611-EMD-200

EOSDIS Maintenance and Development Project

Release 7.21 Mission Operation Procedures for the EMD Project

Revision -

May 2008

Raytheon Company
Riverdale, Maryland

Release 7.21 Mission Operation Procedures for the EMD Project

Revision -

May 2008

Prepared Under Contract NAS5-03098
CDRL Item 23

RESPONSIBLE AUTHOR

Kenneth Prickett Date
EOSDIS Maintenance and Development Project

RESPONSIBLE OFFICE

Timothy W. Ortiz, Program Manager Date
EOSDIS Maintenance and Development Project

Raytheon Company
Riverdale, Maryland

This page intentionally left blank.

Preface

This document is a formal contract deliverable. It requires Government review and approval within 45 business days. Changes to this document will be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office
The EMD Project Office
Raytheon Company
5700 Rivertech Court
Riverdale, Maryland 20737

Revision History

Document Number	Status/Issue	Publication Date	CCR Number
611-EMD-200	Original	May 2008	08-0204

This page intentionally left blank.

Abstract

This document, Mission Operation Procedures for the EMD Project, provides DAAC procedures that assign and describe operators, engineers, operations support, administration and management staff actions required to configure, maintain and operate the ECS applications at maturity. The DAAC portion of this document contains system-level standard procedures that can be modified at the DAACs during subsequent training, operations exercises and procedure review activities to reflect desired uniqueness. The objectives of the current release of the system are to provide capability to support the ingest and archive of raw data obtained from instruments on Earth Observing System (EOS) satellites [e.g., the EOS AM Mission spacecraft 1, morning equator crossing spacecraft series (Terra (AM-1)), EOS PM Mission spacecraft 1 and the afternoon equator crossing spacecraft series (Aqua (PM-1))]. Other capabilities provided by the current release include processing the data obtained, distributing raw or processed data as requested, quality assurance of processed data, supporting communication networks, and systems monitoring via interfaces with the ECS operations staff.

This page intentionally left blank.

Contents

Preface

Abstract

1. Introduction

1.1 Identification 1-1

1.2 Scope 1-1

1.2.1 On-Site Procedures Tailoring Guide 1-1

1.3 Purpose 1-1

1.4 Status and Schedule 1-2

1.5 Organization 1-2

2. Related Documentation

2.1 Parent Documents 2-1

2.2 Applicable Documents 2-1

2.3 Information Documents 2-1

2.3.1 Information Documents Referenced 2-1

2.3.2 Information Documents Not Referenced 2-3

3. System Administration

3.1 Overview 3-1

3.2 Secure Access to DAACs 3-1

3.3 Setting Up SSH 3-1

3.3.1 Initiating SSHSETUP 3-2

3.4 Remote SSH Access 3-2
3.4.1 Setting Up Remote Access SSH 3-2
3.5 Changing Your Passphrase 3-3
3.5.1 Changing Your Passphrase 3-3
3.6 Logging in to System Hosts 3-4
3.6.1 Log in to System Hosts 3-4
3.7 System Startup and Shutdown 3-5
3.7.1 Cold Startup By Subsystem 3-6
3.7.2 Warm Startup 3-7
3.7.3 Updating leapsec.dat and utcpole.dat Files 3-7
3.7.4 Normal Shutdown 3-8
3.7.5 Emergency Shutdown 3-10
3.7.6 System Shutdown by Server 3-11
3.8 Checking the Health and Status of the System 3-11
3.8.1 Whazzup 3-12
3.8.2 Starting EcMsWz-Whazzup 3-12
3.8.3 Host Status 3-13
3.8.4 Verify Mode 3-14
3.8.5 Performance Management 3-14
3.9 ECS Assistant 3-18
3.9.1 Starting ECS Assistant 3-19
3.10 Tape Operations 3-20
3.10.1 Networker Administrator Screen 3-21
3.10.2 Labeling Tapes 3-22
3.11 System Backups and Restores 3-26
3.11.1 System Backup 3-27
3.11.2 System Restore 3-29
3.12 User Administration 3-33
3.12.1 Screening Personnel 3-33
3.12.2 Screening Procedures 3-34
3.12.3 Adding a New User 3-34
3.12.4 Deleting a User 3-35
3.12.5 Changing a User’s Account Configuration 3-37

3.12.6 Changing User Access Privileges 3-37
3.12.7 Changing a User Password 3-38
3.12.8 Checking a File/Directory Access Privilege Status 3-38
3.12.9 Changing a File/Directory Access Privilege 3-39
3.12.10 Moving a User's Home Directory 3-42
3.13 Commercial Off-the-Shelf (COTS) Software Administration 3-42
3.13.1 Installation 3-42
3.13.2 LOG FILES 3-42
3.13.3 COTS Configuration 3-43
3.14 Security 3-43
3.14.1 Generating Security Reports 3-43

4. Database Administration

4.1 System Overview 4-1
4.1.1 Information Model 4-1
4.1.2 Subsystems 4-4
4.1.3 Databases 4-5
4.1.4 Flat Files 4-6
4.1.5 Resident Databases 4-7
4.1.6 Database Directory Locations 4-8
4.2 Database Management 4-9
4.2.1 Database Management Model 4-9
4.2.2 Database Management Implementation 4-10
4.2.3 Hardware, Software, and Database Mapping 4-13
4.3 Database Administrator 4-13
4.3.1 DBA Tasks and Procedures 4-13
4.4 Starting and Stopping Database Servers 4-15
4.4.1 Start Adaptive Server Enterprise (ASE) Servers 4-15
4.5 Creating Database Devices 4-20
4.5.1 Create a Database Device 4-20

4.6 Installing Databases and Patches 4-23
4.6.1 Perform a Database Build Procedure (Example Only) 4-24
4.6.2 Install a Database Patch (Example) 4-24
4.6.3 COTS Databases 4-25
4.7 Configuring Databases 4-25
4.7.1 Configure the ASE Server Parameters 4-25
4.7.2 Configuration Parameters and the Configuration Registry 4-29
4.7.3 Configuration Registry 4-30
4.8 Working with Indexes, Segments, and Caches 4-33
4.8.1 Delete an Index 4-33
4.8.2 Create Database Segments (Example) 4-34
4.8.3 Caches 4-36
4.9 Backing Up and Recovering Data 4-37
4.9.1 Perform Automatic Backups 4-37
4.9.2 Perform Manual Backups 4-40
4.9.3 Perform a User Database Recovery (Order of Procedures) 4-41
4.9.4 Perform a User Database Recovery (Example) 4-42
4.10 Establishing Database Security 4-45
4.10.1 Grant or Revoke Database Access Privileges 4-47
4.10.2 Create an ASE Server Login 4-48
4.10.3 Change a Password 4-50
4.10.4 Perform Auditing 4-51
4.10.5 EMD Security Directive 4-52
4.11 Copying, and Extracting Data 4-52
4.11.1 Copying a Database (Example) 4-53
4.12 Bulk Copying 4-53
4.12.1 Perform Bulk Copying 4-53
4.13 Replication System Administration - Removed 4-55
4.14.1 Monitoring 4-55
4.14.2 Tuning 4-55
4.15 Ensuring Database Quality 4-56
4.15.1 Integrity Monitoring 4-56

4.16 Sybase Troubleshooting 4-57
4.16.1 Space Usage 4-57
4.16.2 Troubleshoot Chronic Deadlock 4-57

5. Security Services

5.1 Scanning Network Vulnerabilities 5-1
5.2 Ensuring Password Integrity 5-1
5.2.1 Detecting Weak Passwords 5-2
5.2.2 ANLpasswd 5-7
5.3 Aging Passwords 5-11
5.4 Secure Access through Secure Shell 5-11
5.4.1 Installation of SSH 5-12
5.4.2 The SSH Encryption Mechanism 5-12
5.4.3 Using Secure Shell 5-13
5.4.4 A Layer of Convenience 5-14
5.4.5 Multiple Connections 5-14
5.4.6 Secure FTP 5-14
5.4.7 Other Notes 5-15
5.4.8 Configuration of Secure Shell 5-15
5.4.9 Administration of Secure Shell 5-17
5.5 Controlling Requests for Network Services (TCP Wrappers) 5-17
5.5.1 Installation, Configuration, and Testing for Wrappers 5-18
5.6 Monitoring File and Directory Integrity (Tripwire) 5-19
5.6.1 Installation of Tripwire 5-20
5.6.2 Updating the Tripwire Database 5-20
5.6.3 Configuring the tw.config File 5-21
5.7 Reporting Security Breaches 5-22
5.8 Initiating Recovery from Security Breaches 5-22

6. Network Administration

6.1 Network Documentation 6-1

6.2 Network Monitoring 6-1

6.2.1 Big Brother - Better Than Free Edition 6-1

6.3 DAAC LAN Topology Overview 6-1

6.4 Network Hardware Components 6-2

6.4.1 Portus Firewall 6-2

6.4.2 VLAN Ethernet Switch 6-2

6.4.3 GigE Switch 6-3

6.5 Domain Name Service (DNS) Structure 6-3

6.6 Host Names 6-3

6.7 Network Security 6-4

6.7.1 Network Connectivity 6-4

6.7.2 Troubleshooting - Verifying Connectivity 6-4

7. System Monitoring

7.1 Overview 7-1

7.2 Checking the Health and Status of the Network 7-1

7.2.1 Big Brother 7-1

7.3 Monitoring and Managing Server Applications 7-3

7.3.1 Whazzup?? 7-4

8. Problem Management

8.1 The Problem Resolution Process 8-1

8.2 Problem Management Procedures 8-2

8.3 Using the Trouble Ticketing System 8-3

8.3.1 Accessing the Trouble Ticket System 8-6

8.3.2 Submit a Trouble Ticket 8-11

8.3.3 Search for a Trouble Ticket 8-20

8.3.4 Assign Trouble Ticket 8-23
8.3.5 Update an Open Trouble Ticket 8-26
8.3.6 Change a Trouble Ticket's Lifecycle State 8-28
8.3.7 Escalate a Trouble Ticket 8-30
8.3.8 Open an NCR 8-33
8.3.9 Close a Trouble Ticket 8-39
8.3.10 Add a New User to the Global User Database 8-41
8.3.11 Grant a User Access to a Trouble Ticket Project 8-46
8.3.12 Reset a User's Password 8-52
8.3.13 Manage Notifications 8-53
8.3.14 Generating Trouble Ticket Reports 8-72
8.4 Emergency Fixes 8-75

9. Configuration Management Procedures

9.1 Configuration Identification Procedure 9-2
9.1.1 Purpose 9-2
9.1.2 Applicability 9-2
9.1.3 References 9-2
9.2 Configuration Change Control Procedures 9-3
9.2.1 Purpose 9-3
9.2.2 Applicability 9-3
9.2.3 References 9-3
9.2.4 Procedures 9-3
9.3 Configuration Status Accounting Procedures 9-18
9.3.1 Purpose 9-18
9.3.2 Applicability 9-19
9.3.3 References 9-19
9.3.4 Procedures 9-19
9.4 Configuration Audits 9-20
9.4.1 Purpose 9-20
9.4.2 Applicability 9-21
9.4.3 References 9-21
9.4.4 Procedures 9-21

9.5 Archiving Procedures for the SW CM Manager (ClearCase) 9-22
9.5.1 Purpose 9-22
9.5.2 Applicability 9-22
9.5.3 References 9-22
9.5.4 Definitions 9-22
9.5.5 General 9-22
9.5.6 Procedures 9-23
9.6 Software Delivery and Installation 9-23
9.6.1 Purpose 9-23
9.6.2 Applicability 9-23
9.6.3 References 9-23
9.6.4 Procedures 9-24
9.7 Baseline Manager 9-25
9.7.1 Overview 9-25
9.7.2 Baseline Terms and Concepts 9-25
9.7.3 Baseline Manager (BLM) Outputs Useful at the Sites 9-29
9.7.4 Procedure for Retrieving Baseline Reports 9-30

10. Metadata Administration

10.1 ESDT Descriptor Files 10-1
10.1.1 Steps in Generating a Descriptor File 10-2
10.1.2 Verifying Descriptor Files 10-2
10.2 Preparation of Earth Science Data Types 10-3
10.2.1 Definitions 10-3
10.2.2 Process 10-3
10.3 Metadata Population 10-5
10.3.1 Collection-Level Metadata 10-5
10.3.2 Granule-Level Metadata 10-5
10.3.3 Product-Specific Metadata 10-6
10.4 ESDT Maintenance 10-6
10.4.1 Launching the ESDT Maintenance GUI 10-9

11. Bulk Metadata Generation Tool

11.1 BMGT Overview 11-1

11.2 BMGT GUI 11-3

11.2.1 BMGT GUI Functions 11-3

11.2.2 Monitoring Recent Packages 11-7

11.2.3 Cancelling Recent Packages 11-9

11.2.4 Reviewing Failed Packages 11-9

11.2.5 Global Tuning Parameters 11-11

11.3 BMGT Manual Mode 11-15

11.4 BMGT Automatic Mode 11-20

12. Quality Assurance

12.1 Using the QA Update Tool 12-1

12.1.1 Configure QA Update Utility 12-2

12.1.2 Configure QA Email Script 12-5

12.1.3 Input File Name Format 12-6

12.1.4 Request Format 12-6

12.1.5 Update QA Metadata Flags Using QA Update Utility 12-8

13. Ingest

13.1 Ingest Process 13-1

13.2 Logging in to System Hosts 13-3

13.2.1 Log in to System Hosts 13-4

13.3 Monitoring the Ingest System 13-5

13.3.1 DPL Ingest GUI 13-5

13.3.2 Monitoring Requests Status 13-10

13.3.3 Viewing Historical Requests 13-22

13.3.4 Provider Status 13-26

13.3.5 File System Status 13-31

13.3.6 Transfer Host Status 13-33

13.3.7 Viewing ECS Service Status 13-35
13.3.8 Monitoring PDR List 13-38
13.4 Interventions & Alerts 13-39
13.4.1 Open Intervention 13-40
13.4.2 Viewing System Alerts 13-49
13.5 DPL Ingest Configuration 13-53
13.5.1 Data Provider Configuration 13-54
13.5.2 Data Type Configuration 13-62
13.5.3 Transfer Host Configuration 13-65
13.5.4 File System Configuration 13-70
13.5.5 ECS Service Configuration 13-72
13.5.6 Global Tuning Configuration 13-80
13.5.7 Configure Volume Groups 13-86
13.5.8 Operator Configuration 13-95
13.6 Reports 13-99
13.6.1 Reports 13-99
13.6.2 Viewing the Volume Groups History Page 13-102
13.7 Help Pages and Context Help 13-104
13.8 Data Pool Maintenance GUI 13-105
13.8.1 Data Pool Maintenance GUI 13-105
13.8.2 Managing Data Pool Collection Groups 13-108

14. Archive Management/DataPool Maintenance

14.1 Archive Management Overview 14-1
14.2 Archive Hardware 14-1
14.3 Archive Software 14-2
14.4 Starting and Stopping StorNext 14-2
14.4.1 Starting the StorNext Application 14-3
14.4.2 Stopping the StorNext Application 14-5
14.4.3 Rebooting the StorNext Metadata Servers 14-6
14.4.4 Avoiding loss of LUN Labels When Installing Red Hat 14-6

14.5 Loading and Removing Archive Media 14-8
14.5.1 Loading Archive Media 14-8
14.6 Deleting Granules 14-15
14.6.1 Generating a GeoID File 14-17
14.6.2 Deleting Granules, Phase 1: Mark Granules for Deletion (Logical) 14-21
14.6.3 “Undeleting” Granules from the Archive and Inventory 14-23
14.7 Backing Up the StorNext Application 14-29
14.7.1 Executing a StorNext Backup 14-30
14.7.2 Scheduling a StorNext Backup 14-33
14.8 ACSLS Procedures 14-34
14.8.1 Entering the Archive After StorNext is Started 14-35
14.8.2 Backing Up the ACSLS Database 14-36
14.8.3 Restoring the ACSLS Database 14-37
14.8.4 Checking Cleaning Cartridges 14-38
14.9 Data Pool Maintenance Tasks 14-38
14.9.1 Features of the Data Pool Maintenance GUI 14-38
14.9.2 Data Pool File Systems 14-47
14.9.3 Cloud Cover 14-52
14.9.4 Batch Summary 14-57
14.9.5 List Insert Queue 14-59
14.9.6 Configuration Parameters 14-62
14.9.7 Aging Parameters 14-67
14.9.8 Collection Groups 14-69
14.9.9 Themes 14-84
14.9.10 Help 14-91
14.10 Working with Data Pool Scripts 14-91
14.10.1 Extending the Period of Retention for Granules in the Data Pool 14-93
14.10.2 Running the Data Pool Cleanup Utility 14-97
14.10.3 Running the Data Pool Access Statistics Utility 14-104
14.10.4 Using the Batch Insert Utility 14-112
14.10.5 Running the Most Recent Data Pool Inserts Utility 14-114
14.10.6 Running the Data Pool Collection-to-Group Remapping Utility 14-115

14.10.7 Running the Data Pool Move Collections Utility 14-117
14.10.8 Running the Data Pool Hidden Scrambler Utility in Rename Mode 14-119

15. Distribution Concepts

15.1 System Overview 15-1
15.2 Order Manager Subsystem (OMS) 15-4
15.3 OM GUI Operator Security 15-5
15.4 Order Manager GUI 15-6
15.4.1 Launching the Order Manager GUI 15-7
15.5 Order Manager GUI Operations 15-8
15.6 OM GUI – Request Management 15-9
15.6.1 Request Management submenu page – Open Interventions 15-11
15.6.2 Request Management submenu page – HEG Interventions 15-22
15.6.3 Request Management Submenu Page – Completed Actions and Interventions Filter 15-30
15.6.4 Request Management Submenu Page – Distribution Requests [filter] 15-31
15.6.5 Request Management Submenu Page – FtpPush/SCP Requests Filters and Staging Requests Filters 15-37
15.6.6 Request Management Submenu Page – Processing Service Requests [filter] 15-40
15.6.7 Request Management submenu page – Operator Alerts 15-41
15.6.8 Exiting the OM GUI 15-44
15.7 OM GUI – Destination Monitor 15-44
15.7.1 Destination Monitor submenu page – Suspended Destinations 15-45
15.8 OM GUI – Archive Data 15-49
15.8.1 Archive Data submenu page – Historical Distribution Requests Filter 15-49
15.8.2 Archive Data submenu page – Historical Processing Requests Filter 15-51
15.9 OM GUI – OM Status Pages 15-53
15.9.1 OM Status Pages Submenu Page – OM Queue Status 15-53
15.9.2 OM Status Pages submenu page – HEG Order Status 15-55
15.9.3 OM Status Pages submenu page – Staging Status (Media Type, FTP Push Destination and SCP Destination) 15-56

15.9.4 OM Status Pages submenu page – Pending HEG Granules 15-59
15.9.5 OM Status Pages submenu page – DPL File System Status..... 15-60
15.10 OM GUI – OM Configuration 15-61
15.10.1 OM Configuration submenu page – Aging Parameters..... 15-63
15.10.2 OM Configuration submenu page – Server/Database 15-65
15.10.3 OM Configuration submenu page – Media 15-69
15.10.4 OM Configuration submenu page – Media Creation..... 15-71
15.10.5 OM Configuration submenu page – ODL Metadata Users 15-73
15.10.6 OM Configuration Submenu Page – External Processing..... 15-75
15.10.7 OM Configuration Submenu Page – FtpPush/SCP Policy 15-77
15.11 OM GUI – Help 15-81
15.11.1 Help Submenu Page – About HelpOnDemand…..... 15-82
15.11.2 Help Submenu Page – Help 15-82
15.12 OM GUI – Physical Media Distribution..... 15-83
15.12.1 Physical Media Distribution Submenu Page – Media Creation Console 15-84
15.12.2 Physical Media Distribution Submenu Page – Device Configuration..... 15-103
15.12.3 Physical Media Distribution submenu page – Open Interventions..... 15-109
15.12.4 Physical Media Distribution submenu page – Printer Configuration..... 15-116
15.12.5 Physical Media Distribution submenu page – PM Configuration 15-118
15.12.6 Physical Media Distribution Submenu Page – Reports..... 15-121
15.12.7 Physical Media Distribution Submenu Page – ESDT Configuration..... 15-122
15.13 OM GUI – Logs 15-124
15.13.1 Logs Submenu Page – OM GUI Log Viewer..... 15-124
15.14 Using the Order Manager Command Line Utility 15-126
15.14.1 Order Manager Command Line Utility..... 15-126
15.14.2 Running the OM Command Line Utility 15-126
15.14.3 OMS Configuration Script (OMS Configuration CI) Activities 15-133
15.14.4 Configuring How Long Order-Tracking Information is Kept in the OMS Database 15-137
15.14.5 Getting OMS Configuration CI Help..... 15-142
15.14.6 Science Command Line Interface (SCLI) in OMS..... 15-142

15.15 Tuning Order Manager Subsystem and Data Pool Parameters 15-145
15.15.1 Throttling Archive Staging for Output Devices and FTP Connections 15-146
15.15.2 Ensuring the Staging of Low-Priority Requests at a Reasonable Pace 15-146
15.15.3 Ensuring That High-Priority Requests Are Expedited 15-148
15.16 OMS Database Cleanup Guidelines 15-149
15.16.1 Removal of Completed OMS Actions, Interventions and Notifications 15-150
15.16.2 Removal of Order-Tracking Information for Completed Orders 15-150
15.16.3 Fault Handling 15-151
15.17 Troubleshooting a Order Manager GUI Failure 15-152
15.17.1 Checking Log Files 15-165
15.17.2 Checking Database Connections 15-166
15.17.3 Recovering from Order Manager Failures 15-167
15.17.4 Determining the Permissions for Creating an Ftp Pull Subdirectory 15-172
15.17.5 HEG Failures 15-173
15.17.6 Checking HEG Server Log Files 15-191
15.17.7 Checking Files in the HEG Tempfiles Directory 15-202

16. User Services

16.1 Spatial Subscription Server 16-1
16.1.1 Spatial Subscription Server GUI 16-2
16.1.2 List Subscribable Events 16-4
16.1.3 Manage Subscriptions 16-6
16.1.4 Add a Subscription to the NBSRV Database 16-13
16.1.5 Subscriptions Associated with a Theme 16-19
16.1.6 Manage Bundling Orders 16-22
16.1.7 Monitor Queues 16-32
16.1.8 Using the SSS Command Line Interface (CLI) 16-36

17. Library Administration

17.1 EMD Library Administration Overview 17-1
17.1.1 Data Management (DM) 17-1

17.2 Configuration Management (CM) Overview 17-3
17.2.1 Configuration Management (CM) 17-3
17.3 Systems Monitoring Center (SMC) System Overview 17-4
17.3.1 Systems Monitoring Center (SMC) System 17-4
17.4 On-Site Documentation Overview 17-4
17.4.1 On-Site COTS Document and Software Maintenance 17-4

18. COTS Hardware Maintenance

18.1 Overview 18-1
18.2 COTS Hardware Maintenance - General 18-1
18.2.1 Corrective Maintenance 18-2
18.2.2 Preventive Maintenance 18-2
18.2.3 Configuration Management 18-2
18.2.4 COTS Hardware Maintenance Safety 18-2
18.3 COTS Hardware Maintenance - Contract Information 18-2
18.3.1 COTS Hardware Maintenance Contract 18-3
18.3.2 Information Required to Obtain COTS Hardware Maintenance 18-3
18.4 Hardware Repairs - Standard 18-3
18.4.1 Hardware Problem Reporting 18-4
18.4.2 Hardware Corrective Maintenance Actions 18-4
18.4.3 Contract On-Site Hardware Maintenance 18-6
18.4.4 Return-to-Depot Support 18-8
18.5 Maintenance Spares 18-8
18.5.1 Use of Maintenance Spares 18-9
18.5.2 Return of Failed LRUs 18-9
18.6 Non-Standard Hardware Support 18-9
18.6.1 Escalation of COTS Hardware Support Problem 18-9
18.6.2 Low Cost Equipment – Not Repaired 18-10

19. COTS Software Maintenance

19.1 Introduction 19-1

19.2 COTS Software Maintenance 19-1

19.2.1 Management of COTS Software Maintenance Contracts 19-2

19.2.2 Management of COTS Software Licenses 19-2

19.2.3 COTS Software Installation and Upgrades 19-3

19.2.4 Obtaining COTS Software Support 19-4

19.2.5 COTS Software Problem Reporting 19-4

20. Property Management

20.1 Receipt of Equipment and Software from Vendor 20-1

20.2 Receipt of Equipment and Software from the ILS Property Administrator 20-3

20.3 Equipment Tagging 20-4

20.4 Property Records and Reporting 20-5

20.4.1 Maintaining Property Records 20-5

20.4.2 Reporting Loss, Theft, Damage or Destruction 20-6

20.5 Equipment Relocation 20-6

20.5.1 Intra-Site Relocation 20-6

20.5.2 Inter-Site Relocation 20-6

20.5.3 External Transfers 20-7

20.6 Inventories and Audits 20-7

20.7 Storage 20-7

20.7.1 Segregation Requirements 20-7

20.7.2 Stock Rotation 20-8

20.7.3 Physical Security 20-8

20.8 Packing and Shipping 20-8

20.9 Electrostatic Discharge (ESD) Program 20-8

21. Installation Planning

21.1 Overview 21-1

21.2 Responsibilities 21-1

21.3 Process Description 21-1

21.4 Maintenance of Hardware Diagrams 21-2

22. COTS Training

22.1 Requesting COTS Training 22-1

22.2 Coordinating COTS Training 22-2

22.3 Canceling/Rescheduling COTS Training 22-3

22.4 Contractor COTS Training Funds Accounting 22-3

23. Inventory Logistical Management (ILM)

23.1 ILM [Inventory, Logistics and Maintenance (ILM) Manager] 23-1

23.2 Remedy User Tool Overview 23-6

23.2.1 Navigating Remedy User Tool 23-6

23.2.2 Defining Search Criteria 23-8

23.2.3 ILM Predefined Reports 23-12

23.3 Property Management 23-13

23.3.1 ILM-EIN GUI 23-13

23.3.2 ILM-EIN Structure GUI 23-42

23.3.3 ILM-EIN Transaction GUI 23-43

23.3.4 ILM-Transaction Log 23-60

23.3.5 ILM-OEM Parts 23-64

23.3.6 ILM-Vendor-MFR GUI 23-65

23.3.7 ILM-HwSw Codes GUI 23-67

23.3.8 ILM-Status Codes GUI 23-68

23.3.9 ILM-Maint Contract GUI 23-69

23.3.10 ILM-Sites GUI 23-74

23.3.11 ILM-Inventory Location GUI 23-75

23.4 Maintenance Management 23-76
23.4.1 ILM-MWO GUI 23-76
23.4.2 ILM-MWO Line Item GUI 23-88
23.5 License Management 23-100
23.5.1 ILM-License Products GUI 23-101
23.5.2 ILM-License Entitlement GUI 23-103
23.5.3 ILM-License GUI 23-110
23.5.4 ILM-License Mapping GUI 23-121
23.5.5 ILM-Additional Host GUI 23-123
23.6 System Administrator Functions 23-124
23.6.1 ILM-System Parameters 23-124
23.6.2 User GUI 23-126
23.6.3 Remedy's Admin Tool GUI 23-128
23.6.4 Databases 23-130
23.6.5 Special Constraints 23-130
23.6.6 Event and Error Messages 23-130

24. Maintenance of Configuration Parameters

24.1 Parameter Change Control Procedure 24-1
24.2 Overview of Configuration Parameter Files 24-2
24.3 Overview of Configuration Registry 24-2
24.3.1 Registry Deployment and Baseline Maintenance 24-3
24.3.2 How to Run a Mkcfg 24-4
24.3.3 Registry 24-4
24.3.4 How to Apply a Registry Patch 24-4
24.3.5 How to Run the Registry Population Tool 24-4
24.4 Configuration Registry Procedures 24-6
24.4.1 Registry Preparation Procedure 24-6
24.4.2 Registry Database Backup Procedure 24-7
24.4.3 Registry Patch Procedure 24-7
24.4.4 Display Parameters Using the Configuration Registry GUI 24-8

List of Figures

Figure 3.8-1. ECS Whazzup Initial Display 3-13
Figure 3.8-2. Host Status Pop-Up Display 3-14
Figure 3.8-3. Host Status Data Display 3-15
Figure 3.8-4. Mode Status Pop-Up Display 3-15
Figure 3.8-5. Mode Status Data Display 3-16
Figure 3.8-6. Verify Mode Pop-Up Display 3-16
Figure 3.8-7. Verify Mode Data Display 3-17
Figure 3.8-8. Performance Management Selection Display 3-17
Figure 3.8-9. Performance Management Data Display 3-18
Figure 3.9-1. ECS Assistant GUI Manager Windows 3-19
Figure 3.11-1. Networker Backup Window 3-28
Figure 3.11-2. Networker Recovery Window 3-31
Figure 3.12-1. /etc/passwd File Fields 3-35
Figure 3.12-2. /etc/group File 3-36
Figure 3.12-3. Access Permissions 3-40
Figure 4.1-1. Earth Science Information Model 4-2
Figure 4.1-2. An Example of Data Product Levels 4-3
Figure 4.2-1. Sybase Central 4-12
Figure 4.5-1. Example of an add_devices.sql File for Creation of a Database Device 4-22
Figure 4.7-1. Example of sp_conOutput 4-28
Figure 4.7-2. Configuration Registry 4-31
Figure 4.7-3. Configuration Registry Attributes Pop-Up Window 4-32
Figure 4.8-1. Example of Creation of a Database Segment Template File 4-36
Figure 4.9-1. Sample template.sql File for Creation of a Database 4-44
Figure 4.9-2. Completed Create Database Script 4-45
Figure 4.10-1. Sample template.sql File for New Database User Login 4-50

Figure 7.2-1. Big Brother Home Page 7-1
Figure 7.2-2. Big Brother Toolbar 7-2
Figure 7.3-1. ECS Whazzup Initial Display 7-5
Figure 8.3-1. Login to TestTrack Web Page 8-7
Figure 8.3-2. Login to TestTrack Web Project Page 8-8
Figure 8.3-3. Work with Trouble Tickets Web Page 8-8
Figure 8.3-4. Add TestTrack Server GUI 8-9
Figure 8.3-5. TestTrack Studio Login GUI 8-10
Figure 8.3-6. TestTrack Project Selection GUI 8-10
Figure 8.3-7. Trouble Tickets List GUI 8-11
Figure 8.3-8. Add Trouble Ticket Web Page (1 of 2) 8-14
Figure 8.3-9. Add Trouble Ticket Web Page (2 of 2) 8-14
Figure 8.3-10. Add Trouble Ticket GUI (1 of 3) 8-16
Figure 8.3-11. Add Trouble Ticket GUI (2 of 3) 8-17
Figure 8.3-12. Add Trouble Ticket GUI (3 of 3) 8-18
Figure 8.3-13. Find Trouble Tickets Web Page 8-20
Figure 8.3-14. Advanced Find Web Page 8-21
Figure 8.3-15. Find Trouble Ticket GUI 8-22
Figure 8.3-16. Find Trouble Ticket GUI 8-22
Figure 8.3-17. Advanced Find GUI 8-23
Figure 8.3-18. Edit Trouble Ticket Web Page 8-24
Figure 8.3-19. Assign Web Page 8-25
Figure 8.3-20. Assign GUI 8-26
Figure 8.3-21. Fix Event’s Web Page 8-29
Figure 8.3-22. Fix Event’s GUI 8-30
Figure 8.3-23. Escalate Page 8-31
Figure 8.3-24. Escalate GUI 8-32
Figure 8.3-25. Work with NCRs Web Page 8-34

Figure 8.3-26. Edit NCR Web Page 8-35
Figure 8.3-27. Open Web Page 8-36
Figure 8.3-28. Operations_NCRs GUI 8-37
Figure 8.3-29. Edit NCRs GUI 8-38
Figure 8.3-30. Open GUI 8-38
Figure 8.3-31. Close Page 8-40
Figure 8.3-32. Close GUI 8-41
Figure 8.3-33. License Server Admin Utility GUI 8-42
Figure 8.3-34. Global Users GUI 8-43
Figure 8.3-35. Add User GUI 8-43
Figure 8.3-36. Add User GUI (Security tab) 8-44
Figure 8.3-37. Add User GUI (Licenses tab) 8-45
Figure 8.3-38. Add User GUI (Address tab) 8-46
Figure 8.3-39. Users Web Page 8-48
Figure 8.3-40. Retrieve Global User GUI 8-49
Figure 8.3-41. Edit Users Web Page 8-50
Figure 8.3-42. Users GUI 8-51
Figure 8.3-43. Retrieve Global User GUI 8-51
Figure 8.3-44. Edit User GUI 8-52
Figure 8.3-45. Project Configuration Web Page 8-54
Figure 8.3-46. Configure Automation Rules Web Page 8-55
Figure 8.3-47. Add Notification Rule (Precondition tab) Web Page 8-55
Figure 8.3-48. Add Notification Rule (Trigger When tab) Web Page 8-56
Figure 8.3-49. Add Notification Rule (Actions tab) Web Page 8-57
Figure 8.3-50. Add Rule Action Web Page 8-58
Figure 8.3-51. User Options Web Page 8-59
Figure 8.3-52. Add Notification Rule (Precondition Tab) Web Page 8-60
Figure 8.3-53. Add Notification Rule (Trigger When Tab) Web Page 8-61

Figure 8.3-54. Add Notification Rule (Actions Tab) Web Page 8-61
Figure 8.3-55. Work with Trouble Tickets Web Page 8-62
Figure 8.3-56. Work with Trouble Tickets (Detail Tab) Web Page 8-63
Figure 8.3-57. Edit Trouble Ticket (Email Tab) Web Page 8-64
Figure 8.3-58. Configure Automations Rules GUI 8-65
Figure 8.3-59. Add Notification Rule (Precondition Tab) GUI 8-65
Figure 8.3-60. Add Notification Rule (Trigger When Tab) GUI 8-66
Figure 8.3-61. Add Notification Rule (Actions Tab) GUI 8-67
Figure 8.3-62. Add Rule Action GUI 8-67
Figure 8.3-63. User Options (Notification Category) GUI 8-68
Figure 8.3-64. Add Notification Rule (Precondition Tab) GUI 8-69
Figure 8.3-65. Add Notification Rule (Trigger When Tab) GUI 8-69
Figure 8.3-66. Add Notification Rule (Actions Tab) GUI 8-70
Figure 8.3-67. Trouble Tickets GUI 8-71
Figure 8.3-68. Edit Trouble Ticket (Email Tab) GUI 8-71
Figure 8.3-69. Reports List GUI 8-73
Figure 8.3-70. Print Options GUI 8-74
Figure 9.2-1. ESDIS Configuration Change Request (CCR) Form 9-4
Figure 9.2-2. EMD Configuration Change Request (CCR) Form 9-5
Figure 9.2-3. TestTrack Pro Workflow of Events 9-7
Figure 9.2-4. EMD CCR Impact Analysis (Part 1) 9-10
Figure 9.2-5. EMD CCR Impact Summary (Part 2) 9-11
Figure 9.2-6. Workflow Diagram for EMD CM Administrator 9-14
Figure 9.2-7. Workflow Diagram for Site-level CM Administrator 9-17
Figure 9.7-1. EMD Baseline Concept from a Design (CIL/CAL) View 9-27
Figure 9.7-2. EMD Baseline Concept from an Operational (Network) View 9-28
Figure 9.7-3. EMD Baseline Concept from an Operational (Subsystem) View 9-28
Figure 9.7-4. Sample EBIS Page 9-32

Figure 10.2-1. Steps in ESDT Development 10-5
Figure 10.4-1. ESDT Descriptor File Transformations in ECS 10-7
Figure 10.4-2. Adding/Updating an ESDT using the ESDT Maintenance GUI 10-8
Figure 10.4-3. Removing an ESDT using the ESDT Maintenance GUI 10-9
Figure 10.4-4. ESDT Maintenance GUI Log-in Screen 10-10
Figure 10.4-5. Installed ESDT Page 10-11
Figure 10.4-6. XML Descriptor Information Page 10-12
Figure 10.4-7. ESDTs to be Installed, Updated, or that Have Failed Page 10-15
Figure 10.4-8. ESDTs Failure Screen 10-16
Figure 11.1-1. BMGT Context diagram 11-2
Figure 11.2-1. BMGT Login Page 11-5
Figure 11.2-2. BMGT Login Page 11-6
Figure 11.2-3. Recent Package Page 11-8
Figure 11.2-4. Package Details Page 11-8
Figure 11.2-5. Failed Package Page 11-10
Figure 11.2-6. Failed Package Page 11-11
Figure 11.2-7. Global Tuning Page 11-15
Figure 12.1-1. Sample Metadata QA Update Request ESDT with Temporal Range 12-6
Figure 12.1-2. Sample Metadata QA Update Request with LGID 12-7
Figure 12.1-3. Sample Metadata QA Update Request with GranuleUR 12-7
Figure 13.1-1. Data Pool Ingest High Level Architecture 13-2
Figure 13.3-1. Data Pool Ingest GUI Home Page 13-7
Figure 13.3-2. General Ingest Status/Resume Button 13-8
Figure 13.3-3. General Ingest Status/Resume Buttons 13-9
Figure 13.3-4. Ingest GUI Login Screen 13-10
Figure 13.3-5. Active Ingest Request List Filter Panel 13-12
Figure 13.3-6. Ingest Request Page 13-14
Figure 13.3-7. Ingest Request Detail Page 13-15

Figure 13.3-8. Cancel Request/Suspend Requests Buttons 13-19
Figure 13.3-9. Change Priority Box 13-20
Figure 13.3-10. Request Detail Page 13-21
Figure 13.3-11. Historical Ingest Requests Page 13-23
Figure 13.3-12. Historical Ingest Requests Detailed Page 13-25
Figure 13.3-13. Provider Status Page 13-28
Figure 13.3-14. Provider Status Detail Page 13-28
Figure 13.3-15. File System Status Page 13-31
Figure 13.3-16. Transfer Host Status Page 13-34
Figure 13.3-17. ECS Services Status Page 13-36
Figure 13.3-18. PDR List Page 13-39
Figure 13.4-1. Open Interventions Page 13-41
Figure 13.4-2. Open Interventions Detail Page 13-44
Figure 13.4-3. Open Interventions Detail Page 13-49
Figure 13.5-1. Provider Configuration Page 13-55
Figure 13.5-2. Edit a Provider Page 13-56
Figure 13.5-3. Existing Polling Location Page 13-57
Figure 13.5-4. Add a Provider Page 13-59
Figure 13.5-5. Data Type Configuration Page 13-63
Figure 13.5-6. Host Configuration Page 13-66
Figure 13.5-7. FTP Host Configuration Add a New Host Page 13-67
Figure 13.5-8. Host Configuration for DAAC Screen 13-69
Figure 13.5-9. Host Configuartion for FTPDEFAULT 13-70
Figure 13.5-10. File System Configuartion 13-71
Figure 13.5-11. ECS Services Configuartion Page 13-75
Figure 13.5-12. ECS Services Configuartion Add Service Host Page 13-77
Figure 13.5-13. Global Tuning Page 13-85
Figure 13.5-14. Volume Groups Configuration (listing page) 13-86

