stage: '. The 'SLA' section has fields for 'RFC Type 1: Network Changes', 'RFC Type 2: lan', 'SLA Alert1: 12/27/01 13:58:38', 'SLA Target: 01/02/02 09:58:38', and 'SLA Deadline: 01/06/02 13:58:38'. At the bottom, a status bar indicates 'Selected line is row 1 of 1 records' and a file path 'insert cm3.qbe.g [P]'.

Figure 10-46: Change Record in Edit Mode

Select a change record from the record list. The appropriate information displays.

Change Queue

Searching for records with the change queue presents a list of changes by *inbox*. For information about creating and using inboxes, refer to the *User's Guide*.

To search in the Change queue:

- 1 Click **Change Queue** in the Change Management menu. Figure 10-47 shows a typical change inbox that lists all changes in the user's initial inbox. (By default, this is: Changes assigned to the current user.)

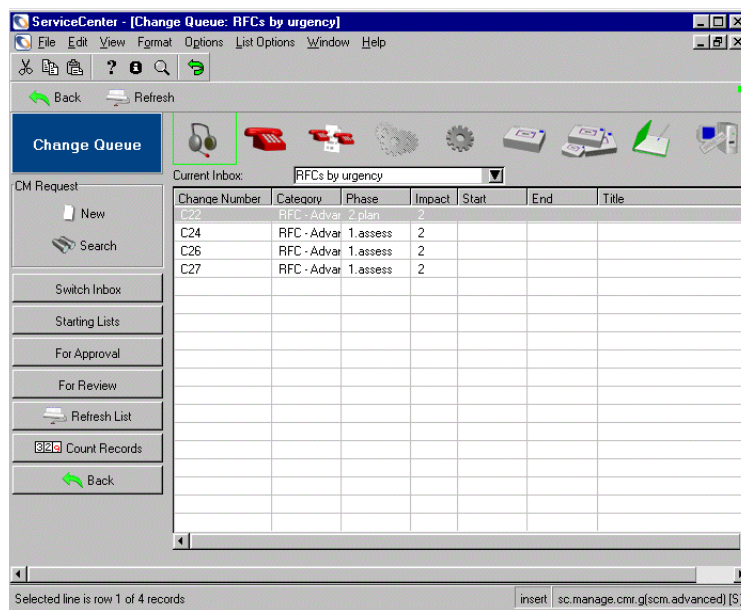


Figure 10-47: Change Management Inbox

- 2 Click **Switch Inbox** if you want to search for changes using a different inbox.
- 3 You may select a change from this list by double-clicking on it or by clicking **Search** to display a Change Management search form, as shown in Figure 10-43 on page 410.

Figure 10-48 on page 415 shows the selected change record in edit mode.

ServiceCenter - [Change C1 - Prompt]

File Edit View Format Options List Options Window Help

OK Cancel Save Close Find Fill Clocks

Number	Category	Priority	Phase	Asset	Start	End	Title
C1	RFC - Advanced	3	1. assess				

Change Number: **C1** Ext. Project Ref.:

Category: RFC - Advanced Planned Start:

Phase: 1. assess Planned End:

General Description Contact Assets Attachments Related Records

Coordinator:

Name: Joe User

Department: customer service

Phone:

RFC Cost Center:

Assigned To:

Name: BOB.HELPPDESK

Department: LAN SUPPORT

Phone: 619-481-5000

SLA:

RFC Type 1: Network Changes

RFC Type 2: Jan

SLA Alert1: 12/27/01 13:58:38

SLA Target: 01/02/02 09:58:38

SLA Deadline: 01/06/02 13:58:38

General:

Impact: 2 - Business Change

Priority: 3 - Normal Change

Status: initial

Approval Status: approved

Alert Stage:

Selected line is row 1 of 1 records insert cm3r.qbe.g [P]

Figure 10-48: Change Record Selected from an Inbox

- 4 Click **Save** or **OK** to save any changes to the record and to return to the inbox.
- 5 Click **Close** to close this phase of the change if all processing and tasks for this phase are complete. or click **Cancel** to return to the inbox without making any changes.

Options Menu

The following is a list of items that are displayed in a change record options menu. Menu items visible may change depending on the selection.

Menu Item	Description
Set Reminder	Displays a form that allows you to schedule a reminder to yourself about some aspect of Change Management. Schedule a reminder by the clock or when certain task conditions exist using the following delivery methods: <ul style="list-style-type: none"> ■ Pop-up ■ Page ■ Email ■ SCMail
Print	Offers three print options: <ul style="list-style-type: none"> ■ Print Change record ■ Print all pages of this Change ■ Print Change and associated Tasks
Audit History	Displays the Audit Log showing the audit history of the current record, if audit history is in use.
Search Duplicates	Allows the user to query the Change Management database for duplicate changes. If you place your cursor in the field of a record and select Search Duplicates, a QBE list of records displays that contains the same values as the field in which the cursor was placed.
Validity Lookup	Validates the field in which the cursor is located.
Next Phase	Advances the phase of the current change record to the next level.
Change Category	Presents a QBE list of available categories, and allows the user to change the category of the current change record.
Change Phase	Presents a QBE list of available phases, and allows the user to select a different phase for the current change.
Alerts	Displays a list of alerts, if any exist for that change.
Approval > Approve Deny Retract	Allows you to approve, deny, or retract a change. <ul style="list-style-type: none"> ■ Click Approve to approve a change. ■ Click Deny to deny a change. ■ Click Retract to remove a previously approved or denied change.
List Pages	Lists all the pages associated with this change.

Menu Item	Description
Calculate Risk	Performs risk calculations in validity records previously set up for automatic calculation based on values in the change or task. If selected, Calculate Risk displays as either a change or task option, depending on what area the profile covers.
Copy Record	Copies an existing change request for use as a template and assigns a new change number. Use this option for adding a closely related change. Note: All copied changes are opened with the first phase.
Affected SLAs	Displays a table listing the affected SLA, downtime for that object (device), and the cost of the outage.
Related > Incidents > View Open Associate	View incident tickets related to this change, open incident tickets related to this change, or associate the change to an existing incident ticket.
Related > Calls > View Associate	View call reports related to this change or associate the change to an existing call report.
Related > Quotes > View Open Associate	View request management quotes related to this change, open request management quotes related to this change, or associate this change to an existing request management quote.
Related > Root Causes > View Open Associate	View root cause tickets related to this change, open root cause tickets related to this change, or associate this change to an existing root cause ticket.
Find Solution	Accesses the ServiceCenter Knowledge Base and brings up Hot News entries.
Notify	Allows the user to send a message (e-mail, fax, ServiceCenter mail) to other users about the status of the current change report.
Expand Array	Displays an array editing window for adding or deleting items to an array.
Generate Maintenance	Option available for changes only. Allows you to schedule the creation of changes, using the current record as a template.
Refresh	Returns the record to its last saved state.
View IND Device	Allows you to view the IND device data, including the device state, status, port information, and the device address.

Updating an Existing Change

To update a change record:

- 1 Access the change record you want to update, using one of the methods described in *Searching for an Existing Change* on page 409.
- 2 Modify the record as appropriate.
- 3 Save the updated record. Do one of the following:
 - Click **Save** or press F4 to save the record and leave it displayed.
 - Click **OK** or press F2 to save the record and return to the search form.

The status bar displays this message: **Change *unique ID* Phase *phase name* Updated by *operator*.**

Closing a Change Phase

Before closing a change phase, all tasks *must* be closed. Depending on your setup, approvals may also be necessary before closing a phase. The phase record controls the close control criteria required for closure. This criteria can vary between phases. For more information, see *Creating a Phase* on page 400.

To close a change phase:

- 1 Access the change record, using one of the methods described in *Searching for an Existing Change* on page 409.
- 2 Select **View Opened Tasks** from the Options menu.

Figure 10-29 on page 392 shows a task record form with a record list containing all the tasks related to the change.

The screenshot shows a software window titled "ServiceCenter - [Task T3 - Prompt]". It features a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Save, Close, Find, Fill, and Clocks. Below the toolbar is a table with columns: Number, Category, Phase, Start, End, Status, and Description. The first row is highlighted in blue and contains the following data:

Number	Category	Phase	Start	End	Status	Description
T3	Hardware	Hardware			initial	move printer 001 to accounting

Below the table is a form for task details. It includes fields for Task No. (T3), Category (Hardware), Phase (Hardware), Planned Start, and Planned End. Below this is a tabbed interface with tabs for General, Description, Inventory, Work Notes, Backout Method, Approvals, Parts & Labor, and Attachments. The General tab is active, showing fields for Risk Level (1 - low risk), Priority (2 (normal)), Status (initial), Approval Status (approved), Alert Stage, Scheduled Downtime (Start and End), Assigned To (Name: SUSIE SUPERTECH, Department: OPERATIONS, Phone: 619-481-5000, Assigned On), Work Manager (Name), Coordinator (Name: CM 1, Phone No.), and a status bar at the bottom indicating "Selected line is row 1 of 1 records" and a command line "insert cm3t.hardware.g[cm.view.display] [S]".

Figure 10-49: QBE List of Open Tasks

- 3 Select a task from the record list. Click Close or press F5.

- 4 Figure 10-50 shows the task record with a closing prompt.

ServiceCenter - [Task T3 - Close Prompt]

File Edit View Format Options List Options Window Help

OK Cancel Find Fill

Numbe	Category	Phase	Start	End	Status	Description
T3	Hardware	Hardware			initial	move printer 001 to accounting.

Task

Task No.: T3 Risk Level: 1 - low risk

Category: Hardware Priority: 2 (normal)

Phase: Hardware Status: closed

Planned Start: Approval Status: approved

Planned End: Alert Stage:

Close Info

Completion Code: 1 - successful Hours Worked:

Closing Comments

Selected line is row 1 of 1 records insert cm3t.close.g[cm.close.display] [S]

Figure 10-50: Closed Task Record

- 5 Complete all required inputs. If an Hours Worked field is required, enter the time used to complete this task, in this format: *ddd hh:mm:ss* and so on.

Important: You must include the time format even if the task was completed in whole days. For example, if a task was completed in exactly three days, enter 3 00:00:00.

- 6 Enter any comments you might have in the **Closing Comments** field.
- 7 Click **OK**.

The task is complete. The status bar displays this message: Task *T##* Phase *phase name* Closed by *login name*, as shown in Figure 10-51.

The screenshot shows the 'ServiceCenter - [Change C18 - Prompt]' window. It has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Prev, Next, Save, Close, Find, Fill, and Clocks. Below the toolbar is a table with columns: Number, Category, Prior, Phase, Asset, Start, End, Title. The table contains three rows of task data. Below the table is a form with fields for Change No., Category, Phase, Alert Stage, Planned Start, Planned End, Status, and Approval Status. Below the form are tabs for General, Description, Inventory, Justification, Outage, Backout Method, Approvals, Tasks, and Parts & Labor. The 'General' tab is active, showing fields for Change Type (Move, Add, Change), Coordinator (Name, Phone No.), Work Manager (Name), Scheduled Downtime (Start, End), Risk Level, Priority, and Initiated By (Name, Department, Phone, Initiated On). The status bar at the bottom displays the message: 'Task T3 Phase Hardware Closed by FALCON, JENNIFER' and a command line: 'insert cm3r.mac_g(cm.view.display) [S]'.

Number	Category	Prior	Phase	Asset	Start	End	Title
C17	RFC	3	Building	Printer 001	02/04/0	02/05	Move printer from marketing to
C18	MAC	2	Analysis				move printer 001 to accounting
C19	RFC	2	RFC Imple	Printer 001	02/19/0	02/26	Move printer 001 from marketing to

Change No.: C18
 Category: MAC
 Phase: Analysis
 Alert Stage:
 Planned Start:
 Planned End:
 Status: initial
 Approval Status: approved

General | Description | Inventory | Justification | Outage | Backout Method | Approvals | Tasks | Parts & Labor

Change Type
☐ Move ☐ Add ☐ Change

Coordinator
 Name: CM 1
 Phone No.:
 Work Manager
 Name:
 Scheduled Downtime
 Start:
 End:
 Risk Level: 1 - low risk
 Priority: 2 (normal)
 Initiated By
 Name: BUTLER, RICHARD
 Department: ACME/Customer Support
 Phone: (800) 422-5505
 Initiated On: 02/04/02 14:03:10

Task T3 Phase Hardware Closed by FALCON, JENNIFER
 insert cm3r.mac_g(cm.view.display) [S]

Figure 10-51: Closed Task in Browse Mode

Note: If you are closing a single task, the system exits to the change record shown in Figure 10-51. If you are closing a task in a task record list, the system exits to the task record in browse mode.

- 8 Select the next task in the record list.
- 9 Repeat steps 3 to step 9 until all open tasks have been closed.
- 10 Click **Close**. The close form of the change record appears.
- 11 Complete all required inputs. If an Hours Worked field is required, enter the time used to complete this task, in this format: *ddd hh:mm:ss* and so on.

Important: You must include the time format even if the task was completed in whole days. For example, if a task was completed in exactly three days, enter 3 00:00:00.

- 12 Enter any comments you might have in the **Closing Comments** field.
- 13 Click **OK**. The change phase closes and the system exits to the closed change record in browse mode shown in Figure 10-52. The status bar displays this message: **Change C## Phase phase name closed by login name.**

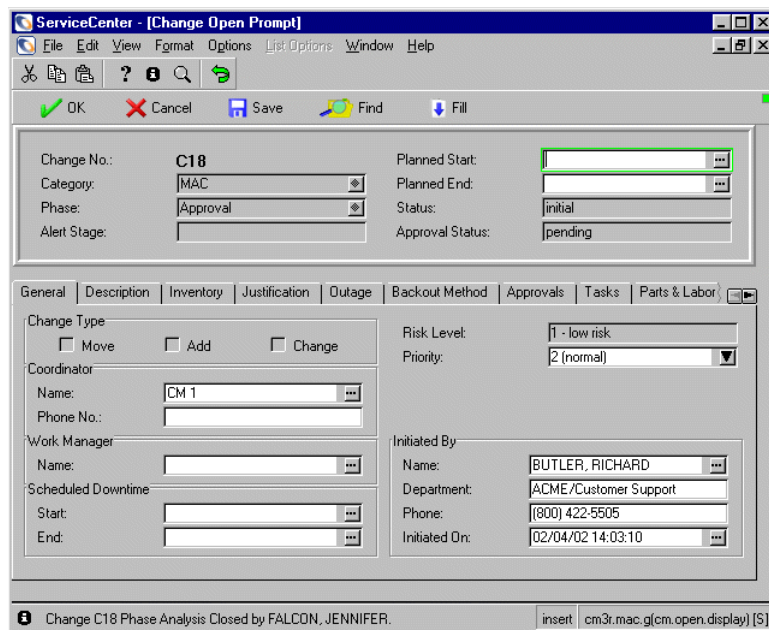


Figure 10-52: Closed Change in Browse Mode

Note: You need to take into consideration how the open behavior is set for this phase and whether or not your change request involves more than one phase. It is possible this operation will not close the entire change, but only the current phase. If that is the case, the next phase is then opened for your action.

Reopening a Change Request

To reopen a change request:

- 1 Click **Search Changes** in the Changes tab of the Change Management menu. A blank change search screen appears, as shown in Figure 10-43 on page 410.
- 2 Enter **closed** in the **Status** field of the Search form shown in Figure 10-53.

ServiceCenter - [Display Which Changes?]

File Edit View Format Options List Options Window Help

Back New Search Clear Find Fill

Basic Search Advanced Search IR Query

Search for Changes Where:

Number:

Status:

Approval Status:

Category:

Cost Center:

Assigned To:

Assigned Dept:

Change Initiator:

Coordinator:

External Ref:

Phase:

Impact:

Priority:

Affected Asset:

Closure Code:

Company:

Corp Struct/Div:

☒ Smart Search

Changes that are:

☐ Active

☐ Inactive

☐ Deferred

☒ All

Ready insert | cm3t.search.g(cm.search.display) [P]

Figure 10-53: Search Form — Searching for Closed Changes

- 3 Click **Search** or press **F6**.

Figure 10-54 shows a QBE record list that shows all closed change reports in the system.

The screenshot shows a window titled "ServiceCenter - [Display Which Changes?]" with a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar (Back, New, Search, Clear, Find, Fill). Below the toolbar are tabs for "Basic Search", "Advanced Search", and "IR Query". The "Basic Search" tab is active, showing a "Search for Changes Where:" section with fields for Number, Status, Approval Status, Category, Cost Center, Assigned To, Assigned Dept, Change Initiator, Coordinator, External Ref, Phase, Impact, Priority, Affected Asset, Closure Code, Company, and Corp Struct/Div. To the right of these fields is a "Smart Search" checkbox (checked) and a "Changes that are:" section with radio buttons for Active, Inactive, Deferred, and All (selected). The status bar at the bottom shows "Ready" and "insert cm3r.search.g[cm.search.display] [P]".

Figure 10-54: Record List of Closed Change Requests

- 4 Select the record you want to display from the record list.
- 5 Click **Reopen** or press **F5**.

The record appears in a form with editable fields. Make the appropriate changes to the record.

- 6 Click **Save** or press **F4** to save changes to the reopened record.

The status bar displays this message: **Change C## Phase *phase name* Updated by *login name*.**

Note: You can reopen a closed change immediately after closing the record by clicking **Reopen** or pressing **F5**.

Tasks

The appearance and function of the Tasks tab in the Change Management menu is identical to that of the Changes tab with the exception that you are viewing tasks instead of changes. The procedures for updating tasks are similar to those described in *Updating an Existing Change* on page 418. For more information, see the *ServiceCenter User's Guide*.

Searching for an Existing Task

ServiceCenter is shipped with sample tasks for you to use while you are learning the system. You can access an existing task record from the Change Management menu in one of two way, the Search form or the Task queue.

Search Form

To search for an existing task:

- 1 Click **Change Management** in the ServiceCenter home menu.
- 2 Select the **Tasks** tab in the Change Management menu.
- 3 Click **Search Tasks** in the Change Management menu. The task search form appears, as shown in Figure 10-55.

Figure 10-55: Task Search form

- 4 To search for a task record, do one of the following:
 - Perform a *true* query
 - Leave all the fields blank and click **Search** or press **Enter**. A QBE list of all current change records appears.
 - Enter search criteria in one or more of the fields in the Basic Search tab shown in Figure 10-55. Click **Search** or press **Enter**. A QBE list of all current task records that meet the selected criteria appears.

Advanced Search

Figure 10-56 shows the Advanced Search form.

Figure 10-56: The Advanced Search form

Enter time frame criteria for your search in the fields provided and click **Search** or press **Enter**.

The date and time information is optional. Enter the **After** **And Before** dates and times the task was opened or updated. The default format is *mm/dd/yyyy hh:mm:ss*. If a time is not entered, the default is *00:00:00*.

- Starting After And Before
- Ending After And Before
- Closed After And Before
- Created After And Before

Note: The date and time format can be set in the System Wide Company Record or in individual operator records. Therefore, the date and time format you use may vary from the default described here.

IR Query

Figure 10-57 shows the IR Query form.

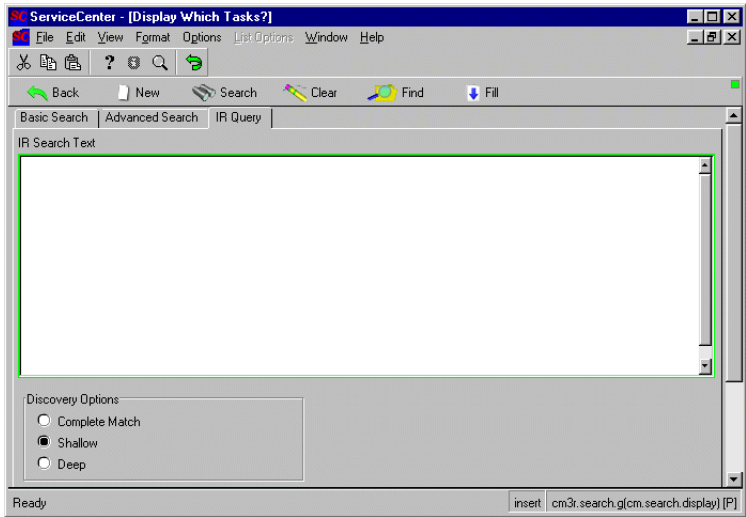


Figure 10-57: The IR Query tab

The following table describes the fields on the IR Query tab.

Field	Description
IR Search Text	Access ServiceCenter’s IR Expert application, an intelligent, concept-based information retrieval engine that searches the ServiceCenter database for similar or related information, based on a simple, natural language query. Enter a plain text query in the blank text box. ServiceCenter adds the plain text to the search parameters.
Discovery Options	<ul style="list-style-type: none">■ Complete Match — system searches for an absolute match to the text you have typed.■ Shallow — system uses narrow parameters and returns fewer records than with a deep search.■ Deep — systems performs a broad search. This is a good option if a shallow search does not return the desired records.

Figure 10-58 shows a task record list that displays the first record.

The screenshot shows the ServiceCenter application window titled "ServiceCenter - [Task T2 - Prompt]". The window has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Prev, Next, Save, Close, Find, Fill, and Clocks. Below the toolbar is a table with columns: Number, Category, Phase, Start, End, Status, and Description. The table contains three records: T2 (HW maintain, HW maintain, initial, move printer 001 to accounting), T3 (Hardware, Hardware, closed, move printer 001 to accounting), and T4 (plan.1/2 tas, plan.1/2, initial, Move development PCs to new cubicles within Building 3). The first record (T2) is selected. Below the table is a form for editing the selected task. The form has fields for Task No. (T2), Category (HW maintain), Phase (HW maintain), Planned Start, and Planned End. Below the form is a tabbed interface with tabs: General, Description, Inventory, Work Notes, Backout Method, Approvals, Parts & Labor, and Attachments. The General tab is active, showing fields for Risk Level, Priority (2 (normal)), Status (initial), Approval Status (approved), Alert Stage, Scheduled Downtime (Start, End), Assigned To (Name, Department, Phone, Assigned On), Work Manager (Name), Coordinator (Name, Phone No.), and a status bar at the bottom indicating "Selected line is row 1 of 3 records" and "insert cm3t.qbe.g [S]".