Figure 13.5-15. Volume Group Configuartion Page 13-90
Figure 13.5-16. Volume Group Configuartion Page 13-90
Figure 13.5-17. Add Volume Group Configuartion Page..... 13-91
Figure 13.5-18. Volume Group Configuration: Add Volume Group 13-93
Figure 13.5-19. Operator Configuration Page 13-96
Figure 13.6-1. Detailed Report Layout 13-100
Figure 13.6-2. Request Summary Report Layout 13-100
Figure 13.6-3. Granule Summary Report Layout 13-101
Figure 13.6-4. Group History Page..... 13-103
Figure 13.7-1. Help – General Topics 13-104
Figure 13.8-1. DPM GUI Home Page 13-107
Figure 13.8-2. Collection Group Page 13-109
Figure 13.8-3. List of Collection 13-110
Figure 13.8-4. Detail Information..... 13-112
Figure 13.8-5. Modify Collection Group..... 13-114
Figure 13.8-6. Add Collection Group 13-116
Figure 13.8-7. List of Collections..... 13-117
Figure 13.8-8. Collections Not In Data Pool Page 13-118
Figure 13.8-9. Add New Collection Page..... 13-118
Figure 13.8-10. Modify Collection Page 13-121
Figure 14.4-1. StorNext GUI Home Page..... 14-4
Figure 14.4-2. Admin Pull-Down Menu..... 14-4
Figure 14.4-3. Start/Stop StorNext Page 14-5
Figure 14.5-1. Add Media Page..... 14-10
Figure 14.5-2. Associated Library Page 14-10
Figure 14.5-3. Associated Library Bulk Load Page 14-11
Figure 14.5-4. Complete Add Media Task Page 14-11
Figure 14.5-5. Remove or Move Media Page..... 14-12

Figure 14.5-6. Select Media Screen 14-12
Figure 14.5-7. Complete/Remove Media Task Page 14-12
Figure 14.7-1. StorNext Admin Pull- Down Screen 14-30
Figure 14.7-2. Backup StorNext Screen 14-31
Figure 14.7-3. Complete Backup Screen 14-32
Figure 14.7-4. Feature Schedules Screen 14-33
Figure 14.7-5. Selected Feature Schedules Screen 14-33
Figure 14.9-1. Security Login Prompt 14-41
Figure 14.9-2. DPM GUI Home Page 14-42
Figure 14.9-3. DPM GUI Home Page 14-44
Figure 14.9-4. Data Pool File System Page 14-48
Figure 14.9-5. Add New File System Page 14-49
Figure 14.9-6. Modify File System Information Page 14-51
Figure 14.9-7. Cloud Cover Information Page 14-53
Figure 14.9-8. Add New Cloud Cover Information Page 14-54
Figure 14.9-9. Modify Source Description Page 14-56
Figure 14.9-10. Batch Summary Page 14-58
Figure 14.9-11. List Insert Queue Page 14-59
Figure 14.9-12. Sample DPM GUI Pages for .XML File Path and Content 14-60
Figure 14.9-13. List of Configuration Parameters Page 14-62
Figure 14.9-14. List of Aging Parameters Page 14-68
Figure 14.9-15. Collection Groups Page 14-70
Figure 14.9-16. List of Collection Page 14-71
Figure 14.9-17. Collection Detail Information Page 14-72
Figure 14.9-18. Modify Collection Page 14-76
Figure 14.9-19. Add Collection Group Page 14-76
Figure 14.9-20. Collections Not in Data Pool Page 14-79
Figure 14.9-21. Add New [ECS] Collection Page 14-80

Figure 14.9-22. Modify Collection Page 14-82
Figure 14.9-23. Detailed List of Data Pool Themes Page 14-85
Figure 14.9-24. Add New Theme Page 14-86
Figure 14.9-25. Modify Theme Page 14-88
Figure 14.9-26. Help Page 14-91
Figure 15.1-1. System Context Diagram 15-2
Figure 15.1-2. Order Manager Subsystem (OMS) Context Diagram 15-3
Figure 15.4-1. Security Login Prompt 15-7
Figure 15.4-2. Order Manager Home Page 15-8
Figure 15.6-1. Open Interventions Page – Fields and Options 15-12
Figure 15.6-2. Order Manager GUI Tools: Find (A), Navigation (B), and Refresh (C) 15-12
Figure 15.6-3. Open Interventions Page 15-14
Figure 15.6-4. ECS Order <ID> Details Page 15-15
Figure 15.6-5. Open Intervention For Request <ID> Page 15-15
Figure 15.6-6. Worker Assignment 15-16
Figure 15.6-7. Request Attributes 15-18
Figure 15.6-8. Request Level Disposition 15-19
Figure 15.6-9. Close Confirmation for Intervention (FTP/SCP Push & Hold) 15-20
Figure 15.6-10. Close Confirmation for Intervention <ID> with E-Mail 15-21
Figure 15.6-11. Intervention Closed 15-22
Figure 15.6-12. Open HEG Interventions Page 15-23
Figure 15.6-13. Open HEG Interventions – Fields and Options 15-24
Figure 15.6-14. Open HEG Intervention For Request <ID> Detail Page 15-25
Figure 15.6-15. Open HEG Interventions For Request <ID> Detail – Fields and Options ... 15-26
Figure 15.6-16. Processing Instructions Window 15-27
Figure 15.6-17. Close Confirmation for Intervention <ID> Page 15-29
Figure 15.6-18. Completed Action and Interventions – Fields and Options 15-30
Figure 15.6-19. Completed Action and Interventions Page 15-31

Figure 15.6-20. Distribution Requests Page and Filter Window 15-32
Figure 15.6-21. Distribution Requests Page – Fields and Options 15-33
Figure 15.6-22. Profile for ECSGuest OrderID <ID> 15-35
Figure 15.6-23. Distribution Requests <ID> Profile 15-36
Figure 15.6-24. FtpPush/SCP (A) and Staging (B) Distribution Requests Filters 15-39
Figure 15.6-25. Processing Services Requests Page and Filter 15-41
Figure 15.6-26. Operator Alerts Page (A) and Alert Details Page (B-C) 15-42
Figure 15.6-27. Operator Alerts Page – Fields and Options 15-43
Figure 15.7-1. Suspended Destinations Monitor (A) and Ftp Push Monitor-Suspended Configured Destination (B) Pages 15-46
Figure 15.8-1. Historical Distribution Requests Page (A) and Filter (B) 15-49
Figure 15.8-2. Historical Distribution Requests Page – Fields and Options 15-50
Figure 15.8-3. Historical Processing Requests Page (A) and Filter (B) 15-51
Figure 15.8-4. Historical Processing Requests Page – Fields and Options 15-52
Figure 15.9-1. OM Queue Status Page 15-54
Figure 15.9-2. HEG Order Status Page 15-56
Figure 15.9-3. Staging Status Pages and Table (Fields) 15-57
Figure 15.9-4. Pending HEG Granules Page (Frame A) and Tables (Frames 1-2) 15-59
Figure 15.9-5. Data Pool File System Status Page 15-61
Figure 15.10-1. Aging Parameters Page 15-64
Figure 15.10-2. OMS Server and Database Configuration Page 15-66
Figure 15.10-3. OM Server/Database Configuration - Parameters 15-68
Figure 15.10-4. Media Configuration Page 15-69
Figure 15.10-5. Media Creation Configuration Page 15-72
Figure 15.10-6. ODL Metadata File Users Configuration Page 15-74
Figure 15.10-7. External Processing Services Policy Configuration Page 15-75
Figure 15.10-8. FtpPush/SCP Policy Configuration Page 15-77
Figure 15.10-9. FtpPush/SCP Policy Configuration Page – Fields and Options 15-78
Figure 15.10-10. Context-Sensitive Help for Retry Interval Parameter 15-79

Figure 15.11-1. Help Page (A) and HelpOnDemand Example (B) 15-82
Figure 15.12-1. Media Creation Console Page 15-84
Figure 15.12-2. PMD Disk and Tape – Activity List 15-85
Figure 15.12-3. Activate QC Dialog Box 15-87
Figure 15.12-4. Activate (A, A1); Annotate (B); Fail (C) Requests Dialog Boxes 15-88
Figure 15.12-5. Confirm Package Assembled for RequestID Dialog Box 15-89
Figure 15.12-6. Media Collection Complete Page 15-91
Figure 15.12-7. Fail Media Collection Page 15-93
Figure 15.12-8. Mark Request Shipped Page 15-96
Figure 15.12-9. Confirm Package Assembled Page 15-98
Figure 15.12-10. Package Not Assembled Page 15-100
Figure 15.12-11. Print Outputs Page 15-102
Figure 15.12-12. PMD Device Configuration Page 15-105
Figure 15.12-13. PMD Device Details Page 15-107
Figure 15.12-14. Frames B-B3 Add New Device Pages 15-109
Figure 15.12-15. Open Physical Media Interventions Page (A) and Bulk Action (B) 15-110
Figure 15.12-16. Open PM Interventions Page – Fields and Options 15-111
Figure 15.12-17. Open PM Interventions For Request ID Details (A), Order ID Details (B), and Filters (C) 15-113
Figure 15.12-18. Granule List for Volume <VolNumber> of Request <ID> 15-114
Figure 15.12-19. PMD Printer Configuration Page 15-117
Figure 15.12-20. PMD Production Module Configuration Page 15-119
Figure 15.12-21. PMD Report Summary Page 15-121
Figure 15.12-22. PMD Compressed Format ESDTs Page 15-123
Figure 15.13-1. OM GUI Log Viewer Page 15-125
Figure 15.14-1. OMS Configuration CI Main Menu 15-136
Figure 15.14-2. Configure Order Tracking Data Menu 15-138
Figure 16.1-1. Spatial Subscription Server GUI Home Page 16-4
Figure 16.1-2. List Events Page 16-5

Figure 16.1-3. Manage Subscription 16-7
Figure 16.1-4. Update Subscription 16-9
Figure 16.1-5. Add Subscription 16-14
Figure 16.1-6. String Qualifiers 16-15
Figure 16.1-7. Subscription Qualifier 16-16
Figure 16.1-8. List Themes Request Page 16-19
Figure 16.1-9. Spatial Subscription Server GUI Theme List Page 16-20
Figure 16.1-10. List Subscriptions for Theme page 16-21
Figure 16.1-11. Manage Bundling Orders Page 16-23
Figure 16.1-12. Manage Bundling Orders Page 16-24
Figure 16.1-13. Add Bundling Order Detail Page 16-27
Figure 16.1-14. Update Bundling Order Page 1 16-29
Figure 16.1-15. Update Bundling Order Page 2 16-30
Figure 16.1-16. Configure Completion Criteria Default Values Page 16-31
Figure 16.1-17. Configure Completion Criteria Default Values Page 16-33
Figure 16.1-18. List Failed Action Page 16-34
Figure 16.1-19. List Statistic Page 16-35
Figure 17-1. The EDHS Home Page, the EMD Baseline Information Home Page, and the Systems Monitoring Center Home Page 17-1
Figure 20.3-1. EMD Property Tags (Actual Size) 20-4
Figure 23.2.1-1. Open GUI 23-6
Figure 23.2.2.1-1. Search by Example 23-8
Figure 23.2.2.2-1. Using the Advanced Search Bar 23-10
Figure 23.3.1-1. ILM-EIN (Part Info and Location & Purchasing Info) GUI 23-14
Figure 23.3.1-2. ILM-EIN (Maintenance & Other Info.) GUI 23-15
Figure 23.3.1-3. ILM-EIN (Components) GUI 23-16
Figure 23.3.1-4. ILM-EIN (Maintenance Contract) GUI 23-17
Figure 23.3.1-5. ILM-EIN (History) GUI 23-18
Figure 23.3.1.1-1. ILM-EIN Reports GUI 23-23

Figure 23.3.1.1-2. ILM-DIA Reports GUI 23-29
Figure 23.3.1.1-3. Report To File GUI 23-29
Figure 23.3.1.1-4. Text Import Wizard GUI 23-30
Figure 23.3.1.1-5. Enter Parameter Values GUI 23-30
Figure 23.3.1.1-6. Install/Receipt Report GUI 23-31
Figure 23.3.1.1-7. Installation Report GUI 23-32
Figure 23.3.1.1-8. Purchase Order Cost Report GUI 23-33
Figure 23.3.1.1-9. Parent EIN Report GUI 23-34
Figure 23.3.1.1-10. Parent EIN & Total System Cost Report GUI 23-35
Figure 23.3.1.1-11. Inventory Report GUI 23-37
Figure 23.3.1.1-12. Quarterly Property Management Report GUI 23-38
Figure 23.3.1.1-13. Cost – Selected ECS Managed Report GUI 23-39
Figure 23.3.1.1-14. EIN Transaction History Report 23-40
Figure 23.3.1.1-15. Spare Equipment Report GUI 23-41
Figure 23.3.2-1. ILM-EIN Structure GUI 23-42
Figure 23.3.3-1. ILM-EIN Transaction GUI (Install/Move/Ship/RTS) 23-44
Figure 23.3.3-2. ILM-EIN Transaction GUI (Relocation) 23-45
Figure 23.3.3-3. ILM-EIN Transaction GUI (Archive) 23-46
Figure 23.3.3-4. ILM-TRS Dialog GUI 23-57
Figure 23.3.3.1-1. ILM-Process Component GUI 23-58
Figure 23.3.4-1. ILM-Transaction Log GUI 23-60
Figure 23.3.4-2. ECS Shipping Report GUI 23-63
Figure 23.3.5-1. ILM-OEM Parts GUI 23-64
Figure 23.3.6-1. ILM-Vendor-MFR GUI 23-66
Figure 23.3.7-1. ILM-HwSw Codes GUI 23-67
Figure 23.3.8-1. ILM-Status Codes GUI 23-68
Figure 23.3.9-1. ILM-Maint Contract GUI (1 of 3) 23-69
Figure 23.3.9-2. ILM-Maint Contract GUI (2 of 3) 23-70

Figure 23.3.9-3. ILM-Maint Contract GUI (3 of 3) 23-71
Figure 23.3.9-4. Maintenance Contract Report GUI 23-73
Figure 23.3.10-1. ILM-Sites GUI 23-74
Figure 23.3.11-1. ILM-Inventory Location GUI 23-75
Figure 23.4.1-1. ILM-MWO GUI – Parent Information 23-77
Figure 23.4.1-2. ILM-MWO GUI - Failure and Vendor Contact 23-78
Figure 23.4.1-3. ILM-MWO GUI – ALDT 23-79
Figure 23.4.1-4. ILM-MWO GUI - Total Down Time 23-80
Figure 23.4.1-5. ILM-MWO GUI - Failed & Replacement Components 23-81
Figure 23.4.1-6. Work Order Verification Report GUI 23-86
Figure 23.4.1-7. RMA Report GUI 23-87
Figure 23.4.2-1. ILM-MWO Line Item GUI (1 of 3) 23-88
Figure 23.4.2-2. ILM-MWO Line Item GUI (2 of 3) 23-89
Figure 23.4.2-3. ILM-MWO Line Item GUI (3 of 3) 23-90
Figure 23.5.1-1. ILM-License Products GUI 23-102
Figure 23.5.2-1. ILM-License Entitlement GUI (1 of 3) 23-104
Figure 23.5.2-2. ILM-License Entitlement GUI (2 of 3) 23-105
Figure 23.5.2-3. ILM-License Entitlement GUI (3 of 3) 23-106
Figure 23.5.2-4. License Entitlement Status Report GUI 23-109
Figure 23.5.3-1. ILM-License GUI (1 of 4) 23-110
Figure 23.5.3-2. ILM-License GUI (2 of 4) 23-111
Figure 23.5.3-3. ILM-License GUI (3 of 4) 23-112
Figure 23.5.3-4. ILM-License GUI (4 of 4) 23-113
Figure 23.5.3-5. ILM-DIA-Lic Report GUI 23-118
Figure 23.5.3-6. License Allocation By Host Report GUI 23-119
Figure 23.5.3-7. License Allocation By Product Report GUI 23-120
Figure 23.5.4-1. ILM-License Mapping GUI 23-121
Figure 23.5.5-1. ILM-Additional Host GUI 23-123

Figure 23.6.1-1. ILM-System Parameters GUI 23-125
Figure 23.6.2-1. User GUI 23-127
Figure 23.6.3-1. Admin Tool GUI 23-129

List of Tables

Table 3.3-1. SSH - Activity Checklist 3-2
Table 3.6-1. Login to System Hosts - Activity Checklist 3-4
Table 3.7-1. System Startup and Shutdown - Activity Checklist 3-6
Table 3.8-1. Whazzup?? - Activity Checklist 3-12
Table 3.9-1. ECS Assistant - Activity Checklist 3-18
Table 3.10-1. Tape Operations - Activity Checklist 3-20
Table 3.11-1. System Backup and Restores - Activity Checklist 3-27
Table 3.12-1. User Administration - Activity Checklist 3-33
Table 3.14-1. Security - Activity Checklist 3-44
Table 4.1-1. Data Product Level Definitions 4-3
Table 4.1-2. Subsystem Functions 4-4
Table 4.1-3. Custom Databases 4-5
Table 4.1-4. Flat Files 4-7
Table 4.1-5. Resident Databases 4-8
Table 4.1-6. Location of Principal Database Components 4-8
Table 4.2-1. Sybase Adaptive Server Enterprise (ASE) Components 4-11
Table 4.3-1. DBA Tasks Performed on a Regular Basis 4-14
Table 4.4-1. Starting and Stopping Database Servers - Activity Checklist 4-15
Table 4.5-1. Creating Database Devices - Activity Checklist 4-20
Table 4.6-1. Installing Databases and Patches - Activity Checklist 4-23
Table 4.7-1. Configuring Databases - Activity Checklist 4-25
Table 4.8-1. Working with Indexes, Segments, and Caches - Activity Checklist 4-33
Table 4.9-1. Backing Up and Recovering Data - Activity Checklist 4-37

Table 4.9-2. Automatic Backup Files 4-38
Table 4.9-3. Files That Need to Be Modified before Running Scripts 4-39
Table 4.9-4. Automatic Backup Components 4-40
Table 4.10-1. Roles and Privileges 4-46
Table 4.10-2. Establishing Database Security - Activity Checklist 4-47
Table 4.12-1. Bulk Copying - Activity Checklist 4-53
Table 4.14-1. Tuning Options 4-56
Table 4.16-1. Sybase Troubleshooting - Activity Checklist 4-57
Table 5.2-1. Crack - Activity Checklist 5-2
Table 5.2-2. ANLpasswd - Activity Checklist 5-8
Table 5.4-1. Secure Access through Secure Shell - Activity Checklist 5-12
Table 6.7-1. Network Security - Activity Checklist 6-4
Table 7.2-1. Common Functions Performed by Big Brother 7-2
Table 7.2-2. Color Codes by Order of Severity 7-3
Table 7.3-1. Monitoring and Managing Server Applications - Activity Checklist 7-4
Table 8.3-1. Trouble Ticket System - Task Checklist 8-5
Table 8.3-2. Trouble Ticket Priority/NCR Severity 8-6
Table 8.3-3. TTPro Trouble Tickets Field Descriptions 8-11
Table 8.3-4. TTPro Tab Descriptions 8-13
Table 8.3-5. Workflow Events and Corresponding Lifecycle States 8-28
Table 8.3-6. Trouble Ticket Security Groups 8-47
Table 8.3-7. Sample Reports in TestTrack Pro 8-72
Table 8.4-1. Example of Emergency Change Procedure 8-76
Table 9.2-1. State Table Composition in TestTrack Pro Format 9-6
Table 11.1-1. BMGT - Activity Checklist 11-3
Table 11.2-1. BMGT Configuration/Global Parameters 11-12
Table 11.3-1. Manual Export Command Line Arguments 11-16
Table 12.1-1. Using the QA Update Tool - Activity Checklist 12-1

Table 12.1-2 Configuration File Parameters for QA Update Utility 12-3
Table 13.2-1. Login to System Hosts - Activity Checklist 13-3
Table 13.3-1. Monitoring DPL Ingest 13-6
Table 13.3-2. Home Page Field Descriptions 13-8
Table 13.3-3. Request Status Page Column Descriptions 13-11
Table 13.3-4. Ingest Request Status Allowed Actions 13-11
Table 13.4-1. Interventions & Alerts 13-40
Table 13.5-1. Modifying DPL Ingest Configuration 13-53
Table 13.5-2. Edit a Data Provider Configuration Parameter Descriptions 13-54
Table 13.5-3. Polling Location Page Field Descriptions 13-57
Table 13.5-4. Data Type Configuration Page Field Descriptions 13-62
Table 13.5-5. SCP/FTP Host Page Field Descriptions 13-65
Table 13.5-6. Archive File Systems Configuration Page Field Descriptions 13-71
Table 13.5-7. ECS Services Configuration Field Description 13-73
Table 13.5-8. ECS Services Configurable Field Descriptions 13-73
Table 13.5-9. Global Tuning Parameter Descriptions 13-81
Table 13.5-10. Volume Groups Configuration Page Field Descriptions 13-87
Table 13.5-11. Add Volume Group Page Field Description 13-87
Table 13.5-12. Volume Group Naming 13-89
Table 13.6-1. Reports 13-99
Table 13.6-2. Volume Groups History Page Field Description 13-102
Table 13.8-1. Data Pool Maintenance 13-105
Table 14.4-1. Starting and Stopping StorNext 14-3
Table 14.5-1. Loading and Removing Archive Media - Activity Checklist 14-8
Table 14.6-1. Deleting Granules - Activity Checklist 14-17
Table 14.6.1-1. Command Line Parameters of the EcDsBulkSearch.pl 14-17
Table 14.6.2-1. Command Line Parameters for EcDsBulkDelete.pl 14-21
Table 14.6.3-1. Command Line Parameters for EcDsBulkUndelete.pl 14-24

Table 14.6.4-1. Command Line Parameters for EcDsDeletionCleanup 14-26
Table 14.7-1. StorNext Backup Procedures - Activity Checklist 14-30
Table 14.8-1. ACSLS Command Reference 14-34
Table 14.8-2. ACSLS Utilities 14-35
Table 14.8-3. ACSLS Procedures - Activity Checklist 14-35
Table 14.9-1. Data Pool Maintenance Tasks - Activity Checklist 14-40
Table 14.10-1. Data Pool Scripts - Activity Checklist 14-93
Table 14.10-2. Command Line Parameters 14-99
Table 15.3-1. OM GUI Operator Security Capabilities 15-6
Table 15.4-1. Launch Order Manager GUI - Activity Checklist 15-7
Table 15.5-1. Operator GUI Security Capabilities 15-9
Table 15.6-1. Request Management - Activity Checklist 15-10
Table 15.7-1. Destination Monitor - Activity Checklist 15-44
Table 15.8-1. Archive Data - Activity Checklist 15-49
Table 15.9-1. OM Status Pages - Activity Checklist 15-53
Table 15.10-1. OM Configuration - Activity Checklist 15-62
Table 15.10-2. External Processing Services Parameters 15-76
Table 15.12-1. Physical Media Distribution - Activity Checklist 15-83
Table 15.13-1. OM GUI Log Viewer - Activity Checklist 15-124
Table 15.14-1. Using Order Manager Command Line Utility - Activity Checklist 15-127
Table 15.14-2. Command Line Parameters of the SCLI Tool 15-143
Table 15.17-1. Troubleshooting Order Manager - Activity Checklist 15-152
Table 15.17-2. Order Manager GUI User Messages 15-153
Table 15.17-3. Recovering from Order Manager Failures 15-167
Table 15.17-4. Troubleshooting HEG Problems 15-175
Table 16.1-1. Spatial Subscription Server GUI - Activity Checklist 16-1
Table 18.4-1. DAAC Hardware Problem Reporting Procedures 18-4
Table 18.4-2. Hardware Corrective Maintenance Actions 18-5

Table 18.4-3. Obtaining On-Site Hardware Maintenance Support 18-6

Table 18.4-4. Procedure for Return to Depot (Advance Replacement and Return before Replacement) 18-8

Table 18.6-1. Procedure for Time and Material Support..... 18-9

Table 19.2-1. COTS Maintenance - Activity Outline..... 19-2

Table 20.1-1. Procedure for the Receipt of Property 20-2

Table 20.1-2. Procedure for Completion of the Inventory Worksheet 20-2

Table 20.1-3. Procedure for Completion of the Non Conforming Product Report 20-3

Table 20.1-4. Receiving Process Checklist 20-3

Table 20.2-1. LMC Actions for Property Received from the ILS Property Administrator..... 20-4

Table 21.3-1. Installation Planning Activity Outline..... 21-2

Table 22.1-1. COTS Training - Activity Checklist 22-1

Table 23.1-1. Common Operator Functions Performed with ILM..... 23-2

Table 23.1-2. Remedy-ILM Groups Description..... 23-3

Table 23.2.2.1-1. Relational Operators Used in the Query Window..... 23-9

Table 23.2.2.2-1. Operators Used in the Advanced Search Bar 23-11

Table 23.2.2.2-2. Wildcard Symbols 23-11

Table 23.2.2.2-3. Using Keywords 23-12

Table 23.2.3-1. ILM Pre-Defined Reports..... 23-12

Table 23.3.1-1. ILM-EIN Form Field Description 23-19

Table 23.3.1-2. Add New Inventory Item..... 23-21

Table 23.3.1-3. Modifying EIN Record..... 23-22

Table 23.3.1.1-1. ILM-EIN Pre-Defined Reports..... 23-24

Table 23.3.1.1-2. Procedures to Generate ILM-EIN Predefined Reports..... 23-25

Table 23.3.2-1. ILM-EIN Structure Field Descriptions..... 23-43

Table 23.3.3-1. ILM-EIN Transaction Form Field Descriptions..... 23-47

Table 23.3.3-2. Procedures to Perform EIN Transactions..... 23-49

Table 23.3.3.1-1. ILM-Component to Process Field Descriptions..... 23-59

Table 23.3.4-1. ILM-Transactions Field Descriptions 23-61

Table 23.3.4-2. Procedures to Generate EIN Shipment Report 23-62
Table 23.3.5-1. ILM-OEM Parts Field Descriptions 23-65
Table 23.3.6-1. ILM-Vendor-MFR Field Descriptions 23-67
Table 23.3.7-1. ILM-HwSw Codes Field Descriptions 23-68
Table 23.3.8-1. ILM-Status Codes Field Descriptions 23-69
Table 23.3.9-1. ILM-Maint Contract Field Descriptions 23-72
Table 23.3.9-2. Procedures to Generate Maintenance Contract Report 23-72
Table 23.3.10-1. ILM-Sites Field Descriptions 23-74
Table 23.3.11-1. ILM-Inventory Location Field Descriptions 23-76
Table 23.4.1-1. ILM-MWO Field Descriptions 23-82
Table 23.4.1-2. Procedure to Add a New Work Order 23-84
Table 23.4.1-3. Procedures to Generate ILM-MWO Predefined Reports 23-85
Table 23.4.2-1. ILM-MWO Line Item Field Descriptions 23-91
Table 23.4.2-2. Effects on Property Records by MWO Line Item Processing 23-93
Table 23.4.2-3. Procedure to Add Work Order Line Items 23-97
Table 23.5.1-1. ILM-License Products Field Descriptions 23-103
Table 23.5.2-1. ILM-Entitlement Field Descriptions 23-107
Table 23.5.2-2. Procedure to Add New License Entitlement 23-108
Table 23.5.2-3. Procedures to Generate ILM-License Entitlement Predefined Reports 23-109
Table 23.5.3-1. ILM-License Field Descriptions 23-114
Table 23.5.3-2. Procedure to Add New License and Allocate It to a Machine 23-115
Table 23.5.3-3. Procedures to Generate ILM-License Predefined Reports 23-117
Table 23.5.4-1. ILM-License Mapping Field Descriptions 23-122
Table 23.5.5-1. ILM-Additional Host Field Descriptions 23-124
Table 23.6.1-1. ILM-System Parameters Field Descriptions 23-126
Table 23.6.2-1. User Form Field Descriptions 23-128
Table 23.6.3-1. Admin Tool GUI, Workflow Object Descriptions 23-129

Table 23.6.6-1. Non System-Failure Related Error Messages 23-130
Table 24.4-1. Configuration Registry - Activity Checklist 24-6

Abbreviations and Acronyms

This page intentionally left blank.

1. Introduction

This document, Release 7.21 Mission Operation Procedures for the Earth Observing System Data and Information System (EOSDIS) Maintenance and Development (EMD) Project, provides procedures to configure, maintain and operate the EOSDIS Core System (ECS).

1.1 Identification

This document meets the milestone specified as Contract Data Requirements List (CDRL) Item 23, under contract NAS5-03098. It reflects the system as delivered at Release 7.21.

1.2 Scope

The scope of this document is directed to Distributed Active Archive Center (DAAC) operations activities to support the Release 7.21 ECS system. Both procedures and instructions are identified. Operations procedures are defined as the step-by-step commands or on-line procedures needed to perform a function. The Operations Instructions are the off-line procedures or directives for performing administrative, operations, management, or operations support activities (e.g., Configuration Management, Problem Management, or Quality Assurance).

1.2.1 On-Site Procedures Tailoring Guide

Each DAAC may modify these procedures and instructions to accommodate site-specific operations requirements. Such documentation should be versioned and dated in MS Word format with a master copy forwarded to the following address:

EMD Training
The EMD Project Office
Raytheon Company
5700 Rivertech Court
Riverdale, MD 20737

For specifics on authoring, formatting, importing, exporting and maintenance of procedures and instructions see Chapter 20, Library Administration.

1.3 Purpose

The purpose of this document is to identify the procedures and instructions to operate and maintain Release 7.21 systems. In addition, DAAC staff responsibilities are identified. The DAAC operations staff is comprised of operators, engineers, as well as operations support, administration and management staff personnel.

This document will also be used as a training aid for operations staff who are located at the sites. The operations procedures and operations instructions were derived from, and are intended to be

consistent with, the system functions and capabilities specified in the system design specifications.

1.4 Status and Schedule

This document is to be delivered on an annual basis. Updates are made to reflect new system releases. Changes are submitted through established configuration management procedures, such as configuration change requests or published revisions known as interim updates published to the web site at http://edhs1.gsfc.nasa.gov/ at an "Interim Updates" link on the abstract page for this document (611-EMD-200).

1.5 Organization

The contents subsequent to this first section are presented as follows:

- Section 2 **Related Documentation.** Lists documents that drive, support or expand on the material in this manual.
- Section 3 **System Administration.** Identifies the operations procedures and/or operations instructions for system administration activities, such as backup and restore, log maintenance, user account administration, and workstation installation.
- Section 4 **Database Administration.** Identifies the operations procedures and/or operations instructions for database administration activities, such as product installation, disk storage management, login and privileges administration, database validation, backup and recovery, database configuration, tuning and performance monitoring.
- Section 5 **Security Services.** Identifies the operations procedures and/or operations instructions for security services activities, such as user authentication and authorization, data access control, network services monitoring, password protection, file modification monitoring.
- Section 6 **Network Administration.** Identifies the operations procedures and/or operations instructions for network administration activities, such as network and system configuration monitoring, and network services monitoring.
- Section 7 **System Monitoring.** Identifies the operations procedures and/or operations instructions for network system monitoring, such as problem monitoring and resolution.
- Section 8 **Problem Management.** Identifies the operations procedures and/or operations instructions for submitting, processing and resolving Trouble Tickets.

- Section 9 **Configuration Management.** Identifies the operations procedures and/or operations instructions for configuration management activities, such as Configuration Control Board (CCB) support, configuration item identification, submission and processing of configuration change requests (CCRs), configuration status accounting, configuration audits, data management, operational database maintenance, software transfer and installation.
- Section 10 **Metadata Administration.** Identifies the operations procedures and/or operations instructions for metadata administration activities, such as establishing collections, populating the database, and specifying Earth Science Data Type (ESDT) services.
- Section 11 **Bulk Metadata Generation Tool.** Identifies the Bulk Metadata Generation Tool (BMGT) procedures established to support the generating of the external representation of the ECS metadata holdings.
- Section 12 **Quality Assurance.** Identifies the operations procedures and/or operations instructions to perform DAAC manual non-science quality assurance activities, such as visualization of science data products and updating quality assurance metadata.
- Section 13 **Data Pool Ingest.** Identifies the operations procedures and/or operations instructions to support data acquisition.
- Section 14 **Archive Procedures.** Identifies the operations procedures and/or operations instructions for archiving activities, such as archive repository maintenance, fault monitoring and notification, and temporary data storage.
- Section 15 **Data Distribution.** Identifies the operations procedures and/or operations instructions to support data distribution activities, such as media operations and product shipment.
- Section 16 **User Services.** Identifies the operations procedures and/or operations instructions to support user services activities to address user requests for data.
- Section 17 **Library Administration.** Identifies the operations procedures and/or operations instructions to support librarian administration activities, such as change package preparation and distribution, master document control and maintenance.
- Section 18 **COTS Hardware Maintenance.** Identifies the operations procedures and/or operations instructions for preventive and corrective maintenance activities of commercial off-the-shelf (COTS) hardware for the EMD project.

- Section 19 **Software Maintenance.** Identifies the operations procedures and/or operations instructions to support maintenance activities for COTS software, custom software, and science software.

- Section 20 **Property Management.** Identifies the operations procedures and/or operations instructions for the receipt, control, and accountability of EMD property at all affected sites.

- Section 21 **Installation Planning.** Identifies the operations procedures and/or operations instructions to support installation planning activities for conducting site surveys, ensuring that site preparations/coordination are completed on schedule, facilitating receipt and installation of the hardware.

- Section 22 **COTS Training.** Identifies the operations procedures and/or operations instructions to support COTS training activities, such as training request processing, training coordination, training scheduling, and training record maintenance.

- Section 23 **Inventory Logistical Management (ILM).** ILM helps the operations staff at the DAACs, EOC, and SMC to maintain records that describe all inventory components and their assembly structures and interdependencies. The database maintained by this tool keeps chronological histories (a record of the transactions) of receipt, installation, and relocation of inventory items. There is a license management section and general updates to work order processes, forms, and report formats.

- Section 24 **Maintenance of Configuration Parameters**. These procedures describe the overall maintenance of the system configuration parameters baseline for custom software and hardware, including patches, database, operating systems, COTS software, and networks.

- **Abbreviations and Acronyms.** Identifies abbreviations and acronyms used throughout this document.

2. Related Documentation

2.1 Parent Documents

The parent documents are the documents from which the Mission Operation Procedures' scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-46-03	EMD Task 201 Statement of Work for ECS SDPS Maintenance
423-46-02	Contract Data Requirements Document for EMD Task 201 ECS SDPS Maintenance

2.2 Applicable Documents

The following documents are referenced within the Mission Operation Procedures document, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume.

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS F&PRS)
423-46-01	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) Science Data Processing System (EMD F&PRS)

2.3 Information Documents

2.3.1 Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the Mission Operation Procedures for the EMD Project.

105-EMD-001	Property Management Plan for the EMD Project
110-EMD-001	Configuration Management Plan for the EMD Project
170 EMD 003	A Data Formatting Toolkit for Extended Data Providers to NASA's Earth Observing System Data and Information System (V5.0)

500-EMD-001	Terra Spacecraft Ephemeris and Attitude Data Preprocessing
500-EMD-002	Aqua Spacecraft Ephemeris and Attitude Data Preprocessing
500-EMD-003	Aura Spacecraft Ephemeris and Attitude Data Preprocessing
609-EMD-200	Release 7.21 Operations Tools Manual for the EMD Project (Available July 2008)
910-TDA-003	COTS Software Version Baseline Report
910-TDA-005	Site-Host Map Report
910-TDA-021	SYBASE SQLServer 11.0.x ALL DAAC Database Configurations
910-TDA-022	Custom Code Configuration Parameters for ECS
910-TDA-023	Critical COTS Software List
910-TDA-030	COTS [Software] Where Used Report
914-TDA-337	Whats Up Professional 2006 Maintenance Upgrade for the EMD Project: Release Notes
914-TDA-370	AMASS to StorNext
914-TDA-376	Luminex Physical Media
921-TDx-001	DAAC LAN Topology
921-TDx-002	[DAAC] Hardware/Network Diagram
921-TDx-003	IP Address Assignment (DAAC Hosts)
921-TDx-004	IP Address Assignment (DAAC Network Hardware)
921-TDx-005	Dual-Homed Host Static Routes
CM-004	EMD Project Instruction: CCB Change Control Process
CM-1-032-1	EMD Project Instruction: COTS and Custom Software Preparation and Delivery
CM-045	EMD Project Instruction: EMD Software Build Process
DM-002	EMD Project Instruction: Data Identification Numbering
MIL-HDBK-263B	Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices) (Metric)

MIL-STD-1686C	Department of Defense Standard Practice: Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)

2.3.2 Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the Mission Operation Procedures for the EMD Project.

290-004	Goddard Space Flight Center, Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements
423-10-21	Earth Science Data and Information System Project Configuration Management Procedures
423-16-01	Data Production Software and Science Computing Facility (SCF) Standards and Guidelines
305-EMD-200	Release 7.21 Segment/Design Specification for the EMD Project (Available August 2008)
311-EMD-200	Release 7.21 INGEST (INS) Database Design and Schema Specifications for the EMD Project (Available August 2008)
311-EMD-203	Release 7.21 Systems Management Subsystem Database Design and Schema Specifications for the EMD Project (Available August 2008).
311-EMD-204	Release 7.21 Order Manager Database Design and Database Schema Specifications for the EMD Project (Available August 2008).
311-EMD-205	Release 7.21 Spatial Subscription Server (SSS) Database Design and Schema Specifications for the EMD Project (Available August 2008)
311-EMD-206	Release 7.21 Data Pool Database Design and Schema Specifications for the EMD Project (Available August 2008)
311-EMD-207	Release 7.21 Inventory (EcInDb) Database Design and Schema Specifications for the EMD Project
508-EMD-001	ACRONYMS for the EOSDIS Maintenance and Development (EMD) Project
905-TDA-001	EMD System Baseline Specification
914-TDA-331	Solaris_8_OS_patches_0905
920-TD*x*-001	Hardware-Design Diagram
920-TD*x*-002	Hardware-Software Map

905-TDA-002	ECS Host Naming Convention
920-TD*x*-009	DAAC HW Database Mapping
920-TDx-019	Hosts' Custom Code Baseline
152-TP-003	Glossary of Terms for the EOSDIS Core System (ECS) Project
FB9401V2	EOSDIS Core System Science Information Architecture
NPR 1600.1	NASA Procedural Requirements: NASA Security Program Procedural Requirements
NPR 2810.1	NASA Procedural Requirements: Security of Information Technology
OMB Circular A-130	Office of Management and Budget, Management of Federal Information Resources

3. System Administration

3.1 Overview

Secure Shell (ssh) is an application that greatly improves network security. Secure Shell is the standard for remote logins, solving the problem of hackers stealing passwords. Secure Shell secures connections by encrypting passwords and other data. Once launched, it provides transparent, strong authentication and secure communications over any IP-based connection. The SSH Secure Shell application is virtually invisible during day-to-day use. It provides an extensive library of features for securing and authenticating terminal connections, file transfers or almost any other type of connection that might be created over an IP network. Secure Shell is to be used for communication among system platforms and among the DAACs.

3.2 Secure Access to DAACs

The Local Area Network (LAN) that has been implemented at the DAACs is more secure than most other LANs. From the Internet, it is not possible to directly connect with all hosts at a DAAC. There is a set of hosts that are externally advertised to the Internet. This will require an interactive user to first use SSH to access an externally advertised host and then use ssh to access a non-advertised production host. In order to minimize the impact on the user, a single login has been implemented.

3.3 Setting Up SSH

SSH programs have client and server components much like other network programs. The user only needs to be concerned with the client configuration as the server side is set up by a systems administrator. The amount of effort that it takes to get SSH going depends on how many different home directories the user has. At Riverdale, for instance, there are separate directories for the EDF, PVC and VATC.

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. Prior to executing **ssh** commands, use **setenv DISPLAY <*IP address*>:0.0** at your local host. To ensure system security, do not use the **setenv DISPLAY** command on subsequent hosts accessed via **ssh**. The process is started by running the **SSH setup (sss)** script, which will enable **ssh** to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

Table 3.3-1 contains the activity checklist for setting up SSH.

Table 3.3-1. SSH - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Initializing SSHSETUP	(P) 3.3.1	
2	SA	Setting Up Remote Access SSH	(P) 3.4.1	
3	SA	Changing Your Passphrase	(P) 3.5.1	

3.3.1 Initiating SSHSETUP

1 Log in into your normal UNIX workstation where your home directory resides.

2 Initiate Secure Shell setup by typing **sss** then press the **Return/Enter** key.

- You will see an information statement:

  Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces

3 At the **New passphrase:** prompt type ***passphrase*** then press the **Return/Enter** key.

4 At the **Retype new passphrase:** prompt type ***passphrase*** then press the **Return/Enter** key.

- You will then see:

  Generating ssh2 keys. This can take up to 180 seconds.
  Done with sshsetup!
  %

- This establishes the **.ssh2** sub-directory in your **/home/<userid> directory**, creates the local ssh key and creates the necessary files.

3.4 Remote SSH Access

If you need to access a host with a different home directory, you will need to run the **sshremote** script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

3.4.1 Setting Up Remote Access SSH

1 Log in into your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell remote setup by typing **ssr** then press the **Return/Enter** key.

- You will see the following prompt:

  Remote user name: (Default: <name>):

  NOTE: You have to have an account on the remote system first!

  You have a local passphrase. Do you want to setup for:
  1 VATC
  2 PVC
  3 EDC DAAC
  4 LaRC DAAC
  5 NSIDC DAAC
  x Exit from script
  Select:

3 At the **Select:** prompt, type in the corresponding number to the desired host then press the **Return/Enter** key.

- You will receive a message similar to the following:

  Enter the password for the remote system: <password>

4 At the prompt **Enter existing passphrase for remote system:** type <***passphrase***> then press the **Return/Enter** key.

- A prompt similar to the following will be displayed:

  Working...

NOTE: The ssh keys at remote sites can be different from the local host ssh key.

3.5 Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The **ssh** keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

3.5.1 Changing Your Passphrase

1 Log in to your normal Unix workstation where your home directory resides.

- Initiate passphrase change by typing **ssp** then press the **Return/Enter** key.
- You will see an information statement:

  Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces

2 At the **Old passphrase:** prompt type old_***passphrase*** then press the **Return/Enter** key.

3 At the **New passphrase:** prompt type ***new_passphrase*** then press the **Return/Enter** key.

4 At the **Retype new passphrase:** prompt type ***new_passphrase*** then press the **Return/Enter** key.

- You will then see an information prompt similar to the following:

  ssh-keygen will now be executed. Please wait for the prompt to Return!
  /home/*userid*/.ssh2/authorized_keys permissions have already been set.
  %

3.6 Logging in to System Hosts

Logging in to system hosts is accomplished from a UNIX or Linux command line prompt. It is an initial step that is performed when accomplishing many other tasks.

Logging in to system hosts starts with the assumption that the applicable hosts are operational and the operator has logged in to a workstation or X-term that has access to the applicable network in the system.

Table 3.6-1 contains the activity checklist for Login to System Hosts.

Table 3.6-1. Login to System Hosts - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Log in to System Hosts	(P) 3.6.1	

3.6.1 Log in to System Hosts

NOTE: Commands in Steps 1 and 2 are typed at a UNIX system prompt.

1 In the terminal window (at the command line prompt) start the log-in to the appropriate host by typing **ssh <*hostname*>** then press the **Return/Enter** key.

- The **-l** option can be used with the ssh command to allow logging in to the remote host (or the local host for that matter) with a different user ID. For example, to log in to *x4dpl01* as user cmops enter:

  ssh -l cmops *x*4dpl01

- Depending on the set-up it may or may not be necessary to include the path (i.e., /usr/local/bin/) with the ssh command. Using ssh alone is often adequate. For example:

  ssh *x*4dpl01

  - or -

  ssh -l cmops *x*4dpl01

- Examples of Linux Evolution host names include **e4dpl01, l4spl01, n4eil01** and p4oml01.
- If you receive the message, **"Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?"** enter **yes** ("y" alone will not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to ***Passphrase* for key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase, go to Section 3.3.1 Step 4.

2 If a prompt to **Passphrase for key <*user@localhost*>** appears, type your <***passphrase***> then press the **Return/Enter** key.

- If a command line prompt is displayed, log-in is complete.
- If the passphrase is unknown or entered improperly, press the **Return/Enter** key, which should cause a **<user@remotehost>'s password:** prompt to appear (after the second or third try if not after the first one), then go to Step 3.

3 If a prompt for **<*user@remotehost*>'s password:** appears, type your ***password*** then press the **Return/Enter** key.

- A command line prompt is displayed.
- Log-in is complete.

3.7 System Startup and Shutdown

The interdependency of the various servers may require the System Administrator to startup or shutdown the servers in a particular order. Depending on the situation, the entire computer system may be started or stopped (cold) or only selected servers may be started or stopped (warm). The next sections cover the procedures and details of cold and warm startups and shutdowns.

Table 3.7-1 contains the activity checklist for System Startup and Shutdown.

Table 3.7-1. System Startup and Shutdown - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Performing Cold Subsystem Startup	(P) 3.7.1.1	
2	SA	Performing Warm Subsystem Startup	(P) 3.7.2.1	
3	SA	Updating leapsec.dat and utcpole.dat Files	(P) 3.7.3.1	
4	SA	Performing Normal Shutdown	(P) 3.7.4.1	
5	SA	Performing Emergency Shutdown	(P) 3.7.5.1	

3.7.1 Cold Startup By Subsystem

A cold startup is indicated when there are no subsystems currently running, e.g., when the system is to be turned on for the first time, following a system maintenance operation that requires all power to be turned off or following a power failure. In most situations a cold startup is also indicated by the power switch being in the OFF position.

3.7.1.1 Performing Cold Subsystem Startup

1 Determine which machines perform the following functions (some machines may perform multiple functions).

- Primary and Secondary Name Servers
  - Domain Name System (DNS) Servers
  - Network Information Service (NIS) Servers
  - FlexNet License Server
- Network File System (NFS) Server (/home and /tools directories)
  - ClearCase Server
- Mail Server
- Sybase ASE Server
- Client Subsystems (CLS)

2 Startup the DNS, NIS Primary and Secondary Servers.

- Once the systems have booted without error, proceed to Step 3.

3 Power on the NFS and ClearCase server.

- Once the system has booted without error, proceed to Step 4.

4 Power on the Mail Server.

- Once the system has booted without error, proceed to Step 5.

5 Power on the Sybase ASE Server.

- Once the system have booted without error, proceed to Step 6.

6 Power on the Client Subsystems.

- Once the system(s) have booted without error, proceed to Step 7.

7 Power on any remaining servers and hosts.

3.7.2 Warm Startup

A warm startup is indicated when there are some subsystems currently running while others have been shutdown either due to operator intervention or an external malfunction. The subsystems not actively running need to be started without interfering with the current active operations. In some instances, a warm startup may require some active subsystems to be shutdown and restarted so that their interaction and connectivity will be properly resumed.

3.7.2.1 Performing Warm Subsystem Startup

---

1 Determine which machines perform the following functions:

- Primary and Secondary Name Servers
  - Domain Name System (DNS) Servers
  - Network Information Service (NIS) Servers
  - FlexNet License Server
- Network File System (NFS) Server (/home and /tools directories)
  - ClearCase Server
- Mail Server
- Sybase ASE Server
- Client Subsystems (CLS)

2 Determine which machine is currently down.

3 Determine the interoperability dependencies among the machines.

4 Turn on machines in an order consistent with the dependencies.

3.7.3 Updating leapsec.dat and utcpole.dat Files

In order to ensure proper operation of Product Generation Executives (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are

${PGSHOME}/database/common/TD/leapsec.dat
${PGSHOME}/database/common/CSC/utcpole.dat. The updating of these files is accomplished by executing **leapsec_update.sh** and **utcpole_update.sh** in the **/usr/ecs/OPS/CUSTOM/TOOLKIT/toolkit/bin/linux** directory on each Science Processor with root privileges. If the tasks have not been set up to be accomplished via cron job, they must be done manually.

3.7.3.1 Updating leapsec.dat and utcpole.dat Files

NOTE: The user account performing the update must have write permission in the Toolkit directories.

1 Log in to one of the x4spl01 machines.

2 Type **cd /usr/ecs/*MODE*/CUSTOM/TOOLKIT/toolkit/bin/linux** then press the **Return/Enter** key.

3 Type **source pgs-env.csh** then press the **Return/Enter** key.

4 Type either **update_leapsec.sh** (to update the leap seconds file) or **update_utcpole.sh** (to update the leap seconds file) as appropriate then press the **Return/Enter** key.

5 Type responses to program prompts as appropriate.

6 Repeat Steps 4 and 5 to update the other file.

7 Repeat Steps 1 through 6 for each additional Science Processor host (if any).

3.7.4 Normal Shutdown

A normal shutdown occurs when the operator is required to turn off the power to the entire system or any of the component subsystems. The Resource Manager schedules normal shutdowns (with prior approval of DAAC management) at a time that minimizes disruption to system users, e.g., during off-hours. No loss of data is anticipated from a normal shutdown. All subsystems are shut down in a routine fashion.

The system shutdown procedure is performed by the System Administrator, usually for the purpose of repair. The system shutdown is normally performed in reverse order of the system startup as previously described. Prior to a normal shutdown, the System Administrator sends broadcast messages to all users on the system at Shutdown Minus 30 minutes, Shutdown Minus 15 minutes, and Shutdown Minus one minute. At the scheduled shutdown time, the System Administrator blocks all incoming requests from the gateway and allows active jobs to complete (unless it is anticipated that they will take longer than 10 minutes, in which case the System Administrator will terminate the processes and notify the originator). The System Administrator then begins to shut down all subsystems in the order prescribed in the procedure below. Total time from shutdown initiation to completion may be as long as 45 minutes.

3.7.4.1 Performing Normal Shutdown

Steps 1 through 7 below are preliminary steps to shutting down each subsystem and are repeated (as necessary) for each subsystem.

1 Log in to the server as **root**.

2 Type ***root_password*** then press the **Return/Enter** key.

3 Type **wall** then press the **Return/Enter** key.

4 Type "This machine is being shutdown for *reason* in *n* minutes. Please save your work and log off now. We are sorry for the inconvenience." Then press the **Ctrl** and **D** keys simultaneously to exit the wall message.

5 Wait at least five minutes.

6 At the UNIX prompt type **shutdown -g0 -i0** or **shutdown now -i0** then press the **Return/Enter** key.

7 Power off all peripherals and the CPU if necessary.

8 Determine which machines perform the following functions:

- Primary and Secondary Name Servers
  - Domain Name System (DNS) Servers
  - Network Information Service (NIS) Servers
  - FlexNet License Server
- Network File System (NFS) Server (/home and /tools directories)
  - ClearCase Server
- Mail Server
- Sybase ASE Server
- Client Subsystems (CLS)

9 .Power off the Client servers by following Steps 1 through 7 above for each machine.

- Once the system(s) have shutdown without error, proceed to Step 10.

10 Power off the Sybase ASE server by following Steps 1 through 7 above for each machine.

- Once the system(s) have shutdown without error, proceed to Step 11.

11 Power off the Mail server by following Steps 1 through 7 above for each machine.

- Once the system(s) have shutdown without error, proceed to Step 12.

12 Power off the Network Files System and ClearCase server by following Steps 1 through 7 above for each machine.

- Once the system(s) have shutdown without error, proceed to Step 13.

13 Power off the Secondary, then Primary Name server(s) by following Steps 1 through 7 above for each machine.

3.7.5 Emergency Shutdown

An emergency shutdown is indicated when the System Administrator determines that the entire system or a component subsystem requires immediate maintenance. Indications that an emergency shutdown is in order include:

- The system or subsystem is locked up and users are unable to access or maneuver through the system
- An impending or actual power failure
- An actual system or subsystem hardware or software failure

Every effort should be made to minimize loss of data during an emergency shutdown by informing users to save files and log off if at all possible. However, circumstances may be such that a large-scale loss of data is unavoidable. In such instances, data will be restored from the most recent backup tapes and temporary backup files provided by the system (if applicable).

If the entire system or major subsystems are locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If one or only a few of the subsystems are experiencing problems and only some of the users are affected, the subsystem problem(s) should be resolved first. If the System Administrator determines that all efforts to resolve the subsystem problems are exhausted and a shutdown is necessary, only the affected subsystems should be shutdown. Only if these steps provide no relief should the entire system be brought down. In any case, every effort should be made to accommodate users that are still on the system and to minimize data loss.

3.7.5.1 Performing Emergency Shutdown

---

1 Log in to the server as root.

2 Type ***root_password*** at the UNIX prompt then press the **Return/Enter** key.

3 Type **sync** at the UNIX prompt then press the **Return/Enter** key.

- The **sync** command causes all information in memory that should be on disk to be written out including modified super blocks, modified inodes, and delayed block I/O. If the system is to be stopped, **sync** must be called to insure file system integrity.

4 Type **sync** (again) at the UNIX prompt then press the **Return/Enter** key.

5 Type **halt** at the UNIX prompt then press the **Return/Enter** key.

6 Shutdown all client workstations.

7 Determine which machines perform the following functions (some machines may perform multiple functions).

- Sybase ASE/Rep
- Mail Hub
- NFS/ClearCase
- DNS/NIS

8 Power off the Sybase ASE/Rep server(s).

- Once the system has shutdown without error, proceed to Step 9.

9 Power off the Mail Hub server(s).

- Once the system has shutdown without error, proceed to Step 10.

10 Power off the NFS/ClearCase server(s).

- Once the system has shutdown without error, proceed to Step 11.

11 Power off the DNS/NIS server(s).

3.7.6 System Shutdown by Server

In situations where only a single server requires maintenance, the System Administrator will need to determine if and how the faulty server affects other servers on the network. One server may be able to be shutdown without affecting the rest of the network, or several dependent servers may have to be shutdown in addition to the target server. Because of these interdependencies, each case will have to be uniquely evaluated.

3.8 Checking the Health and Status of the System

The system is heavily dependent on the use of computer networks. Graphical tools available to monitor system status include **WhatsUp Professional.** This program provides real-time status of the system and indications of potential problem areas.

3.8.1 Whazzup

A powerful COTS program that has been modified for monitoring the system is EcMsWz – Whazzup??. It is a web-accessed program that provides a graphical display of Host Status, Mode Status, Mode Verification and Performance Management.

These functions of Whazzup provide graphical displays of host and software-server status in real-time mode. When used in conjunction with ECS Assistant, System Administrators can acquire a comprehensive knowledge of the system's status.

Table 3.8-1 contains the activity checklist for Whazzup??.

Table 3.8-1. Whazzup?? - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Starting EcMsWz-Whazzup	(P) 3.8.1	

To start EcMsWz-Whazzup, execute the following procedure:

3.8.2 Starting EcMsWz-Whazzup

1 Log in to a host machine.

2 At the UNIX prompt on the host from which Whazzup is to be run, type **setenv DISPLAY <*hostname*>:0.0** press the **Return/Enter** key.

- ***Note:*** If the host has been remotely accessed via ssh then do not use the setenv DISPLAY command again. Doing so will compromise system security.
- ***hostname*** is the name of the machine on which Whazzup is to be displayed, i.e., the machine you are using.
- To verify the setting, type **echo $DISPLAY** then press the **Return/Enter** key.

3 At the UNIX prompt, using secure shell, log on to the Whazzup host, x4eil01. Type **ssh *x4eil01*** then press the **Return/Enter** key.

4 Type ***Passphrase*** then press the **Return/Enter** key.

- You are logged into the Whazzup host machine.

5 To start the Mozilla Firefox web browser type **/tools/firefox/firefox &** then press the **Return/Enter** key.

- You are in the web browser on the Whazzup host **e4eil01**

6 In the **Location** field of the Netscape browser type the URL for Whazzup (e.g., **http://x4eil01:5150/**) then press the **Return/Enter** key.

- The Whazzup intro screen appears (Figure 3.8-1).

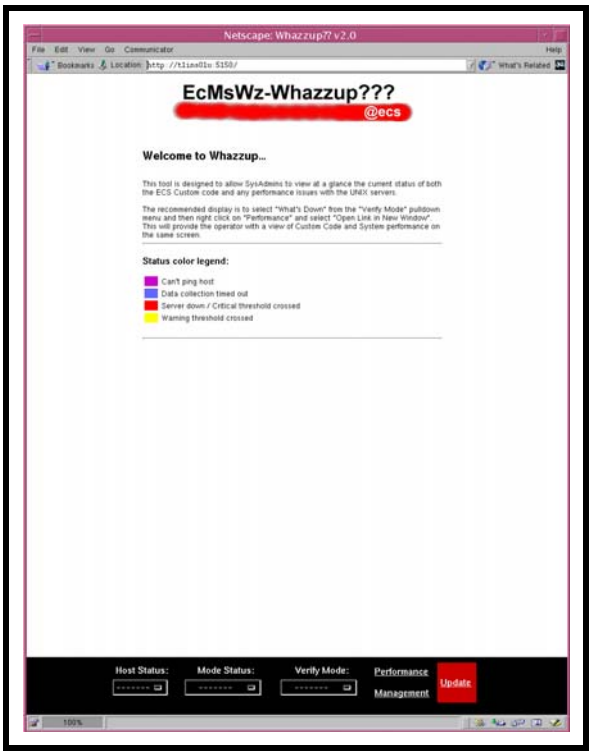


Figure 3.8-1. ECS Whazzup Initial Display

7 Select a monitoring function:

- **Host Status** to determine individual host parameters.
- **Mode Status** to determine "up" servers for the selected Mode.
- **Verify Mode** to determine status of all servers for a selected Mode.
- **Performance Management** to determine the performance status of all hardware/software servers for all modes.

3.8.3 Host Status

Selecting Host Status provides a pop-up box (Figure 3.8-2) from which to choose a specific host to determine its status. Host Status data include percent of CPU used, Swap Free space, Memory Free space, and Server information (Figure 3.8-3).

Selecting Mode Status (Figure 3.8-4) enables a pop-up window showing Modes available. Subsequent to selecting the desired Mode, a display of "up" system servers is provided as shown in Figure 3.8-5.

3.8.4 Verify Mode

Selecting **Verify Mode** and choosing a desired mode (Figure 3.8-6) will provide a thorough display of system server status, by host, for the mode (Figure 3.8-7). Alternatively, selecting **What's Down** will provide a display indicating all down system servers, by mode, by host.

3.8.5 Performance Management

Following recommended monitoring procedures, the optimum method of system monitoring is to select **What's Down** from **Verify Mode** and then **Right Click** on **Performance Management** (Figure 3.8-8) and open the link in a new window (Figure 3.8-9).

Having these two displays active simultaneously will provide the Systems Administrator the status of "down" system servers and the performance status of individual hosts.

Figure 3.8-2. Host Status Pop-Up Display

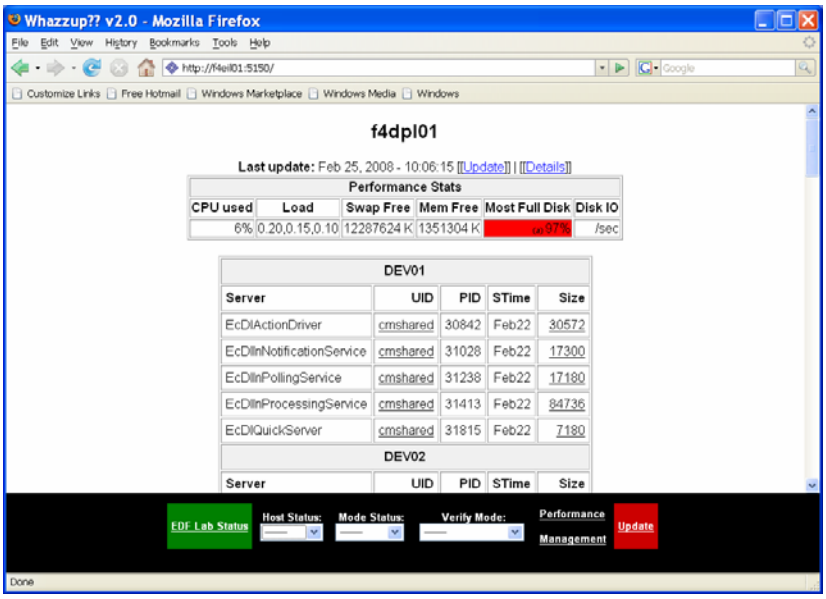


Figure 3.8-3. Host Status Data Display

Figure 3.8-4. Mode Status Pop-Up Display

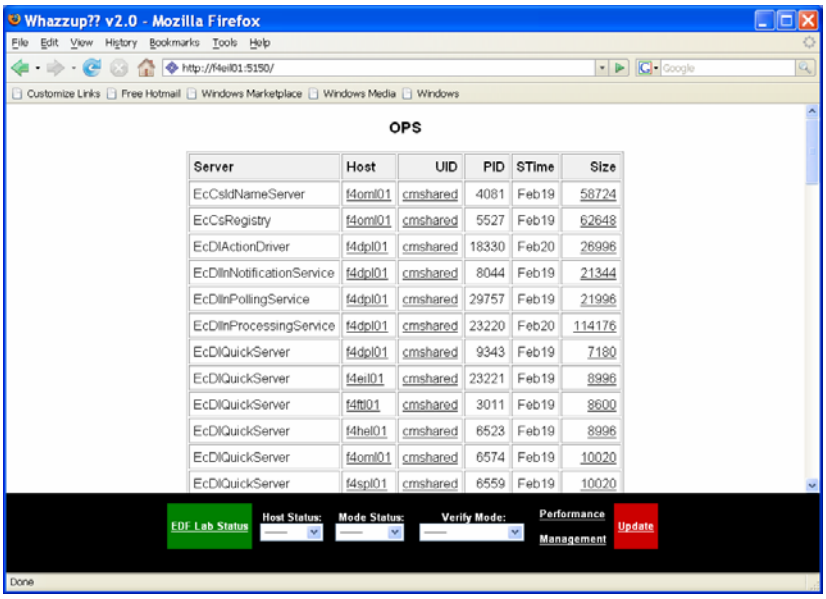


Figure 3.8-5. Mode Status Data Display

Figure 3.8-6. Verify Mode Pop-Up Display

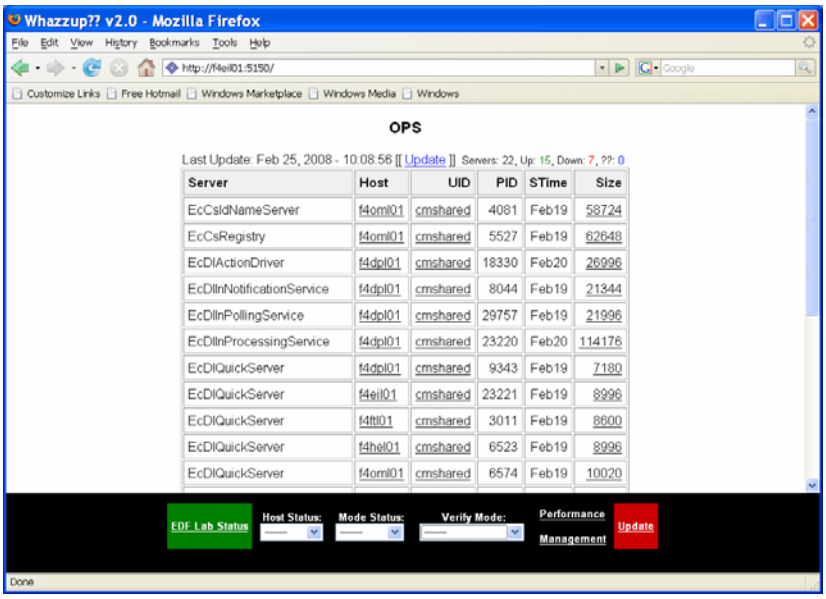


Figure 3.8-7. Verify Mode Data Display

Figure 3.8-8. Performance Management Selection Display

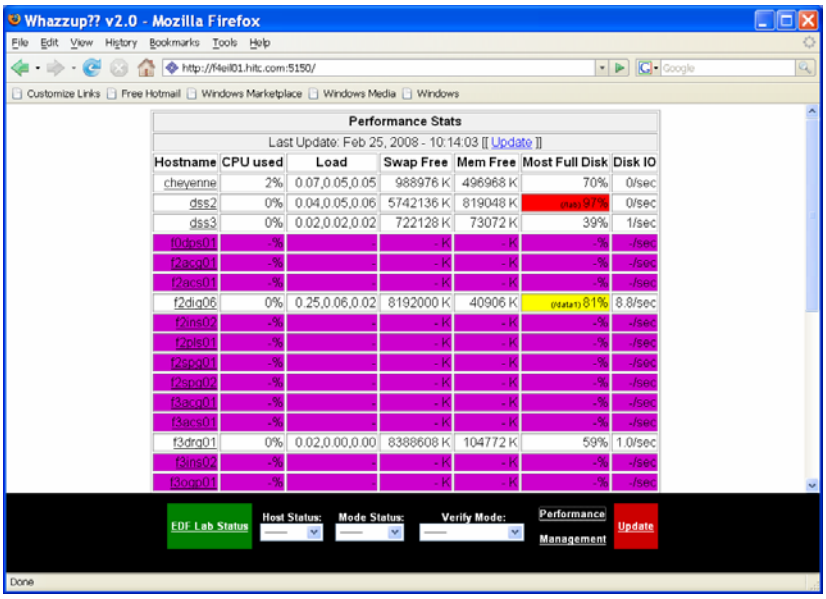


Figure 3.8-9. Performance Management Data Display

3.9 ECS Assistant

The Whazzup tool provides a quick look capability to identify whether any servers are down. The ECS Assistant tool provide an additional easy-to-use tool that offers a server monitoring tool as well as a capability to start and stop servers. Figure 3.9-1 shows the ECS Assistant GUI for access to manager functions, the ECS Assistant subsystem manager GUI, and an example of a confirmation dialog.

Table 3.9-1 contains the activity checklist for ECSAssistant.

Table 3.9-1. ECS Assistant - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Starting ECS Assistant	(P) 3.9.1	

3.9.1 Starting ECS Assistant

1 Log in to one of the host machines.

2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs** then press the **Return/Enter** key.

- To verify the setting, type **echo $ECS_HOME** then press the **Return/Enter** key.

3 At the UNIX prompt, type **cd /tools/common/ea** then press the **Return/Enter** key. Then type **EcCoAssist /tools/common/ea &** then press the **Return/Enter** key.

- **/tools/common/ea** is the path where ECS Assistant is installed, and also where EcCoScriptlib may be found.
- The ECS Assistant GUI is displayed.

4 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.

- The Subsystem Manager GUI is displayed.

5 Select a mode by clicking on the down arrow at the right end of the **Mode** field and then on the desired mode name in the resulting list.

- The selected mode is displayed in the **Mode** field and colored indicators show the installation status for components in that mode on the host; the legend for the color indications is at the lower right on the Subsystem Manager window.

6 In the list of subsystems, double click on the name of the subsystem of interest.

One or more component groups appear below the selected subsystem name.

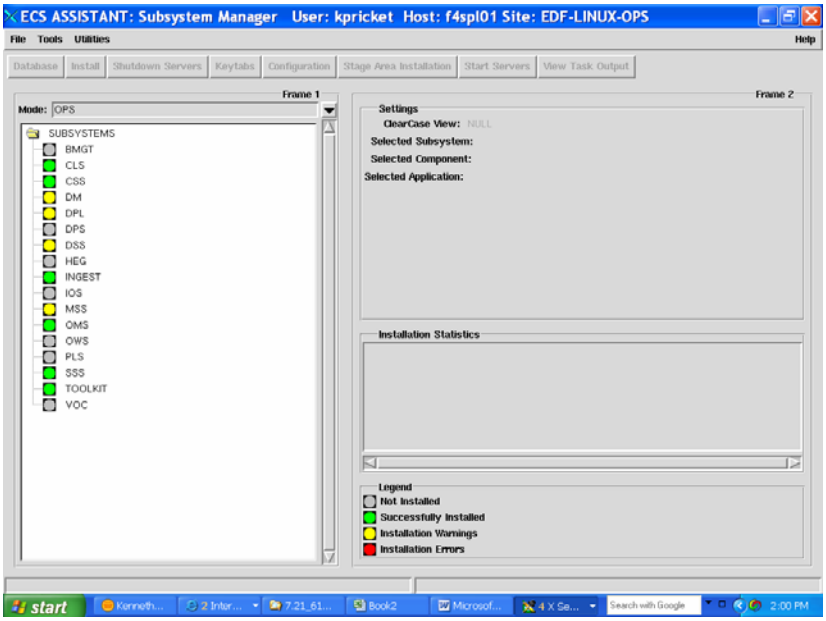


Figure 3.9-1. ECS Assistant GUI Manager Windows

7 Double click on the name of a component group.

- One or more application groups appear below the selected component group name.

8 Double click on the name of the application group of interest.

- The applications or servers in the selected group are listed below the name of the group.

9 Single click on the name of an application or server of interest.

- The selected application or server is highlighted.
- Detailed installation information is displayed in the **Installation Statistics** window.

3.10 Tape Operations

In this document you will learn how Networker Administrative software and the Pathlight appliance work together to administer the use of tapes for system backups and file restorations. Functions such as how to label a new tape, how to index a tape cartridge, and how to perform backups and restores are covered.

Table 3.10-1 contains the activity checklist for Tape Operations.

Table 3.10-1. Tape Operations - Activity Checklist

Role	Task	Section	Complete?
SA	Networker Login Procedures	3.10.1.1	
SA	Pathlight Login Procedure	3.10.1.2	
SA	Performing Tape Labeling For Pathlight	3.10.2.1	
SA	Tape Rotation Procedures for Pathlight When Reusing Tapes Already in Library	3.10.2.2	

Key Terms:

- **Cartridge** – We use LTO3 tapes and they can hold up to 400GB of data in uncompressed mode and up to 800GB when compressed.
- **Drive** - Hardware device into which the tape or tape cartridge is inserted that performs the actual recording of data. We are using LTO3 drives.
- **Inventory** - The action of making an index.
- **Jukebox** - A hardware device that stores more than one tape used for system backups and restores. Working in conjunction with specialized software, it can automatically select the proper tape, load the tape into the tape drive, and return it to its appropriate slot upon completion of the task. A Scalar 100 is attached directly to the Pathlight

appliance by a fibre cable. It has 2 LTO3 tape drives and can hold up to 60 LTO3 tapes.

- **Label -** A unique name assigned to a tape by Networker.
- **Volume -** A recording medium; in the case of this course, a volume and a tape are synonymous.

3.10.1 Networker Administrator Screen

3.10.1.1 Networker Login Procedures

1 Login to <***Backup Server***> as root.

2 Start mozilla (/usr/ecs/OPS/COTS/mozilla/mozilla).

3 Browse to Networker NMC (URL http://<***Backup Server***>:9000).

4 Choose OK when asked "What should mozilla do with this file?".

- Default is (/usr/ecs/OPS/COTS/jre/jre/javaws/javaws).

5 Login to Networker

- **Pathlight Login Procedure**Username: administrator Password: <***Password set by System Admin***>

6 Choose enterprise at the top.

7 Left click <servername> in left pane.

8 Double click Networker in right pane (launches Networker application)

- Backup Servers by DAAC:
  - NSIDC n4msl20 198.118.205.32
  - EDC e4msl20 198.118.202.109
  - ASDC l0msp20 198.118.219.19

3.10.1.2 Pathlight Login Procedure

1 Login to <***Backup Server***> as root

2 Start mozilla (/usr/ecs/OPS/COTS/mozilla/mozilla).

3 Browse to Pathlight Admin page (URL http://<***Pathlight Appliance IP***>).

4 Login to Pathlight.

- Username: admin Password: ***<Password set by System Admin>.***
- Pathlight Appliances by DAAC:
  - NSIDC 192.168.54.21
  - EDC 192.168.52.39
  - ASDC 192.168.53.24

3.10.2 Labeling Tapes

Files and directories have unique names that are assigned by the user to identify them. In much the same manner, tapes are given unique names, or labels. This allows such programs as Networker and such hardware devices such as the Pathlight appliance to automate the tape selection process when performing system backups and restores. When a tape is initialized, Networker assigns it a label. Networker then stores the tape's label with a file that is written to the tape so that when a file restoration request is received, Networker will know exactly which tape to select from the jukebox.

3.10.2.1 Performing Tape Labeling For Pathlight

Blank Tape Rotation Procedures for Pathlight

Note: These steps require bouncing back and forth between the Networker GUI and the Pathlight GUI. Thus, you preferably want to be on a machine that is on both the production and private networks. (i.e. Navisphere station)*Note: These steps assume the tape being newly labeled is brandnew or does not have a label. If it is an old tape being reused see the section titled "Tape Rotation Procedures for Pathlight When Reusing Tapes Already in Library".

1 Stop all backups (if running) and unmount all mounted virtual tapes to ensure you are starting at a stable point.

2 Launch Networker application.

3 Check backup group status.

- Select **Monitoring** (top left)
- Choose **Groups** tab (middle - far left)
- Look at **% Complete** for status
- If not **100% Complete**…
- Right click **Backup Group** and click on **Stop**.

4 Unmount all virtual tapes from the virtual tape drives.

- Bring up GUI via. web browser (IP address w/ :9000).

- Click on **Devices** icon (top).
- Click "+" in front of **Storage Nodes** (left pane).
- Click "+" in front of **Node Name** (left pane).
- Right click **Jukebox Name.**
- Choose **Library Operations.**
- Right click **Tapes** and choose **Unmount** (middle left pane).

5 Verify if the tape status from Pathlight is "identical" or "virtual". Ultimately we are copying data from virtual tape to physical tape and then deleting the virtual tape. If the status is identical the copy and delete process happens in seconds. If the tape is virtual the copy process will take approximately 2.2 hours per tape before the virtual tape is deleted.

- Check tape status from Pathlight.
- Bring up Pathlight GUI from browser (IP address of Pathlight appliance).
- Click on the **Reports** pull down and choose **Media Tracking**.
- Click **Barcode** to sort by numerical order.
- Make note of the barcode number and its status.

6 Eject/withdraw older full tapes from Networker GUI. Remember that just because a tape is full you don't necessarily want to delete it. You want to keep as much data on disk as possible for speedy recoveries.

- From the Networker web base GUI go to the **Library Operations** section.
- Right click the virtual tape that you want to remove and choose **Eject/Withdraw**.
- This will start a copy of virtual tape to physical (if not identical) and then delete the virtual tape.
- Refresh **Library Operations** by clicking on **Storage Node** followed by right clicking on library ***<adic 1.0.1>*.**
- The tape slot should become blank when the tape is **Ejected/Withdraw**.

7 Go back to Pathlight GUI to check status of virtual tape and create a new virtual tape.

- Click on **Hom**e within Pathlight GUI (top right).
  - You should see 622 GB available once the virtual tape has been copied and deleted.
- Click **Action Required** box (yellow box at bottom right).
- Click action "**Unknown media in the system, indicate media pool**".

- Click top box (first available in numerical order) in front of barcode number.
- Choose **Application** from the **Operations→Media Management→Physical→Application** pull-down window.
  - Enter Username: admin Password: ***<Password set by System Admin>***
- You have just created a new virtual tape and should now see 222GB available from the Pathlight home page.

8 From the Networker GUI, label the new virtual tape:

- Right click the <unlabeled> tape and choose Label.
- Make the following choices:
- First slot number: Enter slot number the <unlabeled> tape is in.
- Last slot number: Same as first slot number (if only labeling one tape).
- Select Pools: Put the new tape in the desired pool.
- Press OK.
- From the Networker web base GUI go to the Library operations section and Refresh by clicking on Storage Node followed by right clicking on library <adic 1.0.1>.
- You should now see a new virtual tape in the virtual jukebox slot.

3.10.2.2 Tape Rotation Procedures for Pathlight When Reusing Tapes Already in Library

Note: These steps require bouncing back and forth between the Networker GUI and the Pathlight GUI. Thus, you preferably want to be on a machine that is on both the production and private networks. (i.e. Navisphere station).

1 Verify if the tape status from Pathlight is "identical" or "virtual". Ultimately we are copying data from virtual tape to physical tape and then deleting the virtual tape. If the status is identical the copy and delete process happens in seconds. If the tape is virtual the copy process will take approximately 2.2 hours per tape before the virtual tape is deleted.

- Check tape status from Pathlight.
  - Bring up Pathlight GUI from browser (IP address of Pathlight appliance).
  - Click on the **Reports** pull down and choose **Media Tracking**.
  - Click **Barcode** to sort by numerical order.
  - Make note of the barcode number and its status.

2 Eject/withdraw older full tapes from Networker. Remember that just because a tape is full you don't necessarily want to delete it. You want to keep as much data on disk as possible for speedy recoveries.

- Eject/withdraw tapes from the Networker GUI.
  - Click on **Devices** (Top Menu).
  - Click on **Storage Node.**
  - Right click on library ***<adic 1.0.1>*.**
  - Go to the **Library Operations** section.
  - Right click the virtual tape that you want to remove and choose **Eject/Withdraw**.
  - This will start a copy of virtual tape to physical (if not identical) and then delete the virtual tape.
  - Refresh Library Operations by clicking on **Storage Node** followed by right clicking on library ***<adic 1.0.1>*.**
  - The tape slot should become blank when the tape is ejected/withdrawn.

3 Go back to Pathlight GUI to check status of virtual tape and create a new virtual tape.

- Click on blue **Admin Alert** box at bottom right.
- Click on button in front of tape that you ejected and delete the alert message.
- Click on the Home key within Pathlight GUI (top right).
  - You should see 622GB available once the virtual tape has been copied and deleted
- Choose **Application** from the **Operations→Media Management→Physical→Application** pull-down windows.
- Click **Import Offline Media to Virtual Library** button.
- Click **Next.**
- Click box in front of barcode number – choose oldest expired tape (beneath current virtual media).
- Make the following choices.
  - Select **ADIC_PVX** from the **Virtual Library** pull-down window.
  - Select **Scratch** from **Media Action**: window.
  - Select **Slot** from the **Entry Method**: window.
  - Select **Export to Storage Slot** from the **Select Export Rule** pull-down window.

- Select **Apply**.

You have just created a new virtual tape and should now see 222GB available from the Pathlight home page

4 From the Networker GUI, label the new virtual tape. Since the tape is being reused it will exist in the Networker media & file indexes, the volume will need to be deleted before attempting a label operation.

- Deleting a Networker tape volume.
  - From the Networker GUI click on **Media** button.
  - Click on **Volumes** in left pane.
  - Right click the **Tape Label** that you are going to reuse and choose **Delete**.
  - Choose **Delete Media** and **File and Media Index Entries** and click on **OK**.
- Label tape
- From the Networker web base GUI go to the library operations section (Refresh it)
  - Right click the **<unlabeled>** tape and choose **Label**.
  - Make the following choices:
  - First slot number: Enter slot number the **<unlabeled>** tape is in.
  - Last slot number: Same as first slot number (if only labeling one tape).
  - Select **Pools**: Put the new tape in the desired pool.
  - Press **OK.**
  - From the Networker web base GUI go to the Library operations section and Refresh by clicking on **Storage Node** followed by right clicking on library ***<adic 1.0.1>*.**
  - You should now see a new virtual tape in the virtual jukebox slot.

3.11 System Backups and Restores

Performing regular and comprehensive backups is one of the most important responsibilities a System Administrator performs. Backups are the insurance that essentially all of the system data is always available. If the system crashes and all disks are damaged, the System Administrator should be able to restore the data from the backup tapes depending on backup method (e.g., full or partial).

Table 3.11-1 contains the activity checklist for System Backup and Restores.