Number	Category	Phase	Start	End	Status	Description
T2	HW maintain	HW maintain			initial	move printer 001 to accounting.
T3	Hardware	Hardware			closed	move printer 001 to accounting.
T4	plan.1/2 tas	plan.1/2			initial	Move development PCs to new cubicles within Building 3

Task No.: T2
 Category: HW maintain
 Phase: HW maintain
 Planned Start:
 Planned End:

General | Description | Inventory | Work Notes | Backout Method | Approvals | Parts & Labor | Attachments

Risk Level:
 Priority: 2 (normal)
 Status: initial
 Approval Status: approved
 Alert Stage:
 Scheduled Downtime: Start: End:
 Assigned To: Name: Department: Phone: Assigned On:
 Work Manager: Name:
 Coordinator: Name: BOB.HELPDESK Phone No.: 619-481-5000

Selected line is row 1 of 3 records insert cm3t.qbe.g [S]

Figure 10-58: Task Record in Edit Mode

- 1 Select a task record from the record list. The appropriate information appears in the form.

Task Queue

Searching for records with the task queue presents a list of tasks by *inbox*. For information about inboxes, refer to the *User's Guide*.

To search with the task queue:

- 1 Click **Task Queue** in the Change Management menu. Figure 10-59 on page 429 shows a task inbox that lists all the user's assigned tasks.

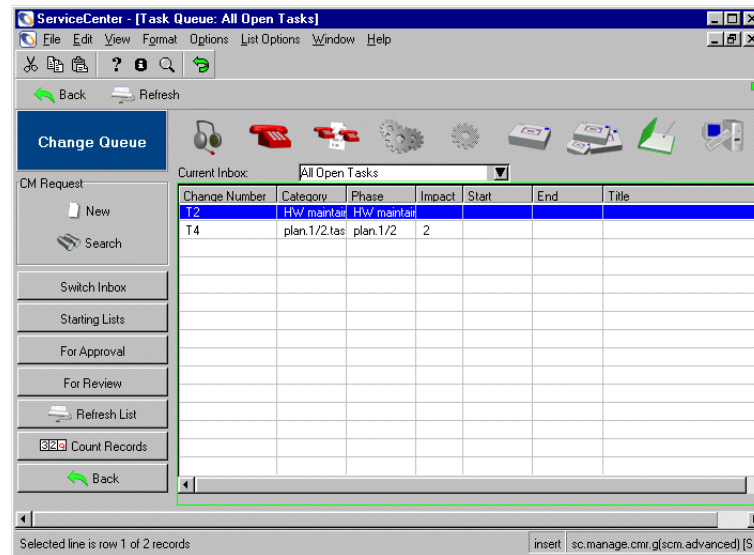


Figure 10-59: Task Inbox

- 2 Click **Switch Inbox** if you want to search for tasks assigned to a different inbox.
- 3 You may select a task to open from this list or click **Search** to display the task search form, as shown in Figure 10-55 on page 425.

Figure 10-60 shows the desired task record in edit mode.

Number	Category	Phase	Start	End	Status	Description
T2	HW maintain	HW maintain			initial	Move development PCs to new cubicles within Building 3, F
T4	plan.1/2.task	plan.1/2			initial	Move development PCs to new cubicles within Building 3, F

Task No.: T2 Planned Start:

Category: HW maintain Planned End:

Phase: HW maintain

General | Description | Inventory | Work Notes | Backout Method | Approvals | Parts & Labor | Attachments

Risk Level: Assigned To: Name:

Priority: 2 (normal) Department:

Status: initial Phone:

Approval Status: approved Assigned On:

Alert Stage:

Scheduled Downtime: Start: Work Manager: Name:

End: Coordinator: Name: BOB HELPDISK Phone No.: 619-481-5000

Selected line is row 1 of 2 records insert cm3t.HW.maintain.g(cm.view.display) [S]

Figure 10-60: Task Record Selected from an Inbox

- 4 Click **Save** to save any changes to the record.
- 5 Click **Close** to close the task.
- 6 Click **OK** to return to the inbox.

Options Menu

The following is a list of items that can display in a task record Options menu. The items visible may change.

Field	Description
Set Reminder	Displays a form that allows you to schedule a reminder to yourself about some aspect of Change Management. You may schedule a reminder by the clock or when certain task conditions exist using the following delivery methods: <ul style="list-style-type: none"> ■ Pop-up ■ Page ■ Email ■ SCMail
Print	Offers two print options: <ul style="list-style-type: none"> ■ Print task record ■ Print all pages of this task
Audit History	Displays the Audit Log showing the audit history of the current record.
Search Duplicates	Allows the user to query the Change Management database for duplicate changes. If you place your cursor in the field of a record and select Search Duplicates, a QBE list of records displays that contains the same values as the field in which the cursor was placed.
Validity Lookup	Validates the field in which the cursor is located.
Show Parent Change	Displays the change record to which the current task is attached.
Change Category	Presents a QBE list of available categories, and allows the user to change the category of the current change report.
Change Phase	Presents a QBE list of available phases, and allows the user to select a different phase for the current change.
Alerts	Displays alert control button in the system tray, allowing the user to schedule alerts and switch the function off or on.
Next Phase	Advances to the next task phase without closing the current phase.
List Pages	Allows the user to access all the pages in a task record.

Field	Description
Calculate Risk	If you have previously set up validity records so that risk is automatically calculated based on values in the task, this option performs the calculation at that time. If selected, Calculate Risk displays as either a change or task option, depending on what area the profile covers.
Copy Record	Copies an existing task record for use as a template and assigns a new task unique ID. Use this option for adding a closely related task.
Affected SLA	Displays a table listing the affected SLA, downtime for that object (device), and the cost of the outage.
I/R Query	Provides access to the I/R Query feature.
Expand Array	Displays an array editing window for adding, or deleting items to an array.
Notify	Allows the user to send a message (e-mail, fax, ServiceCenter mail) to other users about the status of the current task report.
Refresh	Returns the record to its last saved state.

Figure 10-61 shows the form where you can set a reminder.

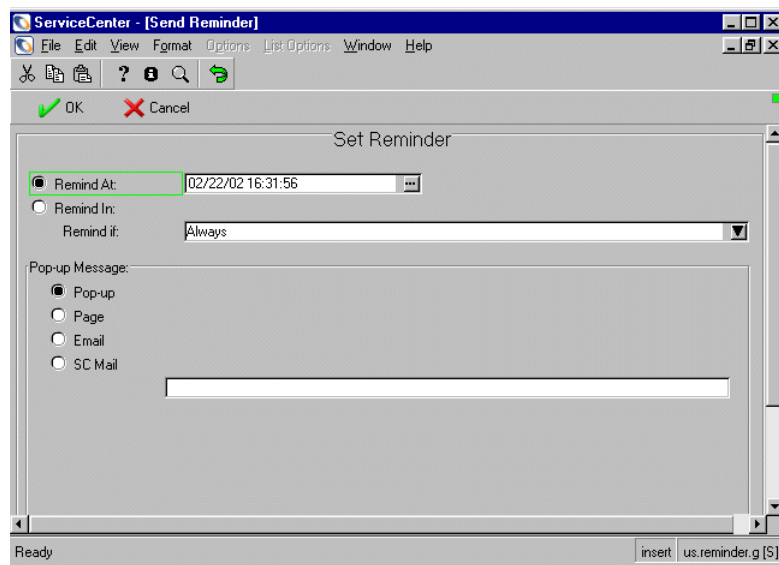


Figure 10-61: Set Reminder Form in a Task Record

Updating an Existing Task

To update a task:

- 1 Access the task record you want to update using one of the methods described in *Searching for an Existing Task* on page 425.
- 2 Modify the record as appropriate.
- 3 To save the updated record, do one of the following:
 - Click **Save** or press **F4** to save the record and leave it displayed.
 - Click **OK** or press **F2** to save the record and return to the QBE list or the search form.

The status bar displays this message: **Task *unique ID* Phase *phase name* Updated by *operator*.**

Closing a Task Phase

To close a task:

- 1 Access the task record you want to close, using one of the methods described in *Searching for an Existing Task* on page 425.
- 2 Click **Close** or press **F5**.
The record displays in a form with a Close Info structure.
- 3 Complete all required inputs. If an Hours Worked field is required, enter the time used to complete this task, in this format: *ddd hh:mm:ss* and so on.

Important: You must include the time format even if the task was completed in whole days. For example, if a task was completed in exactly three days, enter 3 00:00:00.

- 4 Enter any comments you might have in the **Closing Comments** field.
- 5 Click **OK** or press **F2** to close the task.

The task record appears in browse mode. The status bar displays this message: **Task *task unique ID* Phase *phase name* Closed by *operator name*.**

Reopening a Task

To reopen a task:

- 1 Click **Search Tasks** in the Tasks tab of the Change Management menu.
A blank task search screen appears.
- 2 Enter **closed** in the **Status** field.
- 3 Click **Search** or press **F6**. Figure 10-62 shows a task record that displays a record list of all closed tasks.

The screenshot shows the ServiceCenter application window titled "ServiceCenter - [Task T3 - Prompt]". The window has a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for Cut, Copy, Paste, Find, and Reopen. Below the toolbar is a record list with columns: Number, Category, Phase, Start, End, Status, and Description. The list contains one record: T3, Hardware, Hardware, (blank), (blank), closed, move printer 001 to accounting. Below the record list is a form for task details. The form has tabs: General, Description, Inventory, Work Notes, Backout Method, Approvals, Parts & Labor, and Attachments. The General tab is selected. The form contains fields for Task No. (T3), Category (Hardware), Phase (Hardware), Planned Start, Planned End, Risk Level (1 - low risk), Priority (2 (normal)), Status (closed), Approval Status (approved), Alert Stage, Assigned To (Name: SUSIE.SUPERTECH, Department: OPERATIONS, Phone: 619-481-5000), Work Manager (Name: CM 1, Phone No.: (blank)), and Scheduled Downtime (Start: (blank), End: (blank)). The status bar at the bottom indicates "Selected line is row 1 of 1 records" and "insert | cm3t.qbe.g [S]".

Figure 10-62: Closed Task in Browse Mode

- 4 Select the record you want to display from the record list. The appropriate task information displays in the form.
 - 5 Click **Reopen** or press **F5**. The record appears in a form with editable fields.
 - 6 Click **Save** or press **F4** to save changes to the reopened record. The status bar displays this message: **Task T## Phase phase name Updated by login name.**
- Note:** You can reopen a closed task immediately after closing the record by clicking **Reopen** or pressing **F5**.

Approvals

If you are making a change and the change needs an approval, the change may be submitted to one or more approval groups, which can consist of one or multiple ServiceCenter users.

Approvals are defined as a list of groups or operators who must acknowledge or accept the risk, cost, and so on associated with the implementation of a change request or task. Once the approval requirements are set up, approvals give controlling authorities the ability to stop work and to control when certain work activities can proceed. Approvers manually approve changes before tasks are assigned.

An approval sequence is an order in which approval requirements are made active. The process first makes the lowest sequence numbers available for approval activity. Once these are approved, the next highest number is made available. Groups with the same sequence number can approve in any order.

Approval groups are defined in the operator record, based on the User Role. For more information, see [Security Profiles](#) on page 358.

As an approver, you can also be part of a change message group. A change message group member list consists of reviewers and approvers. If you are an approver for a change message group, your task is to accept or deny the changes your group must approve. For more information, see [Approving Changes and Tasks](#) on page 439.

Approval Sequence

Phases have an approval status of *approved*, *denied*, or *pending*. Individual approval requirements within a phase have a status of *approved*, *denied*, *pending*, or *future*. *Pending* approvals are awaiting action. *Future* approvals will be acted on following action on the pending approvals. Approval groups are placed in sequences in the order that their approval is required. If groups have the same sequence number, their approvals can be made independent of each other.

When a *pending* phase is approved, its status becomes *approved*. The next set of future approvals become pending, and subsequent approvals remain in the *future* status.

Figure 10-63 shows four approval groups are in three sequences. Box 1 shows Group A in a *pending* status; groups B, C and D are in *future* status. Group A approves the phase and moves to the *approved* status. In Box 2, the sequence 2 groups, B and C, move to a *pending* status. The sequence 3 group, D, remains in the *future* approval status.

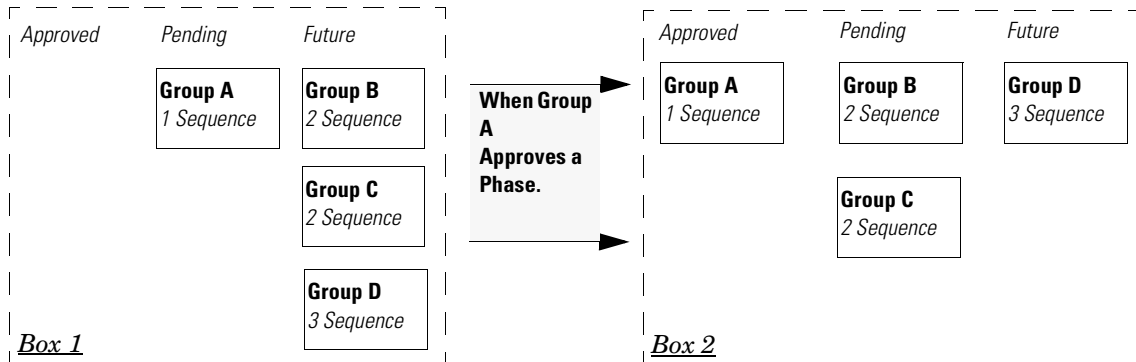


Figure 10-63: Approval Sequence

Approvals tab

To view the Approvals tab in an existing change or task:

- 1 Open an existing change or task record. For more information, see [Updating an Existing Change](#) on page 418 and [Updating an Existing Task](#) on page 433.

Note: Some changes and tasks in the standard system do not have Approval tabs.

- 2 Select the Approvals tab in the record to check the approvals history for the change, as shown in Figure 10-64.

Approval Type	Approval Status	# Approved	# Denied	# Pending
Assessment	pending	0	0	1

Figure 10-64: Approvals tab

The Approvals tab has three sub-tabs, which include approval and review history for the approvals listed for the change or task being viewed:

- Current Approvals
- Approval Log
- Pending Reviews

Current Approvals subtab

Current approvals for this change or task phase appear on this tab, shown in Figure 10-64.

Field	Description
Approval Type	<p>The authorization type needed for this change or task. Click on Approval Type for each approval and see:</p> <ul style="list-style-type: none"> ■ Who requested the change ■ What the currently pending approvals and future approvals are ■ Completed approval actions ■ Added comments
Approval Status	<p>Approval status for each approval type:</p> <ul style="list-style-type: none"> ■ Pending ■ Approved ■ Denied ■ Retracted
Approved	Number of approved changes or tasks.

Pending Reviews subtab

Reviewers member list that reviewed the pending approval for this change or task. Figure 10-66 shows the Pending Reviews Subtab.

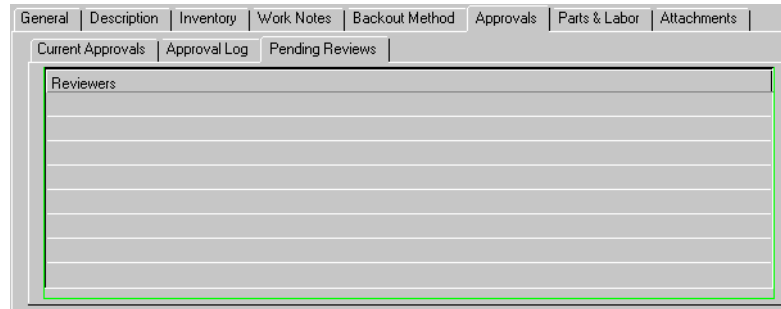


Figure 10-66: Approving Changes and Tasks

If you are an authorized approver for any approval groups, the group names (for example, CHGCOMM, CUS) are displayed in your Security Profile. For more information, see [Security Profiles](#) on page 358. You may approve all changes and tasks assigned to your approval groups.

The process for approving a change is the same as for approving a task. You may access the Approval options in any of three locations:

- Change/Task Queue
- Change/Task Search Form
- Options menu in an existing change or task

For a full description of approvals, approvers, approval groups, and approving changes and tasks, see the *ServiceCenter User's Guide*.

Change/Task Queue

The Change Queue is used for purposes of this example. The process is the same for the Task Queue.

To access Approval options from a queue:

- 1 Click **Change Queue** in the Changes tab of the Change Management menu. Figure 10-67 shows the change inbox.

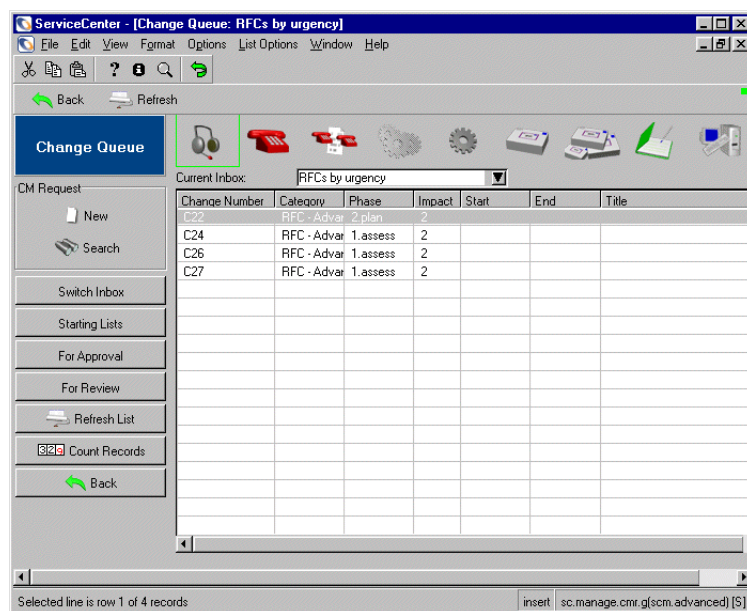


Figure 10-67: Change Inbox

- 2 Click **For Approval**. Figure 10-68 shows a dialog box that lists your approval groups.

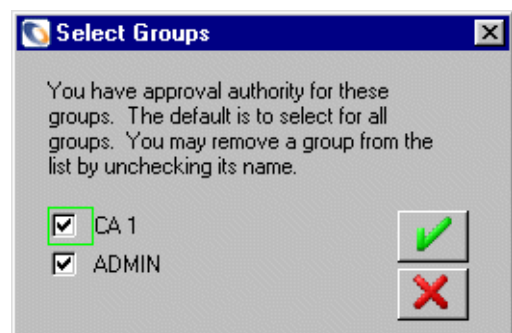


Figure 10-68: Approval Group Membership

- 3 Select a group for which you want change records displayed, or leave the list blank to approve for all your groups.

- 4 Click OK. A list of all Changes requiring the approval of the groups you have selected displays in the inbox. Figure 10-69 shows a typical change queue.

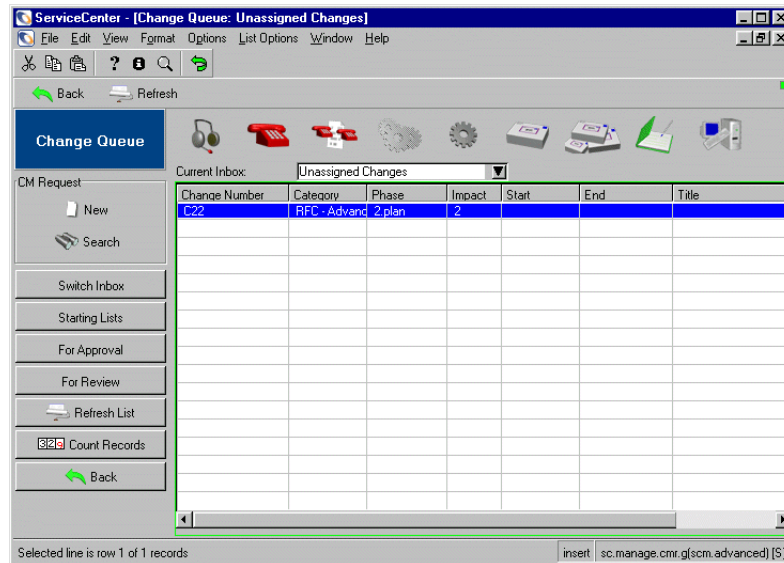


Figure 10-69: Inbox List of Change Phases Requiring Approval

- 5 Double-click a record to open it for approval. The record appears.
- 6 Do one of the following:
 - Select **Approval** from the Options menu of the change record.
 - Click **For Approval** on the Inbox screen.

ServiceCenter displays the Change Approval Group Selection dialog box shown in Figure 10-70.

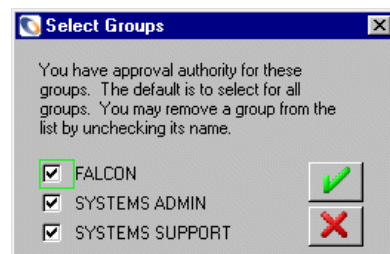


Figure 10-70: Approval dialog box

- 7 Click the appropriate box, or leave all checked to default to all groups.



If you click **OK**, you are returned to the Unassigned Changes inbox of the Change Sponsor's queue.

A new set of buttons displays in the system tray.

- 8 Select an approval option from those in the following table.

Approval Option	Description
Approve	<p>Approver accepts the need for the change and approves commitment of the resources required to fulfill the request. Once all approvals are complete, work can begin on the phase.</p> <p>When this option is selected, the record shifts to the browse mode, and the Retract option displays in the system tray. The status bar displays this message: <i>change unique ID Phase phase name Approved by operator name</i>.</p> <p>If you are not a member of a group with approval rights to this change request, the status bar displays this message: You may not approve for any of the Pending Approval Groups.</p>
Deny	<p>Approver does not accept the need for the change and/or is unwilling to commit the required resources. No further approvals are allowed until the denial is removed. An administrative procedure should be set up to handle a denial.</p> <p>When this option is selected, a dialog box appears with a prompt to specify the reason for your action. Type an explanation for your action and click OK. The status bar displays this message: <i>change C## Phase phase name Denied by login name</i>.</p>
Retract	<p>Approver accepts the need for the change, but is unwilling to commit the resources or perhaps there are technical Incidents at the present time. This removes a previous approval or denial and resets the change request to pending approved status, requiring a new approval cycle.</p> <p>When this option is selected, a message displays that asks you to state the reason for your action. Enter an explanation for your action and click OK. The status bar displays this message: <i>change unique ID Phase phase name Retracted by operator name</i>.</p>

Change Task Search Form

The change search form is used for purposes of this example. The process is the same for the task search form.

To access Approval options from a search form:

- 1 Click **Search Changes** in the Changes tab of the Change Management menu. Figure 10-71 shows a blank change search form.