Table 3.11-1. System Backup and Restores - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Performing System Backup	(P) 3.11.1.1	
2	SA	Performing System Restore	(P) 3.11.2.1	
3	SA	Set Pathlight Tape(s) to Direct Access for Recovery	(P) 3.11.2.2	

3.11.1 System Backup

A full system backup is a snapshot of the data on the entire system as of a particular date. The data is stored on tapes that are used to recreate the system in the event of a total system failure. The full system backup is run by the System Administrator on a regular schedule, usually weekly. Full system backup tapes are stored offsite for security reasons.

3.11.1.1 Performing System Backup

1 Log in to a system terminal.

2 To set the display to the current terminal type **setenv DISPLAY <*IPNumber*>:0.0** then press the **Return/Enter** key.

3 To log in to the machine to be backed up type **ssh *BackedUpSystemName*** then press the **Return/Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter Passphrase for key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase go to Step 4.

4 If a prompt to **Enter Passphrase for key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

6 To log in as root type **su** then press the **Return/Enter** key.

- A password prompt is displayed.

7 Type the ***RootPassword*** then press the **Return/Enter** key.

- You are authenticated as root and returned to the UNIX prompt.

8 To execute the Networker Backup program type **nwbackup** then press the **Return/Enter** key.

- A Networker Backup window opens (Figure 3.11-1). You are now able to perform a full backup.

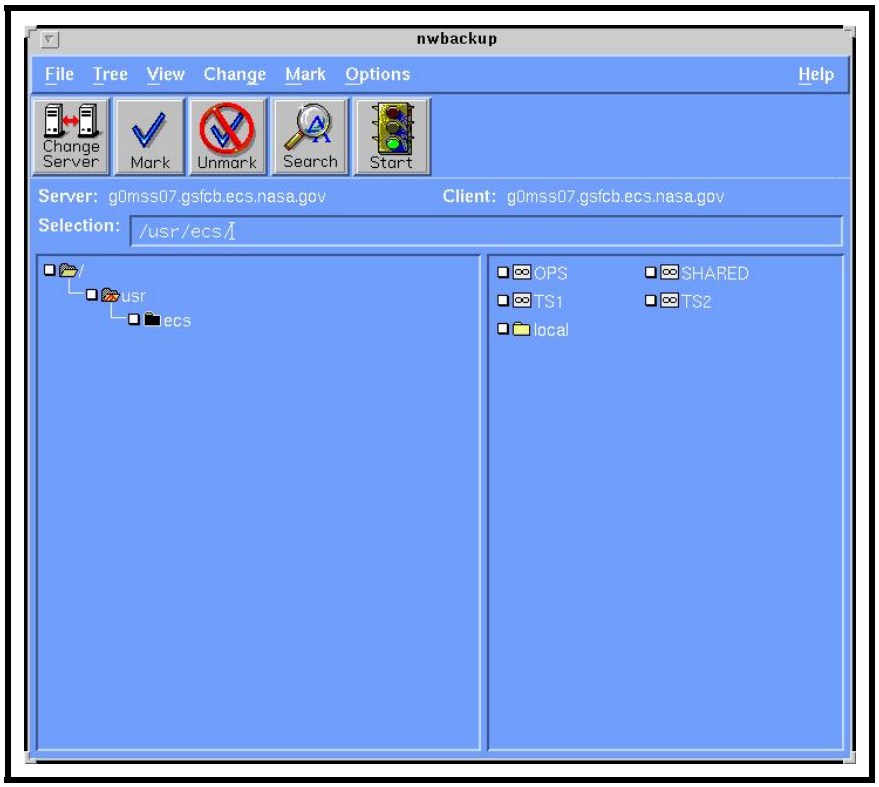


Figure 3.11-1. Networker Backup Window

9 If no files/directories to be backed up were provided by the requester, i.e. the whole machine is to be backed up, then type **/** in the **Selection** field and click the **Mark** button.

- **/** is designated for backup and has a check next to it.

10 If **files/directories to be backed up** were provided, then select the <**files/directories to be backed up**> in the directory display and click the **Mark** button.

- Drag scroll bar with the mouse to scroll the list up and down.
- Double-click on directory name to list its contents.
- To move up a directory level, type the path in the **Selection** field.
- Clicking the **Mark** button designates the file for backup and puts a check next to it.

11 Click on the **Start** button.

- A **Backup Options** window opens.

12 Click on the **OK** button.

- The **Backup Options** window closes.

- The **Backup Status** window opens providing updates on the backup's progress.

13 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.

- The **Backup Status** window closes.
- The backup is complete.

14 To quit the Networker Backup program select **File** → **Exit** from the pull-down menu.

- The Networker Backup window closes.

15 At the UNIX prompt for the machine to be backed up, type <**exit**> then press the **Return/Enter** key.

- Root is logged out.

16 Type <**exit**> again then press the **Return/Enter** key.

- You are logged out and disconnected from the machine to be backed up.

3.11.2 System Restore

From time to time individual files or groups of files (but not all files) will have to be restored from an incremental backup tape due to operator error or system failure.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- Name of machine to be restored.
- Name of file(s) to be restored.
- Date from which to restore.
- User ID of the owner of the file(s) to be restored.
- Choice of action to take when conflicts occur. Choices are:
  - Rename current file
  - Keep current file
  - Write over current file with recovered file

3.11.2.1 Performing System Restore

1 Log in to a system terminal.

2 To set the display to the current terminal type **setenv DISPLAY <*IPNumber*>:0.0** then press the **Return/Enter** key.

3 To log in to the machine to be restored type **ssh <host name>** ***Machine Restored*** then press the **Return/Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter Passphrase for key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase, go to Step 4.

4 If a prompt to **Enter Passphrase for key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

6 To log in as root type **su** then press the **Return/Enter** key.

- A password prompt is displayed.

7 Type the ***RootPassword*** then press the **Return/Enter** key.

- You are authenticated as root and returned to the UNIX prompt.

8 To log in as the user type **su *UserID.***

- You are authenticated as the owner of the file(s) to be restored.

9 To execute the Networker Recovery program type **nwrecover** then press the **Return/Enter** key.

- A window opens for the **Networker Recovery** program (Figure 3.11-2). You are now able to restore files.

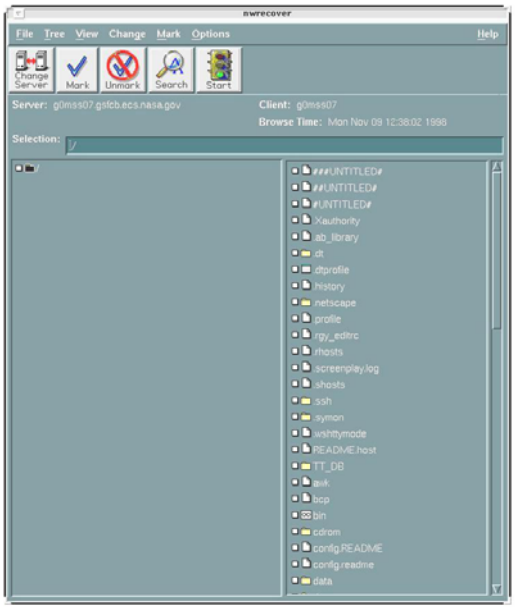


Figure 3.11-2. Networker Recovery Window

10 Select **file(s) to be restored** and click the **Mark** button.

- Drag scroll bar with the mouse to scroll the list up and down.
- Double-click on directory name to list its contents.
- Clicking on the **Mark** button designates the file for restore and puts a check next to it.

11 Select **Change → Browse Time** from the pull-down menu.

- The **Change Browse Time** window opens.

12 Select the **date from which to restore**.

- Networker will automatically go to that day's or a previous day's backup which contains the file.

13 Click on the **Start** button.

- The **Conflict Resolution** window opens.

14 In response to the question "Do you want to be consulted for conflicts" click on the **yes** button.

15 Click on the **OK** button.

- If prompted with a conflict, choices of action will be: rename current file, keep current file, or write over current file with recovered file.

- Select the requester's **choice of action to take when conflicts occur**.
- The **Recover Status** window opens providing information about the to be restored.
- If all the required tapes are not in the drive, a notice will appear.
- Click on the **OK** button in the notice window.

16 When a **recovery complete** message appears, click on the **Cancel** button.

17 Select **File → Exit** from the pull-down menu.

- The Networker Recovery program quits.

18 Type **exit** then press the **Return/Enter** key.

- The owner of the file(s) to be restored is logged out.

19 Type **exit** again then press the **Return/Enter** key.

- Root is logged out

20 Type **exit** one last time then press the **Return/Enter** key.

- You are logged out and disconnected from the **machine to be restored**.

3.11.2.2 Procedure to Set Pathlight Tape(s) to Direct Access for Recovery

If during a Networker recovery you notice that a tape(s) is saying “not all tapes are on-line” make a note as to which tape(s) are being requested.

1 Login to the Pathlight and Networker GUI’s. From the Pathlight GUI

2 Choose **Application** from the **Operations→Media Management→Physical→Application** pull-down windows.

3 Click on **Import Offline Media to Virtual Library** button.

4 Press **Next**

5 Make the following choices:

- Select ADIC_PVX from the Virtual Library pull-down window.
- Select Direct Access from Media Action: window.
- Select Slot from the Entry Method: window.
- Select Export to Storage Slot from the Select Export Rule pull-down window.
- Select Apply.

Go to Networker GUI

1 Refresh **Library Operations to see exported tape in a slot <unlabeled>.**

2 Right click **<unlabeled>** tape and choose **inventory from list.** You may have to inventory the tape several times before it recognizes the label.

3 **Restart the restore operation and the needed tape will now be available.**

Once the restore has completed you can put the imported tape back into "Offline Media" mode by doing the following from the Networker GUI.

4 Right click the imported tape and choose **Eject/Withdraw** from the list**.**

3.12 User Administration

3.12.1 Screening Personnel

Table 3.12-1 contains the activity checklist for User Administration.

Table 3.12-1. User Administration - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Checking File/Directory Access Privileges	(P) 3.12.8.1	
2	SA	Changing a File/Directory Access Privilege	(P) 3.12.9.1	

3.12.1.2 Screening Criteria

Some positions require special access privileges in order to do the assigned job or duties. These are called public trust positions because they can affect the integrity, efficiency or effectiveness of the system to which they have been granted privileged access. Screening for suitability, prior to being granted access is required. This screening, National Agency Check (NAC), is required to ensure that granting any special access privileges to someone would not cause undue risk to the system for which that employee has these privileges. Line Management is responsible for requesting suitability screening for the employees in their respective organizations.

OMB Circular A-130, Appendix III and NPR 2810.1 require the following employees to undergo personnel screening:

- All employees who require privileged access or limited privileged access to a Federal computer system or network.
- Privileged access – Can bypass, modify, or disable the technical or operational system security controls.
- Limited privileged access – Can bypass, modify or disable security controls for part of a system or application but not the entire system or application.

Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements (290-004) requires the following employees to undergo suitability screening:

- All employees who require privileged access, limited privileged access, or access to the Closed Segment of the Internet Protocol Operational Network (IONet) (formerly NASCOM).
- All employees having access to IONet network control devices.

NPR 1600.1 requires that all employees granted unescorted access to a NASA Resource Protection (NRP) facility or area and/or a NASA-designated Limited Area undergo screening.

3.12.2 Screening Procedures

The line manager will submit NASA Form 531 containing the following information for each employee needing suitability screening.

- Full name (first, middle initial and last)
- Goddard badge number if badged employee
- Reason for requesting screening
- Type and date of any previous security investigation or clearance if known
- Phone number and email address

The request should be sent to the EDF Security Administrator. The GSFC Security Office (GSO) will search the personnel security database to determine if a current NAC has been performed. If not the employee will be contacted to obtain additional information. The GSO will report a favorable or unfavorable result back to the EDF Security Administrator upon completion of the suitability screening.

3.12.3 Adding a New User

Adding a user to the system is accomplished through a series of steps that may be performed as a suite from the command line or by use of a script. The procedure below outlines the individual steps that are required to completely set up a new user on the system. The scripts will accomplish these steps in an interactive manner.

The requester fills out a User Registration Request Form and submits it to the requestor's supervisor. The requester's supervisor reviews the request, and if s/he determines that it is appropriate for the requester to have an account, forwards the request to the System Administrator. If the requester requires a National Agency Check (NAC) before access is granted, the supervisor will forward the request to the Security System Engineer, who will then ensure that proper procedures are followed before the request is sent to the System Administrator (SA). The System Administrator verifies that all required information is contained on the form. If it is, s/he forwards the request to the approval authority, the DAAC Manager. Incomplete forms are returned to the requester's supervisor for additional information. If the request for the

accounts fits within policy guidelines, the DAAC Manager approves the request and returns the request form to the System Administrator to implement.

The System Administrator should be familiar with a UNIX text editor and the files **/etc/passwd** (Figure 3.12-1), **/etc/group** (Figure 3.12-2) and **/etc/auto.home.**

The System Administrator (SA) creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC used a script, *Newuser*, to add new users to the system. The script, which is available to other DAACs, prompts the System Administrator for data input of user information and creates home directories for new users.

3.12.4 Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.

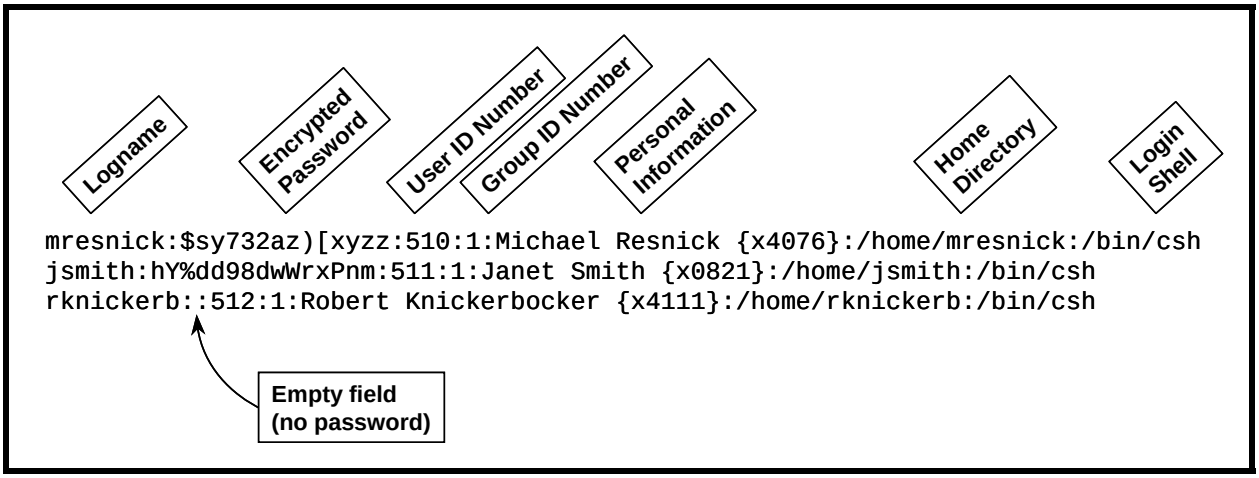


Figure 3.12-1. /etc/passwd File Fields

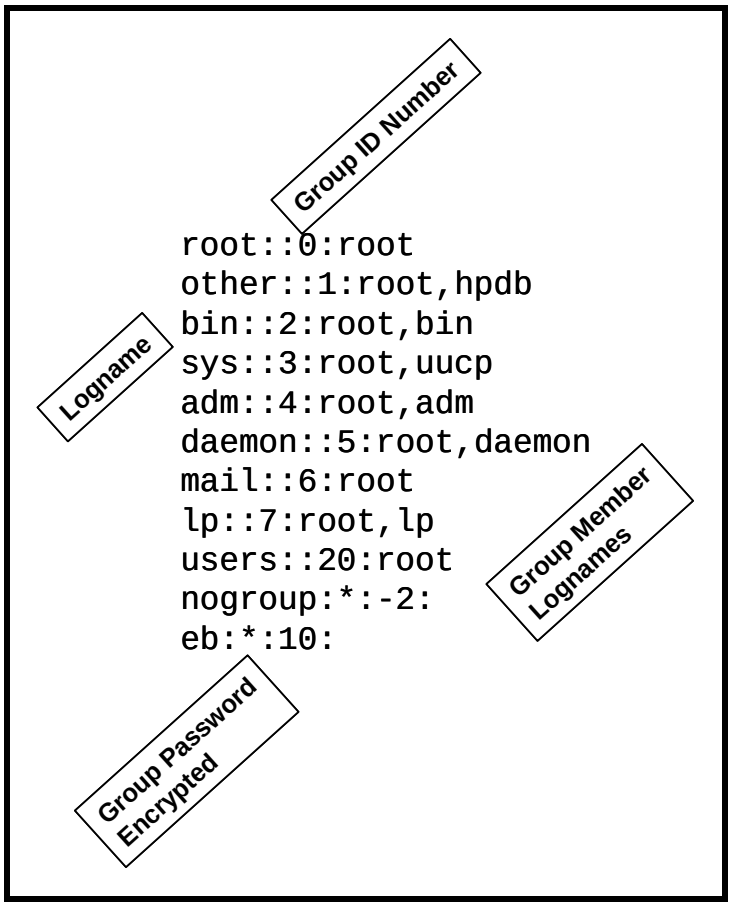


Figure 3.12-2. /etc/group File

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for deleting a user has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

- **UNIX login of the user to be deleted**
- **Role(s) of the user to be deleted**

The System Administrator deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC used a script, *Lockdown*, to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion and deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

3.12.5 Changing a User's Account Configuration

Account configuration is accomplished through command line and script. The DAAC manager must authorize changes to user accounts.

The Changing a User Account Configuration process begins when the requester submits a request to the OPS Super detailing what to change about the account configuration and the reason for the change. Requests for changes to privileged accounts shall be sent to the Security System Engineer. The OPS Supervisor or the Security System Engineer reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and OPS Supervisor.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- What to change and new settings. Can be any of:
  - New Real User Name
  - New Office Number
  - New Office Phone Number
  - New Home Phone Number
  - New UNIX Group
  - New Login Shell
- Current UNIX Login of the User

3.12.6 Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to his/her supervisor. Requests for changes to privileged accounts shall be sent to the Security System Engineer. The supervisor or the Security System Engineer approves or denies the request. Once approved, the request is forwarded to the OPS Super. The Ops Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and Ops Super.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Role(s) to which the user is to be added
- Role(s) from which the user is to be removed
- UNIX login of the user

3.12.7 Changing a User Password

The Changing a Users Password process begins when the requester submits a request to the SA. The System Administrator verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information about the requester:

- UNIX login of the user
- New password for the user

To change a user password for the requester, execute the command line or script procedure steps that have been developed.

3.12.8 Checking a File/Directory Access Privilege Status

3.12.8.1 Checking File/Directory Access Privileges

1 At a UNIX prompt, type **cd *Path*** then press the **Return/Enter** key.

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe, type **cd /home** then press the **Return/Enter** key.

2 From the UNIX prompt, type **ls -la**. The output from the command should appear as follows:

```
drwxrwxrwx    3    mresnick    training    8192    Jun 14 08:34    archive
drwxr-xr-x   11    mresnick    training    4096    Jul 03 12:42    daacdata
-rw-rw-rw-    1    mresnick    training     251    Jan 02 1996     garbage
lrw-r--r--    2    jjones      admin      15237    Apr 30 20:07    junk
-rwxr--rw-    1    mresnick    training    5103    Oct 22 1994     trash
```

- The first column of output is the file access permission level for the file.
- The next column to the right is the number of links to other files or directories.
- The third column is the file owner's user ID
- The fourth column is the group membership of that owner.
- The fifth column shows file size in bytes.
- The sixth column displays the date and time of last modification (if the date is more than six months old, the time changes to the year)
- The last column displays the file name.

3.12.9 Changing a File/Directory Access Privilege

File and directory access privileges are displayed in the first output column of the **ls -l** command and consist of ten characters, known as **bits**. Each bit refers to a specific permission. The permissions are divided into four groupings shown and briefly described in Figure 3.12-3.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Full path of the file/directory on which access privileges will be changed.
- New access privileges to set on the file/directory. Can be any of:
  - New owner
  - New group
  - New user/owner privileges (read, write and/or execute)
  - New group privileges (read, write and/or execute)
  - New other privileges (read, write and/or execute)

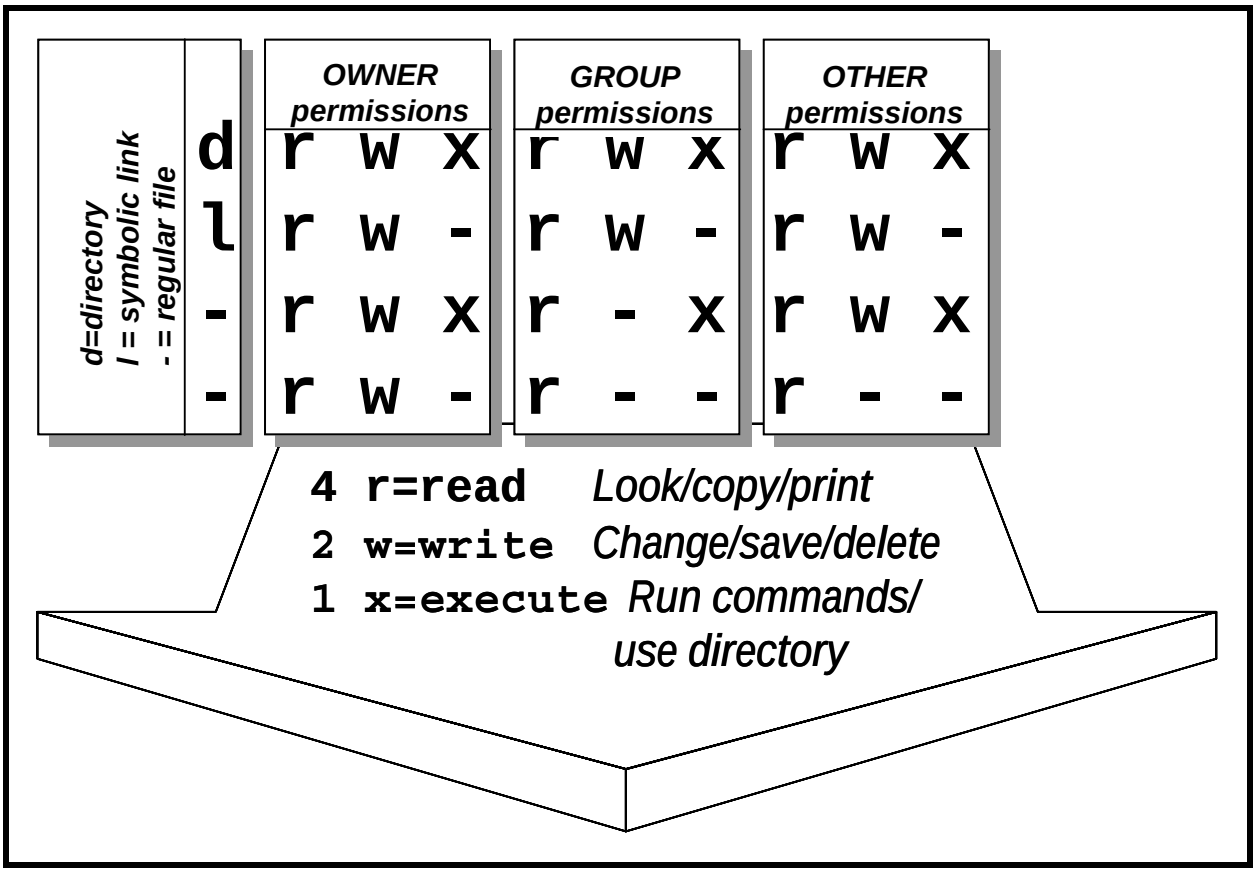


Figure 3.12-3. Access Permissions

3.12.9.1 Changing a File/Directory Access Privilege

1 At the UNIX prompt type **su** then press the **Return/Enter** key.

2 At the **Password** prompt, type <***RootPassword***> then press the **Return/Enter** key.

- Remember that <***RootPassword***> is case sensitive.
- You are authenticated as root.

3 Type **cd *Path*** then press the **Return/Enter** key.

- The ***Path*** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe type **cd /home** then press the **Return/Enter** key.

4 If there is a **New owner** then type **chown** ***NewOwner FileOrDirectoryName*** then press the **Return/Enter** key.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chown** ***NewOwner*** **jdoe** then press the **Return/Enter** key.

5 If there is a **New group** then type **chgrp** ***NewGroup FileOrDirectoryName*** then press the **Return/Enter** key.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chgrp** ***NewGroup*** **jdoe** then press the **Return/Enter** key.

6 If there are **New user/owner privileges** type **chmod u=*NewUserPrivileges*** ***FileOrDirectoryName*** then press the **Return/Enter** key.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod u=*NewUserPrivileges*** **jdoe** then press the **Return/Enter** key.
- The ***NewUserPrivileges*** are "r" for read, "w" for write, and "x" for execute. For example, to give the user/owner read, write and execute privileges, type **chmod u=rwx** ***FileOrDirectoryName*** then press the **Return/Enter** key.

7 If there are **New group privileges** type **chmod g=*NewGroupPrivileges*** ***FileOrDirectoryName*** then press the **Return/Enter** key.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod g=*NewGroupPrivileges*** **jdoe** then press the **Return/Enter** key.
- The ***NewGroupPrivileges*** are "r" for read, "w" for write, and "x" for execute. For example, to give the group read and execute privileges, type **chmod g=rx** ***FileOrDirectoryName*** then press the **Return/Enter** key.

8 If there are **New other privileges** then type **chmod o=*NewOtherPrivileges*** ***FileOrDirectoryName*** then press the **Return/Enter** key.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod o=*NewOtherPrivileges*** **jdoe**, then press the **Return/Enter** key.

- The ***NewOtherPrivileges*** are “r” for read, “w” for write, and “x” for execute. For example, to give others read privileges, type **chmod o=r *FileOrDirectoryName*** then press the **Return/Enter** key.

9 Type **exit** then press the **Return/Enter** key.

- Root is logged out.

3.12.10 Moving a User’s Home Directory

The process of moving a user's home directory begins when the requester submits a request to the Ops Supervisor. The Ops Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user’s home directory. When the changes are complete the SA notifies the requester and Ops Supervisor.

3.13 Commercial Off-the-Shelf (COTS) Software Administration

The EMD organization provides maintenance for EMD hardware, software, and firmware systems delivered under the EMD contract to the EMD sites.

Commercial off-the-shelf (COTS) software and hardware are maintained in accordance with the current *EMD COTS Deployment Plan*, (335-EMD-series document). The project maintenance philosophy for software is to provide EMD centralized support for developed items and vendor support for COTS software.

3.13.1 Installation

EMD Project software consists of COTS, custom-developed and science software.

Software maintenance includes:

- Right to use COTS software products..
- Access to software vendor telephone support
- Access to vendors on-line and email support
- Receive patches and upgrades
- The DAAC maintenance activity includes: software configuration management (CM) including support for change control, configuration status accounting, audit activities, and software quality assurance (QA). Each site is the CM authority over its own resources subject to ESDIS delegation of roles for EMD management.

3.13.2 LOG FILES

Log files must be maintained documenting all COTS installations and modifications. These files delineate manufacturer, product, installation date, modification date and all other pertinent configuration data available.

3.13.3 COTS Configuration

The COTS software upgrades are subject to CCB approval before they may be loaded on any platform. EMD Sustaining Engineering notifies the CCB of the upgrade that has been received. The COTS SW Librarian distributes the COTS software upgrade as directed by the CCB. The site Software Maintenance Engineer, Network Administrator, and the System Administrator are responsible for upgrading the software on the host machine and providing follow-up information to the Configuration Management Administrator (CMA). The site Local Maintenance Coordinator will notify the appropriate personnel (Release Installation Team, System Administrator, Network Administrator, Software Maintenance Engineer) when the COTS software is received and approved by the CCB for installation.

COTS software patches may be provided by the COTS software vendor in response to a DAAC's call requesting assistance in resolving a COTS software problem. The problem may or may not exist at other locations. When a COTS software patch is received directly from a COTS software vendor (this includes downloading the patch from an on-line source), the DAAC's CCB will be informed via CCR prepared by the requesting Operator, System Administrator, Network Administrator or site Software Maintenance Engineer. It is the responsibility of the Operator, System Administrator, Network Administrator or site Software Maintenance Engineer to notify the CCB of the patch's receipt, purpose, installation status and to comply with the CCB decisions. The Operator, System Administrator, Network Administrator or site Software Maintenance Engineer installs COTS software patches as directed by the CCB.

In addition to providing patches to resolve problems at a particular site, the software vendor will periodically provide changes to COTS software to improve the product; these changes are issued as part of the software maintenance contract. Upgrades are issued to licensees of the basic software package. Therefore, the COTS software upgrades will be shipped to the ILS Property Administrator (PA), who receives and enters them into inventory.

3.14 Security

System security architecture must meet the requirements for data integrity, availability and confidentiality. Security Services meet these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity and verify and protect data transfer. To monitor and control access to network services, Security Services use the public domain tool, TCP Wrappers (Note: All DAACs, except for NSIDC do not use TCP Wrapers). Other public domain COTS products — ANLpasswd and Crack— provide additional password protection for local system and network access. The tool Tripwire monitors changes to files and flags any unauthorized changes.

This section defines step-by-step procedures for System Administrators to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management.

3.14.1 Generating Security Reports

Table 3.14-1 contains the activity checklist for Security.

Table 3.14-1. Security - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	User Activity Data	(P) 3.14.1.1	

A log file can be created to keep track of unsuccessful attempts to log into the computer. After a person makes *n* (configurable) consecutive unsuccessful attempts to log in, all these attempts are recorded in the file **/var/log/faillog**. The procedures assume that the file has been created and the operator has logged on as root.

3.14.1.1 User Activity Data

1 At the Linux prompt, type /usr/bin/w [husfV] [user] to show who is logged on and what they are doing.

- w displays information about the users currently on the machine and their processes. The header shows, in this order, the current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes.

2 At the Linux prompt, type /usr/bin/last [-R] [-num] [-n num] [-adiox] [-f file] [-t YYYYMMDDHHMMSS] to show the listing of last logged in users.

- Last searches back through the file /var/log/wtmp (or the file designated by the -f flag) and displays a list of all users logged in (and out) since that file was created. Names of users and tty's can be given, in which case last will show only those entries matching the arguments. Names of ttys can be abbreviated, thus last 0 is the sam as last tty0.

3.14.1.2 User Audit Trail Information

The auditd daemon is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk. Viewing the logs is done with the ausearch or aureport utilities. Configuring the audit rules is done with the auditctl utility. During startup, the rules in /etc/audit.rules are read by auditctl. The audit daemon itself has some configuration options that the admin may wish to customize. They are found in the auditd.conf file.

- OPTIONS
  - -f leave the audit daemon in the foreground for debugging. Messages also go to stderr rather than the audit log.
- SIGNALS
  - HUP causes auditd to reconfigure. This means that auditd re-reads the configuration file. If there are no syntax errors, it will proceed to implement the requested changes. If the reconfigure is successful, a DAEMON_CONFIG event is recorded in the logs. If not

successful, error handling is controlled by space_left_action, admin_space_left_action, disk_full_action, and disk_error_action parameters in auditd.conf.

  - TERM caused auditd to discontinue processing audit events, write a shutdown audit event, and exit.
  - USR1 causes auditd to immediately rotate the logs. It will consult the max log_size_action to see if it should keep the logs or not.

- FILES
  - /etc/auditd.conf - configuration file for audit daemon
  - /etc/audit.rules - audit rules to be loaded at startup
- NOTES
  - A boot param of audit=1 should be added to ensure that all processes that run before the audit daemon starts is marked as auditable by the kernel. Not doing that will make a few processes impossible to properly audit.

This page intentionally left blank.

4. Database Administration

4.1 System Overview

The general system design of the Database Administration system is to receive data from external sources; save data in either long-term or permanent storage; produce from the data higher-level data products; and provides data access support to scientist and other registered clients.

4.1.1 Information Model

The Earth Science Information Model characterizes earth science data as a data pyramid consisting of broad, multi-layered data categories as shown in Figure 4.1-1. Logical collections of data, based on their expected relationships, are developed to capture the variability in remote sensing instruments, science disciplines, and other characteristics of the earth science community. For example, some products have related properties (e.g., cloud type and cloud drop size) while other products are dissimilar (e.g., land vegetation indices and ocean productivity), which suggest certain logical groupings. Characteristics are often similar across a particular science discipline and across products generated from a given instrument but different among the various provider sites because of differing science disciplines focus and organizational autonomy.

Metadata. *Metadata are data about data that are provided to the system by the external data provider or the generating algorithm*. They describe characteristics of data origin, content, format, quality, and condition. They also provide information to process and interpret data. Metadata are required for access to all data in the system.

An earth science metadata model supports the data standardization necessary for total system interoperability within a heterogeneous, open systems environment. (Refer to the latest version of the *Earth Science Data Model*; e.g., 420-EMD-001, Implementation Earth Science Data Model for the EMD Project.) The data model includes diagrams that illustrate the relationships of classes, the attributes contained within the classes, the characteristics of the relationships between classes, and the attribute specifications.

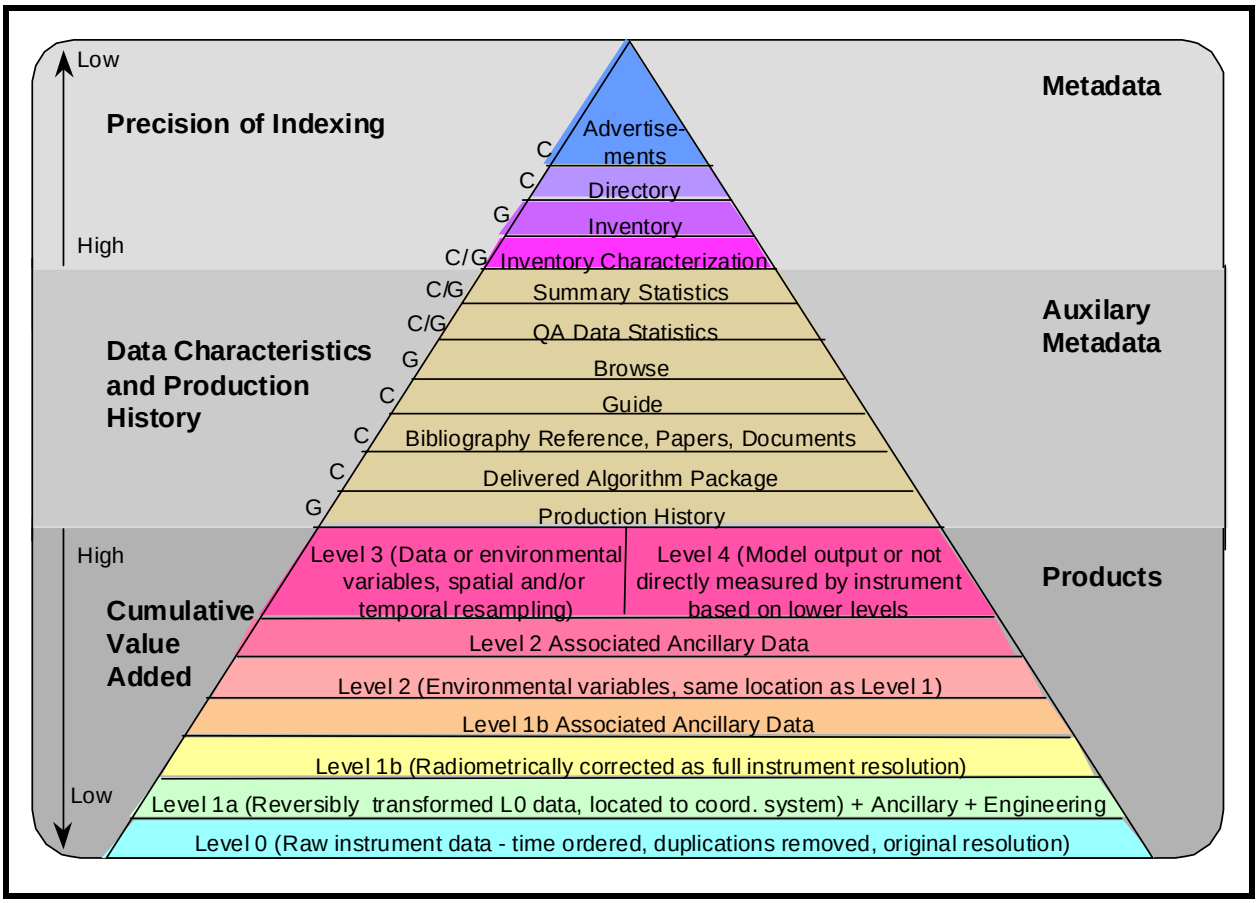


Figure 4.1-1. Earth Science Information Model

Attributes are descriptors of data populating searchable database fields, enabling finite classification of data residing in the system. Attributes can either be collection-level or granule-level attributes and either core or product-specific attributes. A collection is a grouping of related science data. A granule is the smallest aggregation of data that is independently managed (i.e., ingested, processed, stored, or retrieved) by the system. The majority of attributes in the data model are collection-level attributes, which means that they apply to all granules in the collection.

Data Products. *Data products are a processed collection of one or more parameters packaged with associated ancillary and labeling data and formatted with uniform temporal and spatial resolution, e.g., the collection of data distributed by a data center or subsetted by a data center for distribution.* There are two types of data products:

- Standard, which is a data product produced at a DAAC by a community consensus algorithm for a wide community of users.

- Special, which is a data product produced at a science computing facility by a research algorithm for later migration to a community consensus algorithm and can be archived and distributed by a DAAC.

Data products are categorized by levels, which are described in shown in Figure 4.1-2 and described in Table 4.1-1.

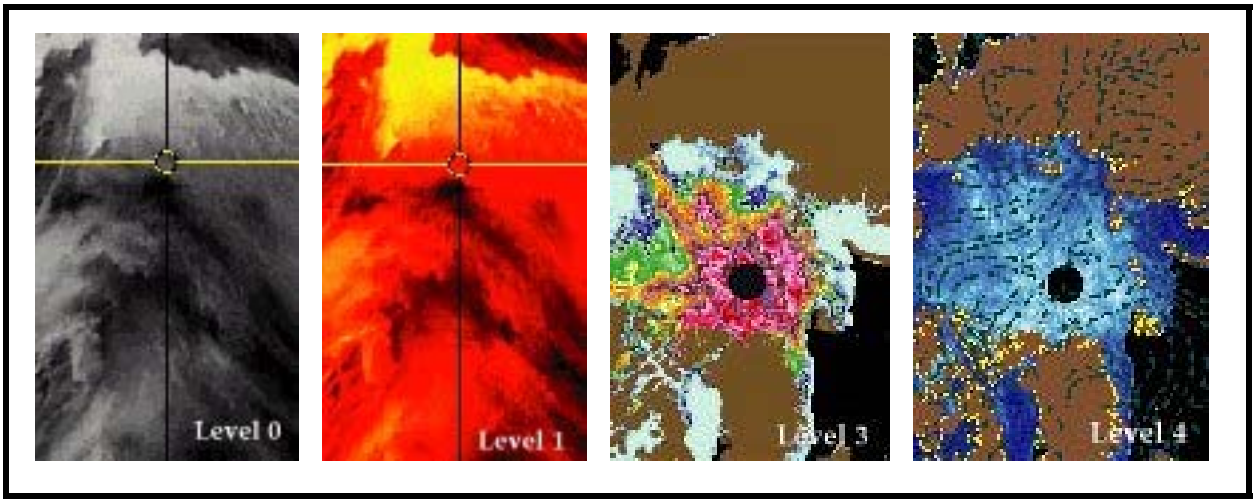


Figure 4.1-2. An Example of Data Product Levels

Table 4.1-1. Data Product Level Definitions

Level	Definition
0	Reconstructed, unprocessed instrument/payload data at full resolution; any and all communications artifacts (e.g., synchronization frames, communications headers, duplicate data removed)
1A	Reconstructed unprocessed instrument data at full resolution, time-referenced, and annotated with ancillary information, including radiometric and geometric calibration coefficients and geo-referencing parameters (e.g., platform ephemeris computed and appended but no applied to the Level 0 data)
1B	Level 1A data that have been processed to sensor units (not all instruments will have a Level 1B equivalent)
2	Derived geophysical variables at the same resolution and location as the Level 1 source data
3	Derived geophysical variables mapped on uniform space-time grid scales, usually with some completeness and consistency
4	Model output or results from analyses of lower-level data (e.g., variables derived from multiple measurements)

4.1.2 Subsystems

The system is comprised several subsystems, see table 4.1-2. More detailed information can be found in the *Segment/Design Specification for the EMD Project* (305-EMD-100). The primary functions of the remaining subsystems can be grouped into the following four categories:

- **Data Ingest**. Ingest is accomplished by means of the Data Pool-Ingest Subsystem (DPL), which interfaces with external applications and provides data staging capabilities and storage for an approximately 1-year buffer of Level 0 data so that reprocessing can be serviced from local storage.
- **Data Storage and Management**. Data storage and management is provided by the Data Server Subsystem (DSS), which can archive science data, search for and retrieve archived data, manage the archives, and stage data resources needed as input to science software or resulting as output from their execution. The Data Server Subsystem provides access to earth science data in an integrated fashion through an application programming interface (API) that is common to all layers.
- **Information Search and Data Retrieval**. Search and retrieval is accomplished by the science user interface functions in the Client Subsystem (CLS), and by information search support functions in the Data Management Subsystem (DMS).

Table 4.1-2. Subsystem Functions (1 of 2)

Subsystem		Functions
Client	CLS	The client part of the client-server access paradigm through graphical user interface and data/service access tools, as well as application program interface (API) libraries to system services
Internetworking	ISS	Provides networking services based on protocols and standards corresponding to the lower four layers of the Open Systems Interconnection (OSI) reference model: the transport layer's TCP and UDP protocol, the network layer's IP protocol, and the physical/data link layer's Ethernet, FDDI, and Gigabit Ethernet protocols.
Data Management	DMS	System wide distributed search and access services with multiple science discipline views of data collections and "one-stop shopping" with location transparent access to those services and data.
Data Server	DSS	Locally optimized search, access, archive and distribution services with a science discipline view of data collections and an extensible Earth Science Data Type and Computer Science Data Type view of the archive holdings
DPL Ingest Service	DPL	Clients for importing data (science products, ancillary, correlative, documents, etc.) into system data repositories (data servers) on an *ad hoc* or scheduled basis and deals with external system interfaces
Management	MSS	Functions for system startup/shutdown, resource management, performance monitoring, error logging, system and science software configuration management, and resource accounting

Table 4.1-2. Subsystem Functions (2 of 2)

Subsystem		Functions
Communications	CSS	The distributed computing infrastructure that enables intra- and inter-site communications between the subsystems. From a scientist user's perspective, the system infrastructure appears as services, and interfaces to services, which are displayed on the user's workstation desktop. This perspective is similar to the view of the World Wide Web (WWW) servers as seen through a local client such as Netscape.
Data Pool Ingest	DPL	Provides on-line access for browsing and FTP download of selected granules, metadata, and browse data.
Spatial Subscription Server	SSS	Permits creation and management of subscriptions for data distribution/ notification and Data Pool insert
Order Manager	OMS	Manages orders from EDG and other sources and either distributes the data through the Data Pool (either electronically or on hard media) or dispatches requests to appropriate system services (e.g., SDSRV).

4.1.3 Databases

Custom Databases. The custom databases described in Table 4.1-3 encompass the majority of the subsystem persistent data requirements. Other data requirements are met through the use of flat files, which are described below. The Science Data Server Database will subsequently be turned off upon successful implementation 7.21. All custom databases are implemented using Sybase.

Table 4.1-3. Custom Databases (1 of 2)

Database Name	Document Number	DB Software	Logical Categories
Science Data Server Subsystem (SDSRV)	311-EMD-101	Sybase	Database Version Information
			System Management Data
			Collection, Granule Metadata
			DAP Metadata
			Spatial Metadata
			Data Originator Metadata
			Granule Metadata
			Contact Metadata
			Collection Metadata
			Temporal Metadata
			Planning Data
			Data Processing Data

Table 4.1-3. Custom Databases (2 of 2)

Database Name	Document Number	DB Software	Logical Categories
EcInDb		Sybase	Database Version Information
			Datatype Information
			Configuration Data
			Active Requests
			Validation Data
			Table Locking Information
Ingest Subsystem (INS)	311-EMD-100	Sybase	Database Version Information
			Datatype Information
			Configuration Data
			Active Requests
			Validation Data
			Table Locking Information
Systems Management Subsystem (MSS)	311-EMD-103	Sybase	Database Version Information
			Order Information
			Site Information
			Validation Data
			User Data
Data Pool (DPL)	311-EMD-106	Sybase	Collection Metadata
			Granule Metadata
			Insert Action Data
Order Manager Server (OMS)	311-EMD-104	Sybase	Queue/Status Information
			Request Information
			Intervention Information
Spatial Subscription Server (SSS)	311-EMD-105	Sybase	Database Version Information
			Subscription Information
			Event Information
			Action Information

4.1.4 Flat Files

A flat file is an operating system file that is read and written serially. Flat file data are fairly static and have no explicit relationship to other data in the enterprise. There are cases when the implementation of certain persistent data is better suited to a flat file than to a database, e.g., system configuration data, external interface data, log files. Flat files used in the system are described in Table 4.1-4.

Table 4.1-4. Flat Files

Database	Flat File Attributes			
	Usage	**Types**	**Formats**	**Descriptions**
SDSRV	Yes	UNIX flat file; ELF 32-bit MSB dynamic lib SPARC Version 1, dynamically linked	Variable length, Dynamic Link Library (DLL)	Log files, configuration files, template used to validate ESDTs on installation, uniquely named ESDT file descriptors, generic to ESDT-specific processing capabilities
DMS	Yes	UNIX flat file	Variable length	Log files, configuration files
INS	Yes	UNIX flat file	Variable length	Log files, configuration files, data delivery records
REGIST	No			
MSS	Yes	ASCII, binary	Single line records, one/two fields; EcAgEvent objects; MsAgMgmtHandle object; integers; string lists	Accountability component files, subagent component files
NM	No			
DPL	Yes	ASCII	Variable length	For Data Pool Access Statistics Utility, temporary storage of data to be exported to database
OMS	No			
SSS	No			

4.1.5 Resident Databases

Table 4.1-5 shows the custom and COTS databases that are resident at the DAACs. Each resident database is individually installed and maintained.

Table 4.1-5. Resident Databases

Databases	SMC	DAAC		
		LaRC	LP DAAC	NSIDC
Custom				
Science Data Server Subsystem (SDSRV)		✔	✔	✔
Data Management Subsystem (DMS)	✔	✔	✔	✔
Registry (REGIST [MSS])	✔	✔	✔	✔
Systems Management Subsystem (MSS)	✔	✔	✔	✔
NameServer (NM)	✔	✔	✔	✔
Data Pool Ingest (DPL_INS)		✔	✔	✔
Order Manager Subsystem (OMS)		✔	✔	✔
Spatial Subscription Server (SSS)		✔	✔	✔

4.1.6 Database Directory Locations

Locations of principal database components are shown in Table 4.1-6.

Table 4.1-6. Location of Principal Database Components

Name	Variant	Vendor	Principal Directory	Comments
Software Developer's Kit (formerly Open Client)	PC	Sybase	c:\windows\system	
Software Developer's Kit (formerly Open Client)	LINUX	Sybase	/tools/sybOCv15.0.0.	Just utilities, not libraries
Software Developer's Kit (formerly Open Client)	LINUX	Sybase	/tools/sybOCv15.0.0	
Red Hat Enterprise Linux 4	Red Hat	Linux		
ASE Server Monitor Client/Svr	LINUX	Sybase	/usr/ecs/<mode>/COTS/sybase	At DAAC discretion/ required for launch
Spatial Query Server (SQS)	Linux	Boeing	/usr/ecs/OPS/COTS/sqs_362	
Sybase Adaptive Svr Enterprise	LINUX	Sybase	/usr/ecs/OPS/COTS/sybase	/usr/ecs/OPS/COTS/sybase_125 or sybase125 is an acceptable install dir.
Sybase Central	PC	Sybase	C:\sybase	

4.2 Database Management

4.2.1 Database Management Model

The concept that forms the basis of database management is described in *EOSDIS Core System Science Information Architecture* (FB9401V2). The EMD database management model is a variant of the ISO Data Management Reference Model (ISO 10032:1994). The variation is in the local (site) data management. The ISO reference model does not provide a structure for local data management. EMD defines local data management as being provided by a local information manager and a collection of data servers.

The model permits the following services and requests:

- *Client is a program requesting data management services*. A client can be an application program, such as a science algorithm, or a user interface, for example, an interface for formulating database queries and displaying query results. The client may use a data dictionary or vocabulary to assist in the formulation of database requests.
- *Data Server is an instance of a service that is capable of executing data access, query, and manipulation requests against a collection of data*. Data server actually refers to a service provider at a logical level. The data server may actually be constructed from multiple physical servers implementing various aspects of the data server's functionality. Data servers use lower layers of data management services, which are described in the data server architecture, section 6.4. Note that a site may choose to provide access to the same data via several different data servers, perhaps supporting different data access and query languages.
- *Data Dictionary Service is* a service that manages and provides access to databases containing information about data. Each data object, data element, data relationship, and access operation available via data servers is defined and described in the dictionary databases. Data dictionaries are intended for access by users (e.g., to obtain a definition of a data item) and programs (e.g., to format a screen).
- *Vocabulary Service is* a service that manages and provides access to databases containing the definition of terminology, e.g., of words and phrases. Vocabularies are intended for access by users (e.g., to obtain the appropriate term given a meaning) and programs (e.g., to let a user identify the intended meaning of a term which has several alternative definitions).

The model identifies the following key data objects supporting these services:

- *Schema is* a formal description of the content, structure, constraints, and access operations available for or relevant to a database or a collection of databases. The reference model contains Data Server and Data Dictionary/Vocabulary schema.

The model provides for the following kinds of requests:

- *Query is a request formulated in a language offered (i.e., supported) by a data server.* It contains data search and access specifications expressed in terms defined either by

the language itself, or in a schema offered by the corresponding server. In general, a query language is paired with a particular type of schema. For example, relational queries reference objects defined in a relational schema.

- *Data Access Request is a service request that invokes an operation offered by a data server on a data object or a set of data*. The object types and the operations that a given service offers for them are described in the schema used by the service.

In addition, Data Servers conform to the general interface requirements as prescribed by the Interoperability Architecture. For example, this means that Data Servers accept requests regarding the status and estimated cost of a query or data access request. The servers also use the Interoperability Services in the course of their interactions. For example, clients use request brokers in order to locate a data dictionary service.

4.2.2 Database Management Implementation

4.2.2.1 Software

As previously described, system databases are primarily based on Sybase software. Primary components include:

- **Sybase Adaptive Server Enterprise (ASE)**. ASE is an integrated set of software products for designing, developing and deploying relational database applications. It consists of a high-performance relational database management system (RDBMS), which runs database servers, and a collection of applications and libraries, which run on database clients. This arrangement, consisting of servers that are accessed by multiple clients over a network, forms the basis for Sybase's client/server architecture. ASE components are described in Table 4.2-1. An illustration of the main screen of Sybase Central, which can be used to perform many of the DBA procedures described in subsequent sections of this document, is shown in Figure 4.2-1.
- **Other Sybase Components:**
  - **Spatial Query Server (SQS)**. The Spatial Query Server (SQS) is a multi-threaded Sybase Open Query database engine that is used by the Science Data Subsystem (SDSRV). This product allows definition of spatial data types, spatial operators, and spatial indexing. SQS communicates with the Sybase ASE Server to process SDSRV requests to push and pull metadata. Both the SDSRV database server and the SQS server resides on the same Linuxmachine.

Table 4.2-1. Sybase Adaptive Server Enterprise (ASE) Components (1 of 2)

Type	Component	Description	Sub-Components and Features
Client	Sybase Central	A Windows application for managing Sybase databases. Helps manage database objects and perform common administrative tasks.	Connecting to, disconnecting from, and stopping servers
			Troubleshooting Adaptive Server problems
			Managing data caches
			Managing Adaptive Server physical resources
			Creating, deleting, backing up, and restoring databases
			Creating and deleting Adaptive Server logins, creating and deleting database users and user groups, administering Sybase roles, and managing object and command permissions
			Monitoring Adaptive Server performance data and tuning performance parameters
Client	Software Developer's Kit (formerly Open Client)		CS-Library, which contains a collection of utility routines used by all client applications.
			Client-Library and DB-Library, which contains a collection of routines that are specific to the programming language being used in an application
			Net-Library, which contains network protocol services that support connections between client applications and Adaptive Server.
			Utilities: isql – an interactive query processor that sends commands to the RDBMS from the command line. bcp – a program that copies data from a database to an operating system file, and vice versa. defncopy - a program that copies definitions of database objects that from a database to an operating system file and vice-versa.

Table 4.2-1. Sybase Adaptive Server Enterprise (ASE) Components (2 of 2)

Type	Component	Description	Sub-Components and Features
Server	Adaptive Server (ASE)	Sybase's high-performance RDBMS	
	Backup Server(TM)	A server application that runs concurrently with Adaptive Server to perform high-speed on-line database dumps and loads.	
	Adaptive Server Monitor	Monitor Server	Allows capture, display, and evaluation of Adaptive Server performance data and tune Adaptive Server performance
		Historical Server	Writes the data to files for offline analysis

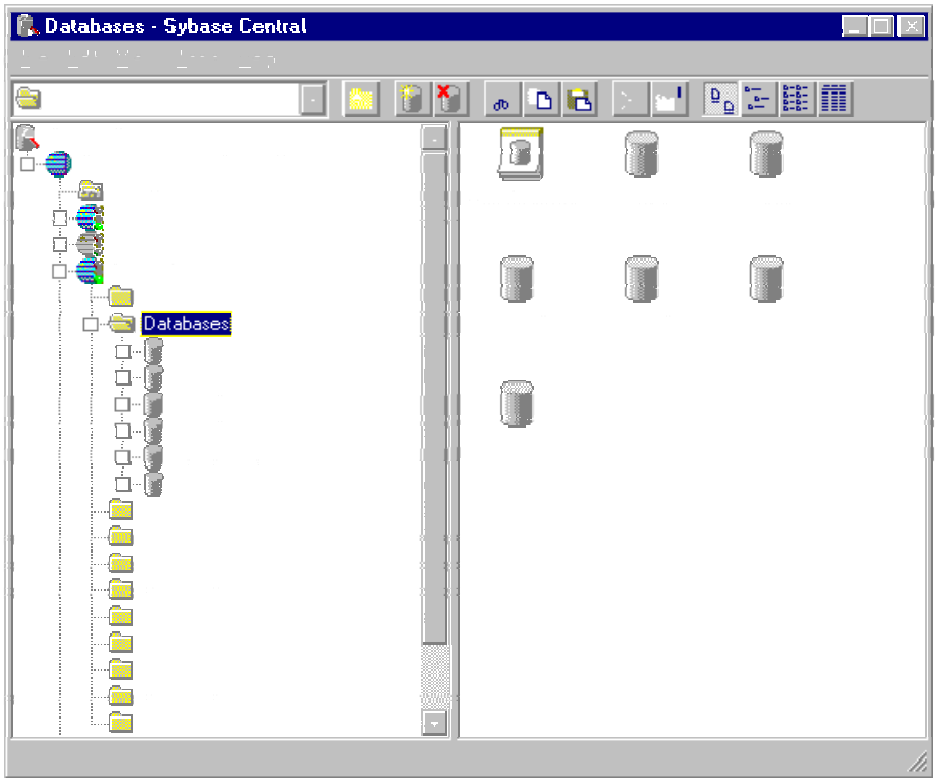


Figure 4.2-1. Sybase Central

4.2.3 Hardware, Software, and Database Mapping

Currently, user database reside on Linux machines. They can be managed using PCs (Sybase Central only). Mapping documents for the DAACs are available on the web at http://cmdm-ldo.raytheon.com/baseline/, through the **Technical Documents** link. The hardware layout diagrams are available in documents 920-TD*x*-001, *Hardware-Design Diagram*. Hardware to software mappings are available in documents 920-TD*x*-002 *Hardware-Software Map*. The hardware database mappings are available in document 920-TD*x*-009 *DAAC HW Database Mapping*.

4.3 Database Administrator

The Database Administrator (DBA) is the individual responsible for the installation, configuration, update/upgrade, maintenance, and overall integrity, performance and reliability of system databases. In general, the DBA is concerned with the availability of the server, the definition and management of resources allocated to the server, the definition and management of databases and objects resident on the server, and the relationship between the server and the operating system. Basic DBA responsibilities include:

- Performing the database administration utilities such as database backup, maintenance of database transaction logs, and database recovery.
- Monitoring and tuning the database system (e.g., the physical allocation of database resources).
- Maintaining user accounts for the users from the external system. The DAAC database administrator creates user registration and account access control permissions in the security databases.
- Creating standard and *ad hoc* security management reports of stored security management data using the Sybase report generator.
- Working with EMD sustaining engineering and DAAC system test engineers to set up a test environment as needed.
- Working with the data specialist on information management tasks involving databases, data sets, and metadata management.

4.3.1 DBA Tasks and Procedures

Basic DBA tasks and procedures are described in the following sections. Table 4.3-1 shows DBA tasks that have to be done on a regular basis and the section where they are addressed in this document.

Table 4.3-1. DBA Tasks Performed on a Regular Basis

Time Period	Task	Importance	Found In …
Daily	Capture database configurations	Absolutely necessary for database recovery if problems occur	Configuring Databases
	Reclaim disk space		/usr/ecs/OPS/CUSTOM/dbms/COMDBAdmin/EcCoDbSyb_Reorg compact
	Run after reorg compact	only necessary if you want statistics for non-leading columns of the index	/usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CustomizedDbStat
	Remove old dump files.	Keeping tack of seven (7) days worth of retrievable data or can specify another value.	/usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CleanupDumps
Weekly	Monitor Sybase disk usage		Monitoring and Tuning Databases
	Clean up old files		
Monthly	Reboot		Starting and Stopping Servers
Before and After Installations	Run DbVerify scripts		Installing Databases and Patches

Subsequent sections related to Database Administration address the following topics:

- **Section 4.4** An overview of the process and step-by-step procedures for starting and stopping database servers.
- **Section 4.5** An overview of the process and step-by-step procedures for creating database devices.
- **Section 4.6** An overview of the process and step-by-step procedures for installing databases and patches.
- **Section 4.7** An overview of the process and step-by-step procedures for configuring databases.
- **Section 4.8** An overview of the process and step-by-step procedures for working with indexes, segments, and caches.
- **Section 4.9** An overview of the process and step-by-step procedures for backing up and recovering data.
- **Section 4.10** An overview of the process and step-by-step procedures for establishing database security.
- **Section 4.11** An overview of the process and step-by-step procedures for copying individual databases.

- **Section 4.12** An overview of the process and step-by-step procedures for bulk copying.
- **Section 4.14** An overview of the process and step-by-step procedures for performance monitoring, tuning, and problem reporting.
- **Section 4.15** An overview of the process and step-by-step procedures for ensuring database quality.
- **Section 4.16** An overview of the process and step-by-step procedures for Sybase troubleshooting.

4.4 Starting and Stopping Database Servers

Each procedure outlined has an **Activity Checklist** table that provides an overview of the task to be completed. The outline of the **Activity Checklist** is as follows:

Column one - ***Order*** shows the order in which tasks could be accomplished.

Column two - ***Role*** lists the Role/Manager/Operator responsible for performing the task.

Column three -***Task*** provides a brief explanation of the task.

Column four - ***Section*** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found.

Column five - **Complete?** is used as a checklist to keep track of which task steps have been completed.

Table 4.4-1, below, provides an Activity Checklist for starting and stopping database servers.

Table 4.4-1. Starting and Stopping Database Servers - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Start ASE Servers	(P) 4.4.1.1	
2	DBA	Start the ASE Backup Server	(P) 4.4.1.2	
3	DBA	Start the ASE Monitor Server	(P) 4.4.1.3	
4	DBA	Stop the ASE Monitor Server	(P) 4.4.1.4	
5	DBA	Stop the ASE Backup Server	(P) 4.4.1.5	
6	DBA	Stop the ASE Server	(P) 4.4.1.6	

4.4.1 Start Adaptive Server Enterprise (ASE) Servers

A server process is started manually when a new server is installed or after a system outage. In order to perform the procedure, the DBA must know the database server name and be assigned sa_role (refer to Section 4.10, Establishing Database Security). The following procedures are applicable.

4.4.1.1 Start ASE Servers

1 Log in to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press the **Return/Enter** key.

3 Log into the server on which the ASE Server Process is to be started by typing: **/tools/bin/ssh *ServerName***, then press the **Return/Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key.

- Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

6 Log into the server as sybase, type, ***su – sybase*** and press the **Return/Enter** key.

- A password prompt is displayed.

7 Enter ***sybase password***, then press the **Return/Enter** key.

- You are authenticated as yourself and returned to the UNIX prompt.

8 At the UNIX prompt, type **cd /ASE-12_5/install** and then press the **Return/Enter** key.

9 At the UNIX prompt, type **./RUN_*servername* &** then press the **Return/Enter** key.

10 At the UNIX prompt, type **showserver**, then press the **Return/Enter** key.

- This displays a listing of the ASE Server processes that are running.

4.4.1.2 Start the ASE Backup Server

NOTE: This procedure should be done after ASE Server is up and running

1 Log in to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press the **Return/Enter** key.

3 Log into the server on which the ASE Server Process is to be started by typing: **/tools/bin/ssh *ServerName***, then press the **Return/Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key.

- Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

6 Log into the server as sybase, type, ***su – sybase*** and press the **Return/Enter** key.

- A password prompt is displayed.

7 Enter ***sybase password***, then press the **Return/Enter** key.

- You are authenticated as yourself and returned to the UNIX prompt.

8 Type **cd /ASE-12_5/install** and press the **Return/Enter** key.

9 Type, **./RUN_*backupservername* &** and press the **Return/Enter** key.

NOTE: You may have to hit the **Return/Enter** key one more time

4.4.1.3 Start the ASE Monitor Server

NOTE: This procedure is be done on an as needed basis and after the ASE Server is up and running

1 Log in to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press the **Return/Enter** key.

3 Log into the server on which the ASE Server Process is to be started by typing: **/tools/bin/ssh *ServerName***, then press the **Return/Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

6 Log into the server as sybase, type, ***su – sybase*** and press the **Return/Enter** key.
- A password prompt is displayed.

7 Enter ***sybase password***, then press the **Return/Enter** key.
- You are authenticated as yourself and returned to the UNIX prompt.

8 Type **cd /ASE-12_5/install** and press the **Return/Enter** key.

9 Type **./ RUN_monitor_srvr** and press the **Return/Enter** key.

Servers are stopped by the DBA when the system needs to be brought down. Servers are brought down in an order that is the reverse of the start-up order. The **shutdown** command issued from within isql shuts down the server where you are logged in. It allows for the completion of any current processes and blocks the start of any new processes before the server is shutdown.

When you issue a **shutdown** command, the server:

- Disables all logins except the sa's.
- Performs a checkpoint in each database, moving changed pages from memory to disk.
- Waits for currently executing SQL statements or procedures to finish.

Adding a **nowait** option to the command immediately terminates all processes and shuts down the server. The **nowait** option should be used sparingly because it may cause data loss and complicate recovery.

4.4.1.4 Stop the ASE Monitor Server

NOTE: This procedure should be done before the ASE Server is shutdown

1 Log on to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press the **Return/Enter** key.

3 Log into the server on which the ASE Server Process is to be stopped by typing: **/tools/bin/ssh *ServerName***, then press the **Return/Enter** key.
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key.
- Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

6 Log into the server as sybase, type, ***su – sybase*** and press the **Return/Enter** key.
- A password prompt is displayed.

7 Enter ***sybase password***, then press the **Return/Enter** key.
- You are authenticated as yourself and returned to the UNIX prompt.

- Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.

NOTE: Environment and DS queary are set when you use su – sybase, if not use $SYBASE/bin/ in command line.

8 Type **isql –Usa** and press the **Return/Enter** key.

9 Type the ***sa-password*** when prompted for it and press the **Return/Enter** key.

10 Type **sms_shutdown** at "**1>**" prompt and press the **Return/Enter** key.

11 Type **go** at "**2>**" prompt and press the **Return/Enter** key.

4.4.1.5 Stop the ASE Backup Server

NOTE: This procedure should be done before shutting down the ASE Server

1 Log on to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press the **Return/Enter** key.

3 Log into the server on which the ASE Server Process is to be stopped by typing: **/tools/bin/ssh *ServerName***, then press the **Return/Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key.

- Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

6 Log into the server as sybase, type, ***su – sybase*** and press the **Return/Enter** key.

- A password prompt is displayed.

7 Enter ***sybase password***, then press the **Return/Enter** key.

- You are authenticated as yourself and returned to the UNIX prompt
- Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.

8 Type, **isql –U<username>** and press the **Return/Enter** key.

9 Type the ***password*** when prompted for it and press the **Return/Enter** key.

10 Type **shutdown SYB_BACKUP** at the "**1>**" prompt and press the **Return/Enter** key.

11 Type **go** at the "**2>**" prompt and press the **Return/Enter** key.

4.4.1.6 Stop the ASE Server

1 Use **shutdown** to bring the server to a halt.

- This command can only be issued by the Sybase System Administrator (sa).
- If you do not give a server name, shutdown shuts down the ASE Server you are using.
- Syntax:

  1> shutdown [with] [wait] [with nowait]
  2> go

2 To see the names of the backup servers that are accessible from your ASE Server, execute **sp_helpserver**.

- Use the value in the name column in the shutdown command.
- You can only shut down a Backup Server that is:
  - Listed in **sysservers** on your ASE Server
  - Listed in your local interfaces file

4.5 Creating Database Devices

Table 4.5-1, below, provides an Activity Checklist for creating database devices.

Table 4.5-1. Creating Database Devices - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Create a Database Device	(P) 4.5.1.1	

4.5.1 Create a Database Device

Database devices store the objects that make up databases. The term "device" can refer to either a physical or a logical device. Logical devices include any portion of a disk, such as a *partition* or a *file* in the file system used to store databases and their objects. A database device can be created when the System Administrator determines that new disk space is available for database use or as part of the recovery process. The System Administrator makes a request to the Data Base Administrator (DBA), who creates the new database device and notifies the System Administrator when the device has been created.

In order to create a new device, the DBA must have the following:

- The name of database device to be created
- A physical device on which to place database device
- The device size in megabytes
- The name of the mirror device, if one is in effect

*The creation of a database device is the mapping of physical space to a logical name and virtual device number (**vdevno**) contained in the master database*. The **disk init** command is used to initialize this space. **Disk init** syntax is:

name = device_name
physname = physicalname
vdevno = virtual_device_number (optional: will use the next available number)
size = number_of_blocks
[vstart = virtual_address
cntrltype = controller_number] (optional)

Before you run **disk init**, see the server installation and configuration guide for your platform for information about choosing a database device and preparing it for use with the server. You may want to repartition the disks on your computer to provide maximum performance for your databases. **Disk init** divides the database devices into allocation units of 256 2K pages, a total of 1/2MB. In each 256-page allocation unit, the **disk init** command initializes the first page as the allocation page, which will contain information about the database (if any) that resides on the allocation unit.

Once initialization is complete, the space described by the physical address is available to the server for storage and a row is added to the **sysdevices** table in the master database. The initialized database can be:

- Allocated to the pool of space available to a user database
- Allocated to a user database and assigned to store a specific database object or objects
- Used to store a database's transaction logs

NOTE: Unless you are creating a small or non-critical database, always place the log on a separate database device.

After you run the **disk init** command, be sure to use **dump database** to dump the master database. This makes recovery easier and safer in case master is damaged. If you add a device and fail to back up master, you may be able to recover the changes with **disk reinit**.

4.5.1.1 Create a Database Device

NOTE: This procedure will assist in creating a database device.

1 Log on to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press the **Return/Enter** key.

3 Log into the server on which the new database device is to be created by typing: **/tools/bin/ssh <*ServerName*>**, then press the **Return/Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key.

- Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

NOTE: For each database device to be created, perform Steps 6 through 9.

6 Using the text editor of your choice, edit ***DeviceName*.sql** and make changes to information enclosed in brackets (including the brackets) as appropriate:

- An example of an **add_devices.sql** file for creation of a database device is shown in Figure 4.5-1.

```
/*******************************************************/
/* name: [add_devices.sql]                             */
/* purpose:                                            */
/* written:                                            */
/* revised:                                            */
/* reason:                                             */
/*******************************************************/
disk init name = [device name],
physname = "/dev/[device name]",
vdevno = [#],
size = [size]
go
sp_helpdevice [device name]
go
```

Figure 4.5-1. Example of an add_devices.sql File for Creation of a Database Device

- In the area delimited by **/* */**, enter an appropriate description of the script including the file name, date written and person who wrote the script, its purpose, and any other information deemed appropriate. Be sure to enclose each line of the comment between **/* */**.
- The **disk init name** is the ***DeviceName*** is used in Step 8 above. You may not use spaces or punctuation except the underscore character (_) in ***DeviceName***. Remember that the name you assign is case-sensitive. Be sure there is a comma after ***DeviceName***
- The physname is the *FullPath_to_DeviceName*. Be sure to enclose *FullPath_to_DeviceName* in double quotes. Be sure to place a comma after ***FullPath_to_DeviceName*** but outside the double quotes.

- The **vdevno**, an optional command in this current version of ASE, is the ***VirtualDeviceNumber***. **vdevno** is a unique identifying number for the database device. It is unique among all the devices used by ASE Server and is never reused. Device number 0 represents the device named **d_master** that stores the system catalogs. Legal numbers are between 1 and 255, but the highest number must be one less than the number of database devices for which your system is configured. For example, for a system with the default configuration of 10 devices, the legal device numbers are 1-9. The default of 10 devices can be changed using **sp_configure**, If a number is specified, ASE assigns the next available virtual device number. This feature helps to eliminate the possibility of using an existing number, which Sybase will usually return the message, "device activation error." The next available number can be determined by looking at the output from the **sp_helpdevice** command and selecting the next number in sequence.
- The **size** is the ***DeviceSize*** in blocks. To compute the number of blocks, multiply the device size in megabytes by 512; e.g., a 1,000 Mb device has 512,000 blocks

7 After the changes have been made, save the file according to the rules of your text editor.

8 At the UNIX prompt, type **isql –U*username* -S*ServerName* -i*DeviceName*.sql -o*Device Name.out*** then press the **Return/Enter** key.

- ***ServerName*** is the name of the server on which the database device will be created.
- ***DeviceName.sql*** is the name of the script file you created in step 8.
- ***DeviceName.out*** is the filename of the script's output for confirmation and/or troubleshooting purposes.)
- The system will prompt you for a password.

9 At the **Password:** prompt, type the **<*password*>** then press the **Return/Enter** key.

- When the UNIX prompt is again displayed the process is complete.

10 At the UNIX prompt, type **more *DeviceName.out***, then press the **Return/Enter** key.

- This allows you to view the ***DeviceName.out*** file to confirm that the device has been created or to check for device creation errors.

4.6 Installing Databases and Patches

Table 4.6-1, below, provides an Activity Checklist for installing databases and patches.

Table 4.6-1. Installing Databases and Patches - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Install a Database Patch (Example)	(P) 4.6.2.1	

4.6.1 Perform a Database Build Procedure (Example Only)

The ECS Assistant is a custom application that simplifies the process of installing, testing and managing system software. The **Subsystem Manager** screen is used in the operational environment. The **Database** option is used to install, drop, patch, and update subsystem-specific databases. The **Install** option is used to install custom software in a particular mode. The **Configuration** option is used to create CFG, ACFG and PCFG files for selected components. The **Stage Area Installation** option is used to input the staging location where the delivered software is stored. The **View Task Output** option is used to view results as the specified task is executing. A detailed description of ECS Assistant use can be found in 609-EMD-001, *Release 7.11 Operations Tools Manual for the EMD Project*.

To perform a database build follow the steps included in the documentation (e.g., release notes) that specifies performing the build. The following steps are an example of a database that was built and populated with data from the version of the database that the new database was replacing. Unless otherwise specified, the scripts that were run are located in the **/usr/ecs/<MODE>/CUSTOM/dbms/<SUBSYSTEM>** directory.

<DBNAME>

4.6.2 Install a Database Patch (Example)

To install a database patch follow the steps included in the documentation (e.g., release notes) that specifies installing the patch. To install database patches, perform the following steps for all subsystems/components and then perform the appropriate subsystem/component-specific procedures.

4.6.2.1 Install a Database Patch (Example)

1 Verify the current version of the database being patched.

 # isql -S <server_ name> -U <db_ user_ name> -P <db_ user_ password>
 # use <db_ name>[_< MODE>]
 # go
 # select * from EcDbDatabaseVersions where EcDbCurrentVersionFlag=" Y"
 # go

2 Compare the current database version against the appropriate version listed in the table provided in the patch instructions.

- If the current version is greater than or equal to the appropriate version listed in the table, continue with the database patch.
- If the current version is less that the appropriate version listed in the table, stop and patch the deficient database.

3 From the **ECS Assist Subsystem Manager** select the appropriate mode, subsystem, and component from the main window.

4 From the **ECS Assist Subsystem Manager** select **DbPatch** from the **Database** menu.

- A **File Selection** window appears.

5 From the **ECS Assist Subsystem Manager** (in the **File Selection** window) select **.dbparms** and **OK**.

6 Follow subsystem-specific installation instructions included in the documentation (e.g., release notes) that specifies installing the patch to complete the database patch process.

- For example:
  1. Logon to the host where the subsystem database package is installed.
  2. Start ECS Assist's Subsystem Manager, select the appropriate mode, subsystem, and component.
  3. Select **DbPatch** from the **Database** menu. A **File Selection** window appears.
  4. In the "**File Selection**" window, select "**.dbparms**" and then "**Ok**". The "**Configurable Database Parameters**" dialog box appears.
  5. Verify the patch number (referring to the table in the patch instructions). If it is not correct, correct it, enter the required information and select **Ok**.

4.6.3 COTS Databases

Remedy has a Sybase databases. The COTS installation is performed by the auto-install applications in the **/usr/ecs/OPS/COTS** directory. The results of the installation are stored in the appropriate subdirectories, e.g., files located in the remedy home directory (**/use/ecs/OPS/COTS/remedy**).

4.7 Configuring Databases

Table 4.7-1, below, provides an Activity Checklist for configuring databases.

Table 4.7-1. Configuring Databases - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Configure the ASE Server	(P) 4.7.1.1	
2	DBA	Display Configuration Parameters	(P) 4.7.3.1	

4.7.1 Configure the ASE Server Parameters

Configuration parameters are user-defined settings that control various aspects of a database server's behavior. The server supplies default values for all configuration parameters. However, some of the configuration parameters need to be customized (refer to *SYBASE SQLServer 11.0.x: ALL DAAC Database Configurations,* 910-TDA-021).

Configuration parameters are grouped according to the area of server behavior that they affect. This makes it easier to identify all parameters that may need to be tuned in order to improve a particular area of ASE Server performance. The groups are:

- Backup/Recovery.

- Cache Manager.
- Component Integration Services
- DTM Administration
- Diagnostics
- Disk I/O
- Error Log
- Extended Stored Procedure
- General Information
- Java Services
- Languages
- Lock Manager
- Memory Use
- Meta Data Cache
- Monitoring
- Network Communications
- Operating System Resources
- Parallel Query
- Physical Memory
- Physical Resources
- Processors
- Red Agent Tread Administration
- SQl Server Administration
- Security Related Unicode
- User Environment

While each parameter has a primary group to which it belongs, many have secondary groups to which they also belong. For instance, the parameter number of remote connections belongs primarily in the Network Communications group, but also secondarily in the SQL Server Administration group and the Memory Use group. This reflects the fact that some parameters have implications for a number of areas of ASE Server behavior.

The configuration parameters are divided between two tables:

- Sybase Configuration Parameter Table
- DAAC-Specific Configuration Parameter Table.

The Sybase Configuration Parameter Table groups the configuration parameters by functionality. It provides a list of configurable parameters under each functional group, and provides recommended values for these parameters:

The following type of information is captured in the Sybase Configuration Parameter Table:

- Group Name.
- Group Description.
- Parameter Name (for each group).
- Parameter Description.
- Command Line.

- Status (Static or Dynamic parameter).
- Recommended Value.
- Range (Minimum and maximum parameter value).
- Display Level (Basic, Intermediate, Comprehensive).
- Impact (Brief description of type of impact when a parameter value is configured).
- Controlling Authority (Entity responsible for controlling changes to a configuration parameter).
- Comments (This will include suggestions and examples).

Configuration parameters can be set or changed in one of two ways:

- By executing the system procedure **sp_configure** with the appropriate parameters and values.
- By hand-editing your configuration file and then invoking **sp_configure** with the configuration file option.

Configuration parameters are either dynamic or static. *Dynamic parameters go into effect as soon as **sp_configure** is executed. Static parameters require the ASE server to reallocate memory and take effect only after ASE Server has been restarted.*

The roles required for using **sp_configure** are as follows:

- Any user can execute **sp_configure** to display information about parameters and their current values.
- Only System Administrators and System Security Officers can execute **sp_configure** to modify configuration parameters.
- Only System Security Officers can execute **sp_configure** to modify values for allow updates, audit queue size and remote access.

The system procedure **sp_configure** displays and resets configuration parameters. One can restrict the number of parameters **sp_configure** displays by using **sp_displaylevel** to set the display level to one of the three values: Basic, Intermediate, or Comprehensive.

Figure 4.7-1 shows a sample **sp_configure** output. **Name** column is the description of the variable. The **minimum** column is the minimum allowable configuration setting**.** **Maximum** is the theoretical maximum value to which the configuration option can be set. The actual maximum value is dependent on the specific platform and available resources to the ASE server. **Config_value** reflects the current system default values. **Run_value** reflects the values the system is currently using, which may be different from the default values.

SQL Server configuration can be done either interactively by using **sp_configure** or non-interactively by invoking sp_configure with a configuration file. Configuration files can be used for several reasons:

- To use a configuration file as a baseline for testing configuration values on your server.
- To use a configuration file to do validation checking on parameter values before actually setting the values.

- To create multiple configuration files and to switch between them as your resource needs change.

Previous releases of ASE Server required that reconfigure be executed after executing **sp_configure**. This is no longer required. The reconfigure command still exists, but it no longer has any effect.

name	minimum	maximum	config value	run value
recovery interval	1	32767	0	5
allow updates	0	1	0	0
user connections	5	2147483647	0	25
memory	3850	2147483647	0	5120
open databases	5	2147483647	0	12
locks	5000	2147483647	0	5000
open objects	100	2147483647	0	500
procedure cache	1	99	0	20
fill factor	0	100	0	0
time slice	50	1000	0	100
database size	2	10000	0	2
tape retention	0	365	0	0
recovery flags	0	1	0	0
nested triggers	0	1	1	1
devices	4	256	0	10
remote access	0	1	1	1
remote logins	0	2147483647	0	20
remote sites	0	2147483647	0	10
remote connections	0	2147483647	0	20
pre-read packets	0	2147483647	0	3
upgrade version	0	2147483647	1002	1002
default sortorder id	0	255	50	50
default language	0	2147483647	0	0
language in cache	3	100	3	3
max online engines	1	32	1	1
min online engines	1	32	1	1
engine adjust interval	1	32	0	0
cpu flush	1	2147483647	200	200
i/o flush	1	2147483647	1000	1000
default character set id	0	255	1	1
stack size	20480	2147483647	0	28672
password expiration interval	0	32767	0	0
audit queue size	1	65535	100	100
additional netmem	0	2147483647	0	0
default network packet size	512	524288	0	512
maximum network packet size	512	524288	0	512
extent i/o buffers	0	2147483647	0	0
identity burning set factor	1	9999999	5000	5000
allow sendmsg	0	1	0	0
sendmsg starting port number	0	65535	0	0

Figure 4.7-1. Example of sp_configure Output

Configuration files are not automatically backed up when you back up your master database. As they are part of the operating system files, they should be backed up in the same way other operating system files are backed up.