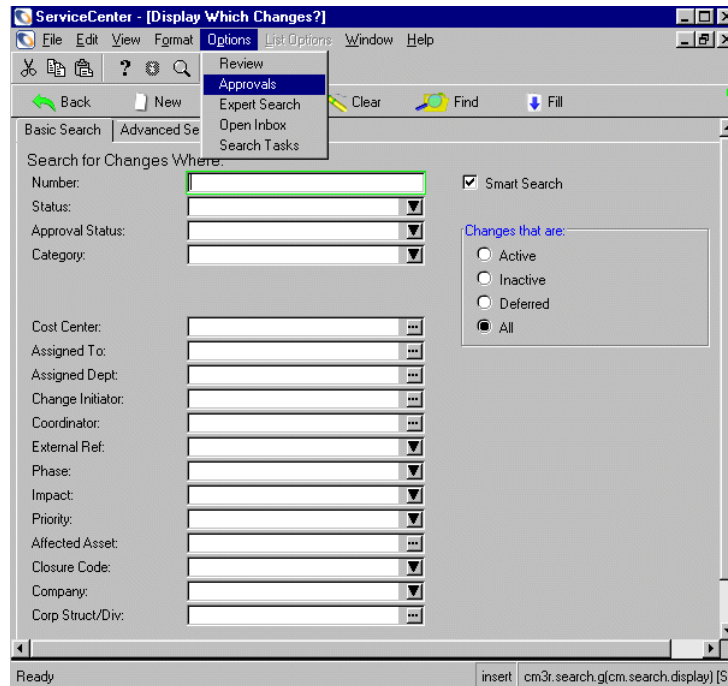


Figure 10-71: Accessing Approvals in a Change Search Form

- 2 Select **Approvals** from the Options menu. A dialog box, listing approval groups that you belong to, appears, as shown in Figure 10-70 on page 441.
- 3 Select a group for which you want change records displayed.
- 4 Click **OK**.

Figure 10-72 shows a change record with a record list of changes requiring group approval.

ServiceCenter - [Change C18 - Prompt]

File Edit View Format Options List Options Window Help

OK Cancel Save Close Find Fill Clocks

Number	Category	Prior	Phase	Asset	Start	End	Title
C18	MAC	2	Approval				move printer 001 to accounting

Change No.: C18
 Category: MAC
 Phase: Approval
 Alert Stage:
 Planned Start:
 Planned End:
 Status: Initial
 Approval Status: pending

General Description Inventory Justification Outage Backout Method Approvals Tasks Parts & Labor

Change Type
☐ Move ☐ Add ☐ Change

Risk Level: 1 - low risk
 Priority: 2 (normal)

Coordinator
 Name: CM 1
 Phone No.:

Work Manager
 Name:

Scheduled Downtime
 Start:
 End:

Initiated By
 Name: BUTLER, RICHARD
 Department: ACME/Customer Support
 Phone: (800) 422-5505
 Initiated On: 04/02/2002 22:03:10

Selected line is row 1 of 1 records

insert cm3r.qbe.g [S]

Figure 10-72: Record List of Changes Requiring Group Approval

- 5 Select **Options > Approval > Approve | Deny | Retract**. For more information, see [Approvals](#) on page 435, [Approving Changes and Tasks](#) on page 439, and the *ServiceCenter User's Guide*.
- 6 Select **MassApprove** from the List Options menu to approve all the changes in the record list. You are prompted to confirm the action.
- 7 Click **Yes** only if you want to approve all the records in the list.

Known Change Request

An approver may learn of a change request that requires attention from a message event generated by the system. When this occurs, the approver can search for the change report by unique ID, using the following procedures:

- 1 Click **Search Changes** in the Changes tab of the Change Management menu. Figure 10-73 shows a blank change search form.

Figure 10-73: Change Search Form

- 2 Type the unique ID of the change request in the **Number** field.
- 3 Click **Search**. The requested change report appears.

- 4 Select Options > Approval > Approve | Deny | Retract, as shown in Figure 10-74.

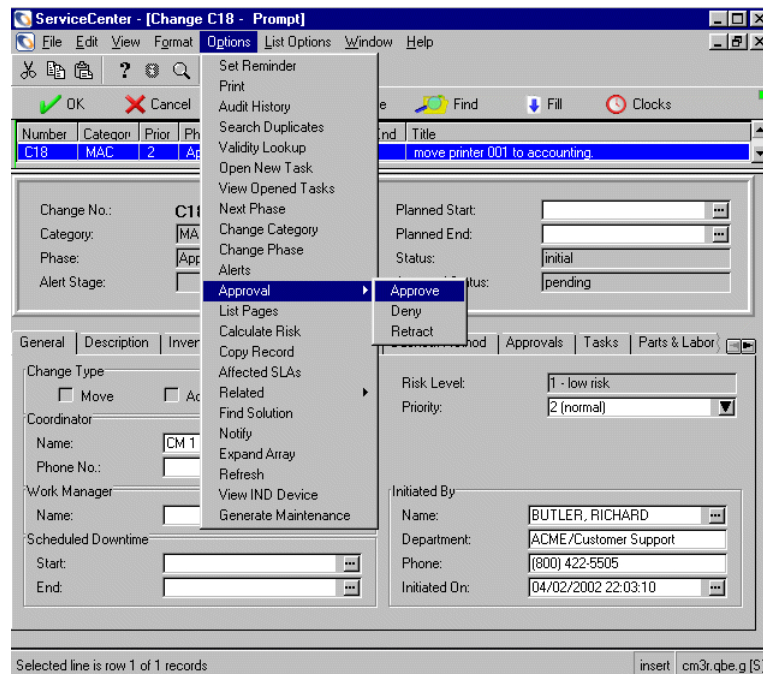


Figure 10-74: Approval in the Options menu

The change search form is used for purposes of this example. The process is the same for the task search form.

Risk Calculation

Risk is a rating that summarizes the probability and/or consequences of implementation failure. With many Change Management systems, risk is a subjective rating. The user making the change, or perhaps the change administrator, will determine and assign a risk rating. This type of process can result in inaccurate risk ratings. For example, a one-line code change to a software module may pose little threat in itself; however, the fact that the module being changed will affect all online users raises the issue to another level. Change Management allows you to replace *subjective* risk evaluation with *objective* risk evaluation. This is done by basing the risk calculation on the actual data contained in the record.

Change Management risk assessment determines the risk assessment of a change or task based on the values of certain fields within the record. Each field used in the risk assessment process carries a field weight and each possible value for that field (assuming there are a finite number of values) carries a value weight. Each field's total weight is calculated by multiplying the field weight by the value weight. The change or task risk assessment is then calculated by totalling the total weights and rounding the average. Change Management uses the ServiceCenter validity tables to define the field weights, value weights and to determine the risk assessment of a record.

Note: You can use the calculated risk to control the standard features that support the evaluation of complex conditions such as approval requirements, alert conditions, event processing, and scripting.

Example

In the following examples, the fields **planned.start**, **ipl.required**, **duration**, and **recovery.time** are used to calculate risk. The valid values and the value weights are shown below. The risk range is defined as 0 (low) and 3 (high). The following table describes the input fields.

Input Field	Values	Value Weight
ipl.required	>=21 days from today	1
	yes	3
	no	0
duration	> 1 hour	3
	<= 1 hour and 15 minutes	2
	<= 15 minutes and > 1 minute	1
	<= 1 minute	0
recovery.time	> 30 minutes	3
	<= 30 minutes and > 1 minute	2
	<= 1 minute	0

Based on these definitions, the following sample changes would have the indicated risk value. Only the data for the risk input fields is shown.

Note: Assume the current date is 11/01/02.

Example 1: Change Data

The following table describes the change data.

Input Field	Value	Value Weight	Field Weight	Total Weight
planned.start	11/30/02	1	1	1
ipl.required	no	0	1	0
duration	0 mins.	0	1	0
recovery.time	0 mins.	0	1	0
Total				1
Average				0.2
Risk Value				0

Example 2: Change Data

The following table describes the change data.

Input Field	Value	Value Weight	Field Weight	Total Weight
planned.start	11/30/02	1	1	1
ipl.required	yes	3	1	3
duration	40 mins.	2	1	2
recovery.time	40 mins.	3	1	3
Total				9
Average				2.2
Risk Value				2

The following examples demonstrate how you can use the field weight to influence the outcome of the risk assessment process. In [Example 3: Change Data](#) on page 449, the field weight for **planned.start** has been updated to be 5. This allows us to assign a high risk to any request that does not meet established lead time requirements, regardless of the values for the other risk fields. In [Example 4: Change Data](#) on page 449, the field weight of **planned.start** is changed back to 1. Therefore, the risk value drops to 1.

Example 3: Change Data

The following table describes the change data.

Input Field	Value	Value Weight	Field Weight	Total Weight
planned.start	11/02/02	3	5	15
ipl.required	no	0	1	0
duration	0 mins.	0	1	0
recovery.time	0 mins.	0	1	0
Total				15
Average				3.8
Risk Value	Based on Risk Max=3			3

Example 4: Change Data

The following table describes the change data.

Input Field	Value	Value Weight	Field Weight	Total Weight
planned.start	11/02/02	3	1	3
ipl.required	no	0	1	0
duration	0 mins.	0	1	0
recovery.time	0 mins.	0	1	0
Total				3
Average				.8
Risk Value				1

It is important that the range of the field weights be the same as the risk range. For instance, if the risk range is 1, 2, 3, 4 and 5, the field weights should also be within this range. If the field weights are outside of this range, it is possible that the value calculated for risk value will also be outside of the range. If you do assign a high number to a field weight as is shown in [Example 3: Change Data](#) on page 449, you may also want to consider setting on upper limit in the Maximum field in the Phase definition. As is shown in [Example 3: Change](#)

Data on page 449, it is possible that the risk calculation process would return a value outside of the valid risk range. If we don't establish a limit, the risk calculation process would, by default, return a value of 4. In our example, this would be an invalid value, because the valid risk range is 0 to 3.

Events, Alerts, and Messages

During the life cycle of change requests and tasks, certain critical events occur, which warrant notification of the appropriate individuals. Examples of such events include open, update, close, and approval of the changes or tasks. There may also be other events unique to an organization that warrant notification.

Events in Change Management can spawn messages to designated parties (operators or groups) within the system. For example, messages can indicate if a request has been opened, and set into action the need for a user to provide additional interaction, namely providing an approval for the request.

In the event a certain time limit set for accomplishing an approval is not met, an alert is triggered. An alert is an optional timed-delayed event, which triggers another event to send out a message.

As soon as a request is approved, that action constitutes an event. A message is sent by that event, indicating the state of the request.

In this way, events, alerts, and messages build the communication chain, notifying users of pending requests and the status of requests for change throughout their life cycles.

This section discusses the following issues with regards to setting up and managing the use of standard and special events (such as messages and alerts) in Change Management:

- *Alert Processing* on page 453
- *Events* on page 460
- *Messages* on page 465
- *Background Processing* on page 467

Alerts

Alerts are timed, or delayed, events. Change Management treats alerts as events when the alert condition evaluates to *true*. This allows sending notifications when a change or task reaches an alert condition. When the scheduled alert occurs, an associated event is triggered.

Messages can be sent (but are not required) as a result of events and alerts. Requests for change progress in phases, according to a predefined schedule. Alerts monitor the progress of these phases and take action when circumstances warrant an automated response, such as when the progression is delayed. For example, the *late notice* alert notifies a designated management group that a request for change is overdue for approval, and updates the alert status to include *late notice*.

The user can define any number of standard or customized alerts for any phase, control who is notified for each alert, and control the naming convention used for the alert itself.

Alerts support several functions within the system:

- Alert Messaging — alerts trigger events. The event manager generates messages to certain designated recipients as a result of an alert, which update the original request.
- Batch Scheduling — all alerts associated with a phase are scheduled at once when the phase appears.

To access Phase Definition Alert controls:

- 1 Click **Change Management** on the ServiceCenter Home menu.
- 2 From either the Changes or Tasks tab, select **Change Phases or Task Phases**.
- 3 Click **Search** to perform a *true* query without entering any values in the blank *cm3rcatphase.main* form. A record list of alert records displays. Make your selection by clicking on a phase name.
- 4 Click the Alerts/Open & Close Behavior tab. Figure 10-75 on page 452 shows the Phase Definition Alert controls.

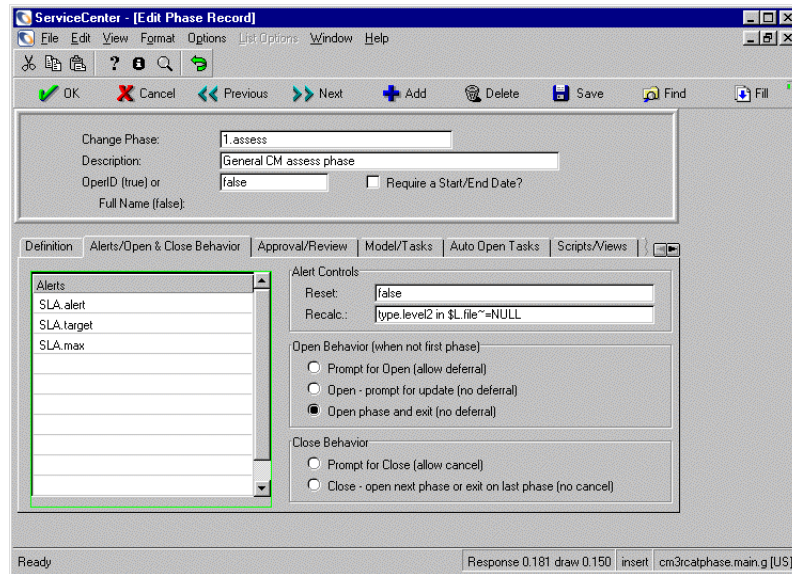


Figure 10-75: Phase Definition Alert Controls

Certain alert controls are specified on the Phase (cm3r options) record. The following table describes the Alert Control fields.

Alert Control	Description
---------------	-------------

Reset	Sets the status of all current Alert records associated with the current request for change to inactive and marks the last action field as reset. Then, it schedules a calculate alert record to recalculate the item's alerts and restart the alerts process.
Recalc	<p>Retrieves each Alert associated with the request for change and performs the following processing:</p> <ul style="list-style-type: none"> ■ If current alert status is active, the alert condition is reevaluated and the alert is updated to reflect the correct status; processing ends. ■ If current status is not active, the Schedule Condition field is reevaluated. If this evaluates to true, the following fields are updated: <ul style="list-style-type: none"> ■ Status is set to scheduled. ■ Last Action is set to recalc. ■ Action Time is set to current date/time. ■ Schedule Condition is reevaluated. If true, Alert Time is recalculated and Status updated to scheduled. If false, Status is set to not required.

Alert Processing

There are two primary files used in alert processing:

- Alert Definition (**AlertDef**) defines the alerts used by all phases (static file).
- Current Alerts (**Alert**) tracks the alerts created for each phase (active alert file).

Alert Definitions

The Alert Definition is a static file, which defines the basic alert information for each named alert and all general alert definitions.

To access the Alert Definition File:

- 1 Click **Change Management** on the ServiceCenter Home menu.
- 2 Select **Alerts** in the Maintenance tab. An empty Alert Definition form (**AlertDef**) appears.
- 3 Click **Search** to pass a *true* query and display a list of all current Alert Definition records.

- 4 Select a record to view from the list by clicking on the alert name. Figure 10-76 shows the selected record.

The screenshot shows a window titled "ServiceCenter - [AlertDef Pending.1]". It contains a menu bar (File, Edit, View, Format, Options, List Options, Window, Help) and a toolbar with icons for OK, Cancel, Previous, Next, Add, Save, Delete, Find, and Fill. Below the toolbar is a table with columns: Alert Name, Description, Alert Status, Sched Cond, and Alert Cond. The first row is selected and highlighted in blue.

Alert Name	Description	Alert Status	Sched Cond	Alert Cond
Pending.1	Pending Appro	Pending.1	open in \$.file=true and \$.approval.status in \$.file="pending"	
Pending.2	Pending Appro	Pending.2	open in \$.file=true and \$.approval.status in \$.file="pending"	
Request Late Notice		Request Late Notice	open in \$.file=true	open in \$.file=true

Below the table is the "Alert Definition" form. It has tabs for "Scheduling", "Update Info", "Parents", and "Duty Table". The "Scheduling" tab is active. The form contains the following fields:

- Alert Name: Pending.1
- Description: Pending Approval
- Alert Status: Pending.1
- Schedule Condition: open in \$.file=true and nullsub(alert.stage in \$.file,"")~="off" and approval.status in \$.file="pending"
- Schedule Class: change
- Alert Condition: approval.status in \$.file="pending"
- Calculation Type:
 - ☒ Use field in record + interval
 - ☐ Use expression to set \$.alert.time
- Calc Field: assign.date
- Calc Interval: 1 00:00:00

At the bottom, it says "Selected line is row 1 of 16 records" and "insert | AlertDef.g(db.view) [P]"

Figure 10-76: Alert Definition Record List with first record displayed

The following table describes the fields on the Alert Definition form.

Field	Description
Alert Name (required)	Unique name of the Alert.
Description	A text description of the Alert Condition.

Scheduling tab

See the Scheduling tab shown in Figure 10-76 on page 454. The following table describes the fields on the Scheduling tab.

Field	Description
Alert Status	Status of the alert. Current file referenced by <i>\$L.file</i> .
Schedule Condition	Condition that determines if the Alert is scheduled. The default is <i>false</i> .
Schedule Class	Classification of the scheduled Alert.
Alert Condition (<i>required</i>)	Condition that must evaluate to <i>true</i> before the alert is set. If evaluations are <i>false</i> , the alert goes away. The default is <i>false</i> .
Calculation Type	<p>Calculation method used for setting alert conditions. Use one of the following:</p> <ul style="list-style-type: none"> ■ Use field in record + interval Calc Field — name of the date/time field in the request for change that the interval field value is added to in order to determine the alert time. (Change Management uses the current date/time to apply the alert interval if this field is null in the request for change data record.) Calc Interval — (<i>required</i>) relative interval of time that is added to the Calc Field time to determine the alert time. Can be positive or negative time intervals. ■ Use expression to set <i>\$L.alert.time</i> Calc Expression — text expressions parsed into a message and presented at alert time.

Update Info tab

Figure 10-77 shows the Update Info tab.

Figure 10-77: Update Info tab

The following table describes the fields on the Update Info tab.

Field	Description
Format Control	Name of the Format Control record to be processed in addition to the regular alert processing, when the Alert Condition field evaluates to <i>true</i> .
Triggers Off	Always set to <i>false</i> (unchecked). <i>DO NOT</i> change this setting.
Statements	Processing statements executed in addition to the regular alert processing, when the Alert Condition field evaluates to <i>true</i> .
Update Process	Update process to be used when setting up alerts.
Notifications	Notification process to be used when alerts are processed. For more information, see Notifications on page 470 and see the <i>System Tailoring Guide</i> .

Parents tab

Figure 10-78 shows the Parents tab. *Do not* make any changes to the definitions in this tab.

The screenshot shows the 'Parents' tab with the following options for 'Parent Type':

- ☒ No parent definitions
- ☐ User Defined
- ☐ Use expressions to set \$L.parent.file and \$L.parent.id

Figure 10-78: Parents tab

The parent type that is defined and reflected in the alert status phase.

Field	Description
No parent definitions	No parent definitions to be defined.
User Defined	<ul style="list-style-type: none"> ■ Parent File — unique name of the Parent file. ■ Parent Id — unique identification number of the parent part.
Use expressions to set \$L.parent.file and \$L.parent.id	
Expressions	Enter the expressions to set the <i>\$L.parent.file</i> and <i>\$L.parent.id</i> .

Duty Table tab

The Duty Table is the work table that is used to calculate alert times. When scheduling alerts, the Alert processor determines which shifts are valid for sending alerts. Figure 10-79 shows the Duty Table tab.

The screenshot shows the 'Duty Table' tab with the following options for 'Duty Table Type':

- ☒ No Duty Table (24x7)
- ☐ Define a Duty Table
- ☐ Lookup a specific Duty Table

Figure 10-79: Duty Table tab

Duty Table tab

The following table describes the fields on the Duty Table tab.

Field	Description
No Duty Table (24x7)	Duty Table not defined. Use standard 24x7 clock and calendar.
Define a Duty Table	
Duty Table	User defined Duty Table. Customized to set your office group's working hours.
Lookup a Specific Duty Table	Allows standard validity Table Look-Up processing so that the Alert processor can determine valid shifts, based on an existing Duty Table.
Group Lookup Name	Allows standard validity Table Look-Up by name, so that you can use another Duty Table in the Table Lookup file.
Group Lookup File	Allows standard validity Table Look-Up by file, so that you can use another Duty Table in the Table Lookup file.
Group Lookup Field	Allows standard validity Table Look-Up by field.
Duty Table Field	Uses the definition in the Duty Table field.

Alert Log

The Alert log is a file that lists currently scheduled and active alerts.

To access the Alert Log file:

- 1 Click **Database Manager** in the ServiceCenter Toolkit tab of the Home menu.
- 2 Enter Alertlog in the **File** field, and then click **Search**. An empty Alert Log form (Alertlog) appears.
- 3 Click **Search** to retrieve a list of all current Alert Log records. Then click on a record in the list.

Figure 10-80 shows the selected Alert Log record.

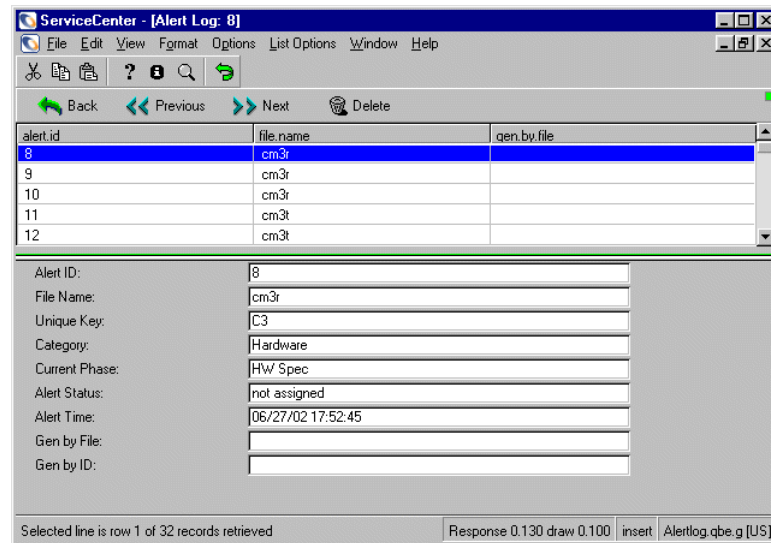


Figure 10-80: Selected record in the Alert Log

The following table describes the fields in the Alert Log.