In order to perform the following procedure, the DBA must have obtained the following information:

- Name of server to be configured
- New values for configuration variables.

To set ASE Server configuration variables, the DBA must have **sa_role** (ASE Server) permissions. To set ASE Server configuration variables **allow updates**, **audit queue size**, **password expiration interval**, or **remote access**, **sso_role** (ASE Server) is also required.

Some parameter values take effect as soon as you reset the value. Others, which involve memory reallocation, do not change until you reset the value and then reboot ASE Server.

4.7.1.1 Configure the ASE Server

1 Log into the server that will be reconfigured by typing: **telnet *ServerName*** or **ssh *ServerName***, then press **Return**.

2 If a **Login**: prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
- A password prompt is displayed.

3 Enter ***YourPassword*** then press **Return**.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press **Return**.

5 Begin the ASE session by typing at the UNIX prompt **isql -S*ServerName*** then press **Return**.

6 Type **sp_configure** then press **Return**.

7 Type **go**, then press **Return.**
- A list of the configurable parameters, their maximum and minimum values, the current setting and the default values is displayed.

8 After determining which parameter(s) to reset, type: **sp_configure "*ParameterName*"**, ***NewValue***, then press **Return**.
- ***ParameterName*** is the name from the list displayed in Step 7 above.
  - Be sure to enclose the name in double quotes.
- ***NewValue*** is the numeric value that you want to assign to ***ParameterName***.

9 Type **go**, then press **Return.**

10 Repeat Steps 7 through 9 for each parameter you want to reconfigure.

11 When complete, type **quit** at the isql prompt, then press **Return**.
- You are returned to the UNIX prompt.

4.7.2 Configuration Parameters and the Configuration Registry

There are many configurable parameters associated with the custom software. Some of them are set by default to values that may be appropriate for most operating conditions. Others may be set to values that may or may not be appropriate for the requirements of operations at a particular DAAC. Some parameters may be changed using system Graphical User Interfaces (GUIs)

specifically designed to monitor and control functions related to particular subsystems. Others may require changes to a configuration file or database.

NOTE: Before changing any configuration parameter, make certain either that it is not under configuration control or that you have obtained any necessary approval specified in local Configuration Management policies and procedures.

4.7.3 Configuration Registry

Configuration parameters for custom software are managed by the Configuration Registry. The Configuration Registry Server provides a single interface to retrieve configuration attribute-value pairs for servers from the Configuration Registry Database, via a Sybase Server. The Configuration Registry Server maintains an internal representation of the tree in which configuration attribute-value pairs are stored. General configuration parameters used by many servers are stored in higher nodes in the tree. Parameters specific to a single server are contained in the leaf nodes of the tree. A script tool is available for loading the Configuration Registry database from data in configuration files. This loading is a one-time event to populate the Registry database with the information contained in **.cfg** files. Once the Configuration Registry is loaded, if the configuration files are moved or otherwise made inaccessible to the software, the software goes to the Configuration Registry to obtain needed configuration parameters. There is also a Configuration Registry application that can be used to view and edit configuration data in the database. Changes to the Configuration Registry typically are under the control of Configuration Management and the Database Administrator.

Data in the Registry database are stored hierarchically, sorted by hostnames. An application may have multiple entries, each under a different hostname where it runs. The application queries the database directly. The application shows the Attribute Tree on the left. It displays parameters and their values in the Attribute Listing on the right. It provides the operator with capability to create, read, update, and delete database entries. A click on a parameter name in the Attribute Listing displays a pop-up window, permitting the user to update or delete the parameter.

4.7.3.1 Display Configuration Parameters

1 On workstation ***x*0dms##**, in a terminal window, type **/usr/ecs/*mode*/CUSTOM/utilities/EcCsRegistryGUIStart *mode* &** at a UNIX command prompt and then press the **Return/Enter** key (where ***mode*** is likely to be **TS1**, **TS2**, or **OPS**).

- The ***x*** in the workstation name is a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the **##** is an identifying two-digit number (e.g., **g0dms03** indicates a data management subsystem workstation at GSFC). If you access the workstation through a secure shell remote login (ssh), you must enter **setenv DISPLAY <local_workstation IP address>:0.0** prior to the ssh before entering the command after the ssh. The **<*ipaddress*>** is the ip address of ***x*0mss##**, and **xterm** is required when entering this command on a Sun terminal.

- The Database Login window is displayed with entries filled in for **User Id:** (e.g., **EcCsRegistry**), **Server:** (e.g., ***x4dpl*02_srv**), and **DB Name:** (e.g., **EcCsRegistry_*mode***). (See Figure 4.7-2 below.)

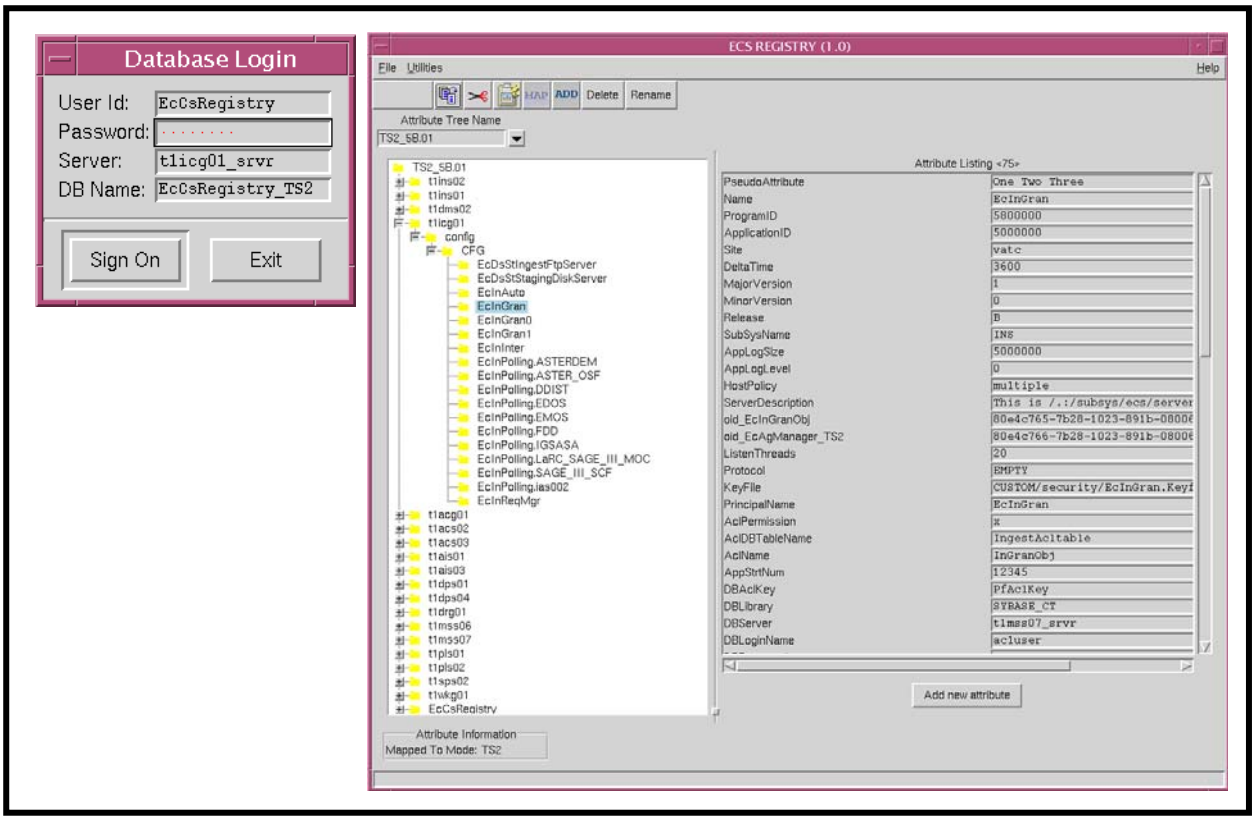


Figure 4.7-2. Configuration Registry

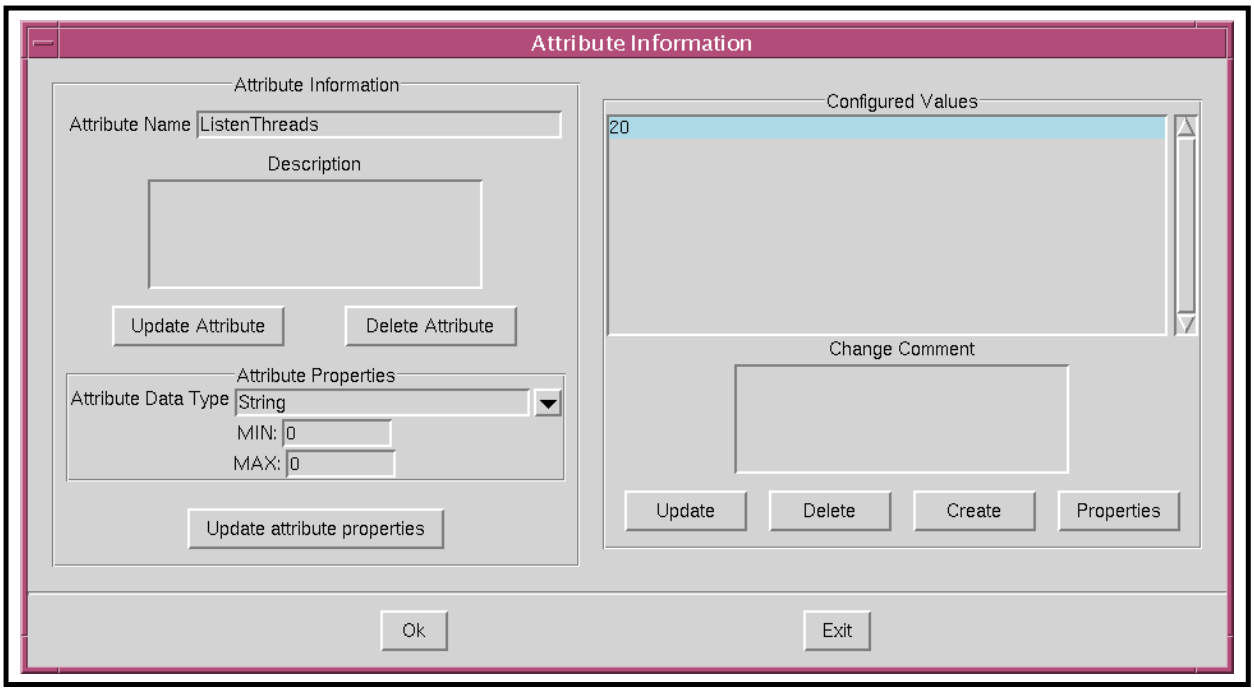


Figure 4.7-3. Configuration Registry Attributes Pop-Up Window

2 In the Database Login window click in the **Password:** field and type the password.
- The typed password is not displayed (dots are displayed in place of the password).

3 Click on the **Sign On** button.
- The Database Login window is closed and the Configuration Registry GUI is displayed.

4 On the tree showing system hosts displayed on the left side of the GUI, click on the "+" sign next to one of the hosts for which parameters are to be displayed.
- The tree displays a **config** branch.

5 Click on the "+" next to **config**.
- The tree displays a **CFG** branch.

6 Click on the "+" next to **CFG**.
- The tree displays the computer software components for the selected host.

7 Click on one of the listed components (or its folder icon).
- The **Attribute Listing** field displays the configuration parameters associated with the selected component. (See Figure 4.7-3.)
- If there are a large number of parameters, the right side of the window will have a scroll bar that may be used to scroll down the list.

8 Click on one of the listed parameters.
- The **Attribute Information** pop-up window for the selected parameter is displayed, showing detailed information concerning the parameter.
- If you are logged in with an account authorized with appropriate permissions, the **Attribute Information** window permits changing or deleting the parameter.

9 To exit from the Configuration Registry GUI, follow menu path **File→Exit**.

4.8 Working with Indexes, Segments, and Caches

Table 4.8-1, below, provides an Activity Checklist for working with indexes, segments, and caches.

Table 4.8-1. Working with Indexes, Segments, and Caches - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Delete an Index	(P) 4.8.1.1	
2	DBA	Create Database Segments (Example)	(P) 4.8.2.1	

4.8.1 Delete an Index

An index provides a means of locating a row in a database table based on the value of a specific column(s), without having to scan all data in the table. When properly implemented, indexes can significantly decrease the time it takes to retrieve data, thereby increasing performance. Sybase allows the definition of two types of indexes:

- *Clustered index, where the rows in a database table are physically stored in sequence determined by the index.* The ASE Server continually sorts and re-sorts the rows of a table so that their physical order is always the same as their logical (or indexed) order. Clustered indexes are particularly useful when data are frequently retrieved in sequential order. Only one clustered index can be defined for a table.
- *Non-clustered indexes differ from their clustered counterpart in that the physical order of rows is not necessarily the same as their indexed order*. Each non-clustered index provides access to the data in its own sort order, giving the appearance of data in that physical order. Up to 249 non-clustered indexes can be defined for one table.

Clustered indexes allow faster searches than non-clustered indexes. Clustered indexes are often called the primary key of the table. If you don't specify which type of index you want, it will be a non-clustered index by default.

There are a lot of options for creating an index, but the most commonly used one is unique. Both clustered and non-clustered indexes can be unique. *A unique index prohibits duplicate values in the column that the index is on.* They cannot be created on text or image datatypes because those datatypes cannot reliably be declared unique.

Index keys need to be differentiated from logical keys. Logical keys are part of the database design, defining the relationships between tables: primary keys, foreign keys, and common keys. *When you optimize your queries by creating indexes, these logical keys may or may not be used as the physical keys for creating indexes.* You can create indexes on columns that are not logical keys, and you may have logical keys that are not used as index keys.

Tables that are read-only or read-mostly can be heavily indexed, as long as your database has enough space available. If there is little update activity, and high select activity, you should provide indexes for all of your frequent queries. Be sure to test the performance benefits of index covering.

Also, remember that with each insert, all non-clustered indexes have to be updated, so there is a performance price to pay. The leaf level has one entry per row, so you will have to change that row with every insert.

4.8.1.1 Delete an Index:

1 To delete an index, type **drop index**.

2 Type the table name that has the index, a period, and the index name that you want to delete.

3 Type **go** then press **Enter**.

4.8.2 Create Database Segments (Example)

Segments are named subsets of the database devices available to a particular ASE Server database. A segment can best be described as a label that points to one or more database devices.

Segmenting can increase ASE Server performance and give the SA or DBA increased control over placement, size and space usage of specific database objects. For example:

- If a table is placed on one device and its non-clustered indexes on a device on another disk controller, the time required to read or write to the disk can be reduced since disk head travel is usually reduced.
- If a large, heavily used table is split across devices on two separate disk controllers, read/write time may be improved.
- The ASE Server stores the data for text and image columns on a separate chain of data pages. By default, this text chain is placed on the same segment as the table. Since reading a text column requires a read operation for the text pointer in the base table and an additional read operation on the text page in the separate text chain, placing the text chain on a separate physical device can improve performance.

Segments are created within a particular database from the database devices already allocated to that database. Each ASE Server database can contain up to 32 segments. The database devices must first be initialized with **disk init** and then be made available to the database with a **create database** or **alter database** statement segment names can be assigned.

When a database is first created, the ASE Server creates three segments in the database:

- System, which stores the database's system tables.
- Logsegment, which stores this database's transaction log.
- Default, which initially stores all other database objects.

Additional segments can be created. Subsystem databases, for example, consist of the following:

- Default data segment used if no other segment specified in the create statement.
- SYSLOGS, transaction logs.
- System tables and indexes.
- OPS mode data and index segments.
- TS1 mode data and index segments.
- TS2 mode data and index segments.

If tables and indexes are placed on specific segments, those database objects cannot grow beyond the space available to the devices represented by those segments, and other objects cannot contend for space with them. Segments can be extended to include additional devices as needed. Thresholds can be used to provide warnings when space becomes low on a particular database segment.

In the following example procedure, the DBA receives a request to create a segment for the storage of the SubServer table indexes in the t1ins01_srvr database on a separate physical disk. Two devices, **subserver_data** and **subserver_index**, have already been created and are located on different physical disks.

In order to perform the procedure, the DBA must have obtained the following information:

- Name of database
- Database device extents
- Space on the database allocated to the Database device

To create a database, the DBA must have **sa_role**:

4.8.2.1 Create Database Segments (Example)

1 At the UNIX prompt, type **cd ASE-12_5/scripts** and then press **Return**.

2 Using the text editor of your choice, edit ***segment*.sql** and make changes to information enclosed in brackets (including the brackets) as appropriate.

3 After the changes have been made, save the file according to the rules of the text editor.

4 At the UNIX prompt, type:**isql –U<username> -S<*ServerName*> -i*Segment*.sql -o*Segment*.out** and then press **Return.**

- The system will prompt you for a password.

5 At the **Password:** prompt, type the **<*password*>**, then press **Return.**

- When the UNIX prompt is again displayed the process is complete.

6 At the UNIX prompt, type **more *Segment.out*** , then press **Return**.

- This allows you to view the ***Segment.out*** file to confirm that the device has been created or to check for database creation errors.

Figure 4.8-1 shows an example of creation of a database segment template file.

```
/*****************************************/
/* name: [segment.sql]                   */
/* purpose:                              */
/* written:                              */
/* revised:                              */
/* reason:                               */
/*****************************************/

 sp_addsegment [seg_name], [DBname],[Device Name]
```

Figure 4.8-1. Example of Creation of a Database Segment Template File

After the segment has been defined in the current database, the **create table** or **create index** commands use the optional clause **"on segment_name"** to place the object on a particular segment. Syntax:

create table table_name (column_name datatype ...) [on segment_name]
create [clustered | nonclustered] index index_name on table_name (columns)

Use **sp_helpdb** database_name to display the segments defined for that database.

Use **sp_helpsegment** segment_name to list the objects on the segment and show the mapped devices.

4.8.3 Caches

A cache is a block of memory that is used by Sybase to retain and manage pages that are currently being processed. By default, each database contains three caches:

- Data caches retain most recently accessed data and index pages
- Procedure caches retain most recently accessed stored procedure pages
- User transaction log caches are transaction log pages that have not yet been written to disk for each user

The size of each of these default caches is a configurable item that must be managed on a DAAC-by-DAAC basis. These caches can be increased or decreased as needed. The data cache can be further subdivided into named caches. *A named cache is a block of memory that is named and used by the database management system (DBMS) to store data pages. The named data caches can be used only by databases or database objects that are explicitly bound to them. All*

objects not explicitly bound to named data caches use the default data cache. A database, table, index, or text or image page chain can be bound to a named data cache.

Assigning a database table to named cache causes accessed pages to be loaded into memory and retained. Named caches greatly increase performance by eliminating the time associated for disk input and output (I/O).

4.9 Backing Up and Recovering Data

Database and transaction log backups and recoveries are probably the most important tasks the DBA must perform. Without regular and complete backups of databases and transaction logs, the potential for enormous amounts of data to be lost is very great. How often you back up a database depends on how frequently the data is updated and how costly it would be to lose it. Databases that are constantly being modified need to be backed up frequently; databases containing relatively static data can be backed up less frequently. You should regularly back up production databases, for example. If you experience a media failure, you can restore the data from the most recent backups the **restore** command. You do not have to shut down servers to back up or restore a database. The Backup Server makes it possible to perform online backup and restore operations while the Adaptive Server is running.

Table 4.9-1, below, provides an Activity Checklist for backing up and recovering data.

Table 4.9-1. Backing Up and Recovering Data - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Perform Automatic Backups	(P) 4.9.1.1	
2	DBA	Perform Manual Backups	(P) 4.9.2.1	
3	DBA	Perform a User Database Recovery	(P) 4.9.3.1	
4	DBA	Perform a User Database Recovery (Example)	(P) 4.9.4.1	
5	DBA	Create a User Database (Example)	(P) 4.9.4.2	

4.9.1 Perform Automatic Backups

Each DAAC is responsible for determining its own backup schedule to meet its individual requirements. It is strongly suggested that a regular schedule of database backups be established and maintained. Although the databases are included in the daily backups of the entire system, separate database backups should be performed nightly.

Database backups are run by a UNIX **cron** job which executes the **EcCoSyb_DumbDb** program located in the **/usr/ecs/CUSTOM/dbms/COM/DBAdmin** directory. No intervention in the automatic backup process is required by the DBA, though periodic checks of the backup subdirectories are recommended.

Manual backups can be performed at any time by the DBA and are recommended for the following situations:

- Any change to the master database, including new logins, devices, and databases.
- Any major change to user databases, such as a large ingest or deletion of data, definition of indexes, etc.
- Other mission-critical activities as defined by the DAAC operations controller.

The following are procedures and scripts files that are currently being used for Sybase backups. There are **cron** jobs running at all Sybase servers that have ASE server installed. All dump files are currently written to local machine. The site DBA is responsible for configuring the backup dump to the remote Sybase directory.

4.9.1.1 Performing Automatic Backups

1 Check if **crontab** is up and running.

> **crontab -l**

- The output will look something like the following:

  019 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpDb
  012 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpTran
  021 * * 1-5 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CkErrorLog

2 If **crontab** is not running, enter:

> **crontab /usr/ecs/OPS/COTS/sybase/run_sybcron**

- The files shown in Table 4.9-2 will be installed by ECS Assistant to the directory **/usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin**:

Table 4.9-2. Automatic Backup Files (1 of 2)

Script	Description
EcCoDbSyb_SetupKsh	This file contains the SYBASE and DSQUERY (server) environment setup. This file is called by EcCoDbSyb_DumpDb, EcCoDbSyb_DrumpTran, and EcCoDbSyb_CkErrorLog scripts.
EcCoDbSyb_DumpDb	This script contains the code to dump the databases. First, it checks for any DBCC error on the master database, if there is any error on the master, the script sends an email to the DBA and exits the program. If the master database dump was successful, then the rest of the databases are dumped. Each database has a DBCC check; if there is any error on the database then the database is NOT dumped and an email is sent to the DBA. At the end, a status email is sent, providing all the database names that were successfully dumped.

Table 4.9-2. Automatic Backup Files (2 of 2)

Script	Description
EcCoDbSyb_DumpTran	This script contains the code to dump the transaction logs. This dumps the transaction logs for each database, it checks the error log file; if the error Msg is 4207 or 4221 it does a dump of the database first, then it does the transaction dump. If there is any other error Msg then the transaction dump fails and email is sent. At the end, the status of the transaction log dumps is emailed to the DBA.
EcCoDbSyb_SedFile	This file contains all the databases that don't need to be dump (i.e., temp, model, etc.)
EcCoDbSyb_DboMail	This file contains the email list of all the DBAs.
EcCoDbSyb_DbStat	This script updates the index table of a database. This script is called from EcCoDbSyb_DumpDb after each successfully database dump.
EcCoDbSyb_CkErrorLog	This script checks for specific database error messages from the Sybase Error Log File every hour and emails the error messages to the DBAs in the EcCoDbSyb_DboMailfile.
EcCoDbSyb_tran_log.awk	This script matches the current hour with the hour the error messages were generated in the Error Log File. If errors found, the messages are saved in a mail file and sent to DBAs.
0 0 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpDb 0 10,13,16 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpTran 0 * ** 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CkErrorLog NOTE: Make sure there is an OPS mode directory with all script files.	

3 Modify the files shown in Table 4.9-3 before running any of the scripts shown in Table 4.9-2.

Table 4.9-3. Files That Need to Be Modified before Running Scripts

File	Modification
EcCoDbSyb_SetupKsh	Make user you have the SYBASE files under /usr/ecs/OPS/COTS/sybase
EcCoDbSyb_SedFile	Add any other database that might not need to be backed up. The databases that are listed in this file do not need to be backed up.
EcCoDbSyb_DboMail	Add/delete the email of the DBA and any other email that might need to be added/deleted. All the errors and status are sent to them.

ASE Server backups are performed nightly by a **cron** job which runs the **sybcron** program located in the **$SYBASE**/ directory. The following table of definitions (Table 4.9-4) is used throughout the rest of this section.

Table 4.9-4. Automatic Backup Components

Name	Function
sybcron	File added with the crontab -e command, contains several executable cron commands. **Example:** 00 19 * * 1-6 /data1/COTS/sybase/sybasedump
EcCoDbSyb_DumpDb	Controlling script that performs the following functions: run isql to create the Backup Statements run isql to execute the Backup Statements record the results of the Backup Statements in Backup Files copy the Backup Files to the Backup Subdirectory create the Backup Summary greps successful Dump statements along with any errors generated, sends e-mail to the DBA and writes them to the backup_summary file
sp	ASE Server password file - contains password for backup role

4.9.2 Perform Manual Backups

Both the **dump database** and **dump transaction** command processing are off-loaded to the backup server and will not affect normal operations of the database. These commands are performed by the System Administrator on appropriate databases using the following syntax.

1> **dump database master to "compress::/usr/ecs/OPS/COTS/sybase/sybase_dumps/dumps/dbname.dat.compress.MMDDHHMM"**

2> **go**

4.9.2.1 Perform Manual Backups

1 Log on to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press **Return**.

3 Log into the server that contains the database to be backed up by typing: **/tools/bin/ssh *gsfcsparc5.gsfcmo.ecs.nasa.gov***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key.

- Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log into Sybase by typing: **su-sybase**, then press **Return.**

- A password prompt is displayed.

7 Enter ***SybasePassword*** then press **Return**.

- Remember that ***SybasePassword*** is case-sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.
- Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.

8 At the UNIX prompt, type **isql -Usa** then press **Return**.

9 To backup the database, at the isql prompt, type **dump database *DBName* to "compress::/*BackupDirectory/DBName*.dat"**, then press **Return**.

10 Type **go**, then press **Return**.

11 To backup the transaction log, at the isql prompt, type **dump transaction *DBName* to "compress::/*BackupDirectory/DBName*_tx.dat"**, then press **Return**.

12 Type **go**, then press **Return**.

4.9.3 Perform a User Database Recovery (Order of Procedures)

Database recovery is performed when the Database Administrator determines that some database data is corrupt or when the System Administrator determines that a database device has failed. The System Administrator makes a request to the Database Administrator, who performs the restore and notifies the System Administrator when the restore is complete.

The symptoms of media failure are as variable as the causes. If only a single block on the disk is bad, your database may appear to function perfectly for some time after the corruption appears; this is why you should run **dbcc** commands frequently. If an entire disk or disk controller is bad, you will not be able to use a database. ASE Server marks it as suspect and displays a warning message. If the disk storing the master database fails, users will not be able to log into the server, and users already logged in will not be able to perform any actions that access the system tables in master.

4.9.3.1 Perform Database Recovery

1 The device failure has been verified by the System Administrator and restoration has been requested from the DBA.

2 If possible, perform a dump of the current database and the current database transaction log for each database on the failed device to be restored. If this is not possible due to the damage to the database device, then the DBA will have to use the most recent database and transaction log dumps.

3 If possible, the DBA examines the space usage for each database on the failed device. The same defaults should be set when the new database device(s) is (are) created.

4 The DBA drops the database(s) on the failed device, then the database device itself is dropped.

5 The DBA initializes a new database device. This is why it is important to keep the device creation scripts.

6 The DBA recreates each user database on the new database device. This is why it is important to keep the user creation scripts.

7 Each database is reloaded with data from the database backups and the transaction log backups. It is this procedure that is detailed below.

8 The DBA notifies the System Administrator when the database restoration is complete.

In order to perform the procedure, the DBA must have obtained the following information:

- Name of database device that has failed
- Name of the replacement device
- Name of the databases that reside on the failed device
- Name of the backup volumes
- Name of the dump files on the backup volumes

Manual recovery of a user database is performed by the System Administrator by the use of the **load database** and **load transaction** commands. For issues concerning the **master** database, please consult your System Administrator's Guide for assistance. It is recommended that any user database to be recovered be dropped and created with the **for load** option. The **databasename**.sql along with any **alter.databasename**.sql scripts can be combined into one script which will re-create the user database with the **for load** option. This will insure the success of the **load database** and **load transaction** commands.

4.9.4 Perform a User Database Recovery (Example)

In the example procedures that follow, the database **UserDB** was created using the following script excerpt (stored in home/scripts/create.databases/userdb.sql):

create database UserDB on data_dev1 = 100 log on tx_log1 = 50 [with override]

and was modified using the following script excerpt (home/scripts/create.databases/alteruserdb.sql):

alter database UserDB on data_dev1=50

For the purposes of this example, the full database backup and transaction log dumps were successful and located in **/usr/ecs/OPS/COTS/UserDB.dat** and **UserDB_tx.dat**.

4.9.4.1 Perform a User Database Recovery (Example)

---

1 In the $SYBASE/ASE-12_5/scripts/ directory, make a script file to load database and save template for future use.

- Syntax:

  % cd /usr/ecs/OPS/COTS/sybase/scripts/,
  % cp template.sql userdb_for_load.sql.

NOTE: If template does not exist, vi userdb_for_load.sql.

2 Modify appropriate items so that the script file resembles the following:

create database UserDB on data_dev2=100 log on tx_log2=50 for load
go

alter database UserDB on data_dev3=50
go

3 Save the script in **$SYBASE/ASE-12_5/scripts/create.databases/userdb_for_load.sql**

4 Run the script from the UNIX command prompt.

%isql -Usa -Sservername -iuserdb_for_load.sql -ouserdb_for_load.out

5 Check the **userdb_for_load.out** file for success.

6 Load the database from the full backup.

1> load database UserDB from
"compress::/usr/ecs/OPS/COTS/sybase/sybase_dumps/week1/dbname.dat.MMDDHHMM"
2> go

7 Load the transaction file from the transaction file dump.

1> load transaction UserDB
from"compress::/usr/ecs/OPS/COTS/sybase/sybase_dumps/week1/dbname.tran.MMDDHHMM"
2> go

4.9.4.2 Create a User Database (Example)

1 Log on to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press **Return**.

3 Log into the server on which the new database device is to be created by typing: **/tools/bin/ssh <*ServerName*>**, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

NOTE: For each database device to be created, perform Steps 6 through 9:

6 At the UNIX prompt, type **cd /ASE-12_5/** then press **Return.**

- This place you in the directory that contains all the scripts used to create database devices.
- It is important that these scripts not be deleted from the system in case it is necessary to restore a database device following a failure (see **Restore Databases**).

7 Using the text editor of your choice, edit ***DBName*.sql** and make changes to information enclosed in brackets (including the brackets) as appropriate (see Figure 4.9-1).

- **DBName** is the name of the database and should describe its function succinctly.
- **DBDeviceName** is the name of the existing, approved database device on which **DBName** will reside.
- **DBSize_in_MB** is the estimated size of the database in megabytes.
- **LogDBDeviceName** is the name of the database device holding the transaction log
- **LogSize_in_MB** is the estimated size of the transaction log in megabytes.
- The **sp_helpdb** command provides feedback at the end of the script to assure that the database has been created.

```
/* ************************************************** */
/* name: template.sql                                 */
/* purpose:                                           */
/* written:                                           */
/* revised:                                           */
/* reason:                                            */
/* ************************************************** */
create database database_name
on data_dev = size, /* in MB */
log on log_dev = size
go
sp_helpdb database_name
go
```

Figure 4.9-1. Sample template.sql File for Creation of a Database

8 After the changes have been made, save the file according to the rules of the text editor.

9 At the UNIX prompt, type:

isql –U<username> -S<ServerName> -i*DBName*.sql -o*DBName*.out

then press **Return**.

- ***ServerName*** is the name of the server on which the database device will be created.
- ***DBName.sql*** is the name of the script file you created in step 8.
- ***DBName.out*** is the filename of the script's output for confirmation and/or troubleshooting purposes. The system will prompt you for a password.

10 At the **Password:** prompt, type the **<*password*>** then press **Return.**

- When the UNIX prompt is again displayed the process is complete.

11 At the UNIX prompt, type **more *DBName.out*** then press **Return**.

- This allows you to view the ***DBName.out*** file to confirm that the device has been created or to check for database creation errors.

A sample of a completed **Create Database** script is shown in Figure 4.9-2.

```
/*****************************************/
/* name: test_db.sql                     */
/* purpose: create a database for testing */
/* written: 12/19/97                     */
/* revised:                              */
/* reason:                               */
/*****************************************/
create database test_db
on test_dev = 3
go
sp_helpdb test_db
go
```

Figure 4.9-2. Completed Create Database Script

4.10 Establishing Database Security

Permissions control access within a database. There are two types of permissions within a database: object and command. Object privileges control select, insert, update, delete, and execute permissions on tables, views, and stored procedures. Command permissions control access to the create statements for databases, defaults, procedures, rules, tables, and views. Access controls allow giving various kinds of permissions to users, groups, and roles with the **grant** command. The **revoke** command rescinds these permissions.

The ability to assign permissions for the commands is determined by each user's status (e.g., system administrator, database owner, database object owner) and by whether or not a particular user has been granted a permission with the option to grant that permission to other users.

Groups are a means of logically associating users with similar data access needs. Once a group has been defined, object and command permissions can be granted to that group. A user who is member of a group inherits all of the permissions granted to that group.

Roles provide a structured means for granting users the permissions needed to perform standard database-related activities and also provide a means for easily identifying such users. They

provide a means of enforcing and maintaining individual accountability. There are six pre-defined roles shown in Table 4.10-1 that may be assigned to a user. Other unique roles can be created and granted to users, groups of users, or other roles. In addition, role hierarchies can be defined. This enables a user assigned one role to automatically have the privileges available to all other roles lower in the hierarchy. Mutually exclusive roles can also be defined. This can be done in terms of membership – a single user cannot be granted both roles – or activation – a single user can be granted two roles but cannot enable both (e.g., both cannot be enabled simultaneously).

Table 4.10-1. Roles and Privileges

Roles		Privileges
System Administrator	sa_role	Grant a specific user permissions needed to perform standard system administrator duties including: Installing SQL server and specific ASE server modules Managing the allocation of physical storage Tuning configuration parameters Creating databases
Site Security Officer	sso_role	Grant a specific user the permissions needed to maintain ASE server security including: • Adding server logins • Administrating passwords • Managing the audit system • Granting users all roles except the sa_role
Operator	oper_role	Grant a specific user the permissions needed to perform standard functions for the database including: • Dumping transactions and databases • Loading transactions and databases
Navigator	navigator_role	Grant a specific user the permissions needed to manage the navigation server
Sybase Technical Support	sybase_ts_role	Grant a specific user the permissions needed to execute database consistency checker (dbcc), a Sybase supplied utility supporting commands that are normally outside of the realm of routine system administrator activities

Table 4.10-2, below, provides an Activity Checklist for establishing database security.

Table 4.10-2. Establishing Database Security - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Grant or Revoke Database Access Privileges	(P) 4.10.1.1	
2	DBA	Create an ASE Server Login	(P) 4.10.2.1	
3	DBA	Change a Password	(P) 4.10.3.1	
4	DBA	Perform Auditing	(P) 4.10.4.1	

4.10.1 Grant or Revoke Database Access Privileges

The DBA uses the **grant** and **revoke** statements to control permissions. The syntax for grant and revoke statements is similar:

> **grant {all [privileges] | command_list} to {public | name_list | role_name}**
> **revoke {all [privileges] | command_list} from { public | name_list | role_name}**.

4.10.1.1 Granting or Revoking Database Access Privileges

1 Determine the privileges that you want to grant and to which user(s).

2 Log on to a local host.

3 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press **Return**.

4 Log into the server where the user database resides by typing: **/tools/bin/ssh *ServerName***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 5.
- If you have not previously set up a secure shell passphrase, go to Step 6.

5 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key.

- Go to step 7.

6 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

7 At the UNIX prompt, type **su-sybase** then press **Return**.

- A password prompt is displayed.

8 Enter ***SybasePassword***, then press **Return**.

- You are authenticated as yourself and returned to the UNIX prompt.
- Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.

9 At the UNIX prompt, type **isql -Usa**, then press **Return**.

10 At the **Password:** prompt, type the ***SybaseSAPassword*** then press **Return.**

- Note: the ***SybaseSAPassword*** is case-sensitive.

11 If you are granting privileges, at the isql prompt, type **grant *Privilege* to *LoginName*** then press **Return**.

- If more than one privilege is to be granted, repeat this step on subsequent lines.

12 If you are revoking privileges, at the isql prompt, type **revoke *Privilege* from *Logname*** then press **Return**.

- If more than one privilege is to be revoked, repeat this step on subsequent lines.

13 When all privileges have been assigned, type **go** then press **Return**.

NOTE: It is recommended that the DBA store the privilege granting and revoking commands in **.sql** files in the **$SYBASE/ASE-12_5/scripts/..** directory along with their results.

4.10.2 Create an ASE Server Login

A user is given a login account with a unique ID. All of that user's activity on a server can be attributed to his or her server user ID and audited. Passwords are stored in the **master..syslogins** table in encrypted form. When users log in from a client, they can choose client-side password encryption before sending the password over the network. A user can be granted the ability to impersonate another user. This proxy authorization allows administrators to check permissions for a particular user or to perform maintenance on a user's database objects. Application servers can execute procedures and commands on behalf of several users.

Providing users with access to ASE servers and their databases consists of the following steps:

- A server login account for a new user is created.
- The user is added to a database and optionally assigned to a group.
- The user or group is granted permissions on specific commands and database objects.

The user needs an ASE Server login to access the DBMS. The login is assigned to a user with the related permissions. During initial database installation, logins used by the custom code were created and permissions assigned for access to subsystem databases. In addition, special database installation logins, **<SUBSYS>_role**, were created to support database installation needs. For each login, the level of access is limited to that associated with their login, group or assigned group/role. Object permissions are set within the installation scripts of the <SUBSYS> subsystem for each object and group/role.

In order for a user to connect to an ASE Server, a login must be created by the DBA. That login must then be assigned to particular database(s) that the user will access. All login details are stored in the syslogins table in the **master** database. Two stored procedures are required:

- The stored procedure **sp_addlogin** adds new login names to the server but does not grant access to any user database. Syntax:
  sp_addlogin login_name, password, [,default database ,language, fullname]
- The stored procedure **sp_adduser** adds the user. Syntax:
  sp_adduserlogin_name [username, group_name]
  go

4.10.2.1 Create an ASE Server Login

1 Log on to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press **Return**.

3 Log into the server for which a new login procedure is to be created up by typing: **/tools/bin/ssh *ServerName***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 At the UNIX prompt, type **su-sybase** then press **Return**. A password prompt is displayed.

7 Enter ***SybasePassword*** then press **Return**.

- Note: ***SybasePassword*** is case-sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.
- Your new home directory is /usr/ecs/OPS/COTS/sybase and all required environment variables have been set.

8 At the UNIX prompt, type **cd ASE-12_5/scripts/server.users** then press **Return**.

9 Using the text editor of your choice, edit ***UserName*.sql** (see Figure 4.10-1) and make changes to information enclosed in brackets (including the brackets) as appropriate:

10 After the changes have been made, save the file according to the rules of the text editor.

```
/*****************************************/
/* name: [template.sql]                  */
/* purpose:                              */
/* written:                              */
/* revised:                              */
/* reason:                               */
/*****************************************/
     sp_addlogin [login name], [password], [default database]
     go
     use [default database]
     go
     sp_adduser [login name]
     go
     /* the following is optional, by database */
     sp_changegroup [group name], [login name]
     go
     sp_helpuser
go
```

Figure 4.10-1. Sample template.sql File for New Database User Login

11 At the UNIX prompt, type **isql -Usa -S*ServerName* -i*UserName*.sql -o*UserName*.out** then press **Return**.

- ***ServerName*** is the name of the server on which the master database is stored.
- ***UserName*.sql** is the name of the script file you created in Step 9.
- ***UserName*.out** is the filename of the script's output for confirmation and/or troubleshooting purposes.
- The system will prompt you for a password.

12 At the Password: prompt, type the ***SybaseSAPassword*** then press **Return**.

- When the UNIX prompt is again displayed the process is complete.

13 At the UNIX prompt, type **more *UserName*.out** then press **Return**.

- This allows you to view the ***UserName*.out** file to confirm that the user login has been created or to check for user login creation errors.

4.10.3 Change a Password

One of the most common problems a DBA encounters is a user who cannot connect to an ASE Server. The following procedure is applicable.

4.10.3.1 Changing a Password

1 At the UNIX prompt, type **isql -U*dbastudent*** then press **Return.**
- The system will prompt you for a password.

2 At the **Password:** prompt, type the ***dbastudentpassword*** then press **Return.**

3 At the Sybase prompt, type the following:

sp_password *old-password, new-password*

NOTE: The dba (or any user with sso_role) may change another user's password with the following syntax: (this is the most common activity performed)

sp_password *sso_role password, new-password, login name*

4.10.4 Perform Auditing

A comprehensive audit system is provided with Adaptive Server. The audit system consists of a system database called sybsecurity, configuration parameters for managing auditing, a system procedure, **sp_audit**, to set all auditing options, and a system procedure, sp_addauditrecord, to add user-defined records to the audit trail. When you install auditing, you can specify the number of audit tables that Adaptive Server will use for the audit trail. If you use two or more audit tables to store the audit trail, you can set up a smoothly running audit system with no manual intervention and no loss of records.

A System Security Officer manages the audit system and is the only user who can start and stop auditing, set up auditing options, and process the audit data. As a System Security Officer, you can establish auditing for events such as:

- Server-wide, security-relevant events.
- Creating, deleting, and modifying database objects.
- All actions by a particular user or all actions by users with a particular role active.
- Granting or revoking database access.
- Importing or exporting data.
- Logins and logouts.

The following statements represent examples for performing auditing:

4.10.4.1 Perform Auditing

1 Run **installsecurity** auditing **located under $SYBASE/ASE-12_5/scripts**.

2 Add a login for auditing:

sp_addlogin ssa, ssa_password, sybsecurity
use sybsecurity
sp_changedbowner ssa
sp_role "grant", sso_role, ssa

3 Enable auditing:

sp_configure "auditing", 1
sp_audit "cmdtext", "dbo", "on"

4 **You can test via these next few steps: C**reate a table in a database with one field.
5 Grant all on the table for the **loginname.**
6 Log into isql using the **loginname.**
7 **Insert a record** into the table.
8 Log into isql as **ssa.**
9 Select ***** from **sysaudits** where **loginname** = **"loginname"**

NOTE: Once auditing is turned on, the **sysaudit** tables will get filled up very quickly. The database option, options of **trunc log on chkpt** needs to be turned on in the **sybsecurity** database so that the **logsegment** of this database can be cleaned up upon checkpoint. This **logsegment** can also be cleaned up by means of transaction dumps if the database is installed on two separate disk devices. Also, as soon as auditing is turned on, a **cron** job needs to be turned on at the same time to **bcp** out and truncate the **sysaudit** table. This is very important.

4.10.5 EMD Security Directive

All System Administrators and Database Administrators at the sites are responsible for reasonable security measures when installing custom software. This means:

- Changing the permissions of online secure files to the minimum level required.
- Backing up secure file(s) to removable media (floppy or tape) and removal of secure files immediately after installation is complete and then keeping the removable medium in a secure location.

The following file is affected as result of this requirement on the EMD program:

/usr/ecs/<MODE>/CUSTOM/dbms/<SUBSYSTEM>/Ec<server>SybaseLogins.sql

Set permissions to 711 (user read, write, execute; group and other read only).

4.11 Copying, and Extracting Data

To create an exact copy of a database (Individual Databases):

- Dump the existing database.
- Create a database to load with this dump.

The new database does not have to be the same size as the original. The only requirement is that the destination database must be at least as large as the dumped database and have the same beginning fragments as the original database. This information can be obtained from saved database creation scripts or by running the following command:

select segmap,'Size in MB'=size/512 from sysusages where dbid= db_id("database_name")

4.11.1 Copying a Database (Example)

A database was created with the following statement:

```
create database dbname on datadevice1 = 1000,
log on Logdevice1 = 200
go
alter device dbname on datadevice2 = 500     running:
select segmap,'Size in MB'=size/512 from sysusages
where dbid= db_id("dbname")
would return:segmap  Size in MB
3      1000
4      200
3      500
```

You could create a 3GB database as follows and load your database into it (using **for load** option will shorten database load time):

```
create database newdatabase on datadevice3 = 1000 log on logdevice3 = 200
for load
go
alter database newdatabase on datadevice 3=500 for load
go
alter database newdatabase on datadevice4=300 for load
go
alter database newdatabase on datadevice5=1000 for load
go
load database newdatabase from dbname_dump
go
```

4.12 Bulk Copying

Table 4.12-1, below, provides an Activity Checklist for bulk copying.

Table 4.12-1. Bulk Copying - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Perform Bulk Copying	(P) 4.12.1.1	

4.12.1 Perform Bulk Copying

The bulk copy (**bcp)** utility is located in the **$SYBASE/OCS-12_5/bin** directory and is designed to copy data to and from ASE Server databases to operating system files. You must supply the following information for transferring data to and from ASE Server:

- Name of the database and table.

- Name of the operating system file.
- Direction of the transfer (in or out).

In order to use **bcp**, you must have an ASE Server account and the appropriate permissions on the database tables and operating system files that you will use. To copy data **into** a table, you must have **insert** permission on that table. To copy data **out** to an operating system file, you must have **select** permission on the following tables:

- The table being copied:
  - **sysobjects**
  - **syscolumns**
  - **sysindexes**

bcp syntax:

bcp [[database_name].owner.]table_name {in | out} datafile [-e errfile] [-n] [-c] [-t field_terminator] [-r row_terminator] [-U username] [-S server]

4.12.1.1 Perform Bulk Copying

1 Log on to a local host.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *ServerName*:0.0**, then press **Return**.

3 Log into the server that contains the database to be backed up by typing: **/tools/bin/ssh *ServerName***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key.

- Go to step 6.

5 At the **<*user@remotehost*>'s password:** prompt type your ***Password*** and then press the **Enter** key.

6 Set Login as sybase and cd to /usr/ecs/OPS/COTS/sybase/scripts/.

- Note: ***SybasePassword*** is case-sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.
- Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.

8 Modify the [table name]_out script with the correct database name, table name, direction, and login name and save.

9 Run the [table name]_out script and press **Return** for each of the prompts except the last.

10 At the last prompt store [your responses] in a [table name].fmt file. This creates a format file for future bulkcopy activity.

11 To copy the data to another already created table, repeat Steps 6, 7, and 8 with the following changes:

- The direction is “in”
- Use the optional **-f [format file name]**

4.13 Replication System Administration - Removed

4.14.1 Monitoring

The easiest way to monitor performance is through the Monitor Server. The Monitor Server provides specific performance data on cache usage, network traffic, device I/O, and locking activity. *Performance is the measure of efficiency of an application or multiple applications running in the same environment*. Performance is usually measured in one of two ways:

- *Response time, which is the time that a single task takes to complete.*
- Throughput, which is the volume of work completed in a fixed time period, e.g. transactions per second (tps).

Most of your tuning efforts should address the amount of time it takes for the server to respond to queries.

You can run **sp_sysmon** both before and after tuning Adaptive Server configuration parameters to gather data for comparison. You can also use **sp_sysmon** when the system exhibits the behavior you want to investigate. In many tests, it is best to start the applications, and then start **sp_sysmon** when the caches have had a chance to reach a steady state. If you are trying to measure capacity, be sure that the amount of work you give the server keeps it busy for the duration of the test. Many of the statistics, especially those that measure data per second, can look extremely low if the server is idle during part of the sample interval. In general, **sp_sysmon** produces valuable information when you use it:

- Before and after cache or pool configuration changes.
- Before and after certain sp_configure changes.
- Before and after the addition of new queries to your application mix.
- Before and after an increase or decrease in the number of Adaptive Server engines.
- When adding new disk devices and assigning objects to them.
- During peak periods, to look for contention.
- During stress tests to evaluate an Adaptive Server configuration for a maximum expected application load.
- When performance seems slow or the system behaves abnormally.

4.14.2 Tuning

Response time can be shortened by reducing contention and waits times, particularly disk I/O wait times; using faster components; and reducing the amount of time the resources are needed. In some cases, Adaptive Server is optimized to reduce initial response time, that is, the time it takes to return the first row to the user. This is especially useful in applications where a user

may retrieve several rows with a query and then browse through them slowly with a front-end tool. Other ways of increasing performance are summarized by system level in Table 4.14-1.

Table 4.14-1. Tuning Options

Layers	Tuning Options
Application	
	Stored procedures to reduce compilation time and network usage
	Minimum locking level that meets application needs
Database	Transaction log thresholds to automate dumps and avoid running out of space
	Thresholds for space monitoring in data segments
	Partitions to speed loading of data
	Devices to avoid disk contention, take advantage of I/O parallelism
Server	Tuning memory, most critical configuration parameters and other parameters
	Configuring cache sized and I/O sizes
	Scheduling batch jobs and reporting for off hours
	Reconfiguring parameters for shifting workload patterns
Devices	More medium-sized devices and more controllers for better I/O throughput
	Distributing databases, tables, and indexes for even I/O load across devices
	Segments, partitions for I/O performance on large tables used for parallel queries
Network	Configuring packet sizes to match application needs
	Configuring subnets
	Isolating heavy network uses
	Configuring for multiple network engines
Hardware	Configuring the housekeeper task to improve CPU use
	Configuring multiple data caches
Operating System	Choosing between riles and raw partitions
	Increasing memory size

4.15 Ensuring Database Quality

4.15.1 Integrity Monitoring

The Database Consistency Checker (**dbcc**) is a set of utility commands for checking the logical and physical consistency of a database. Use the **dbcc** commands:

- As part of regular database maintenance (periodic checks run by the System Administrator). These checks can detect, and often correct, errors before they affect a user's ability to use ASE Server.
- To determine the extent of possible damage after a system error has occurred.
- Before backing up a database.

- Because you suspect that a database is damaged. For example, if using a particular table generates the message “Table corrupt”, you can use dbcc to determine if other tables in the database are also damaged.

The integrity of the internal structures of a database depends upon the System Administrator or Database Owner running database consistency checks on a regular basis. Two major functions of dbcc are:

- Checking allocation structures (the commands checkalloc, tablealloc, and indexalloc).
- Checking page linkage and data pointers at both the page level and row level (checktable and checkdb). The next section explains page and object allocation and page linkage.

The **dbcc** command is used in the database backup scripts to determine if the database is properly configured and without errors. If errors occur, the backup will not proceed and a message is sent to the DBA with notification of the problem.

4.16 Sybase Troubleshooting

4.16.1 Space Usage

Thresholds are defined on segments to provide a free space value at which a procedure is executed to provide a warning or to take remedial action. Use **sp_addthreshold** to define your own thresholds**: sp_addthreshold database_name, segment_name, free_space, procedure_name**, where **free_space** is the number of free pages at which the threshold procedure executes; **procedure_name** is the stored procedure which the threshold manager executes when the number of free pages falls below the **free_space** value.

Table 4.16-1, below, provides an Activity Checklist for Sybase troubleshooting.

Table 4.16-1. Sybase Troubleshooting - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Troubleshoot Chronic Deadlock	(P) 4.16.2.1	

4.16.2 Troubleshoot Chronic Deadlock

A deadlock (also known as a "deadly embrace") is a situation where two database processes are simultaneously attempting to lock data that the other holds. For example, two users (A and B) are updating the same table of data at the same time. User A holds a lock on Page 1 and requests a lock on Page 2. Meanwhile, user B holds a lock on Page 2 and has requested a lock on Page 1. Without intervention, these two jobs would never finish.

Sybase detects these situations, analyzes the two processes and automatically kills the process with less accumulated processor time. Sybase prints out an error message to the killed process

and requests that the user re-submit the job. A Sybase error message similar to the following one is displayed:

> **Msg 1205, Level 13, State 1:**
> **Server 'SERVER', Procedure 'sp_whatever', Line 123:**
> **Your server command (family id #0, process id #99) was deadlocked with another process and has been chosen as deadlock victim. Re-run your command.**
> **(return status = -3)**

4.16.2.1 Troubleshoot Chronic Deadlock

1 Turn on deadlock printing information and **sp_configure** "print deadlock information".

2 Recreate the problem.

3 As deadlocks occur, **tail -f the $SYBASE/ASE-12_5/install/errorlog** (or wherever the errorlog prints out to).

- Detailed information is printed out (e.g., line numbers of code causing deadlocks, tables within Sybase).

4 Run dbcc traceon(3604) and dbcc page(#) on the page numbers printed by traceflag 1204.

- dbcc page will report the tablename and the index that is being used.
- It is helpful to see if it is a non-clustered or a clustered index.

5 Monitor locks and blocked processes during deadlock re-creation.

- Use **sp_lock**, **sp_block** and **sp_blocker** to print out detailed information about locking and blocking.

6 Run **sp_sysmon** while re-creating the problem, and analyze the "Lock Management" section.

- Advanced deadlock diagnosis can be conducted using:
  - **traceflags 602, 603**, which prints out information for deadlock prevention.
  - **traceflag 1205**, which puts a stack trace on the deadlock.
  - **traceflag 8203**, which displays statement and transaction locks.
  - **sp_configure** "deadlock checking period", "deadlock retries", which are configuration parameters related to deadlocking.
- Common deadlock problems and solutions include:
  - **Contention on heap tables**. "Last page contention" problems occur where high insert rates always seem to go on the last page of a table. This creates what is known as a "heap table," which is bound to have performance problems. The end of the table (in terms of a page chain) is a hotspot of activity. If this is the cause of the deadlocks, either partition the table (which creates several insert points for data and eliminates the "heapness") or re-create your clustered index on a field that spreads inserts along the entire page chain of the table (i.e., clustered indexes on surrogate keys as opposed to last name or something similarly random). This can be seen in **sp_sysmon** output "Last page locks on heaps."
  - **Poorly written key generation schemes**. Using a "select max(col)+1" method or high rate OLTP applications generating keys from a badly configured **key_storage** table system are always deadlock candidates. Never use the

"select max+1" method. If you must use a **key_storage** solution (if you can't deal with identity gaps for example), ensure that the key_storage table is configured for Row Level Locking (in Sybase 11.9.2 and above) or has max_rows_per_page=1 (in Sybase 11.5 and 11.0).

- **Lock contention; sp_configure "number of locks"**. If you have configured too few locks for the system, severe lock contention can occur and deadlocking can be common. There is an entire section **of sp_sysmon** devoted to Lock management. Large updating within multi-user applications and long running transactions will definitely lead to deadlocking. Don't issue multiple update statements within the same transaction. If you must update multiple objects within the same transaction, make sure you consistently access the objects in the same order throughout the application. Updating or deleting from tables without covering indexes cause table scans. Other options: System data Lock strategies: In 11.9.2 and above: examine whether it may be wise to go to Row Level locking or Data only locking.
- **Hardware problems**. Slower I/O devices increase deadlock vulnerability.
- **Cursors**. Should be avoided.
- **Parallelism**. y using some of the parallel processing features available in later versions, deadlocking is subdued.
- **ANSI isolation level 3 (**serialization) locking. Avoid when possible.
- **Descending scans in indexes**. Can sometimes cause deadlocks after upgrading where none previously occurred.
- **Application-side deadlocking**. See Section 1.5.1 of the Sybase FAQ for a quick example of Application-side deadlocking and how to avoid it.
- **Deadlocking increases with upgrade**. These deadlocks are frequently caused by the "allow backward scans" option being turned on by default. They can also be caused by differing optimizer paths with new version (after upgrade) or just the engine's sheer speed. Also recommended to increase lock escalation threshold if using RLL (defaults to 200, which is not a lot of rows).

This page intentionally left blank.

5. Security Services

EMD security architecture must meet the requirements for data integrity, availability, and confidentiality. EMD Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. Security logs are monitored and security reports generated by the System Administrator as required. Several open source products provide tools for authentication and network and systems monitoring - Crack, ANLpasswd, TCP Wrappers, and Tripwire. Crack and ANLpasswd provide brute force password cracking and password checking, respectively for local system and network access. Tripwire monitors for intruders by noting changes to files. F-Secure Secure Shell (ssh) provides strong authentication access and session encryption from external, non-trusted networks as well as internally within a DAAC. Security Services also supports detection of, reporting, and recovery from security breaches. Security scans of each system are performed periodically to prepare for the formal security scans done biannually by the ESDIS IV&V contractor. These preliminary scans are done using the FOUNDSTONE Security Scanner product.

The following section defines step-by-step procedures for Operations personnel to run the Security Services tools. These procedures assume that DAAC Management has already approved the requester's application for a Security process. It is recommended that access to these tools be controlled through the **root access only**.

5.1 Scanning Network Vulnerabilities

The EMD project no longer has responsibility for scanning the network and network-attached systems. However, the FOUNDSTONE Security Scanner is a licensed product that NASA uses extensively to detect system level vulnerabilities. GSFC has a site license to use the product and any of the supported DAACs may use that license since all DAACs are using GSFC IP address space. This product does NOT belong to EMD and as such there is not an official release of it. A license key is required which can be obtained from the ESDIS Computer Security Official. The information the ESDIS Computer Security Official needs includes the IP addresses of the Production and M&O LANs. The software runs on Microsoft Windows Server 2003.. A laptop is the only practical way to run it. The software and the keys must be obtained through ESDIS CSO.

5.2 Ensuring Password Integrity

One aspect of system security is discretionary access control based on user passwords. Passwords ideally would be so unique that they are virtually impenetrable to unauthorized users. Two products provide utilities to create effective password practices. "Crack" detects weak passwords that could be easily bypassed. It works in "batch" mode. ANLpasswd enforces strong password rules as the user is changing their password.

Note: This functionality is in flux due to the transition to a linux environment. Replacement packages for ANLpasswd and Crack are being prepared.

Table 5.2-1 contains the activity checklist for Crack.

Table 5.2-1. Crack - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Configure Crack	(P) 5.2.1.1	
2	SA	Launching Crack	(P) 5.2.1.2	
3	SA	Creating Dictionaries	(P) 5.2.1.3.	

Crack and ANLpasswd provide a comprehensive dictionary, which can be shared. These "source" dictionaries provide lists of words, which if used, would create vulnerable passwords. You can add other dictionaries, for example, acronym lists, to eliminate commonly used terms from being used as passwords.

Crack is installed in a secure location that has **root access only**. ANLpasswd is automounted in /tools/bin.

5.2.1 Detecting Weak Passwords

Running Crack against a system's password file enables a system administrator to assess how vulnerable the file is to unauthorized users and how well authorized users select secure passwords. Crack is designed to find standard UNIX eight-character DES-encrypted passwords by standard guessing techniques.

Crack takes as its input a series of password files and source dictionaries. It merges the dictionaries, turns the password files into a sorted list, and generates lists of possible passwords from the merged dictionary or from information gleaned about users from the password file. It does not attempt to remedy the problem of allowing users to have guessable passwords, and it should NOT be used in place of getting a really good, secure password program replacement.

The instructions provided in the following sections are general in nature, because how you configure Crack is DAAC specific. Operations personnel should be familiar with these tasks to:

- Configure the Crack shell script and config.h files based on the README file and on requirements established for your site. See the Section on "Configuring Crack" below.
- Run Crack based on requirements established for your site. See "Running Crack" below.
- Customize the dictionaries. See Section "Creating Dictionaries" below.

Although Crack should already be configured for your system, the instructions are provided should you have to reconstruct the makefile as a result of file corruption. Crack has two configuration files: the Crack shell script, which contains all the installation-specific

configuration data, and the file Sources/conf.h, which contains configuration options specific to various binary platforms. Use the following procedure for configuring crack.

5.2.1.1 Configuring Crack

1 In the Crack shell script, edit the CRACK_HOME variable to the correct value. This variable should be set to an absolute path name on which Crack will be run. (Path names relative to username are acceptable as long as you are using csh.)

- There is a similar variable, CRACK_OUT, which specifies where Crack should put its output files — by default, this is the same as $CRACK_HOME.

2 Edit the file Sources/conf.h and establish which switches to enable. Each #define has a small note explaining its purpose. Portability of certain library functions should not be a problem.

3 If using Crack-network (see Section 5.2.1.4, Options, below), generate a Scripts/network.conf file. This file contains:

- A list of hostnames that are rsh/ssh destinations.
- Their binary type (useful when running a network Crack on several different architectures).
- An estimate of their relative power (take your slowest machine as unary, and measure all others relative to it).
- A list of per-host flags to add to those specified on the Crack command line, when calling that host.
- There is an example of such a file provided in the Scripts directory.

4 To specify a more precise figure as to the relative power of your machines, play with the command *make* tests in the source code directory. This can provide you with the number of fcrypt()s that your machine can do per second. This number can be plugged into your *network.conf* as a measure of your machines' power (after rounding the value to an integer).

Crack is a self-installing program. Once the necessary configuration options for the Crack shell script and config.h have been set, the executables are created via *make* by running the Crack shell script.

NOTE: To run Crack on a YP password file, the simplest way is to generate a passwd format file by running the following command:

 # ypcat passwd > passwd.yp ↵

and then running Crack on the passwd.yp file.

5.2.1.2 Launching Crack

To launch Crack:

---

1 To change directory, type **cd /usr/local/solaris /crack**, and then press the **Return/Enter** key.

2 To execute the program, type **./Crack**, and then press the **Return/Enter** key.

3 For the single platform version, type **./Crack [options] [bindir] /etc/passwd [...other passwd files]** and then press the **Return/Enter** key.

4 To execute over the network, type **./Crack -network [options] /etc/passwd [...other passwd files]** and then press the **Return/Enter** key.

For a brief overview of the [options] available, see Section 5.2.1.4, Options, below. Section 5.2.1.5, Crack Support Scripts, briefly describes several very useful scripts.

Crack works by performing several individual passes over the password entries that are supplied. Each pass generates password guesses based upon a sequence of rules, supplied to the program by the user. The rules are specified in a simplistic language in the files gecos.rules and dicts.rules, located in the Scripts directory (see Section 5.2.1.5, Crack Support Scripts, below).

Rules in Scripts/gecos.rules are applied to data generated by Crack from the pw_gecos and pw_gecos entries of the user's password entry. The entire set of rules in gecos.rules is applied to each of these words, which creates many more permutations and combinations, all of which are tested. After a pass has been made over the data based on gecos information, Crack makes further passes over the password data using successive rules from the Scripts/dicts.rules by loading the whole of Dicts/bigdict file into memory, with the rule being applied to each word from that file. This generates a resident dictionary, which is sorted and made unique to prevent wasting time on repetition. After each pass is completed, the memory used by the resident dictionary is freed up, and re-used when the next dictionary is loaded.

Crack creates the Dicts/bigdict dictionary by merging, sorting, and making unique the source dictionaries, which are to be found in the directory DictSrc and which may also be named in the Crack shell script, via the $STDDICT variable. (The default value of $STDDICT is /usr/dict/words.)

The file DictSrc/bad_pws.dat is a dictionary that is meant to provide many of those common but non-dictionary passwords, such as 12345678 or qwerty.

5.2.1.3 Creating Dictionaries

1	Copy your dictionary into the DictSrc directory (use compress on it if you wish to save space; Crack will unpack it while generating the big dictionary).
2	Delete the contents of the Dicts directory by running Scripts/spotless. Your new dictionary will be merged in on the next run.

5.2.1.4 Options

Options available with the Crack command are:

-f Runs Crack in foreground mode, i.e., the password cracker is not put into the background, and messages appear on stdout and stderr as you would expect. This option is only really useful for very small password files, or when you want to put a wrapper script around Crack.

Foreground mode is disabled if you try running Crack-network -f on the command line, because of the insensibility of rsh'ing to several machines in turn, waiting for each one to finish before calling the next. For more information, read the section about Network Cracking without NFS/RFS in the README.NETWORK file.

-v Sets verbose mode, whereby Crack will print every guess it is trying on a per-user basis. This is a very quick way of flooding your filestore, but useful if you think something is going wrong.

-m Sends mail to any user whose password you crack by invoking Scripts/nastygram with their username as an argument. The reason for using the script is so that a degree of flexibility in the format of the mail message is supplied; i.e., you don't have to recompile code in order to change the message.

-nvalue Sets the process to be nice()ed to value, so, for example, the switch -n19 sets the Crack process to run at the lowest priority.

-network Throws Crack into network mode, in which it reads the Scripts/network.conf file, splits its input into chunks that are sized according to the power of the target machine, and calls rsh to run Crack on that machine. Options for Crack running on the target machine may be supplied on the command line (for example, verbose or recover mode), or in the network.conf file if they pertain to specific hosts (e.g., nice() values).

-r<pointfile>

This is only for use when running in recover mode. When a running Crack instance starts pass 2, it periodically saves its state in a point file, with a name of the form Runtime/P.* This file can be used to recover where you were should a host crash. Simply invoke Crack in exactly the same manner as the last time, with the addition of the **-r** switch (for example, **-rRuntime/Pfred12345**). Crack will startup and read the file, and jump to roughly where it left off. If you are cracking a very large password file, this can save a lot of time after a crash.

5.2.1.5 Crack Support Scripts

The Scripts directory contains a small number of support and utility scripts, some of which are designed to help Crack users check their progress. The most useful scripts are briefly described below.

Scripts/shadmrg

This is a small script for merging /etc/passwd and /etc/shadow on System V style shadow password systems. It produces the merged data to stdout, and will need to be redirected into a file before Crack can work on it.

Scripts/plaster

This is a simple front-end to the Runtime/D* diefiles that each copy of the password cracker generates. Invoking Scripts/plaster will kill off all copies of the password cracker you are running, over the network or otherwise. Diefiles contain debugging information about the job, and are generated so that all the jobs on the entire network can be called quickly by invoking Scripts/plaster. Diefiles delete themselves after they have been run.

Scripts/status

This script rsh's to each machine mentioned in the Scripts/network.conf file, and provides some information about processes and uptime on that machine. This is useful when you want to find out just how well your password crackers are getting on during a Crack -network.

Scripts/{clean,spotless}

These are just front ends to a makefile. Invoking Scripts/clean cleans up the Crack home directory and removes unwanted files, but leaves the pre-processed dictionary bigdict intact. Scripts/spotless does the same as Scripts/clean, but obliterates bigdict and old output files, too, and compresses the feedback files into one.

Scripts/nastygram

This is the shell script that is invoked by the password cracker to send mail to users who have guessable passwords, if the **-m** option is used. Edit it to suit your system.

Scripts/guess2fbk

This script takes your out* files as arguments and reformats the 'Guessed' lines into a feedback file, suitable for storing with the others.

An occasion where this might be useful is when your cracker has guessed a large number of passwords and then died for some reason (a crash?), before writing out the guesses to a feedback file. Running **Scripts/guess2fbk out*** >> **Runtime/F.new** will save the work that has been done.

5.2.1.6 Checking the Log

Crack loads dictionaries directly into memory, sorts and makes them unique, before attempting to use each of the words as a guess for each users' password. If Crack correctly guesses a password, it marks the user as done and does not waste further time on trying to break that user's password.

Once Crack has finished a dictionary pass, it sweeps the list of users looking for the passwords it has cracked. It stores the cracked passwords in both plain text and encrypted forms in a feedback file in the directory **Runtime**. Feedback files have names of the form **Runtime/F***. This allows Crack to recognize passwords that it has successfully cracked previously, and filter them from the input to the password cracker. This provides an instant list of “crackable” users who have not changed their passwords since the last time Crack was run. This list appears in a file with name **out*** in the **$CRACK_OUT** directory, or on **stdout**, if foreground mode (**-f**) is invoked (see Section “Options”, above).

Similarly, when a Crack run terminates normally, it writes out to the feedback file all encrypted passwords that it has NOT succeeded in cracking. Crack will then ignore all of these passwords next time you run it.

Obviously, this is not desirable if you frequently change your dictionaries or rules, so, **Scripts/mrgfbk** is provided to allow for checking the “uncrackable” passwords. This script sorts your feedback files, merges them into one, and optionally removes all traces of "uncrackable" passwords, so that your next Crack run can have a go at passwords it has not succeeded in breaking before.

mrgfbk is invoked automatically if you run **Scripts/spotless** (see Section 5.2.1.5, Crack Support Scripts, above).

5.2.2 ANLpasswd

The Argonne National Laboratory wrote ANLpasswd and has made it available to everyone as freeware. There is a simple install script that will install the components on the automount host for both SGI and Sun architectures. ANLpasswd consists of a setuid C program that is used to call the anlpasswd Perl script. The Perl script uses the Crypt::Cracklib module, which is installed with the package, a dictionary generation tool, and dictionaries that are used to match attempted passwords against possible passwords that are in the dictionary file.

It is assumed that Perl 5.6 is properly installed in /tools/perl for Sun and SGI platforms. The binary ypstuff and the anlpasswd30 script (with its soft links to anlpasswd and yppasswd) are placed in /tools/bin. The Perl includes and dictionary file should also be NFS mounted and placed in /tools/lib/anlpasswd.

Once the package is configured, the only alteration may be in the dictionary files. There are a large number of dictionary files that are included by default in this release. If there are local requirements to change them (i.e. the default has too little security or too much security), the following procedure is applicable.

Table 5.2-2 contains the activity checklist for ANLpasswd.

Table 5.2-2. ANLpasswd - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Configure ANLpasswd	(P) 5.2.2.1	

5.2.2.1 Configuring ANLpassword

1 Login to the automount host as root or **su** to root.

2 Modify the SGI /tools/lib/words directory as required (add files, modify files or remove files).

3 Remove the Sun /tools/lib/words directory contents, then copy the SGI (modified) directory to the Sun directory.

4 Login to an SGI as root or **su** to root.

5 From the SGI window, type **cd /tmp** and then press the **Return/Enter** key to change to the directory where anlpasswd-30.tar.gz is located.

- The directory is changed to **/tmp**.

6 To explode anlpasswd-30.tar.gz, type **gzip –dc anlpasswd-30.tar.gz | tar –xovf –** and ten press the **Return/Enter** key.

- The anlpasswd-30.tar.gz file is exploded.

7 From the SGI window, to change directory to the location of the make dictionary script, type **cd /tmp/anlpasswd/anlpasswd-3.0-sgi/cracklib25_small**, and then press the **Return/Enter** key.

- The directory is changed to /tmp/anlpasswd/anlpasswd-3.0-sgi/cracklib25_small.

8 To run the make dictionary script, type **./makedictionary.pl** and then press the **Return/Enter** key.

- ***Note*:** perl expected to be in /tools/perl
- The script runs.

9 From the SGI window, on completion, copy the pw_dict.* files to the automount host's /tmp directory.

10 From the automount host window, copy the /tmp/pw_dict.* files to the appropriate /tools/lib directories for ***both*** SGI and Sun architectures.

11 Logout from the automount host.

12 From the SGI window, **su** to a normal user account and check that the changes work by running /tools/bin/anlpasswd as a normal user and verify at least one of the changes and that the script still works normally (without errors).

13 From the SGI window, to delete the temp files, type **rm –rf /tmp/anlpasswd**, and then press the **Return/Enter** key.

- The temp files are deleted.

14 Logout from the SGI.

5.2.2.2 Installing ANLpasswd

Use the procedures provided in the Release Notes for the relevant version of ANLpasswd. Release Notes are available through the "Release Notes" link at the following URL:

http://cmdm-ldo.raytheon.com/baseline/

5.2.2.3 ANLpasswd readme

The following is the README.INSTALL from the tar file with comments. This work has already been incorporated in the release. It is provided here to facilitate understanding of how the product is put together.

```
ANLpasswd is used in ECS to provide interactive password checking. It is
installed on the network in the /tools/bin directory. Local installation
is not required.

PREREQUISITES
This installation requires:
Perl 5.6.1
50Mb of disk space
It will take approximately 30 minutes to complete this installation.

INSTALLATION INSTRUCTIONS
1.  Copy the anlpasswd-30.tar.gz file to a staging area. For
convenience, /tmp is used in these instructions.

2.  Login to the automount host as root or su to root.

3.  Change directory to /tmp and explode the tarball using the commands:
# cd /tmp ↵
# gzip –dc anlpasswd30.tar.gz | tar –xovf - ↵

4. Change directory to the top level directory and run the install script using the command:
# cd /tmp/anlpasswd ↵
# ./install_anlpasswd.pl ↵

This will install the /tools/bin/anlpasswd30 script with links to
/tools/bin/anlpasswd and /tools/bin/yppasswd, the dictionaries
themselves, and the dictionary indexes.

5.  If you DO have a password aging method in place, skip to step 8. If
you do not have a password aging method in place and are implementing
the password aging script, copy the
/tmp/anlpasswd/password_aging_notify.pl script to the NIS master server.
To implement this script, the following information needs to be edited
in the passwordage.pl script:

# Master NIS server

$master_host = "<NISMASTER>";

###

# Domain (used when building address to send users email)
$domain = "<DAACDOMAIN>";
```

```
#

# Location of the Shadow file
$shadow_file = "<SHADOWFILELOCATION>";

# The protected accounts - these accounts are immune to password aging


@protected_accounts = ('root');
###


# Location of the directory to backup copies of the shadow file in
$shadow_archive = "<SHADOWFILEARCHIVELOCATION>";
###

# Variables used when sendmail emails messages to users and SAs
# This to address is used when sending emails to the SAs
$to_address = "<SAADDRESSLIST>";
```

where:
<NISMASTER> is the fully qualified host name for the NIS master
<DAACDOMAIN> is the NIS domain name of the DAAC
<SHADOWFILELOCATION> is the location of the shadow file (normally /etc/shadow)
<SHADOWFILEARCHIVELOCATION> is the directory of the shadow file archive backups
< SAADDRESSLIST> is the email account(s) to send messages to SAs

6. Setup cron to run the script at a convenient time.

7. Logoff from the automount host.

8. Checkout the SGI installation from an SGI production host by logging in as a normal user.

9. Change your password using the command:
   % **/tools/bin/yppasswd ↵**

10. Logout

11. Wait a few minutes to make sure that the updates are completed.

12. Checkout the Solaris installation from a Sun production host by logging in as a normal user.

13. Change your password using the command:
   % **/tools/bin/yppasswd ↵**

14. Logout

15. Wait a few minutes to make sure that the updates are completed.

That should be all that is needed to get this program up and running. If there are any problems or inaccuracies in this documentation, or you have any improvements or bug fixes, please send email to "support@mcs.anl.gov"

5.3 Aging Passwords

Password aging is required by NPR 2810.1, *NASA Procedural Requirements: Security of Information Technology*. A perl script is provided as part of the ANLpasswd 3.0 release that will, after configuration, perform 120-day password aging. If your site already has a method of doing password aging, this section may be ignored. If your site does NOT have a password aging method in place and you are implementing the password aging script, copy the /tmp/anlpasswd/password_aging_notify.pl script to the NIS master server.

To implement this script, the following information needs to be edited in the password_aging_notify.pl script:

```
# Master NIS server
$master_host = "<NISMASTER>";
###

# Domain (used when building address to send users email)
$domain = "<DAACDOMAIN>";
#
# The protected accounts - these accounts are immune to password aging
@protected_accounts = ('root');

# Location of the directory to backup copies of the shadow file in
$shadow_archive = "<SHADOWFILEARCHIVELOCATION>";
###

# Variables used when sendmail emails messages to users and SAs
# This to address is used when sending emails to the SAs
$to_address = "<SAADDRESSLIST>";
```

where:
<NISMASTER> is the fully qualified host name for the NIS master
<DAACDOMAIN> is the NIS domain name of the DAAC
<SHADOWFILELOCATION> is the location of the shadow file (normally /etc/shadow)
<SHADOWFILEARCHIVELOCATION> is the directory of the shadow file archive backups
< SAADDRESSLIST> is the email account(s) to send messages to sys administrators

5.4 Secure Access through Secure Shell

The security risks involved in using “R” commands such as rlogin, rsh, rexec and rcp are well known, but their ease of use has made their use tempting in all but the most secure of environments. Ssh is an easy-to-use, drop in replacement for these commands developed by Tatu Ylonen. Ssh is a “user” level application. No changes to the host kernel are required. The UNIX server implements the commercial version of F-Secure. As of the F-Secure 3.2 release, only SSH Version 2 is included in pre-compiled, OS-specific packages.

As of the Secure Shell 2.0 release in May, 2000 and later, all of the files needed to function are loaded locally on each UNIX host in /usr/local/bin.

- ssh - replaces rsh, rlogin and rexec for interactive sessions
- scp - replaces rcp for interactive file transfer

- ssh-agent – application that allows a user to enter the passphrase once, then when other applications (e.g. ssh, scp) are used, one is not prompted for the passphrase – it is automatically negotiated.
- ssh-add - add access to a specific ssh host
- ssh-keygen - generates keys for the local host based on a passphrase (long password)
- ssh-signer – verifies that a key is genuine so that public key authentication may proceed
- sftp - secure ftp

The host daemon is in /usr/local/sbin which includes:

- sshd2 - the ssh version 2 daemon

Several files are generated on installation and when running and are installed locally:

- /etc/ssh2/ssh2_config - system-wide configuration for the ssh2 client
- /etc/ssh2/hostkey - contains the long number used for one of the ssh2 keys
- /etc/ssh2/hostkey.pub - contains the ssh2 key known to the public
- /etc/ssh2/random_seed - base number used in generating keys
- /etc/ssh2/sshd2_config - defines the local ssh2 security policy
- /etc/sshd2_22.pid - the process id of the ssh2 daemon currently running

The amount of disk space that the programs and the configurations require is less than 25 MB.

Table 5.4-1 contains the activity checklist for Services Access through Secure Shell.

Table 5.4-1. Secure Access through Secure Shell - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Using Secure Shell	(P) 5.4.3.1	

5.4.1 Installation of SSH

Use the procedures provided in the Release Notes for the relevant version of ssh. Release Notes are available through the "Release Notes" link at the following URL:

http://cmdm-ldo.raytheon.com/baseline/

5.4.2 The SSH Encryption Mechanism[1]

Each host has a host-specific DSA key (normally 1024 bits) used to identify the host. Additionally, when the daemon starts, it generates a server DSA session key (normally 768 bits). This key is normally regenerated every hour if it has been used, and is never stored on disk.

Whenever a client connects the daemon, the daemon sends its host and server public keys to the client. The client compares the host key against its own database to verify that it has not changed. The client then generates a 256 bit random number. It encrypts this random number

[1] From the *sshd* man page

using both the host key and the server key, and sends the encrypted number to the server. Both sides then start to use this random number as a session key that is used to encrypt all further communications in the session. The rest of the session is encrypted using a conventional cipher. Under EMD the aes128 cipher is used. The client selects the encryption algorithm to use from those offered by the server.

Next, the server and the client enter an authentication dialog. The client tries to authenticate itself using .rhosts authentication, .rhosts authentication combined with DSA host authentication, RSA challenge-response authentication, or password-based authentication. (NOTE: In the EMD configuration, .rhosts is NOT available).

Rhosts authentication is disabled within the DAACs because it is fundamentally insecure.