Field	Description
Alert ID	Unique identification number of this alert.
File Name	Name of the alert file.
Unique Key	Unique key to this record.
Category	The category associated with this alert.
Current Phase	Current phase of this alert.
Alert Status	Status of the alert. Current file referenced by \$L.file .
Alert Time	The date/time the alert condition evaluated to true.
Gen by File	Gen by file items are those items which cause an alert to be required.
Gen by ID	Gen by ID items are those items which cause an alert to be required.

Events

Events are system occurrences triggered by the creation or update of requests for change, such as opening or approving a change. Events can be used to trigger special processing, such as alerts and messages. When these specific activities occur, Change Management sends mail messages to users, as part of the default processing. Other customized routines can be executed for particular events.

Several default events are included with Change Management. Others may be added, according to your business needs (for example, activities or conditions that need to be checked or unique events warranting notification).

When an Alert Condition evaluates to *true*, Change Management treats it as an event, and notifications can then be sent for this alert condition.

Event Controls

- The option for processing messages and events is located on the change or task Phase definition record. For more information, see [Accessing Phase Records](#) on page 386.

The Messages/Events field in the Controls tab sets the controls that define when events are processed for the particular phases named.

- All event names must be defined in the `cm3rmessages` file, or no event processing can occur. For more information, see [Change Management Events File](#) on page 461.
- Events are processed when the phase of the change or task is defined in the Phases field of the `cm3rmessages` file. If the Phase field is NULL on the `ocmevents` record, the event is processed for all phases.

Change Management Events File

This file contains the names and definitions of all valid Change Management events.

To access the event definition form:

- 1 Click **Change Management** on the Services tab of the ServiceCenter Home menu.
- 2 Click **Messages** on the Maintenance tab. A blank Change Management Event Definition form appears.
- 3 Click **Search** to perform a *true* query and display the record list of all currently defined events.
- 4 Select a record to view by clicking on the name of the event. Figure 10-81 shows the selected event record.

ServiceCenter - [Change Mgmt Message]

File Edit View Format Options List Options Window Help

OK Cancel Previous Next Add Save Delete

Events Phases

cm3r approval
cm3r approval mods
cm3r approved

CHANGE MANAGEMENT EVENT DEFINITION

Event: cm3r approval
Description:
Format Name: cm3r.mail.fmt
Event Services Reg.:

Operators

Phases

Message Notification Controls

Input Field Name	Group Member?	Approver?	Append Text
requested by	true		Phase has a new Approval
assigned to	true		Phase has a new Approval - is assigned to you

Selected line is row 1 of 32 records retrieved Response 0.200 draw 0.120 insert cm3messages.g [US]

Figure 10-81: Accessing the ocmevents File

The following table describes the fields on the Change Management Event Definition tab.

Field	Description
Event (<i>required</i>)	Name of the event. Must be unique within each area; quote, order, or line item.
Description	Brief description of the event.
Format Name	Name of the form used to build the message sent to the users. Allows basic information about the record associated with the event to be included in the message; otherwise, the standard message is sent.
Event Services Reg	Defines how the message is sent out through Event Services.
Operators	Login IDs (names) of those operators who should receive a copy of the messages sent via this event.
Phases (change/task)	Control over which events are valid for which phases within each area. If this field is NULL, the event is valid for all phases of the area.

Message Notification Controls

The Message Notification control fields trigger a mail notification and the member lists to be included to receive mail notification.

Field	Description
Input Field Name	The field that triggers a mail notification and defines the recipient of the message. If the recipient is a message group, then the approver or reviewer is used to define designated approvers or members who are to receive the message.
Group Member?	Each operator in the Members array will receive mail notification. Note: Although you can change this field from true to false in the Message Notification Controls area shown in Figure 10-81 on page 461, the cm3r.alert.trigger application that creates alert messages does not evaluate the conditions for the cm3r update record recipients.

Field	Description
Approver?	Each operator in the Approvers array will receive mail notification.
Append Text	<p>The character string added to the generic message that is sent as the first line of the message. The message syntax is:</p> <p><i>event type</i> Notice: <i>cm3r/cm3t number append/text (date)</i> by <i>operator</i></p> <p>For example: cm3r open Notice: cm3r C19 You are the Coordinator for this Change(08/09/2002 14:56) by FALCON, JENNIFER</p>

Event Names and Definitions

Change Management includes several predefined system events, such as cm3r approved and cm3r closed. You can define additional events, as needed. See the *System Tailoring Guide* to learn more about the predefined system events.

Defining Additional Events

A new event can be defined and called by Format Control calculations, in the case that a specific condition must be checked for the event to occur at specialized times.

The following must occur in order for a message to be processed.

- The record must exit.
- The message flag in the phase definition record (cm3rcatphase/cm3tcatphase) must evaluate to true.
- The operators and field names must be valid message groups, contacts, or operators.

The event must either be an alert definition (**AlertDef**) or a message (**cm3messages**). The event syntax generally used to check for an event is as follows:

```
if (condition=true) then ($cm3messages file.$events.pntr in $cm3messages ="event name";$cm3messages file.$events.pntr+=1)
```

- The variable `$cm3messages` is an array of character strings used to track the events that occur during a particular phase of processing.
- The variable `$cm3messages.events.pntr` is a pointer to the next array element that can be used to record an event name.

Important: Once an event has been added to the array, it is important to increment the pointer by *1* (one). If this does not happen, the event previously recorded will be overwritten.

The event that is scheduled if the condition is *true* must be defined in the `cm3rmessages` file.

Adding New Events

The following steps are required for adding new events to the system:

- 1 Activate the Change Management background processor (`cm3r`). For more information, see *Background Processing* on page 467.
- 2 Activate the Change Management (`cm3r`) alerts schedule record. For more information, see *Background Processing* on page 467.
- 3 Set the environment record. For more information, see *Environment* on page 357.
- 4 Define the **Messages/Events** option for the phase. For more information, see *Accessing Phase Records* on page 386.
- 5 Set any RAD or Format Control definition to track a custom event. For more information, see *Event Controls* on page 460 and the *ServiceCenter System Tailoring Guides*.
- 6 Define the operator groups in the `cm3rmessages` record in the `cm3rgroups` file.
- 7 Define the appropriate operator records.
- 8 Define the event in the `cm3rmessages` file.
- 9 Define the **Format Name** in the format file.
- 10 Validate the Message Notification Controls.

Messages

Messages are sent in response to an event. They can be directed to specific operators listed in the *event* record and contain values from certain fields in quote, order, and line item records, which cause the initial event.

Change Management message processing involves:

- The background processor looking at the **cm3roptions** record for the phase or category that generated the event. If the record does not exist, processing ends.
- Evaluation of the Messages/Events option in the **cm3roptions** record. If *false*, processing ends.
- Checking for Field Name and Operators in the **cm3rmessages** record. If none, processing ends.
- Recording in the **msglog** the generic message (from the **cm3rmessages** record Append Text field).
- Sending the standard message and the mail message to the operators defined in the Operators field of the **cm3rmessages** record.
- Sending a message to the operators defined in those fields referenced by the Field Name field of the **cm3rmessages** record.

The content of these fields is first assumed to be a group. If this group name is found in the **cm3rgroups** file, then either the Members or Approvers (depending on the Member List field) of that group are added to a working list.

If this group name does not exist, the system searches the **operator** file; and if an operator record is found, it is added to the working list.

- Checking the working list for operators, and sending the message.

Message Classes

ServiceCenter has several default message classes where a user can define additional messages to display in Change Management.

To display the list of available classes:

- 1 Click **Administration** on the **Utilities** tab of the ServiceCenter home menu.
- 2 Select the **Notifications** tab in the **Administration** menu.

The Message Classes structure contains the buttons for the various message classes. The buttons displayed are: On-Screen (msg), Print (print), Log (log), TSO (TSO), External E-Mail (email) and Internal E-Mail (email). These represent the possible action types for message classes.

Message Button	Description
On Screen	Send a message to the user's screen.
Print	Send a copy of the message to the receiver's default printer.
Log	Send a copy of the message to the msglog file.
TSO	Send a copy of the message to the receiver's TSO ID.
External E-Mail	Send a copy of the message to the receiver's e-mail address as specified in the operator or contacts record.
Internal E-Mail	Send a copy of the message to the receiver's internal ServiceCenter mailbox.

A message class record may be entered into multiple message class types.

To view a Message Class record:

- 1 Click **Administration** on the *Utilities* tab in the ServiceCenter Home menu.
- 2 Select the Notifications tab of the Administration menu.
- 3 Click **Log** in the Message Classes structure.
- 4 Enter a Class Name, or click **Search** to pass a *true* query and display a current class list.
- 5 Select a record to view from the list, which displays by clicking on the name.
- 6 View the desired record. Each class message presents a different form associated with the **msgclass.log** file.

Adding msgclass Records

- 1 Click **Administration** on the *Utilities* tab. of the ServiceCenter Home menu.
- 2 Select the **Notifications** tab of the **Administration** menu.
- 3 Select an action type from the Message Classes area. For more information, see *Message Classes* on page 465. A blank Message Class File record appears.
- 4 Do one of the following:
 - Begin entering the message name and data.

- Call up the message record, select an existing class record on which to base your new record. Make appropriate modifications, including a name change.
- 5 Click **Add** to confirm the new record, as shown in Figure 10-82.

The screenshot shows a window titled "ServiceCenter - [msgclass]". The menu bar includes File, Edit, View, Format, Options, List Options, Window, and Help. The toolbar contains icons for Cut, Copy, Paste, Help, Find, and Undo. Below the toolbar are buttons for OK, Cancel, Add, Save, and Delete. The main area is titled "MESSAGE CLASS FILE" and contains the following fields:

Class Name	Type
sample message quote 01	msg

Below the table, the form fields are as follows:

- Class Name:** sample message quote 01
- Description:** This is a sample message to be sent when a quote is issued.
- Type:** msg
- Default Message Level:** 1
- ALWAYS send to THESE users (true/false):** (empty checkbox)
- User Names:** (five empty text input fields)

The status bar at the bottom shows "msgclass record added." and "insert msgclass.msg.g(db.view) [P]"

Figure 10-82: Sample message in Message Class file

Background Processing

A great deal of the processing which enables the alerts and updating in Change Management occurs in the background. The following figure demonstrates the general event processing flow of the module.

Figure 10-83 shows a typical event processing task.

Request Management Event Processing

runtime

- 1) User/System does something/something happens.
- 2) Events list is appended with an action (something the system must now do) on open or reset.
- 3) End of user/system process.
- 4) Schedule the event process -- schedule the daemon.

background

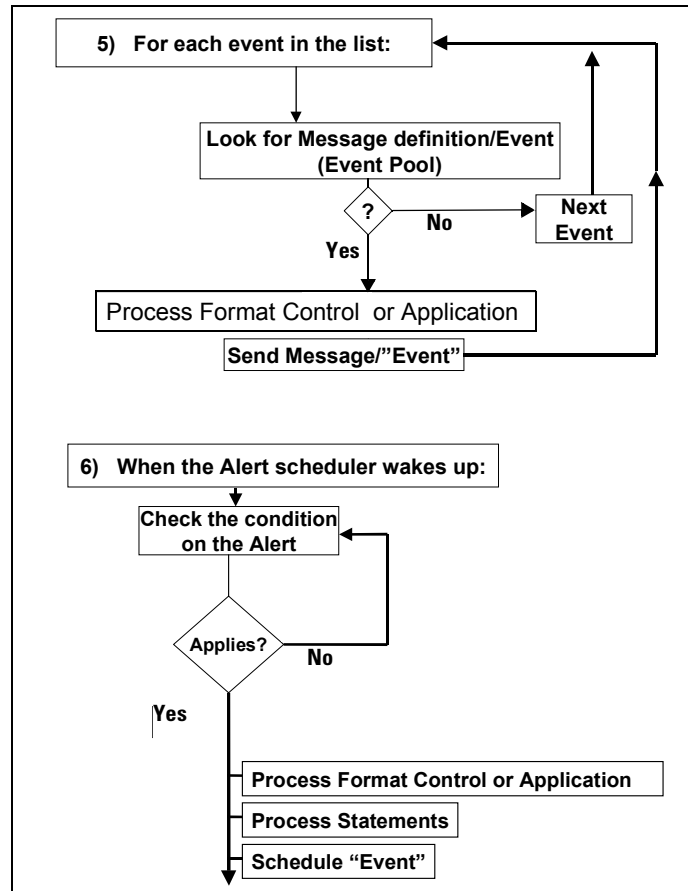


Figure 10-83: Request Management Event Processing

The background processor for Change Management event processing is named *change*. This processor only handles schedule records with a class of *change*. By default, the processor checks for new records every 60 seconds.

Viewing the Processor

- 1 Click **Maintenance** on the **Utilities** tab in the ServiceCenter Home menu.

- 2 Click **Startup Information** in the System tab.

The blank *info.startup* record form displays.

- 3 Type *change.startup* in the **Type** field, and then press **Enter** or click **Search** to do a narrow search for the *change.startup* record type.

Figure 10-84 shows the *change.startup* record displays in the *info.startup* form. This is the default start-up record for the Change Management background processor.

The screenshot shows the ServiceCenter - [Information] window. The menu bar includes File, Edit, View, Format, Options, List Options, Window, and Help. The toolbar contains icons for OK, Cancel, Add, Save, and Delete. Below the toolbar is a table with two columns: Name and Description. The first row is highlighted in blue and contains the text 'change.startup' and 'CM alert/notification processor'. Below the table is the 'Agent Initialization Registry' section. It contains two text boxes: 'Type:' with the value 'change.startup' and 'Description:' with the value 'CM alert/notification processor'. Below these is the 'Agent Information' section. It contains two sets of fields. The first set has a 'Name:' field with the value 'change', a 'Suppress Restart?' checkbox, a 'RAD Application:' dropdown menu with the value 'scheduler', a 'Class:' dropdown menu with the value 'change', a 'Wakeup Interval (secs.):' text box with the value '60', and a 'Priority:' text box with the value '0'. The second set of fields is empty. At the bottom of the window, there is a status bar that reads 'Selected line is row 1 of 1 records' and 'Response 0.431 draw 0.220 insert info.qbe.g [US]'.

Figure 10-84: Change Management Startup Agent Record

- 4 The Change Management background processor should be defined as an agent on the default system start-up record (*startup*).

The system startup default record lists the background agents, or processors, that start up each time ServiceCenter is started. Most are set for 60-second wake-up intervals. This list includes despooler, report, alert (for Incident Management), change, availability, agent, marquee, lister, linker, event, and scautod.

- 5 To add any of the remaining start-up records to the system startup record, enter the start-up record's information at the bottom of the system start-up record's agent array.

This system startup default record processes records that are in the **schedule** file. The appropriate background agent picks up the schedule record and processes it.

Note: Enter **sch** on a command line at any time to display the **schedule** file.

Notifications

The Notification Engine is primarily responsible for sending messages that are generated by ServiceCenter events, such as opening or closing a change or task. Administrators can edit these messages, add new messages, change the conditions that trigger the messages, and select who will receive the messages.

The **notification** file works with the **message** file to define notifications for common system events. Administrators can modify the notification arguments that trigger the notification, as well as define who receives the notification.

To open the notifications file:

- 1 Click **Administration** in the **Utilities** tab in the ServiceCenter main window.
- 2 Click **Notifications** in the **Notifications** tab.

The *notification* form displays.

- 3 Enter the Notification Definition name in the **Name** field and press **Enter** or perform a *true* query by clicking **Search** to see a list of all notification records on your system.

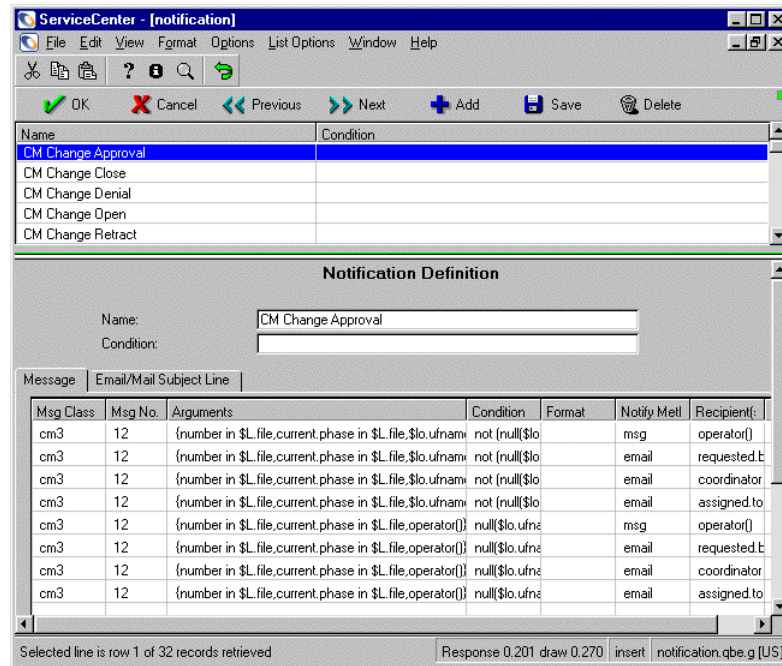


Figure 10-85: Notification definitions

To learn more about notification records and their definitions, see the *System Tailoring Guide, Notification Records*. The following table describes the fields on the Message tab.

Field	Description
Msg Class	Message class relates to the module area. For example: ocm.
Msg No	Message number corresponds to the <code>scmessage.qbe.g</code> file. The Message Class, Message Number, and language fields make up the unique key for this notification. If you add your own message to the message file, the combination of the Msg Class, Msg No and Language fields must not exist in the system already.

Field	Description
Arguments	Message arguments can range from none to many. The arguments correspond to the %S in the message text. If there is only one argument, enter the value directly. List multiple arguments in an array. For example ({<arg1>,<arg2>, <and so on>}). Elements of the array can be string literals or expressions. To reference a value in a record, enter: fieldname in \$L.file. Strings must be enclosed in double quotes.
Condition	Enter the condition under which the message should be sent. Values can be <i>True</i> , <i>False</i> , or an expression that evaluates to either <i>True</i> or <i>False</i> . The default value is <i>True</i> .
Notify Method	Specifies the how the message is sent (for example fax, email, etc.). This field can also specify the name of a message class.
Recipients	Specifies to whom the message should be sent. Enter an expression or string literal that references an individual user or group name.
The following fields are necessary only if the Recipients field contains a group name.	
Group File	Enter the file that the group name is referencing. Use this field with the files ocmggroups , which allow multiple records to be created with the same group name.
Group Area	Acceptable values for use with the ocmggroups file are: All, Quotes, Line Items, and Orders.
Subgroup	The Subgroup field further specifies the user list. Values are: Members/Reviewers, Approvers and All.

A

APPENDIX

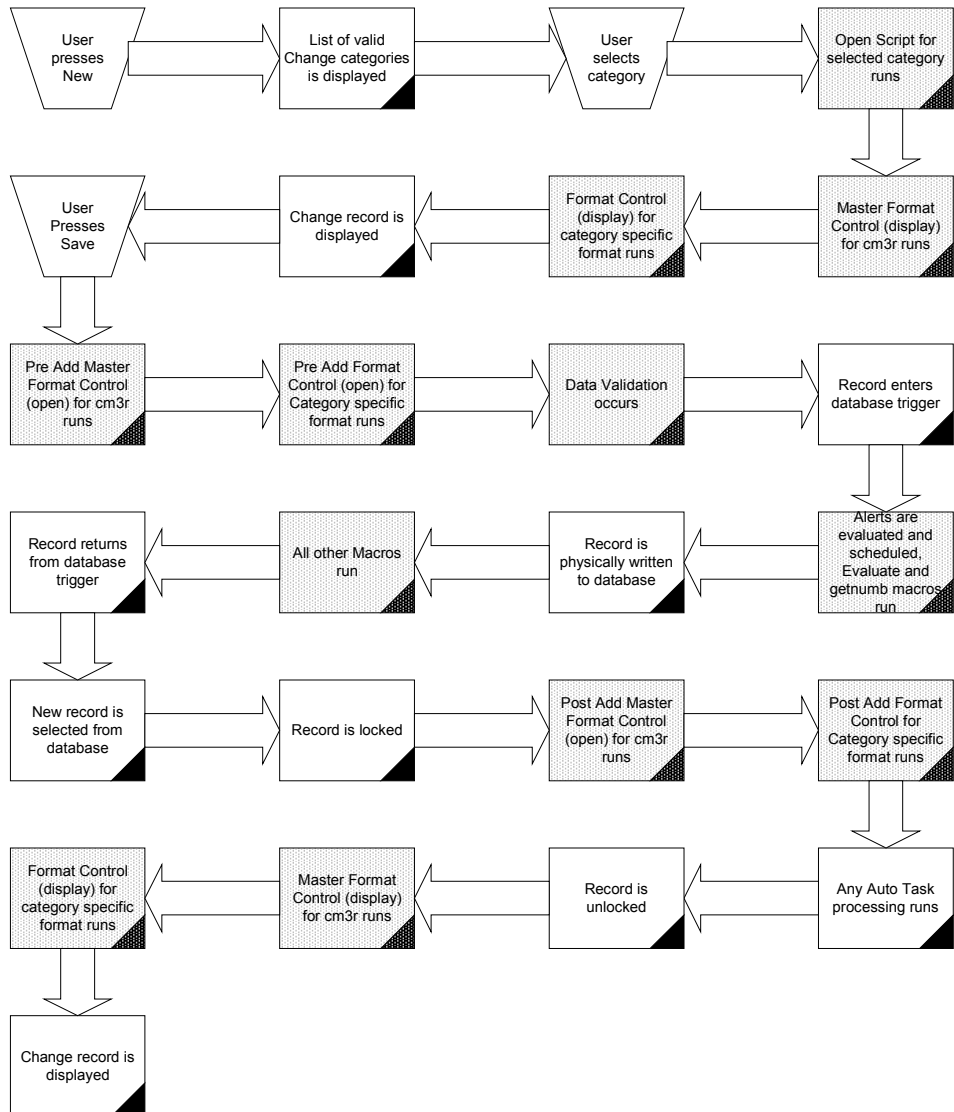
Process Flow Diagrams

This chapter shows the process flow of some user-initiated Change, Incident, Service, and Inventory Management Functions:

- *Change Management Open* on page 474
- *Change Management Update* on page 475
- *Change Management Approval* on page 476
- *Change Management Denial* on page 477
- *Change Management Close* on page 478
- *Change Management Reopen* on page 479
- *Change Management Retract* on page 480
- *Incident Management Open* on page 481
- *Incident Management Update* on page 482
- *Incident Management Close* on page 483
- *Service Management Quick-Open* on page 484
- *Service Management Create Incident* on page 485
- *Service Management Update* on page 486
- *Service Management Close* on page 487
- *Inventory Management Open* on page 488
- *Inventory Management Update* on page 489
- *Inventory Management Delete* on page 490

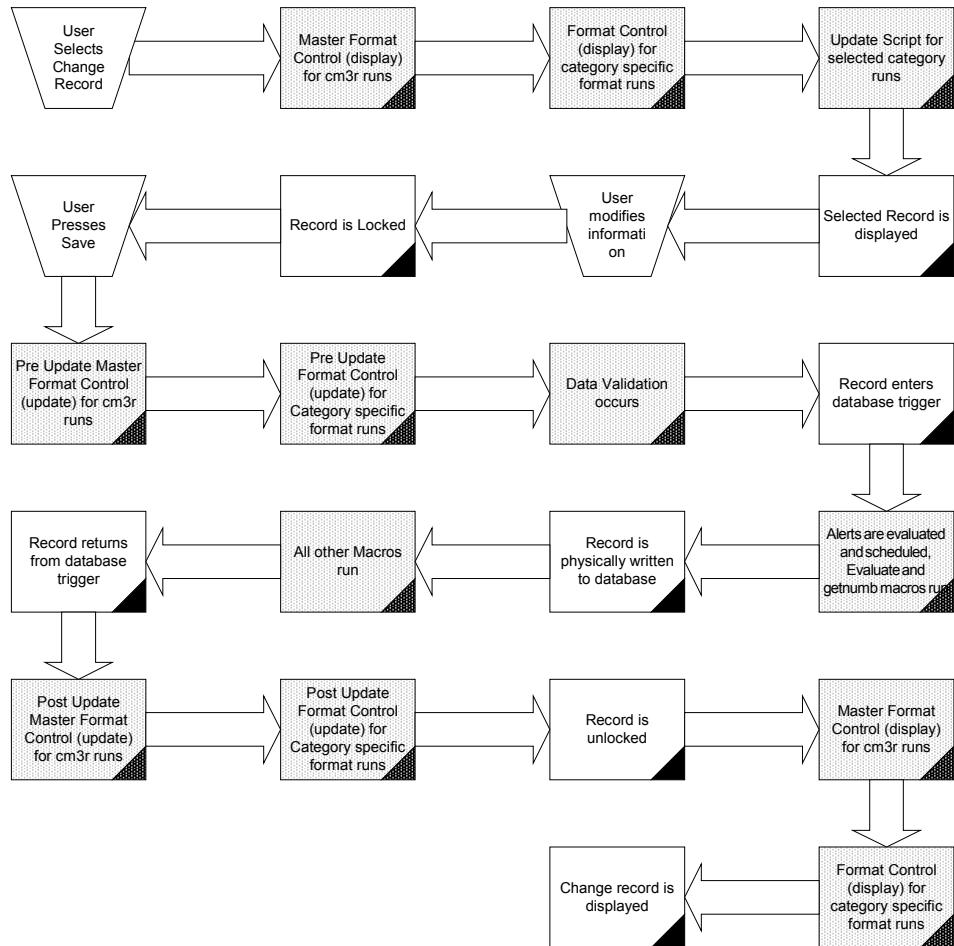
For more information, see the chapters in this guide and the *ServiceCenter System Administrator's Guide*.

Change Management Open



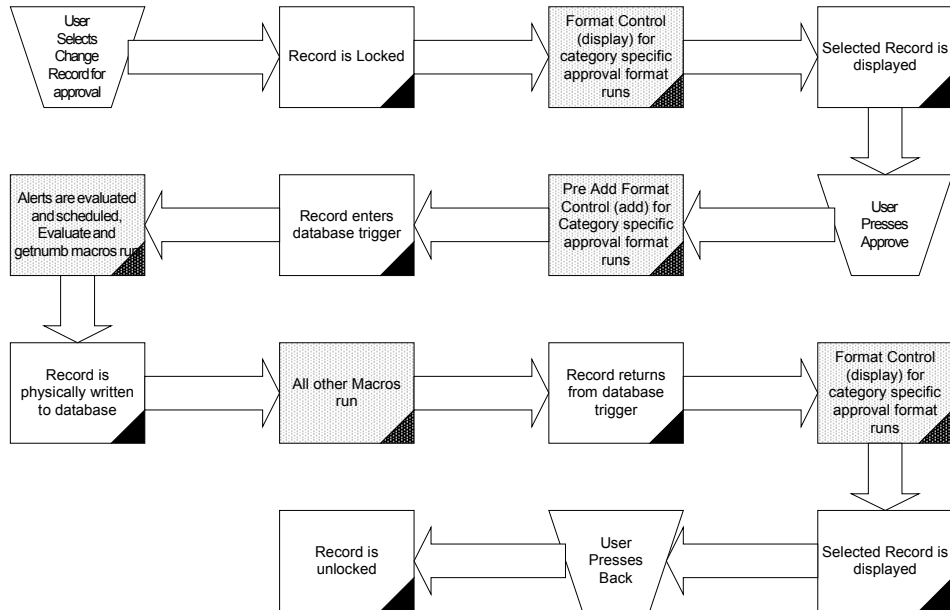
Change Management Update

Change Management Update Data Flow



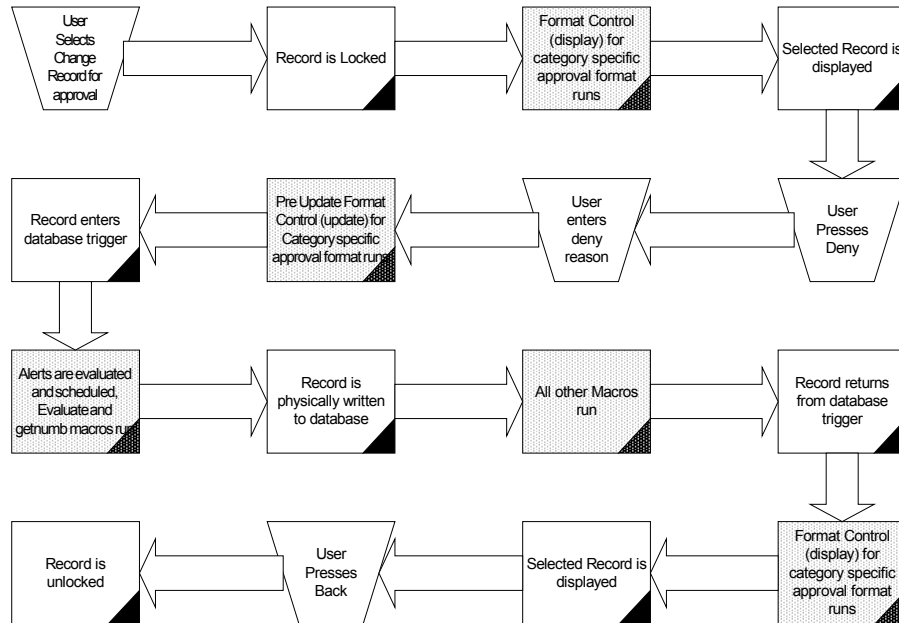
Change Management Approval

Change Management Approval Data Flow



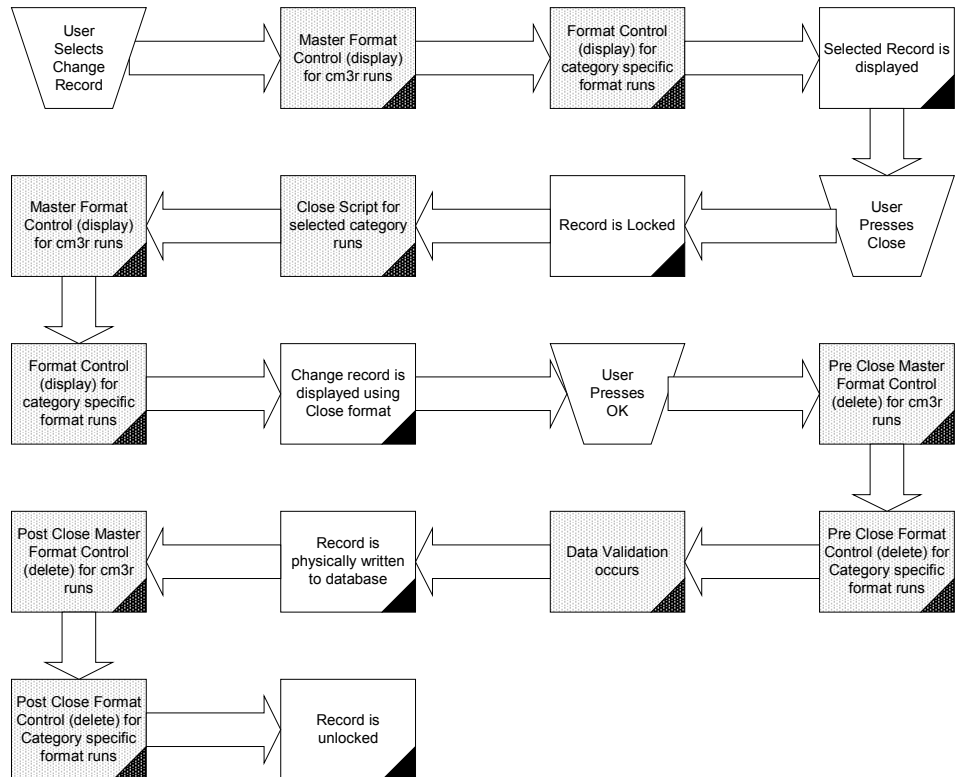
Change Management Denial

Change Management Denial Data Flow



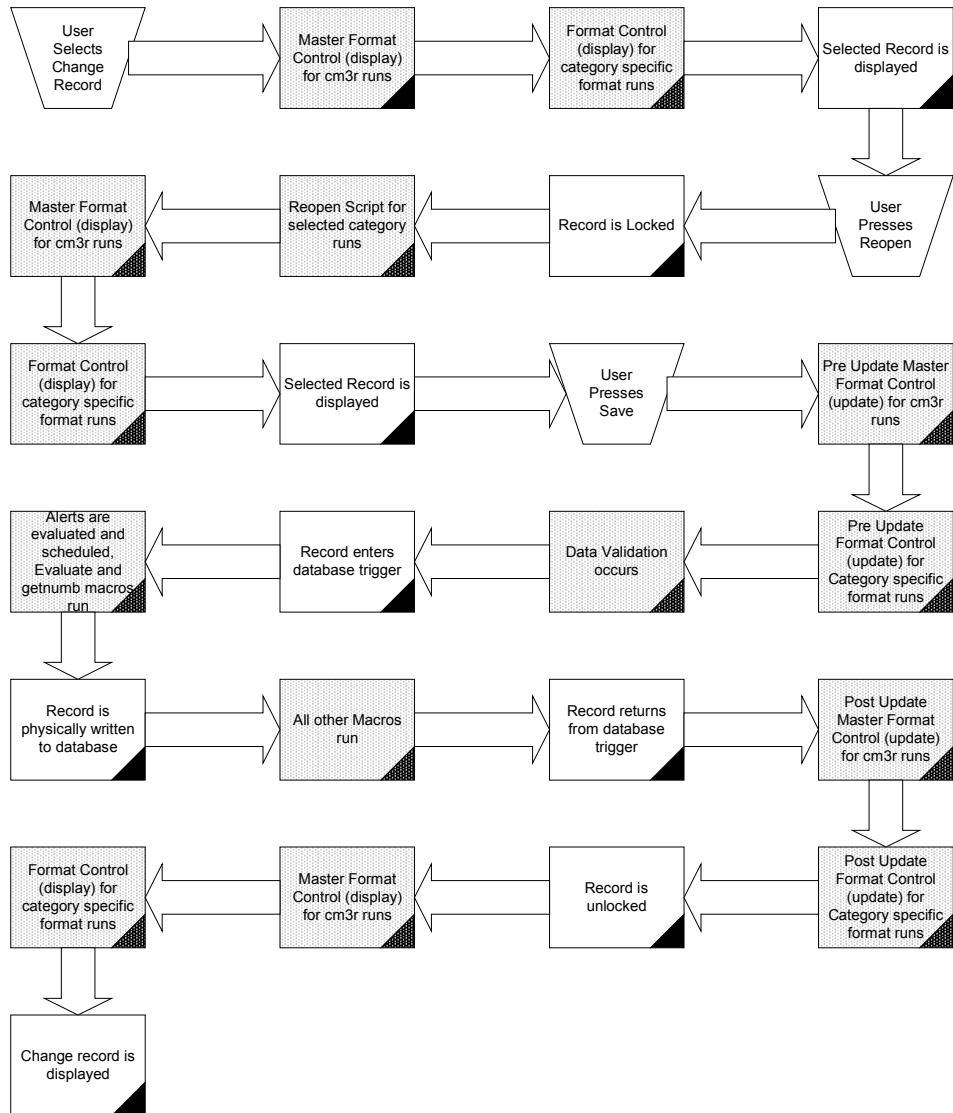
Change Management Close

Change Management Close Data Flow



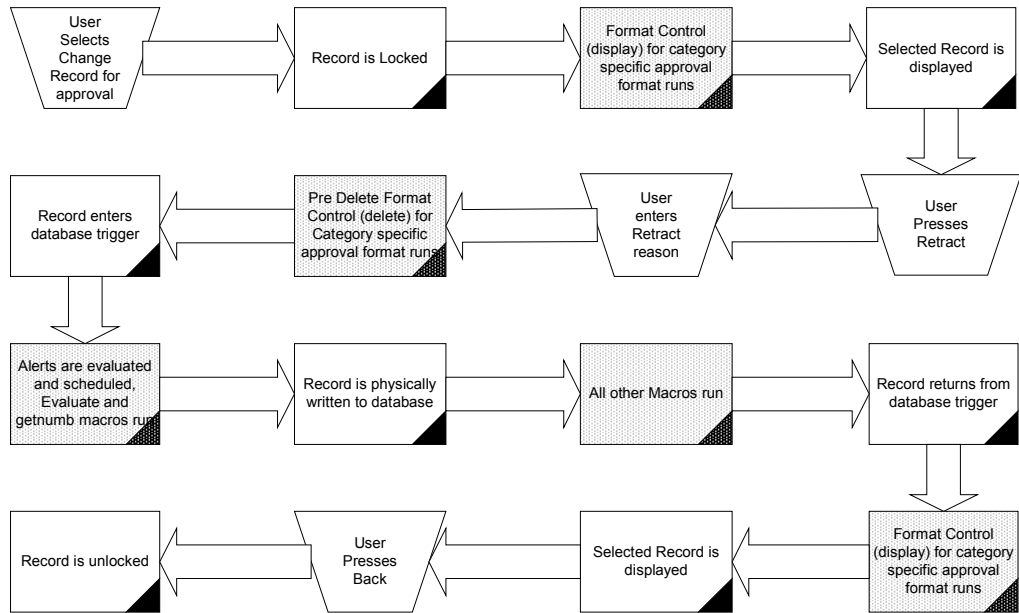
Change Management Reopen

Change Management Reopen Data Flow



Change Management Retract

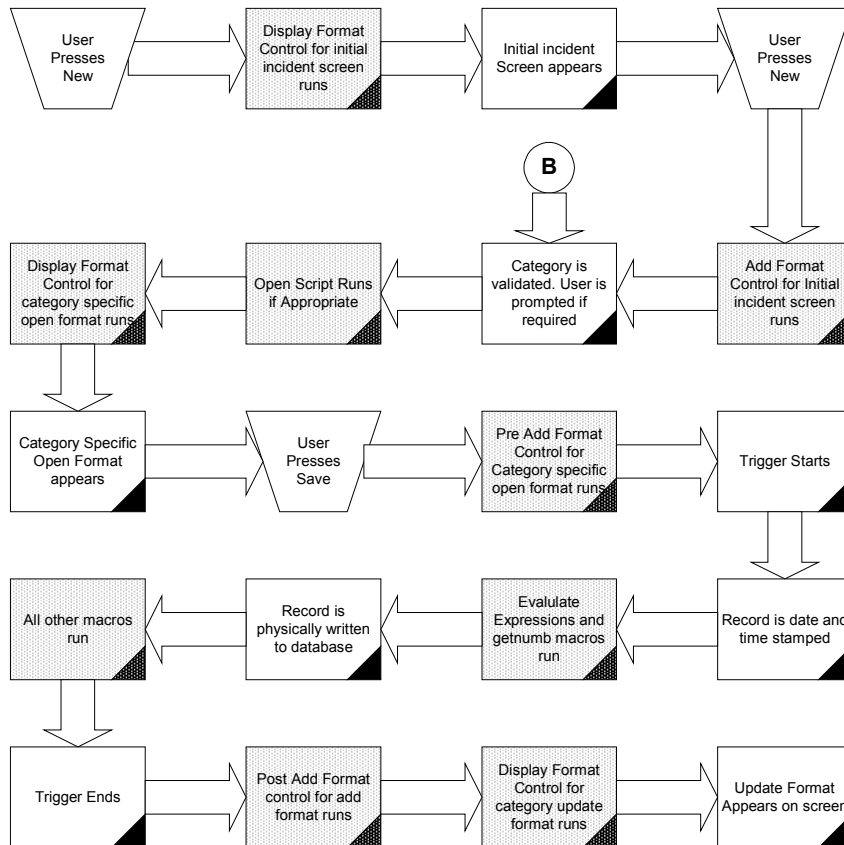
Change Management Retract Data Flow



Incident Management Open

Connector B is from data in *Service Management Create Incident* on page 485.

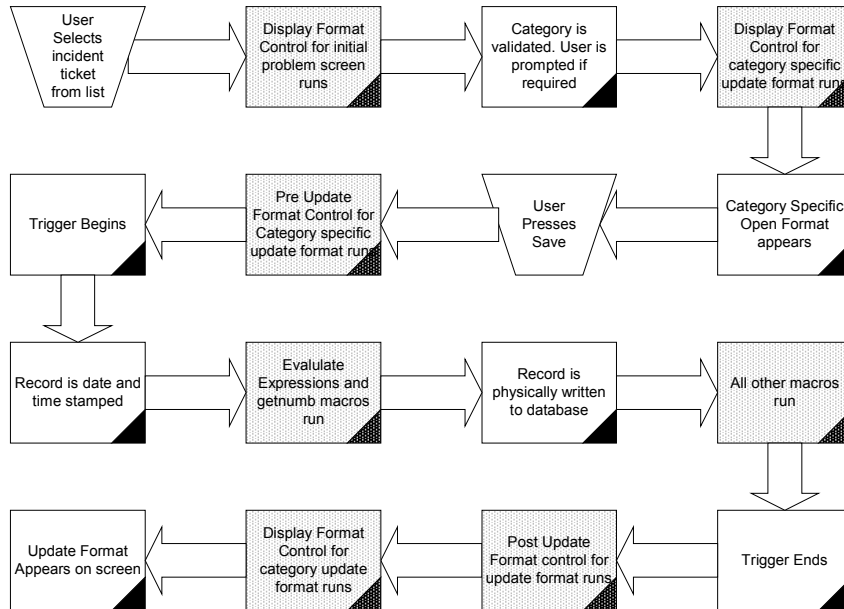
Incident Management Open Data Flow



B - From Service Management Create Incident Data Flow

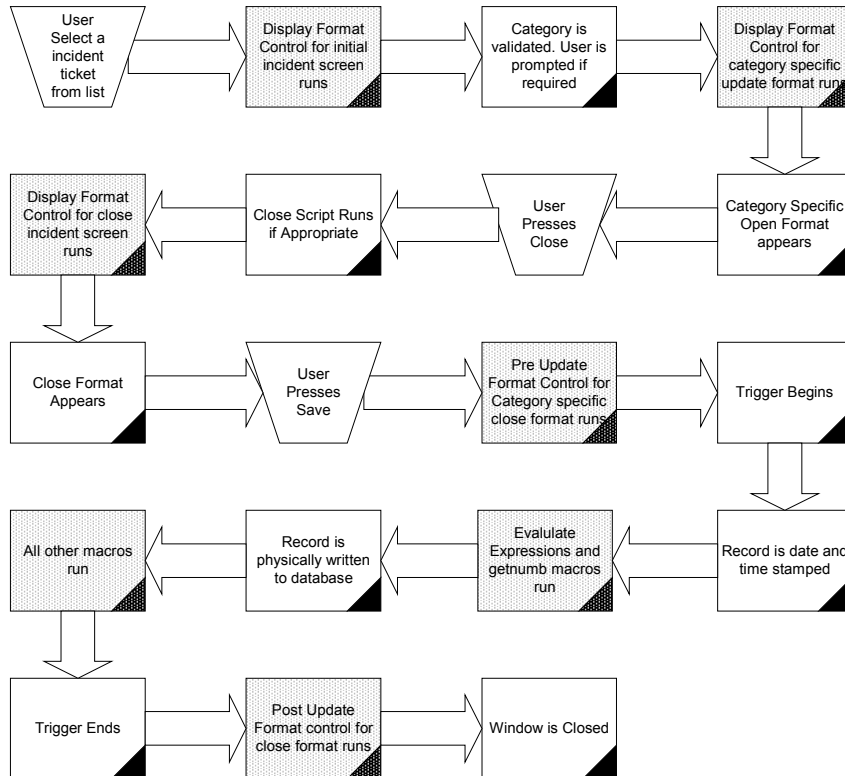
Incident Management Update

Incident Management Update Data Flow



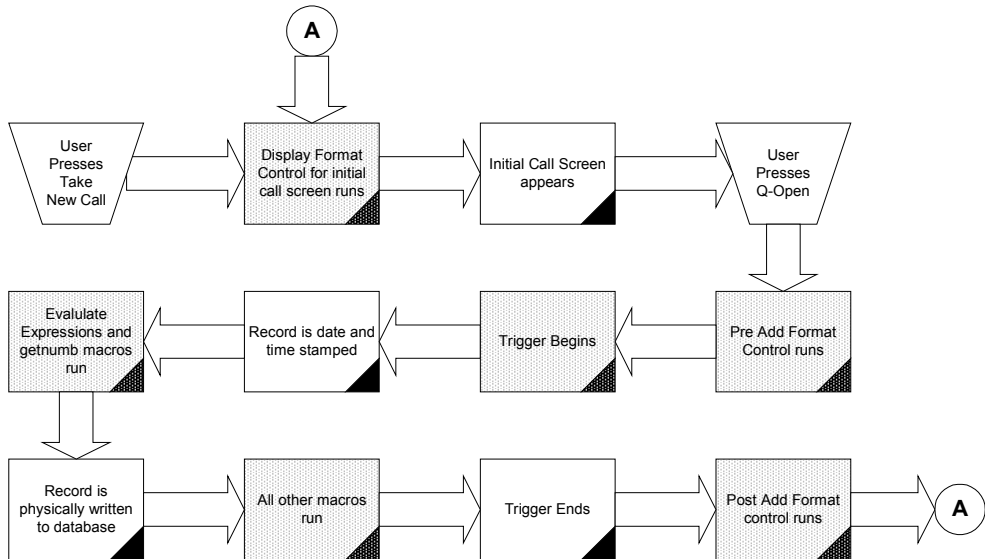
Incident Management Close

Incident Management Close Data Flow



Service Management Quick-Open

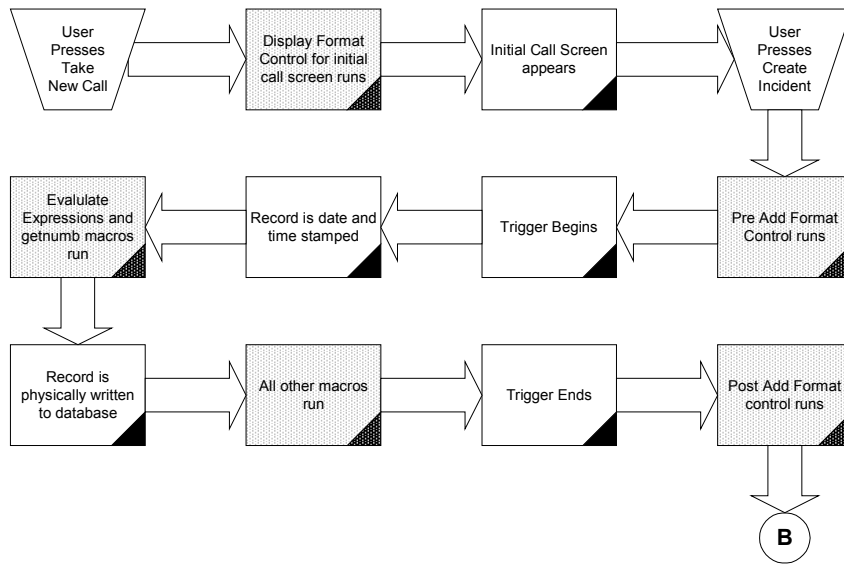
Service Management Quick-Open Data Flow



Service Management Create Incident

Connector B goes to Incident Management Open Data. For more information, see [Incident Management Open](#) on page 481.

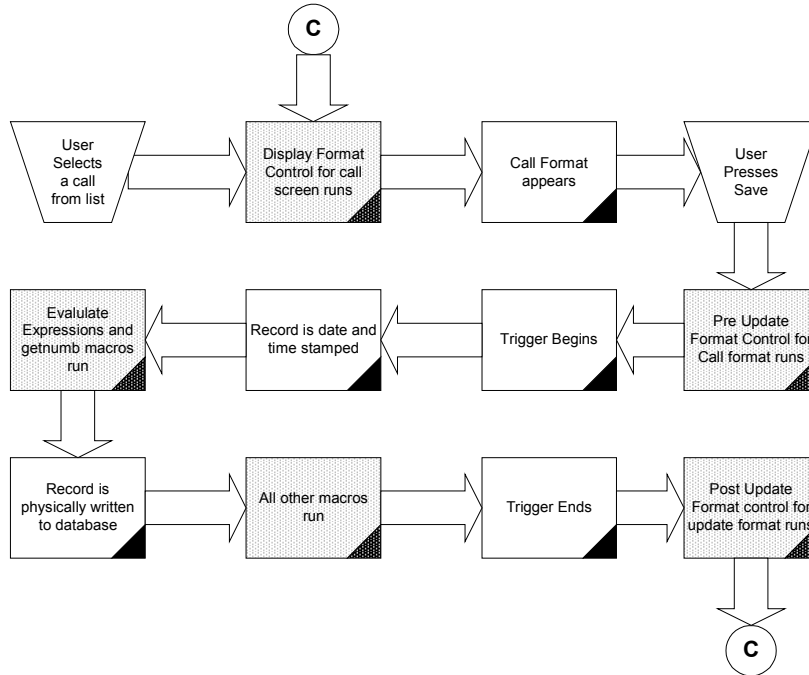
Service Management Create Incident Data Flow



B - To Incident Management Open Data Flow

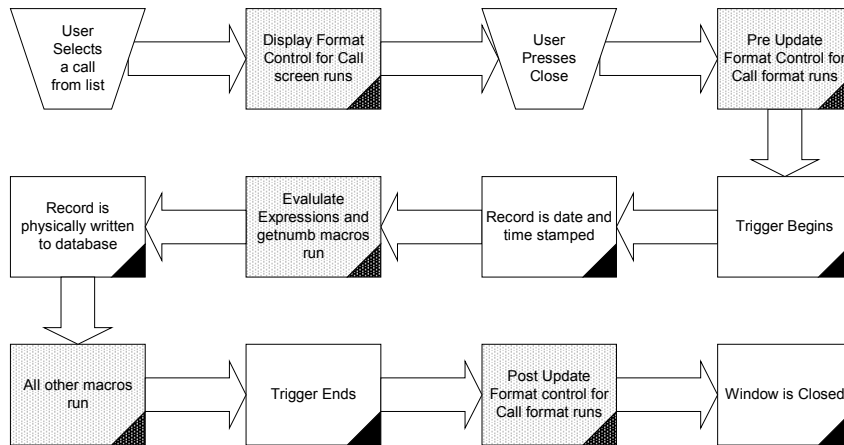
Service Management Update

Service Management Update Data Flow



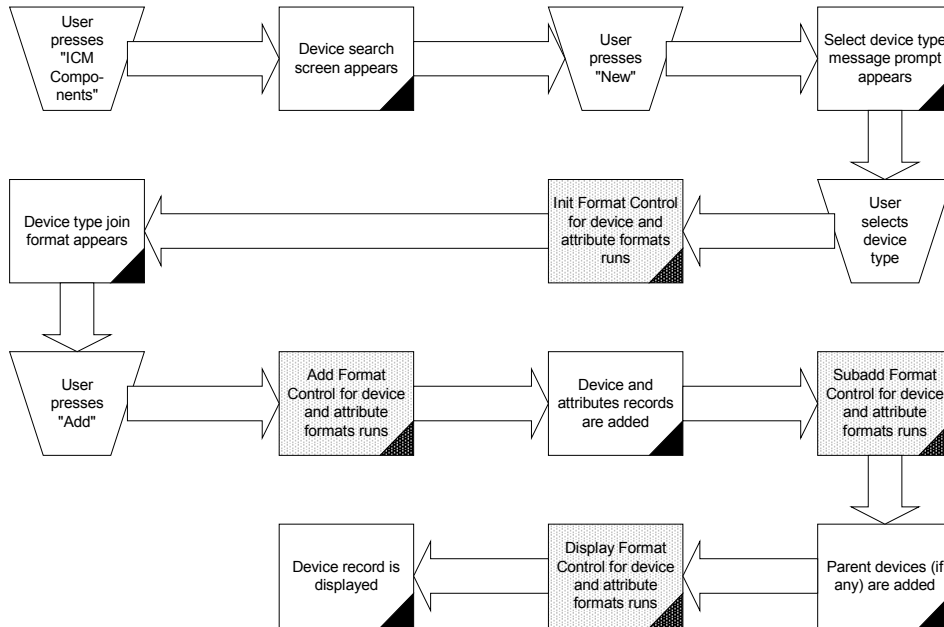
Service Management Close

Service Management Close Data Flow



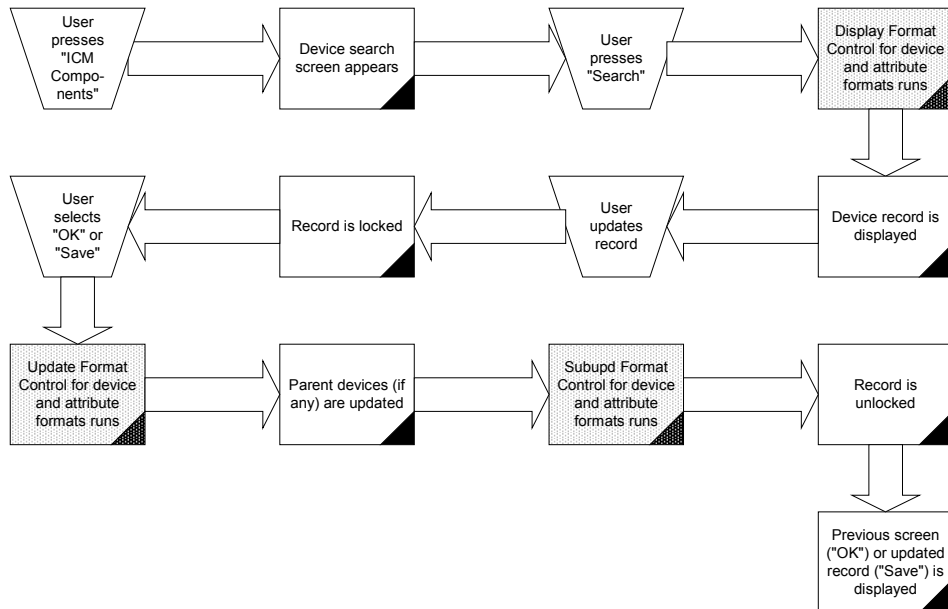
Inventory Management Open

Inventory Management Open Data Flow



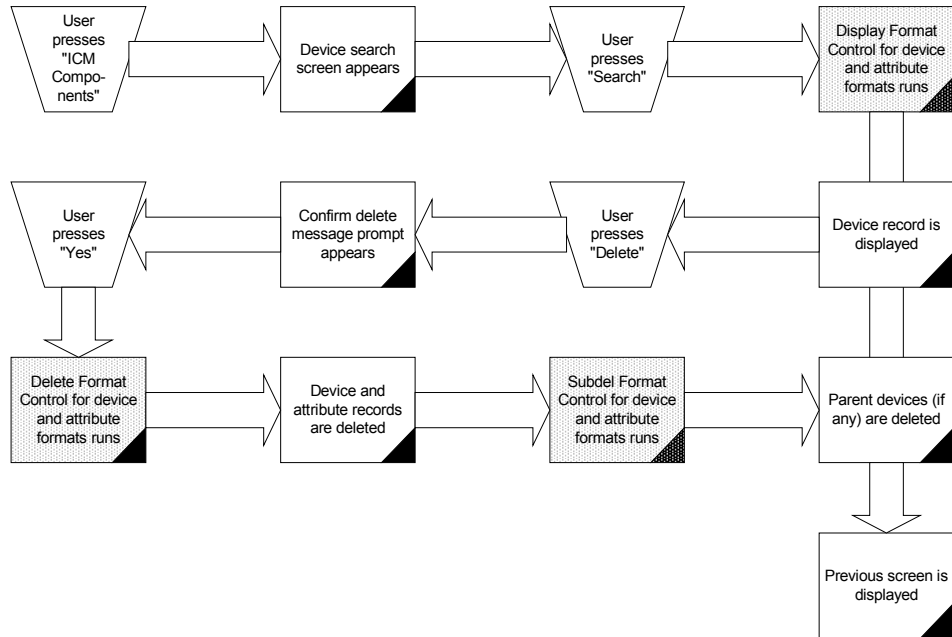
Inventory Management Update

Inventory Management Update Data Flow



Inventory Management Delete

Inventory Management Delete Data Flow



B Field-Level Details

APPENDIX

Overview

The information in this appendix described the out-of-box fields for Service and Incident Management. The following table describes the column headings on the subsequent tables and what they mean.

Column header	Purpose
Field Label	Physical label of the field.
Input Field	Input field as it is defined in the database dictionary (dbdict).
Description	Defines the purpose of the field and any other useful information.
Source	Defines where the field information is derived from. The source can be system-generated, system files, or user input.
Type	Defines the type of field information. The type can be Character, Array, Date/Time, Number, or logical.
Field Characteristics	Describes whether the field is required or optional, protected, combo-box, fill, find, or a check box.

Table 1: New call — Call Detail tab (cc.incquick.g)

The following table describes fields on the Call Detail tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Call ID	A unique identifier for each incident record	incident.id	system generated per numbers file	Character	Protected
Contact Name	Contact name related to the company from which the call was received	contact.name	User Input or contacts file	Character	Required; find; fill
Full Name	Contact's full name	contact.name	contacts file	Character	Protected
Email	Email address of the contact.	contact.name	contacts file	Character	Protected
Payroll No.	Contact's unique payroll id number	contact.name	contacts file	Character	Protected
Corp Struct/Div	A single field that unites both the company and department for this contact.	corp.structure	company/ dept	Character	Optional; find; fill
Phone	Contact's phone number; automatically filled from the contacts record for the caller.	phone	Contacts file	Character	Optional
Ext.	Contact's phone extension; automatically filled from the contacts record for the caller	extension	Contacts file	Character	Optional

Field Label	Description	Input Field	Source	Type	Field Characteristics
Fax	Contact's fax number automatically filled from the contacts record for the caller;	fax	Contacts file	Character	Optional
Reported by Different from Contact Name	Check this box if the name of the caller is different from the contact name in Contacts file.	different.from.contact	User input	Character	Optional
Reported By	Reported by, phone, fax and ext. are fields that display when the Reported by different from Contact Name? box is checked. Enter the caller's contact information.	alternate.contact	contacts file; User input	Character	Optional; fill
Phone/Extension	Phone and/or extension of the contact.	contact.phone extension	contacts file	Character	protected
Location	Office location from where the call originated	location.full.name	company; location files	Character	Optional; fill
Room/Floor Ref	Room/floor references where the asset is located	room	User input	Character	Optional
Cost Center	Cost/Financial Center of the contract	cost.centre	User Input	Character	Optional
User Type	The type of user calling; options are Site, Home, or Mobile.	user.type	User Input	Character	Optional; combo box

Field Label	Description	Input Field	Source	Type	Field Characteristics
Company	Name of company calling to report the incident	company	company file	Character	Optional; Fill
Description	A detailed description of the incident	description	User Input	Array Character	Required
Status	State of the call report: Closed, Open-Idle, or Open-Callback	open	System Generated	Character	Protected; System Generated
Owner	Name of SM operator who opened the call report	owner.name	System Generated from Login	Character	Protected; System Generated from login
Category	Classification of the asset's category within the business, such as network.	category	category file	Character	Required; fill
Subcategory	Classification of the asset's subcategory within the primary category, such as lan.	subcategory	cm3.rsubcat/ subcategory files	Character	Required; fill
Product Type	Device product type	product.type	cms.sla/ product.type	Character	Required; fill
Problem Type	Type of problem being reported.	problem.type	problem.type	Character	Required; fill
Assignment	Assignment group to review the call.	assignment,1	assignment	Character	Required; Combo-box
Severity	Indicates how pressing an incident is for the caller. Can be Critical, Major, Medium, Low, Very Low.	severity	User Input	Character	Required; Combo-box

Field Label	Description	Input Field	Source	Type	Field Characteristics
Total Loss of Service	Indicates severity and priority.	total.loss	User Input	Logical	Check-box
Site Category	Indicates the level of support to be dispersed.	site.category	User Input	Character	Required; Combo-box
Projected SLA	Service Level Agreement covering the affected equipment.	agreement.id	User Input	Number	Protected
Entitlement	Non-editable field. System automatically checks to determine if the caller, based upon the SLA, has the right to help desk service at the current date/time.	entitlement.ref	System Generated	Character	Protected
Notify By	How the caller is to be notified when the call report is closed; can be None, Email, or Telephone	callback.type	User Input	Character	Combo-box
GL Number	Global Ledger Number	gl.number	User Input	Character	Optional
Bill To	To where the bill should be mailed	billto	dept/contact s files	Character	Radio button; Optional; Fill
Asset ID	The identification number of the asset affected by the incident	affected.item	device file	Character	Optional; find; fill
Type	Field automatically filled in from device record of the asset	affected.item	device file	Character	Protected

Field Label	Description	Input Field	Source	Type	Field Characteristics
Critical Asset	Check box to indicate that the asset is critical to normal business operations	affected.item	device file	Logical	Check box
Cause Code	Optional field that links this ticket to a Probable Cause record.	cause.code	probable.cause file	Character	Optional; fill

Table 2: New Call - Resolution Detail Tab (cc.incquick.g)

The following table describes fields on the Resolution Detail tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Call Resolution	Details of the call's resolution	resolution	User Input	Array; Character	Optional
Resolution Code	Code given to the call resolution.	resolution.code	probcause.qbe.g	Character	Optional; Fill

Table 3: Existing call — Update tab (cc.incident.g)

The following table describes fields on the Update tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Call Update:	Description of the update to the call/actions taken.	temp.update	User Input	Array; Character	Optional
Opened By:	Name of person responsible for opening the ticket	opened.by	System-generated	Character	Protected; system-generated
At:	Time at which the ticket was opened.	open.time	System-generated	Date/Time	Protected; system-generated
Updated By:	Name of person responsible for updating the ticket.	updated.by	System-generated	Character	Protected; system-generated
At:	Time at which the ticket was last updated.	update.time	System-generated	Date/Time	Protected; system-generated
Closed By:	Name of person responsible for closing the ticket.	closed.by	System-generated	Character	Protected; system-generated
At:	Time at which the ticket was closed.	close.time	System-generated	Date/Time	Protected; system-generated
GL Number:	Global Ledger Number	gl.number	User input	Character	Optional
Bill to:	Enter Name or Department that is to be billed for the provided service.	billto	User input	Character	Optional; Fill

Field Label	Description	Input Field	Source	Type	Field Characteristics
Bill Type: Department	One of two bill type options to indicate who is to be billed for the service; may select either department or contact.	billtype	dept file	Character	Radio button option
Bill Type: Contact	One of two bill type options to indicate who is to be billed for the service; may select either department or contact.	billtype	contacts file	Character	Radio button option

Table 4: Existing call — Resolution Detail tab
(cc.incident.g)

The following table describes fields on the Resolution Detail tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Resolution Code	Fill function provides a list of similar incidents from which you can choose a resolution. The resolution code and a description of the steps taken to resolve the incident are entered in the incident ticket.	resolution. code	probable.resolution	Character	Optional: Fill
Call Resolution	Text box where you can enter details about the resolution of the incident.	resolution	User Input	Array; Character	Optional

Table 5: New incident — Incident Details tab (apm.quick.g)

The following table describes fields on the Incident Detail tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Ticket Status:	Field changes as the incident progresses through the stages	status	system-generated	Character	Protected; system-generated
Category:	Classifies the Incident ticket. If a default category is already specified, this field will be filled automatically.	category	Category File or User input	Character	Required; fill
Subcategory:	More specific breakdown of the category.	subcategory	Subcategory File or User input	Character	Required; fill
Product Type:	Device product type.	product.type	product.type or User input	Character	Required; fill
Problem Type:	Type of problem being reported.	problem.type	problem.type or User input	Character	Required; fill
Company:	Name of the company from the Company file.	company	companyFile or User input	Character	Optional; fill
Description:	Description of the incident	action	User input	Character	Required
Owner:	ServiceCenter operator opening the ticket. By default, Incident Management automatically enters the name of the user who is currently logged on. Drop-down list allows you to change the ticket owner.	ticket.owner	System Generated from login	Character	Protected; system-generated

Field Label	Description	Input Field	Source	Type	Field Characteristics
Primary Asgn Group:	Group who will be responsible for resolving the incident ticket.	assignment	User input	Character	Optional; combo box
Assignee Name:	Person responsible for solving the problem.	assignee.name	assignment File or User Input	Character	Optional; Fill
Second Asgn Group:	backup assignment group responsible for resolving the incident ticket	secondary.assignment	User Input	Array Character	Optional; Combo-box
Total Loss of Service:	Device has total loss of service.	total.loss	User Input	Logical	Optional; Check-box
Severity:	Indicates how pressing an incident is for the caller. Can be Critical, Major, Medium, Low, or Very Low.	severity.code	User Input	Character	Required; Combo-box
Site Category:	Enter the site category	site.category	User Input	Character	Required; Combo-box
Cause Code:	Defines the probable cause of the incident	cause.code	probable.cause or User Input	Character	Optional; Fill

Table 6: New incident — Actions/Resolutions tab (apm.quick.g)

The following table describes fields on the Actions/Resolution tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Ticket Status:	State of the incident.	problem.status	System Generated	Character	Protected; system-generated
Corrective Actions:	Text box where corrective actions can be entered to show how the incident was resolved.	update.action	User Input	Character	Protected
Candidate for Knowledge Database?	Check this box if the solution would be useful	solution.candidate	User Input	Logical	Protected
Resolution Code:	Provides a list of similar incidents from which you can choose a resolution. Resolution Code.	resolution.code	probable. cause; resolution	Character	Protected
Solution:	A description of the steps taken to resolve the incident are entered in the incident ticket.	resolution	User Input	Array; character	Protected

Table 7: New incident — Contact tab (apm.quick.g)

The following table describes fields on the Contact tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Reported By:	The Contact Name related to the company from which the call was received. Click the Browse button to select a Contact Name from the QBE list of contact names.	contact.name	contacts or user input	Character	Required; fill
Full Name:	Field that is automatically filled in from the contacts record for this caller.	first.name/last.name	contacts or user input	Character	Optional
Phone:	Field that is automatically filled in from the contacts record for this caller.	contact.phone	contacts or user input	Character	Optional
Ext:	Field that is automatically filled in from the contacts record for this caller.	extension	contacts or user input	Character	Optional
Site Name:	Field that is automatically filled in from the contacts record for this caller.	location	location or user input	Character	Optional
Email:	Field that is automatically filled in from the contacts record for this caller.	contact.email	contacts or user input	Character	Optional
Room/Floor Ref:	Field that is automatically filled in from the contacts record for this caller.	room/floor	contacts or user input	Character	Optional
Payroll No.:	Field that is automatically filled in from the contacts record for this caller.	payroll.no	user input	Character	Optional
Cost Center:	Field that is automatically filled in from the contacts record for this caller.	cost.centre	user input	Character	Optional
Critical User:	Field that is automatically filled in from the contacts record for this caller.	critical.user	user input	Character	Optional

Table 8: New incident — Asset tab (apm.quick.g)

The following table describes fields on the Asset tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Affecting Asset:	This field identifies the failing component. It uniquely defines devices in the network, and is linked to the device file in the Inventory/Configuration component of PNMS. If a Logical Name is identified when a problem is opened the device information will be copied to the problem document automatically upon open.	logical.name	device (apm.device.vj)	Character	Optional; fill
Type:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	type	User Input	Character	Optional; fill
Cost Center:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	cost.centre	apm.device.vj	Character	Protected
Serial No.:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	cost.centre	apm.device.vj	Number	Protected

Field Label	Description	Input Field	Source	Type	Field Characteristics
Description:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	cost.centre	apm.device.vj	Character	Protected
Critical Asset:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	cost.centre	apm.device.vj	Number	Protected
Make:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	cost.centre	apm.device.vj	Character	Protected
Model:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	cost.centre	apm.device.vj	Character	Protected
Asset Information:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	logical.name	problem.device.vj	Character	Protected
User:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	logical.name	problem.device.vj	Character	Protected

Field Label	Description	Input Field	Source	Type	Field Characteristics
Install Date:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	logical.name	problem.device.vj	Date/Time	Protected
Maint. Contract:	When you select a Contact Name, information related to the associated Affecting Asset will automatically populate this field.	logical.name	problem.device.vj		Protected

Table 9: Update incident — Incident Details tab (problem.template.update.g)

The following table describes fields on the Incident Details tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Ticket Status:	Current status of the ticket.	problem.status	System Generated	Character	Protected; System Generated
Incident Title:	Title of incident, based on reported incident.	brief.description	User Input	Character	Optional
Alert Status:	Changes as the incident ticket progresses through the stages	status	System Generated	Character	Protected; System Generated
Category:	Classifies the incident ticket.	category	category record; User Input	Character	Protected
Subcategory:	More specific breakdown of the category	subcategory	subcategory record	Character	Required; Fill
Product Type:	Device product type	product.type	product.type record	Character	Required; Fill
Problem Type:	Type of problem being reported.	problem.type	problem.type record	Character	Required; Fill
Manufacturer:	The device manufacturer	vendor	vendor record	Character	Optional; Combo-box
Class:	Related to the Manufacturer; allows the problem to be classified with the type of asset. For example, Manufacturer = Dell, Class = Laptop.	class	class record	Character	Required; Fill

Field Label	Description	Input Field	Source	Type	Field Characteristics
Contact Time:	Time at which the technician starts to work on a solution for the incident.	contact.time	System Generated	Date/Time	Optional; Fill
Elapsed Time:	Amount of time that has passed since the incident ticket was opened.	\$elapsedtime	System Generated	Number	Protected; System Generated
Contract:	Contract covering the affected equipment	contract.id	servicecontract record	Number	Protected
Company:	Name of the company from the company file.	company	company record; User Input	Character	Protected
Contact:	Person to contact about the incident	contact.name	contacts record	Character	Protected
Owner:	Incident Management operator who is responsible for resolving the ticket.	ticket.owner	System Generated	Character	Protected; System Generated from Login
Primary Asgn Group:	The primary assignment group responsible for resolving the ticket.	assignment	User Input	Character	Optional; Combo-box
Assignee Name:	Person responsible for resolving the problem	assignee.name	assignment record; operator record	Character	Optional; Fill
Second Asgn Group:	Backup assignment group responsible for the ticket.	secondary.assignment, 1	User Input	Array; Character	Optional; Combo-box
Hot ticket:	Flags a ticket	hot.tic	User Input	Logical	Optional; Check-box
Total Loss of Service:	Device has total loss of service	total.loss	User Input	Logical	Optional; Check-box
Severity:	Indicates how pressing an incident is for the caller	severity.code	User Input	Character	Required; Combo-box

Table 9: Update incident — Incident Details tab (problem.template.update.g) ◀ 509

Field Label	Description	Input Field	Source	Type	Field Characteristics
User Priority:	Indicates the priority of the ticket; can be Critical, Major, Medium, Low, Very Low.	user.priority	User Input	Character	Optional; Combo-box
Site Category:	Defines the type of site the user is calling from, and indicates the level of support to be dispersed	site.category	User Input	Character	Required; Combo-box
Cause Code:	Defines the probable cause of the incident	cause.code	probable cause record	Character	Protected
Site:	Name/ID of the site	site	User Input	Character	Optional
Phone/Extension:	Phone and/or extension of the contact.	contact.phone extension	contacts file	Character	protected
Incident Description:	Description of the incident details	action	User Input	Character	Required

Table 10: Update incident — Activities tab/Site Visit tab (problem.template.update.g)

The following table describes fields on the Activities and Site Visit tabs.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Date of visit:	Date the technician visited the site.	site.visit.date	User Input	Date/Time	Optional; Fill
Technician:	Name of the technician sent to the site to resolve the incident.	site.visit.technician	User Input	Character	Optional; Fill
(Contract Details)	N/A	N/A	N/A	N/A	N/A
Contracted Incidents:	How many incidents are allowed for this contract.	contract.id	servicecontract.display.g	number	Protected
Used Incidents:	The number of times an incident has occurred at this site.	contract.id	servicecontract.display.g	number	Protected
TAM:	Technical Account Manager	contract.id	servicecontract.display.g	Character	Protected
Phone:	TAM's contact number	contract.id	servicecontract.display.g	Number	Protected
Escalation:	Contact person for the escalation of the incident.	contract.id	servicecontract.display.g	Character	Protected
Phone:	Escalation contact's number	contract.id	servicecontract.display.g	Number	Protected

Field Label	Description	Input Field	Source	Type	Field Characteristics
Start Date:	Date Contract goes into effect.	contract.id	servicecontract.display.g	Date/Time	Protected
End Date:	Date contract ends.	contract.id	servicecontract.display.g	Date/Time	Protected
Contracted Site Visits:	How many site visits allowed for this contract.	contract.id	servicecontract.display.g	number	Protected
Used Site Visits:	The number of times a technician has visited this site.	contract.id	servicecontract.display.g	number	Protected

Table 11: Update incident — Activities tab/Historic Activities tab (problem.template.update.g)

The following table describes fields on the Activities and Historic Activities tabs.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Type:	Indicates type of activity performed.	number.vj	activity.list	Character	Protected
Date/Time:	The date and time that the activity was performed.	number.vj	activity.list	Date/Time	Protected
Operator:	Name of the person performing the activity.	number.vj	activity.list	Character	Protected
Description:	Details of the actions taken.	number.vj	activity.list	Character	Protected
Filter by Activity Type:	Select this button to filter by type of activity.	number.vj	activity.list	N/A	Button

Table 12: Update incident — Activities tab/Action Resolution tab (problem.template.update.g)

The following table describes fields on the Activities and Action Resolution tabs.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Corrective Actions:	Details of actions that have been taken towards resolving the incident.	\$pmc.actions	User Input	Character	Required
Type:	Indicates the type of action taken.	\$apm.activity	User Input	Character	Required; Combo-box
SDU unable to fix:	Check-box to indicate the incident was unresolved.	no.SDU.fix	User Input	Logical	Optional
Solution:	Details of the solution, can include the steps taken for the incident's resolution.	resolution	User Input	Character	Protected
Candidate for Knowledge DB?	Check-box to flag the solution as a good entry for the Knowledge database.	solution.candidate	User Input	Logical	Protected
Resolution Code:	Code for accessing the resolution.	resolution.code	System Generated	Character	Protected

Table 13: Update incident — Contact tab (problem.template.update.g)

The following table describes the Contact tab.

Field Label	Description	Source
(Contact Tab)	This tab contains the contact's user information.	contact.detail.subform

Table 14: Update incident — Asset tab (problem.template.update.g)

The following table describes the Asset tab.

Field Label	Description	Source
(Asset Tab)	This tab populates with information relevant to the affected asset.	asset.subform

Table 15: Update incident — Attachment tab (problem.template.update.g)

The following table describes the Attachment tab.

Field Label	Description	Input Field	Source
(Attachment Tab)	Use this tab to attach relevant documents to the incident ticket.	vj.number.1	asset.subform

Table 16: Update incident — SLA tab (problem.template.update.g)

The following table describes fields on the SLA tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
SLA Contract #:	A unique, system generated id number for the agreement. This number is used internally by the system to track relationships between SLAs and their supporting data.	agreement.id	System-generated	Number	Protected; System Generated
Expiration:	The expiration date of the agreement.	agreement.id	System-generated	Date/Time	Protected; System Generated
Service Hours:	A shift is selected to define the service hours of the SLA. The system uses the value in this field to determine service rights of a caller on this SLA.	agreement.id	problem.sla.vj	Number	Optional; Protected
Target:	Performance target of the SLA. The value is expressed as a percentage and is used by the system to determine if the SLA is meeting its performance goals.	agreement.id	problem.sla.vj	Number	Optional; Protected
Initial State:	Incident ticket states. The system tracks and analyzes the SLAs of all tickets within the range of states defined in each of these fields.	agreement.id	problem.sla.vj	Character	Optional; Protected
Final State:	The range of time the ticket was open.	agreement.id	problem.sla.vj	Character	Optional; Protected

Field Label	Description	Input Field	Source	Type	Field Characteristics
Name:	Response name for the object. The name must be unique within the SLA, but the same name may appear in other SLAs. This name is used in reports and by external feeds to post response data into the system.	agreement.id	System Generated	Character	Protected
Acceptable:	Target time for response of this object. Use the format 00:00:00.	agreement.id	System Generated	Date/Time	Protected
Schedule:	A work shift is predefined. If this field is left blank, the system assumes that 24 x 7 operation is required.	agreement.id	System Generated	Date/Time	Protected

Table 17: Update incident — Parts & Labor tab (problem.template.update.g)

The following table describes fields on the Parts & Labor tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Date:	Date on which the parts were received	parts	User Input	Array/Structure	Optional;
Part Number:	Identification number of the parts that were received	part.no	User Input	Character	Optional;
Quantity Used:	Indicates how many of each part were used.	quantity	User Input	Number	Optional;
Date:	Date on which the technician performed the labor.	date	User Input	Date/Time	Optional;
Technician:	Name of the technician performing the labor.	operator	User Input	Character	Optional; Protected
Hours worked:	Number of hours the technician worked on this incident.	hours.worked	User Input	Number	Optional;

Table 18: Update Incident — History tab (problem.template.update.g)

The following table describes fields on the History tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
(Opened) By:	Name of operator who opened the incident ticket.	opened.by	System Generated	Character	Protected
(Opened) At:	Date and Time at which the incident ticket was first opened.	open.time	System Generated	Date/Time	Protected
(Updated) By:	Name of operator who last updated the incident ticket.	updated.by	System Generated	Character	Protected
(Updated) At:	Date and Time at which the incident ticket was last updated.	update.time	System Generated	Date/Time	Protected
(Closed) By:	Name of operator who closed the incident ticket.	closed.by	System Generated	Character	Protected
(Closed) At:	Date and Time at which the incident ticket was closed.	close.time	System Generated	Date/Time	Protected
(Reopened) By:	Name of operator who reopened the incident ticket.	reopened.by	System Generated	Character	Protected
(Reopened) At:	Date and Time at which the incident ticket was reopened.	reopen.time	System Generated	Date/Time	Protected
This incident has been reassigned x times.	System generated field that indicates the number of times that the incident has been passed from assignment to assignment.	asgnchg	System Generated	Number	Protected

Table 19: Update Incident — Alerts tab (problem.incident.update.g)

The following table describes fields on the Alerts tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
Event:	Description of the Alert.	number	bp.alert.status	Character	Protected
Alert Time:	Date and time that the alert was recorded.	number	bp.alert.status	Date/Time	Protected
Alert Stage:	Current stage of the alert, can be: DEADLINE ALERT, alert stage3, alert stage 2, alert stage 1, closed, open, reopened, resolved, or updated.	number	bp.alert.status	Character	Protected

Update incident — Related Records tab

(problem.template.update.g)

Table 20: Calls tab

The following table describes the Calls tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
(Related Calls Tab)	Tab that provides information about any calls related to this incident ticket. Information provided is: <i>Call ID, Open Time, Owner, and Status.</i>	<i>vj.number.1</i>	<i>screlate.call.vj</i>	Character	Protected

Table 21: Related Incidents tab

The following table describes the Related Incidents tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
(Related Incidents Tab)	Tab that provides information about any changes related to this incident ticket. Information provided is: <i>Incident Id, Open Time, Status, Category, and Description</i>	<i>vj.number.2</i>	<i>screlate.incident.vj</i>	Character	Protected

Table 22: Related Changes tab

The following table describes the Related Changes tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
(Related Changes Tab)	Tab that provides information about any changes related to this incident ticket. Information provided is: <i>Change Number, Category, Phase, Asset, and Description.</i>	vj.number.3	screlate.change.vj	Character	Protected

Table 23: Related Quotes tab

The following table describes fields on the Related Quotes tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
(Related Quotes Tab)	Tab that provides information about any quotes related to this incident ticket. Information provided is: <i>Request No., Category, Current Phase, Status, Approval Status, and Description.</i>	vj.number.4	screlate.quote.vj	Character	Protected

Table 24: Related Root Cause tab

The following table describes fields on the Related Root Cause tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
(Related Root Causes Tab)	Tab that provides information about any root causes related to this incident ticket. Information provided includes: <i>Root Cause ID</i> , <i>Category</i> , <i>Status</i> , and <i>Priority</i> .	vj.number.5	screlate.rootcaus.vj	Character	Protected

Table 25: Billing Information tab

The following table describes fields on the Billing Information tab.

Field Label	Description	Input Field	Source	Type	Field Characteristics
GL Number:	Global Ledger Number	gl.number	User Input	Character	Optional
Bill To:	Name or Department that is to be billed for the provided service	billto	User Input	Character	Optional; Fill
Bill Type; Department:	Radio button option to indicate who is to be billed for the service; select either Department or Contact	billtype	dept file	Character	Radio Button
Bill Type; Contact:	Radio button option to indicate who is to be billed for the service; select either Department or Contact	billtype	Contacts file	Character	Radio Button



C SLM-Related Reports

APPENDIX

This appendix contains a list and description of the SLM-related reports packaged with ServiceCenter.

Read this appendix for information about:

- *SLA Reports* on page 526
- *Device Availability* on page 527
- *Device Outages (Top Ten)* on page 528
- *SLA Device Availability Performance* on page 530
- *SLA Response Time Performance* on page 531

SLA Reports

The ServiceCenter service level agreement (SLA) module is shipped with several prebuilt reports that can be printed with the ReportCenter utility. These reports can be used internally, or they can be distributed to organizations covered by a particular SLA, to describe the status of that agreement. The following table lists the SLM module prebuilt reports. For more information, see the *ServiceCenter ReportCenter Guide*.

Report Name and Description	File Name
Device Availability During the Year X, as shown in Figure C-1 on page 527. This report shows a monthly statistical history of each device's availability over a given year.	Davailyr.rpt
Device Outages (Top Ten) shown in Figure C-2 on page 528. This report shows a count of system failures for each device.	T10dev.rpt
Change History for X between Y and Z shown in Figure C-3 on page 529. This report lists all planned changes for a given device scheduled to start during a known date range.	Devchang.rpt
SLA Device Availability Performance shown in Figure C-4 on page 530. This report lists the target-to-actual device availability ratios for each SLA.	Sladev.rpt
SLA Response Time Performance shown in Figure C-5 on page 531. This report lists the target-to-actual response time ratios for each SLA.	Slaresp.rpt

Device Availability

The **Device Availability** report provides the device (object) availability for each SLA for each month in the year specified. Availability percentages appear in a graphical format with user-defined colors.

The year for which you want data displayed must be set as a parameter before the report can be printed.

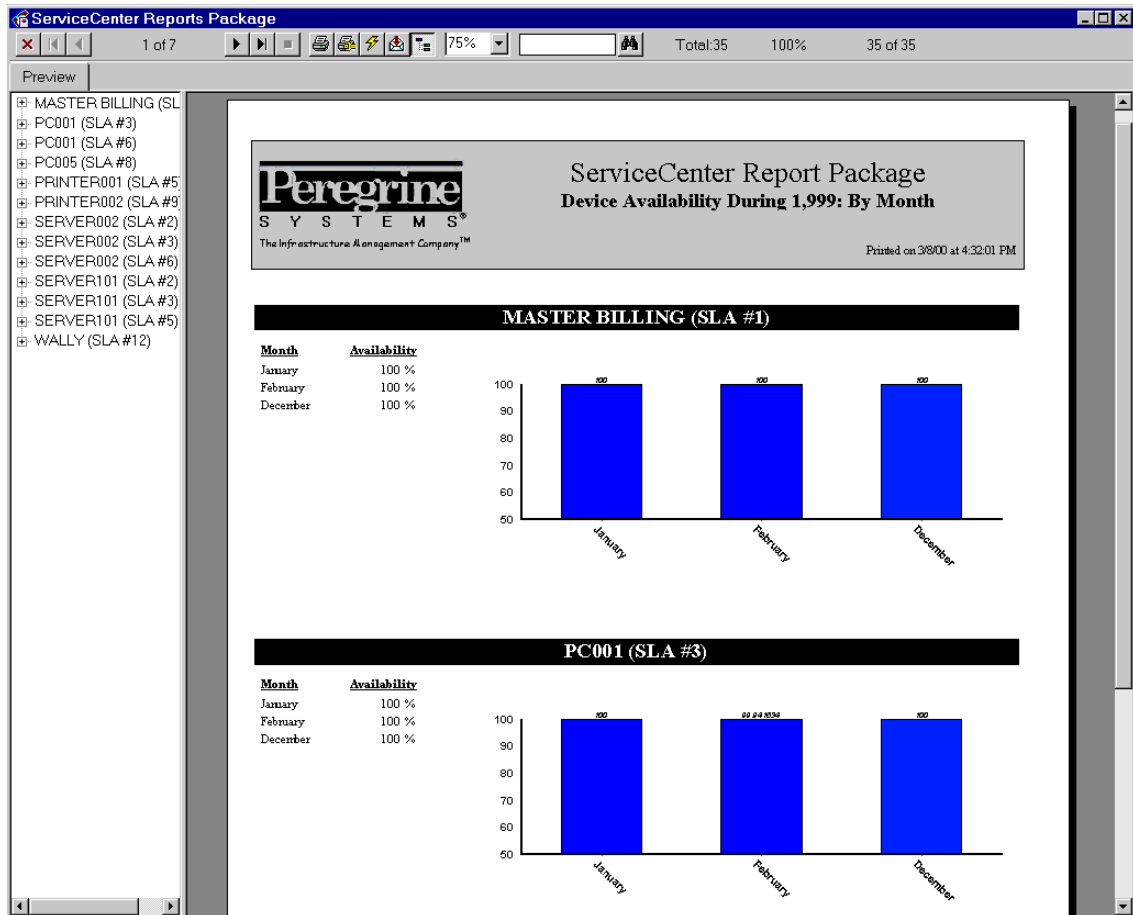


Figure C-1: ReportCenter report on device availability

Device Outages (Top Ten)

The **Device Outages** report displays a count of failures for each object covered by an SLA.

There are no parameters to define for this report.

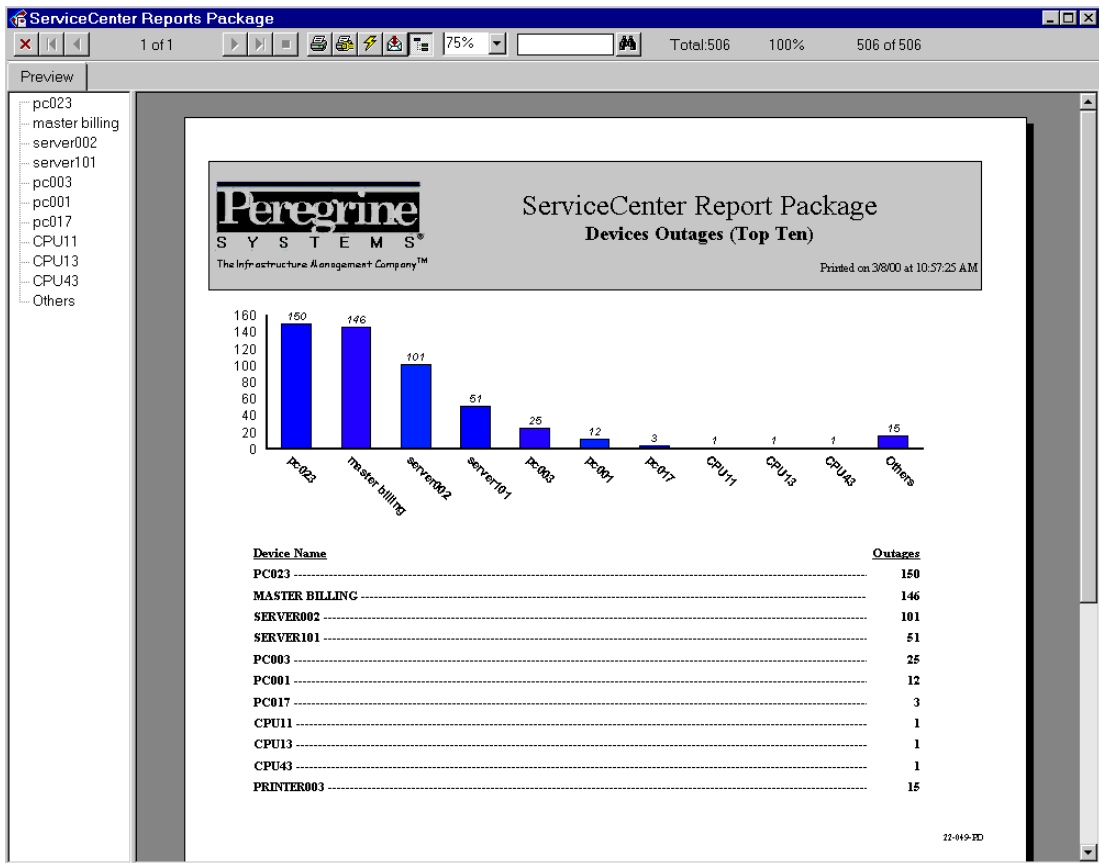


Figure C-2: ReportCenter report on device outages

Change History

The **Change History** report displays a list of all changes for a given device that have been scheduled for a future time interval.

To display data, specify the year as parameter before you print the report.

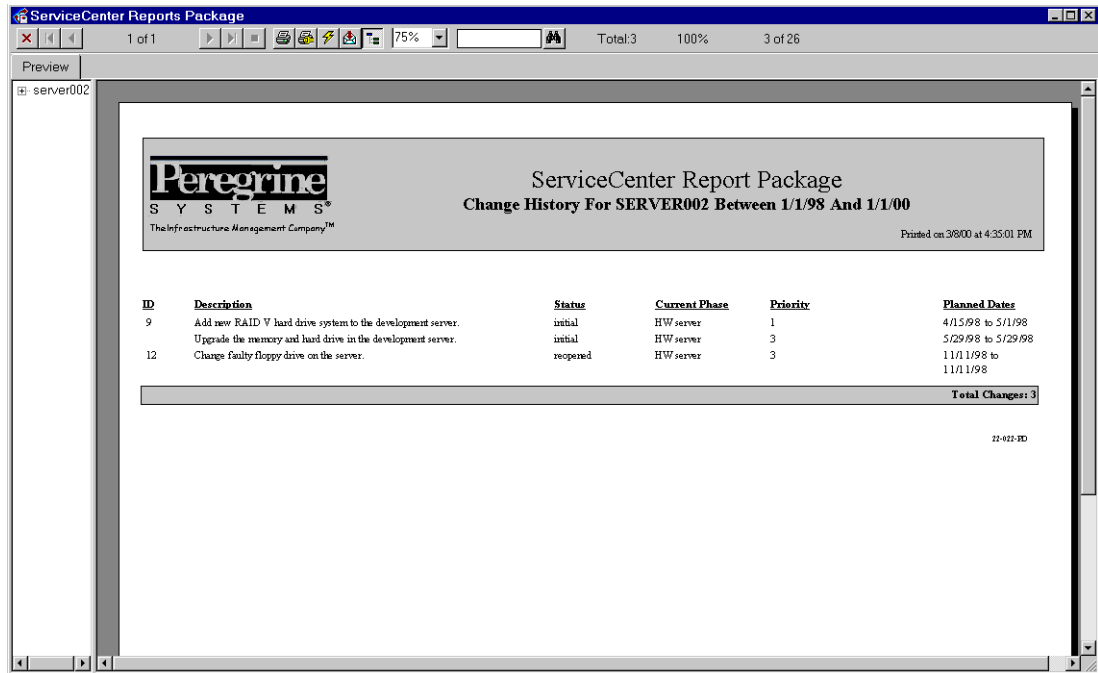


Figure C-3: ReportCenter report on the change history of a device

SLA Device Availability Performance

The SLA Device Availability Performance report displays a listing of the target-to-actual device availability ratios for each SLA. Actual performance is compared to performance percentages guaranteed by the SLA.

The year for which you want the data displayed must be set as a parameter before printing the report.

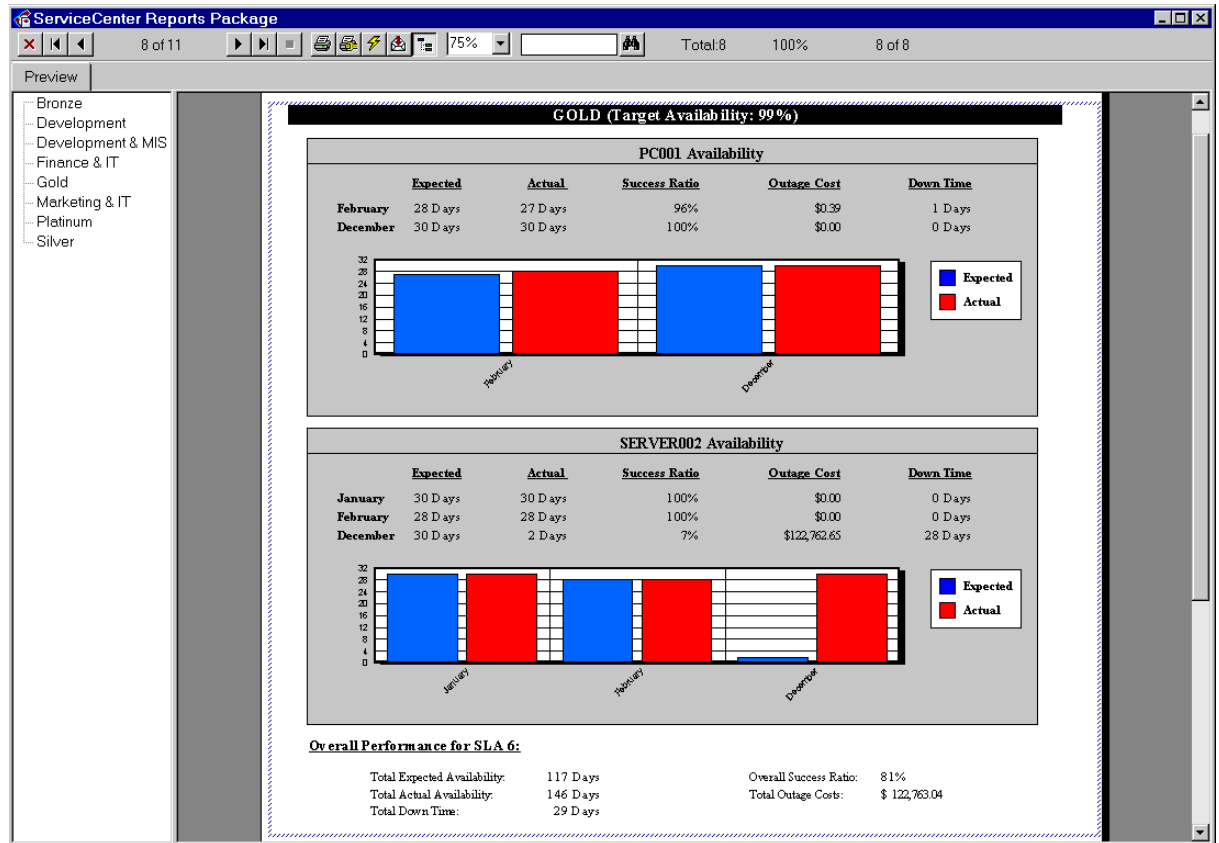


Figure C-4: ReportCenter report of device availability ratios

SLA Response Time Performance

The SLA Response Time Performance report is a listing of the target-to-actual response time ratios for each SLA. Actual performance is compared to performance percentages guaranteed by the SLA.

The year for which you want the data displayed must be set as a parameter before printing the report.

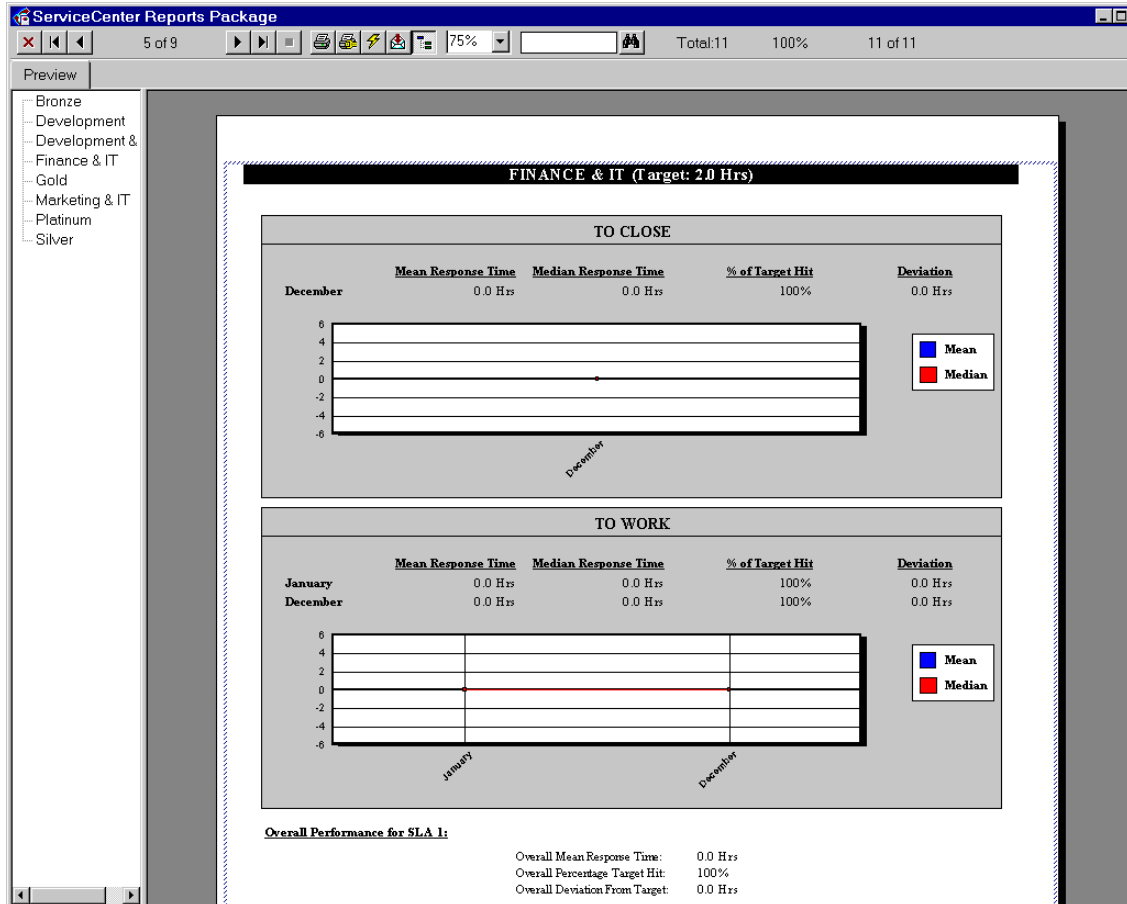


Figure C-5: ReportCenter report on response time performance

D Events

APPENDIX

This appendix explains the integration of the SLM module with Event Services.

Introduction

An interface has been created between the SLM module and Event Services to post appropriate data regarding object availability and response time performance. For more information concerning events and how to display event records, refer to the *Event Services Guide*.

Three new event classes allow a system administrator to create an interface (using SC Automate) with external sources that feeds information into the SLM module. For further information on interfacing with external data sources, refer to the *SC Automate* document for your operating system.

Availability events

Two classes of outage events have been created to track object availability:

- outstart
- outageend

outagestart

This event class is invoked whenever an object begins to experience downtime. It has two parameters:

- Object name
- Start time of the outage

outageend

This event class is invoked when an object experiencing an outage comes back online. It has two parameters:

- Object name
- Time the outage ended

Response event

One event class has been created to track response time data from outside sources.

slareponse

This event provides data to the SLM module about response time metrics. It has five parameters:

- Response name
- Name of applicable SLA
- Start time of the response
- End time of the response
- Reference key (for example, an Incident ticket number) of the event triggering the response

Index

A

- advanced search
 - changes 411, 426
 - option menu 369
 - Root Cause Security Profile 149
 - setting in profile record 364
 - SM Security Profile 54
- alert stages, defaults 265
- alerts
 - alert log 458
 - AlertDef 453
 - Change Management 381, 393
 - current alerts 453
 - description 451
 - duty table 457
 - Incident Management 111
 - log 458
 - risk calculation 447
- approvals
 - accessing options 439
 - risk calculation 447
 - sequence 435
- arrays
 - auto open tasks 397
 - expanding 361
- assignment groups 78
- attribute file
 - defined 172
 - examples 172
- availability

- agreements 287
- escalations 265
- guaranteed 272
- thresholds 266

- availability data
 - objects in single SLA 295–298
 - outage history of single device 299–301
 - single object 298–299
 - status of all SLAs 291
 - status of single SLA 293

C

- calendar 271, 274, 275, 277, 301
- call reports, sample data 19
- capability words
 - Change Management 353, 374
 - Incident Management 67
 - Inventory Management 182–186
- categories
 - adding 89–90
 - capability word access 374
 - change
 - creating 378–381
 - creating related records 379
 - deleting 382–383
 - description 371
 - printing 384
 - updating 381
 - Change Management 371
 - creating from existing record 91–92
 - defining for SLA 285

- editing 90
- overview 81
- predefined 81
- task
 - auto open 397
 - creating 378–381
 - creating related records 379
 - deleting 382–383
 - description 374
 - printing 384
 - updating 381
- category/priority mapping 265
- cause codes 99
- CenterPoint Web site 14
- Change Management
 - alerts 361, 381, 393
 - approvals
 - accessing options 439
 - approvals tab fields 436–439
 - sequence 435
 - capability word access flow 353
 - categories
 - Application 371
 - controlling access 374
 - creating by copying 378–381
 - deleting 382–383
 - description 371
 - overview 370
 - printing 384
 - Security 371
 - updating 381
 - change and task phases
 - accessing records 386–390
 - creating 400–406
 - deleting 407–409
 - description 384
 - printing 407
 - record fields 390–400
 - updating 407
 - validating 405
 - changes
 - accessing 409–417
 - categories 371
 - closing phases 418–422
 - components 348
 - queue 414, 428
 - reopening 423–424
 - sample data 19
 - updating 418
 - closing a task phase 433
 - Format Control 380–381
 - glossary 346–347
 - menu 409
 - phases, overview 370
 - Request for Change (RFC)
 - category 371
 - reviewer requirements 395
 - RFC - Advanced category 371
 - risk
 - calculation 446
 - calculation option 417, 432
 - example 447
 - setting max. 391
 - scripts 381, 398
 - search form 409, 425
 - security
 - capability words 353
 - environment record 357–358
 - group definition record 366–370
 - user profiles 358–366
 - security process flow 352–353
 - tasks
 - accessing 425–430
 - categories 374
 - closing phases 418–422
 - Options menu 431
 - reopening 434
 - updating 433
 - validity lookup option 416
 - workflow 348
- charge back 311
- configure module
 - fields 265
 - SLA configuration record 264
- Contract Management
 - budget 323
 - configuration 312–314
 - contract wizard 340–343

- contracts
 - attachments 326
 - general information 321
 - rules 324
 - cost assessment
 - handle time 333
 - itemizing costs 335
 - labor 333
 - parts 335
 - creating contracts 327
 - currency
 - budgeted currency 323
 - conversion 215–217, 314
 - definition 217–219, 314
 - deleting service contracts 328
 - editing service contracts 328
 - entitlement checking
 - accessing 337
 - description 336
 - expense line 329, 331
 - features 311
 - labor performed detail 317–319
 - overruns 339
 - parts usage detail 315
 - sample data 19
 - service contracts
 - fields 321–326
 - repository 319
 - cost assessment
 - handle time 333
 - itemizing costs 335
 - labor 333
 - parts 335
 - currency
 - conversion 215–217, 314
 - definition 217–219, 314
- D**
- data
 - samples 19
 - samples in system 19
 - define
 - profiles 22
 - device file
 - defined 171
 - form 175
 - primary and attribute files 170
 - device records
 - device availability 105
 - form 175
 - device types
 - creating 193–200
 - deleting a record 200
 - selecting records 191–192
 - updating records 200
 - devtype file 170, 190
 - downtime
 - availability in Incident Management 104
 - devices 105
 - resetting 122
 - duty table, alerts times 457
- E**
- editing an SLA 280–281
 - education services 15
 - entitlement checking
 - accessing 337
 - Contract Determination Wizard 311
 - description 336
 - environment record
 - Change Management 357–358
 - description 44, 66
 - Incident Management 108–111
 - Root Cause Analysis 140
 - escalations
 - availability 265
 - description 112
 - response times 265
 - Event Services 62
 - events
 - availability 533
 - notifications 470
 - response 534
 - risk calculation 447
 - expense line, accessing 331
 - expressions, auto-fill fields 164

F

fields, using expressions to fill 164
 Format Control
 Change Management 380–381
 Scheduled Maintenance 166

G

glossary 346–347
 group definition records 366–370
 group profiles, editing 32, 72

I

inboxes

 administering 94–99
 Change Management 414, 429
 maintaining 56
 Root Cause Analysis 151
 saving 99

Incident Management

 accessing 64
 assignment groups, adding 78–81
 capability words 67
 categories
 adding 89–90
 creating from existing record 91–92
 description 81
 editing 90
 cause codes 99
 downtime 104
 environment record
 configuring 108–111
 description 66
 group profiles, editing 72
 inboxes
 administering 94–99
 saving 99
 incident tickets
 description 62
 severity 113
 status 111
 macro editor 104, 151
 menu 65
 operator record 66

personal profiles

 adding 77
 editing 72

privileges 73

probable cause

 creating records 102
 editing records 100

problem summary records 123

process 62

profiles

 editing 71
 Incident Management Profile 67

resetting downtime 122

security files, accessing 67

summary link 106

two-step close

 inactivating a ticket 119–120
 resolving a ticket 116–119

users, adding 69

incident tickets

 inactivating 119–120
 resolving 116
 sample data 19
 status 111

incident, scheduler 165

Inventory Management

 adding ICM capability to operator record
 182–186
 adding users 203
 attribute file 172
 attribute file definition 172
 creating new device type 193–200
 device file 170
 device types
 deleting a record 200
 selecting records 191–192

forms

 attribute 175
 device 175
 join 175

generating Change requests 160

generating incident tickets 160

generating RM quotes 160

- hierarchy
 - child relation 175
 - container relation 175
 - parent relation 174
- inventory records 205
- join file 173
- maintenance
 - history 160
 - tasks 159
- parent/child relationships 178–180
- PC software, fields 230
- primary files
 - device 170, 171
 - devtype 170
- profiles
 - adding 186
 - user 182
- Scheduled Maintenance 159
- service information (SLA)
 - accessing 208
 - deleting records 281
 - software installation records 253
 - updating device type records 200
- IR Query 412, 427

J

- join file 173

K

- Knowledge Base 60, 152

L

- labor performed 317–319
- load balancing 165–166
- log files 458

M

- macros
 - editor 104, 151
 - list form 57
- messages, notifications 470
- metrics, accessing 289

N

- notifications
 - events 470
 - messages 470

O

- OLE containers
 - contracts 326
 - SLA record 277
- operator record
 - capability words
 - Change Management 353
 - Incident Management 67
 - Inventory Management 182–186
 - description 44
 - Incident Management 66
- Options menu, tasks 431
- outage data, recalculating 282
- outage history 299–301
- outageend 534
- outages
 - auto post 265
 - reports 528
 - tracking 260
- outagestart 534

P

- parent/child relationships 178–180
- parts usage 315
- Peregrine Systems
 - Corporate headquarters 15
 - Worldwide Contact Information 15
- performance views 287
- personal profiles, editing 32, 72
- phases
 - change and task
 - accessing records 386–390
 - creating 400–406
 - deleting 407–409
 - printing 407
 - record fields 390–400
 - updating 407
 - validating 405
 - definitions 347

- printing change and task phase records 407
- priority, defining for SLA 285
- probable cause
 - accessing records 58
 - cause code field 99
 - creating records 102
 - editing records 100
- process flow diagrams
 - Change Management
 - approval 476
 - close 478
 - denial 477
 - open 474
 - reopen 479
 - retract 480
 - update 475
 - Incident Management
 - close 483
 - open 481
 - update 482
 - Inventory Management
 - delete 490
 - open 488
 - update 489
 - Service Management
 - close 487
 - create problem 485
 - quick-open 484
 - update 486
- profiles
 - adding
 - ICM 186
 - Incident Management 77
 - Service Management 32–38
 - Change Management 358–366
 - defining 22
 - editing
 - Incident Management 71
 - Root Cause Analysis 146–150
 - Service Management 51–55
 - group 23
 - Incident Management 67
 - Inventory Management 182
 - Root Cause Analysis 140
 - Service Management 44, 53

R

- reports
 - change history 529
 - device availability 527
 - device outages 528
 - response time performance 531
 - SLA performance 530
- Request for Change (RFC), change category 371
- response agreements 287
- response time
 - escalations 265
 - thresholds 266
- response time data
 - health of all SLAs 302–303
 - health of single SLA 303–306
 - single response type detail 309
 - single SLA 306–307
 - single SLA for one year 308
- Response Times tab 274
- risk, Change Management
 - calculation 361, 417, 432, 446
 - example 447
 - phases 391
- Root Cause Analysis
 - environment record configuration 140
 - inboxes 151
 - Knowledge Base 152
 - profiles 140, 146–150
 - security administration utility
 - environment tab 142
 - security files tab 141
 - security files 140
 - users, adding 144

S

- sample data 19
- schedule records, repeat interval 165
- scripting
 - Change Management 381, 398
 - risk calculation 447
- security
 - CM category 371
 - process flow in Change Management 352–353

- service contracts
 - attachments 326
 - budget 323
 - creating 327
 - currency 323
 - deleting 328
 - editing 328
 - fields 321–326
 - general information 321
 - repository 319
 - rules 324
- Service Management
 - environment record 44
 - group profiles editing 32
 - inboxes
 - administering 94–99
 - maintaining 56
 - saving 99
 - Knowledge Base 60
 - macro list 57
 - menu 43
 - operator record 44
 - personal profiles
 - adding 32–38
 - editing 32
 - probable cause 58
 - profile groups 23
 - profiles
 - description 44
 - determining 23
 - editing 51–55
 - group 23
 - privileges and views 53
 - relationship models 346
 - security administration utility
 - environment tab 46
 - security files tab 45
 - security files 44–45
 - users, adding 49
- severity levels, incident tickets 113
- SLA (Service Level Agreement) Management
 - accessing 208
 - accessing from Change Management 417
 - creating 269–271
 - editing 280–281

- OLE container 277
 - records, field definitions 271
- slaresponse 534
- software installation records 253
- SQL server, moving files to 165
- status, incident tickets 111
- summary link 106

T

- tasks
 - categories 374
 - closing 433
 - definition 347
 - reopening 434
 - template, selecting 162
- templates
 - automated task generation 157
 - generating tasks
 - from Inventory Management 161
 - from RM quotes 158
 - selecting 162
- training services 15
- two-step close
 - inactivating a ticket 119–120
 - resolving a ticket 116–119
- type, duty table 457

U

- user
 - adding
 - how to 203
 - Incident Management 69
 - Root Cause Analysis 144
 - Service Management 49
 - sample data 19

V

- validity lookup option, Change Management 416
- validity table processing, risk calculation 447

W

- workflow, Change Management 348