If the client successfully authenticates itself, a dialog for preparing the session is entered. At this time the client may request things like allocating a pseudo-tty, forwarding X11 connections, forwarding TCP/IP connections, or forwarding the authentication agent connection over the secure channel.

5.4.3 Using Secure Shell

5.4.3.1 Using Secure Shell

1 To login, use the command:

% slogin defiant ↵

Enter the passphrase for the key (lotsofstuffhere): **br0wn cow 3ats grass ↵**
Last login: Sun Feb 22 06:50:59 1998 from echuser.east.hitc.com
No mail.
%

NOTE: The first time you login to a host the following message will pop up asking if you want to continue. In response, type **yes** and [**enter**]:

Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? **yes ↵**
Host 't1acg01' added to the list of known hosts.

2 To transfer a file, use the command:

% scp hostone:/etc/info info ↵
Enter the passphrase for the key (lotsofstuffhere): **br0wn cow 3ats grass ↵**

- This will copy the file /etc/info from hostone to your local host. Note that your passphrase is needed to initiate the transfer.

IMPORTANT NOTE: The default directory on the *target* host is always the users HOME directory.

3 Also, one may send/receive files recursively using "-r" such as:

% scp -r ~/files/* hostone:~/files ↵

will send what is in the home directory files subdirectory to the target host hostone in the home files subdirectory.

4 To execute a command remotely, use the command:

% ssh whoisonfirst ps –ef ↵
Enter the passphrase for the key (lotsofstuffhere): **br0wn cow 3ats grass ↵**

5.4.4 A Layer of Convenience

If you are already a user of "r" commands, you probably know about the .rhost file. Ssh will allow a user to setup the .rhost equivalent called .shost in one's home directory. .Rhost and .shost contain the names of the hosts to which one normally connects. The nice thing about using it is one need not enter one's passphrase. Unlike "r" commands, however, ssh commands use long strings of numbers to authenticate the client, which makes it quite difficult for an intruder to impersonate a legitimate user. One word of caution, however, if you leave your terminal while logged on, a passerby could logon to any host in your .rhost/.shosts file and potentially cause malicious damage to you and your colleagues work. Be aware!

NOTE: ssh checks the mode of .shost, so change permission on .shost by typing:

% chmod 600 /home/JohnDoe/.shost ↵

where you must substitute your own home directory for /home/JohnDoe.

5.4.5 Multiple Connections

If you open multiple connections, it is more convenient to keep your keys in system memory. To do this requires executing two commands:

% ssa ↵
Enter the passphrase for the key (lotsofstuffhere):
Enter passphrase: **br0wn cow 3ats grass ↵**
Identity added: /home/JohnDoe/.ssh/identity (bpeters@nevermor)
%

Now, one may make connections (slogin, scp, ssh) to hosts that are running ssh without being prompted for a passphrase.

5.4.6 Secure FTP

A secure version of ftp is available. Use the command:

% sftp user@remotehost ↵
Enter the passphrase for the key (lotsofstuffhere): **MY PASSPHRASE ↵**

local directory - /home/user
remote directory - /home/user
sftp> get thisisafilename ↵
sftp> put thisotherfilename ↵
sftp> quit ↵

5.4.7 Other Notes

IMPORTANT: SSH will automatically "tunnel" X sessions without user involvement even through multiple hops. However, it is important that you do NOT change the DISPLAY parameter or X will not use the ssh tunnel!

5.4.8 Configuration of Secure Shell

5.4.8.1 Local Setup

Most users will start from the same host whether from an X terminal, a UNIX workstation, or a PC. Running the sss (sshsetup) script generates long strings called keys that make ssh work. One set of keys is needed for each home directory.

The only thing you need to know before executing the script is to pick a good passphrase of at least 10 characters. You can and should use spaces and multiple words with numbers, misspellings and special characters. Note that passwords are NOT echoed back to the screen.

PLEASE DO NOT USE THE PASSWORDS/PASSPHRASES USED HERE OR IN ANY OTHER DOCUMENTATION!

Using the script sss should look like:

% sss ↵
Use a passphrase of at least 10 characters; which should include numbers
or special characters and MAY include spaces
New passphrase: **This is a silly test ↵**
Retype new passphrase: **This is a silly test ↵**
Generating ssh1 keys. Please wait while the program completes...
Generating ssh2 keys. This can take up to 240 seconds...
Done with sshsetup!
%

You are on the way!

NOTE: If you have accounts in the PVC, VATC and/or the EDF, at a DAAC production LAN or DAAC M&O LAN, do sss in EACH environment.

5.4.8.2 Remote Setup

If you need to access a host with a different home directory, you will need to run the ssr (ssh remote) script. NOTE: It is helpful to have run Secure Shell Setup (sss) in each environment

first before doing the ssh remote script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. A new capability is to use different user names on the source and target hosts. This should look something like:

```
% ssr ↵
Remote user name (default: yourusername): ↵
Do you want to setup for:
1   VATC
2   PVC
3  GSFC DAAC
4   SMC
5   GSFC M and O
6   EDC DAAC
7   EDC M and O
8  LaRC DAAC
9   LaRC M and O
10  NSIDC DAAC
11  NSIDC M and O
x   Exit from script
Select:
2
Working...
Accepting host p0spg07.pvc.ecs.nasa.gov key without checking.
yourusername@p0spg07.pvc.ecs.nasa.gov's password:
Authentication complete. Continuing with sshremote...
Downloaded remote keys.
Uploaded local keys.Keys concatenated.

Enter next site (press the enter-key and then x enter-key to exit)
Remote user name (default: yourusername): ↵

Do you want to setup for:
1   VATC
2   PVC
3  GSFC DAAC
4   SMC
5   GSFC M and O
6   EDC DAAC
7   EDC M and O
8  LaRC DAAC
9   LaRC M and O
10  NSIDC DAAC
11  NSIDC M and O

x   Exit from script
```

Select:
x <enter>
bye!
%

5.4.8.3 Changing your Passphrase

To change your passphrase, use the following command:

% ssp ↵

Enter old passphrase: little 1amp jumb3d <enter>
Enter a new passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces

New passphrase: **br0wn cows 3at grass ↵**
Retype new passphrase: **br0wn cows 3at grass ↵**

ssh2 key changed successfully.
Done with sshpass2!

5.4.9 Administration of Secure Shell

There is no administration of secure shell required except for general monitoring to make sure that the daemon process (/usr/local/sbin/sshd2) is running. Note, however, that the standard installation will establish a /var/log/ssh log file. It is recommended to review the /var/log/ssh and the system log file at least once a week.

5.5 Controlling Requests for Network Services (TCP Wrappers)

With TCP Wrappers, you can monitor and filter incoming requests for network services, such as FTP.

TCP Wrapper provides a small wrapper program for inet daemons that can be installed without any changes to existing software or to existing configuration files. The wrappers report the name of the client host and the name of the requested service; the wrappers do not exchange information with the client or server applications, and impose no overhead on the actual conversation between the client and server applications. The usual approach is to run one single daemon process that waits for all kinds of incoming network connections. Whenever a connection is established, this daemon runs the appropriate server program and goes back to sleep, waiting for other connections.

Operations personnel will monitor requests for these network services:

Client	Server	Application
ftp	Ftpd	file transfer
finger	Fingerd	show users

The **/var/log/wrappers log** file should be reviewed at least once a week. The log file provides information concerning who tried to access the network service. TCP Wrapper blocks any request made by unauthorized users. TCP Wrapper can be configured to send a message to any administrator whose request is rejected.

NOTE: All DAACs, except for NSIDC, do not use TCP Wrappers.

5.5.1 Installation, Configuration, and Testing for Wrappers

The installation of TCP Wrappers is part of the Secure Shell 2.0 and later packages. As of F-Secure SSH 3.2, it is a separate package and should be installed as part of the ssh installation. The location of most of the wrappers files have been changed to /etc/wrappers. Libwrap.a is in /usr/local/lib and tcpd.h is in /usr/local/include. The installation is automatic if wrappers have been previously installed. After installation, there are common operator functions, and the following checks should be made:

5.5.2 Quick Start Using Tripwire

The following command is used to execute Tripwire from the command line prompt (as root):

/etc/tripwire/src/tripwire -v > {filename}

The following is the general syntax of executing Tripwire

tripwire [***options*** *...] >****filename***

Where ***options*** are:

-initialize	Database Generation mode -init
-update entry	update entry (a file, directory, or tw.config entry) in the database
-interactive	Integrity Checking mode with interactive entry updating
-loosedir	use looser checking rules for directories
-d dbasefile	read in database from dbasefile (use `-d -' to read from stdin)
-c configfile	read in config file from configfile (use `-c -' to read from stdin)
-cfd fd	read in config file from specified fd
-dfd fd	read in the database file from specified fd
-Dvar=value	define a tw.config variable (ala @@define)
-Uvar	undefine a tw.config variable (ala @@undef)
-i # or –i all	ignore the specified signature (to reduce execution time)
-q	quiet mode
-v	verbose mode

-preprocess	print out preprocessed configuration file
-E	save as -preprocess
-help	print out interpretation help message
-version	print version and patch information

filename is a complete filename (including path) for the output report file.

Tripwire is automatically invoked on all machines by a “cron” run, which periodically executes Tripwire.

The operator receives information from Tripwire by email for files whose current signature does not match the datastore signature.

The operator must verify the file changes and update the datastore or report a security violation. Tripwire may be run manually to update the datastore or create reports. The Operator can also generate Tripwire reports via the command line.

The differences between the behaviors of Tripwire started from the “Cron” run and started by the operator result from the use of appropriate parameters on the start command. These parameters are listed and explained below.

5.6 Monitoring File and Directory Integrity (Tripwire)

Tripwire is a tool that aids in the detection of unauthorized modification of files resident on UNIX systems. One important application of Tripwire is its use as the first and most fundamental layer of intrusion detection for an organization. Tripwire is automatically invoked at system startup. This utility will check the file and directory integrity by comparing a designated set of files and directories against information stored in a previously generated database. Tripwire flags and logs any differences, including added or deleted entries. When run against system files regularly, Tripwire spots any changes in critical system files, records these changes into its database, and notifies system administrators of corrupted or tampered files so that they can take damage control measures quickly and effectively. With Tripwire, system administrators can conclude with a high degree of certainty that a given set of files remain free of unauthorized modifications if Tripwire reports no changes. Tripwire works in conjunction with these other solutions to provide a "Defense in Depth"(trademark) security solution.

NOTE: Since system files should not change and users' files change constantly, Tripwire should be used to **monitor only system files**. The list of system files you want to monitor is stored in **./configs/tw.conf**.

The system administrator should install Tripwire on a clean system. This baseline database will then be used to compare possible changes to files and directories to make sure the system has not been compromised. If the system has been compromised, information provided by Tripwire can be used to carry out a forensics investigation of the compromise. Forensics is the compiling of the chain of evidence necessary to prosecute offenders after an attack has occurred.

The system administrator should check any changes made to the system on a weekly basis or after an alert from a security organization like NASIRC or CERT has put out an alert on security vulnerabilities for any of the baseline operating systems or COTS software.

All reported changes need to be investigated right away. The investigator should be aware that most of the file changes are due to system updates. But each change should be traceable to a specific, baselined change. If no unexplained changes are detected, then the Tripwire database needs to be updated to reflect file updates. Tripwire should be configured to mail the system administrator any output that it generates.

5.6.1 Installation of Tripwire

Use the procedures provided in the Release Notes for the relevant version of Tripwire. Release Notes are available through the “Release Notes” link at the following URL:

http://pete.hitc.com/baseline/CUSTOM_SOFTWARE/ReleaseNotes.html

5.6.2 Updating the Tripwire Database

You can update your Tripwire database in two ways. The first method is interactive, where Tripwire prompts the user whether each changed entry should be updated to reflect the current state of the file, while the second method is a command-line driven mode where specific files/entries are specified at run-time.

5.6.2.1 Updating Tripwire Database in Interactive Mode

Running Tripwire in Interactive mode is similar to the Integrity Checking mode. However, when a file or directory is encountered that has been added, deleted, or changed from what was recorded in the database, Tripwire asks the user whether the database entry should be updated.

For example, if Tripwire is run in Interactive mode and a file's timestamp changed, Tripwire will print out what it expected the file to look like, what it actually found, and then prompt the user to specify whether the file should be updated. For example:

```
/etc/hosts.equiv
    st_mtime: Wed May  5 15:30:37 2006      Wed May  5 15:24:09 2006
    st_ctime: Wed May  5 15:30:37 2006      Wed May  5 15:24:09 2006
---> File:  /etc/hosts equiv
---> Update entry?  [YN(y)n?] y ↵
```

You could answer yes or no, where a capital 'Y' or 'N' tells Tripwire to use your answer for the rest of the files. (The 'h' and '?' choices give you help and descriptions of the various inode fields.)

While this mode may be the most convenient way of keeping your database up-to-date, it requires that the user be "at the keyboard." A more conventional command-line driven interface exists, and is described next.

5.6.2.2 Updating Tripwire Database in Database Update Mode

Tripwire supports incremental updates of its database on a per-file/directory or tw.config entry basis. Tripwire stores information in the database so it can associate any file in the database with the tw.config entry that generated it when the database was created.

Therefore, if a single file has changed, you can:

 # tripwire -update /etc/newly.installed.file ↵

Or, if an entire set of files that made up an entry in the tw.config file changed, you can:

 # tripwire -update /usr/local/bin/Local_Package_Dir ↵

In either case, Tripwire regenerates the database entries for every specified file. A backup of the old database is created in the **./databases** directory.

Tripwire can handle arbitrary numbers of arguments in Database Update mode.

The script **twdb_check.pl** script is an interim mechanism to ensure database consistency. Namely, when new entries are added to the tw.config file, database entries may no longer be associated with the proper entry number. The twdb_check.pl script analyzes the database, and remaps each database entry with its proper tw.config entry.

5.6.3 Configuring the tw.config File

Edit your **tw.config** file in the **./configs** directory, or whatever filename you defined for the Tripwire configuration file, and add all the directories that contain files that you want monitored. The format of the configuration file is described in its header and in the "man" page. Pay especially close attention to the select-flags and omit-lists, which can significantly reduce the amount of uninteresting output generated by Tripwire. For example, you will probably want to omit files like mount tables that are constantly changed by the operating system.

Run Tripwire with **tripwire -initialize**. This will create a file called **tw.db_[hostname]** in the directory you specified to hold your databases (where [hostname] will be replaced with your machine hostname).

Tripwire will detect changes made to files from this point on. You ***must*** be certain that the system on which you generate the initial database is clean; however, Tripwire cannot detect unauthorized modifications that have already been made. One way to do this would be to take the machine to single-user mode, reinstall all system binaries, and run Tripwire in initialization mode before returning to multi-user operation.

This database must be moved someplace where it cannot be modified. Because data from Tripwire is only as trustworthy as its database, choose this with care. It is recommended to place all the system databases on a read-only disk (you need to be able to change the disk to writeable during initialization and updates, however), or exporting it via read-only NFS from a "secure-server." (This pathname is hardcoded into Tripwire. Any time you change the pathname to the database repository, you must recompile Tripwire. This prevents a malicious intruder from spoofing Tripwire into giving a false "okay" message.)

We also recommend that you make a hardcopy printout of the database contents right away. In the event that you become suspicious of the integrity of the database, you will be able to manually compare information against this hardcopy.

Once you have your database set up, you can run Tripwire in Integrity Checking mode by typing **tripwire** on the command line from the directory in which Tripwire has been installed.

5.7 Reporting Security Breaches

Reporting of Security breaches shall be in accordance with NPR 2810.1, *NASA Procedural Requirements: Security of Information Technology*. The specific location in the 2810 is the section on IT Security Incidents Reporting and Handling.

5.8 Initiating Recovery from Security Breaches

Recovery from Security breaches shall be in accordance with NPR 2810.1, *NASA Procedural Requirements: Security of Information Technology*. The specific location in the 2810 is the section on IT Security Incidents Reporting and Handling.

6. Network Administration

This section covers the procedures necessary for the management operations that monitor and control the system network capabilities.

Detailed procedures for tasks performed by the Network Administrator are provided in the sections that follow. The procedures assume that the administrator is authorized and has proper access privileges to perform the tasks (i.e., root).

6.1 Network Documentation

EMD Network Administration requires access to restricted documents that are posted on the EMD Baseline Information System (EBIS) Site (http://pete.hitc.com/baseline/) but are not available on the public mirror site (http://cmdm-ldo.raytheon.com/baseline/). The following restricted documents provide network documentation:

- DAAC LAN Topology 921-TD*x*-001
  (*x* = DAAC designation: L = LaRC; N = NSIDC; E = LP DAAC)
- [DAAC] Hardware/Network Diagram 921-TD*x*-002
- IP Address Assignment (DAAC Hosts) 921-TD*x*-003
- IP Address Assignment (DAAC Network Hardware) 921-TD*x*-004

The documents describe and depict the network layout and inter/intra-connections necessary to understand the system. Contact EMD Configuration Management for versions relevant to an individual site.

6.2 Network Monitoring

6.2.1 Big Brother - Better Than Free Edition

Big Brother Better Than Free Edition (BTF) is a network monitoring and notification COTS application. DAAC network administrators use it to monitor network devices and the services on those devices and to get feedback on their network's performance. Basic procedures common activities and additional information is available in 609-EMD-003, Release 7.21 Operations Tools Manual for the EMD Project

6.3 DAAC LAN Topology Overview

The LAN topology at each DAAC is unique. The detailed network topology for each DAAC is not presented in the student guide due to network security concerns. However, the details will be discussed during the class presentation.

In spite of the unique design of each DAAC's LAN, there are some common features.

- The Production Network at each Distributed Active Archive Center (DAAC) consists of an Ethernet Virtual Local Area Network (VLAN) supported by Ethernet 10-Mb/s, 100-Mb/s, and Gigabit Ethernet (GigE) connections and a GigE switch.
- The VLAN Ethernet switch is connected to a Portus Firewall by a Gigabit Ethernet connection.
- The firewall provides access to both the M&O Network and a VLAN outside the firewall that provides connections to external networks, such as the following services:
  - Campus network.
  - Very high performance Backbone Network Service (vBNS+).
  - Internet Protocol Network Operations Center (IPNOC) and other parts of the NASA Integrated Services Network (NISN).

System hosts within a DAAC are connected to the VLAN Ethernet switch. The switch is used to connect hosts at 10/100/1000 Mb/s. The VLAN Ethernet switch is connected to the Portus Firewall via a 1000-Mb/s (GigE) connection.

In addition to their connections to the VLAN Ethernet switch the ACM/Ingest hosts, PDR Server hosts, Data Server hosts, and science processors are interconnected through a backend GigE switched network. This setup provides a high-speed network to handle the large data transfers among subsystems. The GigE switch shifts the numerous transfers of large volumes of data onto a dedicated high-speed topology, freeing the VLAN to handle control flows and DAAC-to-DAAC processing flows.

6.4 Network Hardware Components

The DAAC LANs consist of the following major hardware components:

- Portus Firewall.
- VLAN Ethernet Switch.
- GigE Switch.

6.4.1 Portus Firewall

The Portus Firewall hardware consists of an IBM RS6000 server installed with the basic AIX 5.3operating system. It contains two 9GB internal disk drives that are mirrored, as well as a pair of redundant power supplies. Distributed FTProxy SOCKS is provided by Portus Firewall, which has replaced E-Borders Server.

6.4.2 VLAN Ethernet Switch

The Ethernet switch at each DAAC is a Cisco Catalyst 6506E , which provide a large number of 10/100/1000-Mb/s interfaces. The VLAN1 Ethernet switch interfaces with all Production hosts and the Portus Firewall. The VLAN10 Ethernet switch interfaces with the Portus Firewall and routers to external networks.

Maintenance and configuration of the Ethernet switch is considered non-trivial functions. Such tasks are addressed in special technical training provided by the vendor and supplemental training provided by EMD.

6.4.3 GigE Switch

The GigE Switch is Cisco Catalyst 3550. It connects some of the SGI hosts to a high-speed switching fabric.

Maintenance and configuration of the GigE Switch are considered non-trivial functions. Such tasks are addressed in special technical training provided by the vendor and supplemental training provided by EMD.

6.5 Domain Name Service (DNS) Structure

The parent DNS domain for the system is **ecs.nasa.gov**. These DNS servers reside at the SMC, and the NSIDC DAAC. In this domain are the SMC hosts, User hosts for all DAACs, and pointers to the DAACs' external DNS servers. The external DNS resides on the Portus Firewall.

The ecs.nasa.gov DNS servers are:

- m0isi08.ecs.nasa.gov
- n0fwi09u.ecs.nasa.gov

The LP and NSIDC DAACs' Production networks are a child domain of ecs.nasa.gov. They are:

- LP DAAC Production network:
  - e4nsl01.edcb.ecs.nasa.gov (internal)
  - e4nsl02.edcb.ecs.nasa.gov (internal)
  - e0fwi09.edcb.ecs.nasa.gov (external)
- NSIDC Production network:
  - n4nsl01.nsidcb.ecs.nasa.gov (internal)
  - n4nsl02.nsidcb.ecs.nasa.gov (internal)
  - n0fwi09.nsidcb.ecs.nasa.gov (external)

The LP DAACs' M&O network is also a child domain of ecs.nasa.gov. It is:

- LP DAAC M&O network.
  - edcmo.ecs.nasa.gov

The LaRC DAACs' Production network is a child domain of larc.nasa.gov. It is:

- LaRC Production network:
  - nasans4.nasa.gov (extenal)
  - dns1.larc.ecs.nasa.gov (external)
  - dns2.larc.ecs.nasa.gov (external)

6.6 Host Names

A letter is appended to the production host name to distinguish which interface (and IP address) a user is accessing.

As an example, a LP DAAC host named e0acg11.edcb.ecs.nasa.gov is a host attached to the Production network.

6.7 Network Security

6.7.1 Network Connectivity

The system network was designed to minimize unauthorized user access, including the use of a firewall at each site. Ingest network access at a DAAC is limited to its Level 0 data provider(s), the SMC, and hosts attached to the DAAC's Production and M&O networks. No local campus, Internet or other DAAC access is provided. Access to a DAAC's Production network is limited to the SMC, the DAAC's M&O network, and other DAACs. No local campus, Internet, or Level 0 data provider(s) access is provided. Table 6.7-1 contains the activity checklist for Network Security.

Table 6.7-1 Network Security - Activity Checklist

Order	Role	Task	Section	Complete?
1	Network Admin	Checking Local Host Access to another Local Host Over the Network	(P) 6.7.2.1	

6.7.2 Troubleshooting - Verifying Connectivity

One of the key reasons for failure of data access and transfer is an error or problem in system connectivity. This can be caused by a myriad of glitches such as incorrect/outdated lookup tables, incorrectly assigned IP addresses, missing default route and more. Besides checking individual host/server operation with various tools such as ECS Assistant, you can use several command line entries to verify point-to-point communication between components.

There are three initial steps to help verify system connectivity:

- Ensuring connectivity is authorized (check the Network Connectivity matrix).
- Determining whether the Domain Name Service (DNS) is resolving host name and IP addresses correctly.
- Actively testing the connectivity using the ping function.

6.7.2.1 Checking Local Host Access to Another Local Host over the Network

1 To check the Domain Name Service entries (DNS) for the source host on workstation ***x0xxx##*** at the UNIX prompt enter:

nslookup <local_host>

- The screen display will be similar to the following:

g0spg01{mblument}[204]->nslookup g0spg01
Server: g0css02.gsfcb.ecs.nasa.gov

Address: xxx.xxx.xxx.xx
Name: g0spg01.gsfcb.ecs.nasa.gov
Address: xxx.xxx.xxx.xx

2 To check the DNS entries for other host on the Production network enter:

nslookup <other host>

- The screen display will be similar to the following:

```
g0spg01{mblument}[201]->nslookup g0css02
Server: g0css02.gsfcb.ecs.nasa.gov
Address: xxx.xxx.xxx.xx
Name: g0css02.gsfcb.ecs.nasa.gov
Address: xxx.xxx.xxx.xx
```

3 To determine the host's network interface parameters enter:

netstat -i

- The **netstat -i** command will provide the following information:

```
g0spg01{mblument}[201]->netstat –i
Name Mtu   Network     Address          Ipkts Ierrs    Opkts Oerrs  Coll
ipg0 4352  xxx.xxx.xxxg0spg01.gsfcb.   9182666     1  8103032     0     0
hip0 65280 xxx.xxx.xg0spg01h.gsfcb.  5554524     0  6776651     0     0
xpi0 4352  xxx.xxx.xxx.xxg0spg01u.ecs.   37850320     0 14109683     3     0
xpi1 0     none       none                0     0       0     0     0
et0* 1500  none       none                0     0       0     0     0
lo0  8304  loopback   localhost        314800     0   314800     0     0
```

4 To determine the host's network interface enter:

ifconfig <interface>

- Using **ipg0** from the **ifconfig <interface>** data as the interface parameter, **ifconfig ipg0**, will result in the following display:

```
g0spg01{mblument}[203]->ifconfig ipg0
ipg0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>
inet xxx.xxx.xxx.xx netmask 0xffffff00 broadcast xxx.xxx.xxx.xxx
```

5 To ping the local host to verify inter-connectivity enter:

ping <local host>

- For example:

```
g0spg01{mblument}[232]->ping g0spg01
PING g0spg01.gsfcb.ecs.nasa.gov (xxx.xxx.xxx.xx): 56 data bytes
64 bytes from xxx.xxx.xxx.xx: icmp_seq=0 ttl=255 time=0 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=1 ttl=255 time=0 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=2 ttl=255 time=0 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=3 ttl=255 time=0 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=4 ttl=255 time=0 ms
 ----g0spg01.gsfcb.ecs.nasa.gov PING Statistics----
```

5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
g0spg01{mblument}[233]->

6 To verify inter-connectivity with other hosts on the Production network enter:

ping <remote host>

- For example:

g0spg01{mblument}[202]->ping g0css02
PING g0css02.gsfcb.ecs.nasa.gov (xxx.xxx.xxx.xx): 56 data bytes
64 bytes from xxx.xxx.xxx.xx: icmp_seq=0 ttl=255 time=2 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=1 ttl=255 time=1 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=2 ttl=255 time=1 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=3 ttl=255 time=1 ms
64 bytes from xxx.xxx.xxx.xx: icmp_seq=4 ttl=255 time=1 ms
----g0css02.gsfcb.ecs.nasa.gov PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1/1/2 ms

Note: You cannot ping hosts outside of the Production network because of the Protus firewall implemetation. See your local firewall administrator for assistance when troubleshoot connectivity issues with hosts outside of the Production LAN.

7 To check the health of the interface enter:

netstat -i

- The following type of result is returned:

```
g0spg01{mblument}[218]->netstat -i
Name Mtu   Network     Address              Ipkts       Ierrs       Opkts       Oerrs  Coll
ipg0 4352  xxx.xxx.xxxg0spg01.gsfcb.        9197317     1           8113487     0      0
hip0 65280 xxx.xxx.xg0spg01h.gsfcb.         5554541     0           6776668     0      0
xpi0 4352  xxx.xxx.xxx.xxg0spg01u.ecs.      37851779    0           14109837    3      0
xpi1 0     none            none             0           0           0           0      0
et0* 1500  none            none             0           0           0           0      0
lo0  8304  loopback    localhost            325510      0           325510      0      0
```

8 Examine the output of the **netstat** command to determine whether there are any Ierrs and/or Oerrs.

- One or two errors are acceptable, 100 errors are not.
  - A lot of errors indicate an interface problem; check the syslog for any startup or logged problems from the OS.

6.7.2.2 Checking Host Communication Across External Networks

You cannot ping or traceroute to hosts outside the Production network because of the firewall implemetation. See your local firewall administrator for assistance when troubleshooting connectivity issues with hosts outside of the Production network.

7. System Monitoring

7.1 Overview

This chapter covers procedures for the management operations that monitor the network and server applications. Graphical tools available to monitor system status include **Big Brother (BTF)**, and **EcMs-Whazzup**. These programs provide system monitors with real-time status of the system and indications of potential problem areas.

7.2 Checking the Health and Status of the Network

7.2.1 Big Brother

Big Brother Better Than Free Edition (BTF) is a network monitoring and notification COTS application. DAAC network administrators use it to monitor network devices and the services on those devices and to get feedback on their network's performance.

Big Brother is a Web-based COTS application used to monitor network devices and services on the EMD Production LANs. (URL Example; http://f4msl10.hitc.com). Big Brother capabilities are executed through the use of GUIs. Figure 7.2-1 is an example of the standard Big Brother home page.

Figure 7.2-1. Big Brother Home Page

Common functions performed by Big Brother are shown below in Table 7.2-1:

Table 7.2-1. Common Functions Performed by Big Brother

Operating Function	GUI	Description	When and why to Use
View network devices/services status	View icon color and on web GUI; view quick status dialog box.	Icon color indicates the status of network devices and services.	To verify that all network devices and services on the devices are operational. To ascertain network devices and services that is not operating properly.
View network devices/services performance data	Logs and Report menus on GUI	A set of reports that can be viewed, printed, and/or its content transmitted to a file.	To obtain status information about monitored devices and services.

7.2.2 Menu Toolbar

The Big Brother Server Display web page has a "Toolbar" at the upper left portion of the main page and sub-pages. This toolbar has four icons which are explained below in detail. Figure 7.2-2 represents the Toolbar icons.

Figure 7.2-2. Big Brother Toolbar

Notification/Page Acknowledgement – Clicking on this icon navigates to a page where administrators enter acknowledgment of events to pause notification alerts.

Condensed View – Clicking on this icon toggles the main page view from "full" list of hosts and services to a "condensed" view of hosts and services. The condensed view displays only hosts and services that are displaying warnings or error conditions.

Availability Report – Clicking on this icon provides access to the availability reports, where an operator or administrator can investigate availability for a customized time-frame.

Help – Clicking on this icon will display a menu of help topics.

7.2.3 Indications of a Device or Service Problem

Big Brother automatically provides notification of device and service problems on devices. A device's service icons remain green if the device and its services are responding to the Big Brother polls and the service is not impaired. If a device is down, or its service impaired beyond preset thresholds, the color of this device's service changes from green or yellow to red animated starburst shape as shown in Figure 7.2-1. The color codes are shown in Table 7.2-2. An operator can further drill down to find details of the condition that caused the impairment or outage, specifically in the case of a service impairment where a level such as CPU, or disk space crossed a predefined threshold.

Table 7.2-2. Color Codes by Order of Severity

Code	Description
	Red – Critical Problem
	Purple - No report - No report from this client in the last 30 minutes. The client may have died.
	Yellow - Attention - The reporting system has crossed a threshold you should know about.
	Green - OK – Status of host or service is normal.
	Clear - Unavailable -The associated test has been turned off, or does not apply. A common example is connectivity on disconnected dialup lines.
	Blue - Disabled - Notification for this test has been disabled. Used when performing maintenance.
	Acked - A current event has been acknowledged by one or many recipients. The acknowledgement is valid until the longest delay has expired

7.3 Monitoring and Managing Server Applications

Whazzup??? is a management tool that provides operators and maintainers with a means of monitoring and checking servers, for quickly identifying servers that may have problems, and for isolating faults. It is a web-based application, and is therefore accessed by means of browser software. It provides the following general features:

- Host and mode views of network resources.
- Status information on resources (indicated by color coding: purple indicates inability to ping the specified host, blue indicates incomplete data collection, red indicates that the server is down, and yellow indicates that a warning threshold has been exceeded).
- Performance monitoring capability.

Table 7.3-1 contains the Activity Checklist for Monitoring and Managing Server Applications.

Table 7.3-1. Monitoring and Managing Server Applications - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Launching Whazzup	(P) 7.3.1.1	

7.3.1 Whazzup??

A powerful COTS program that has been modified for monitoring the system is EcMsWz-Whazzup??. It is a web-accessed program that provides a graphical display of Host Status, Mode Status, Mode Verification and Performance Management. The welcome screen has buttons and links at the bottom permitting an operator to view status by various means (e.g., host, mode), verify modes and view what servers may be down, and access data on performance. The **Performance Stats** screen provides a quick overview of the system status; if Whazzup is unable to ping a host, the row for that host is highlighted in purple.

These functions of Whazzup?? provide graphical displays of host and software-server status in real-time mode. When used in conjunction with WhatsUp Professional and ECS Assistant, Whazzup?? can provide System Administrators with a comprehensive knowledge of the system's status.

7.3.1.1 Launching WhazzUp??

Log in to a host machine.

1 At the UNIX prompt on the host from which Whazzup is to be run, type **setenv DISPLAY <*hostname*>:0.0** press the **Return/Enter** key.

- ***Note:*** If the host has been remotely accessed via ssh, do not use the setenv DISPLAY command again. Doing so will compromise system security.
- ***hostname*** is the name of the machine on which Whazzup is to be displayed, i.e., the machine you are using.
- To verify the setting, type **echo $DISPLAY** then press the **Return/Enter** key.

2 At the UNIX prompt, using secure shell, log on to the Whazzup host, x4eil01. Type **ssh *x4eil01*** then press the **Return/Enter** key.

3 Type ***Passphrase*** then press the **Return/Enter** key.

- You are logged into the Whazzup host machine.

4 To start the Mozilla Firefox web browser type **firefox &** then press the **Return/Enter** key.

- You are in the web browser on the Whazzup host **e4eil01**

5 In the **Location** field of the Netscape browser type the URL for Whazzup (e.g., **http://x4eil01:5150/**) then press the **Return/Enter** key.

- The Whazzup intro screen appears (Figure 7.3-1).

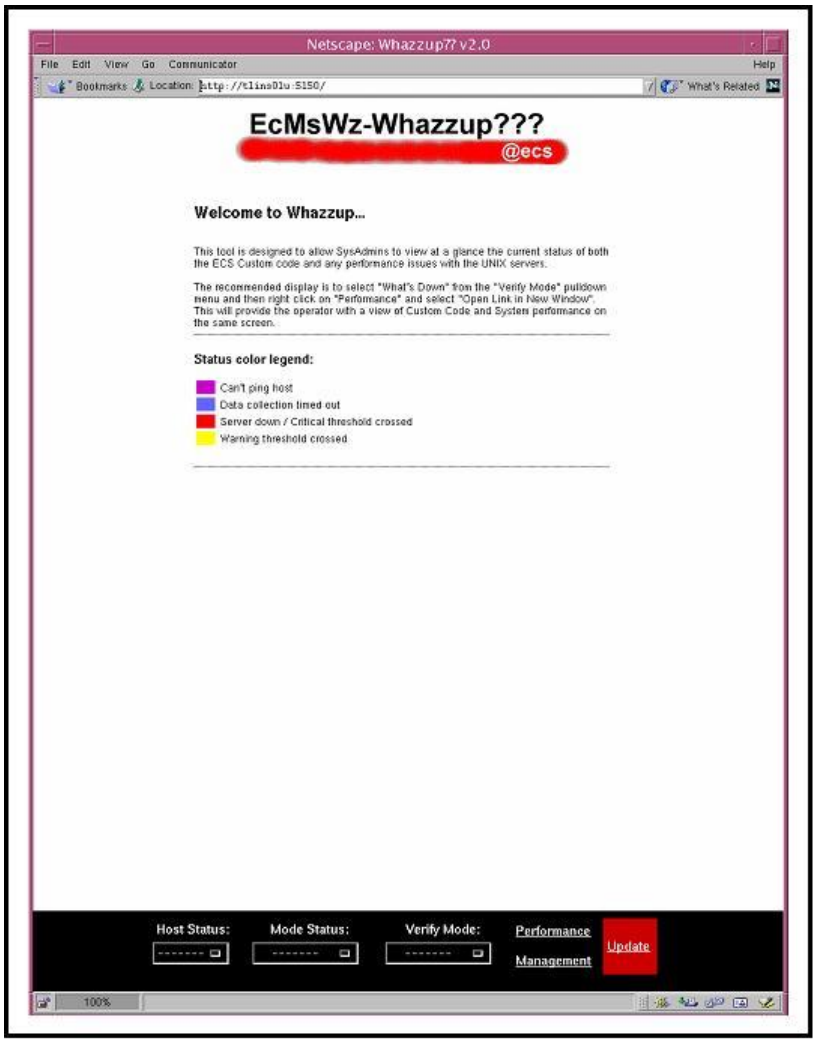


Figure 7.3-1. ECS Whazzup Initial Display

6 Select a monitoring function:

- **Host Status** to determine individual host parameters.
- **Mode Status** to determine “up” servers for the selected Mode.
- **Verify Mode** to determine status of all servers for a selected Mode.
- **Performance Management** to determine the performance status of all hardware/software servers for all modes.

This page intentionally left blank.

8. Problem Management

Problem management is the practice of monitoring and controlling problem reporting and resolution. EMD problem management is administered through system-level and site-level control boards and reviews. The control boards oversee the analysis, recommendations, and actions taken to resolve system/site problems concerning ECS hardware, software, documentation, and procedures. Site-level organizations typically resolve routine maintenance issues at the site-level, while system-level organizations address issues that are beyond the site's capabilities to repair or that require a change to the ECS operational baseline.

ECS sites use trouble tickets to track system problems that occur locally. The trouble ticket is the vehicle used first to record and report problems with the operational system. Trouble tickets can be generated by operations, maintenance, development, and customer personnel as well as by external users. The CM Administrator at each operational ECS site (DAAC) serves as trouble ticket system administrator.

Many trouble tickets can be resolved locally. However, those that cannot are elevated to the system-level at the ECS Development Facility (EDF), where Non-Conformance Reports (NCRs) are used to track problems that require resolution at the system-level or a change to system-level configuration baselines.

Trouble tickets and NCRs are managed using EMD's automated defect tracking system, TestTrack Pro (TTPro). This centralized system at the EDF stores problem descriptions, assessments and fixes; notifies users of progress towards resolution; and generates reports for metrics. Documentation not well suited for the system is stored elsewhere but is referenced in related TTs or NCRs.

The following sections provide an overview of the Trouble Ticketing process and define the procedures for submitting, working with, and closing trouble tickets. In addition, they provide a scenario for handling Emergency Fixes.

8.1 The Problem Resolution Process

Any ECS user may submit trouble tickets (TTs), either directly into TTPro or through User Services. TT submission triggers an internal review by the site’s review board. Primary objectives of the internal review are to identify quickly which problems fall within the site’s capability to resolve; review and validate the priority of each problem; assign TTs to local staff members; and elevate to system-level any problems that exceed local capabilities or that require a change to the system-level baseline. Emergency fixes (High TTs) can be made locally with the approval of the local CCB, with the solution forwarded to the EDF in a trouble ticket.

As technicians and engineers work to resolve problems they are assigned, they update trouble tickets to document their activities. This information is used to determine critical maintenance concerns related to frequency of occurrence, criticality level, and the volume of problems experienced. TTPro notifies selected individuals whenever a TT is assigned or changes state.

User Services representatives monitor trouble tickets in order to notify users concerning problem resolution and status.

When TTs need to be elevated to the system-level, site CMAs or their designees "escalate" them in TTPro. TTPro notifies affected parties, including senior EMD staff when problems rated "critical" are reported, and forwards the tickets to the EDF for review by the EMD PRB.

The PRB tracks trouble tickets that have been forwarded to the EDF. The PRB is not a voting board. Membership is appointed for the purpose of providing timely, direct technical support to the Chair, who has decision-making responsibility and authority. CMAs support this Board by reporting status, maintaining priority lists, and implementing actions as the Board may direct.

The PRB performs a preliminary review of each forwarded trouble ticket. It confirms the severity assigned by the site, checks that the information provided is complete and relevant to the problem, and determines whether a change to the system-level operational baseline would be required.

The PRB refers escalated TTs to EMD's sustaining engineers for analysis and recommendations, These engineers have the authority to direct resolutions to problems that do not change, or in any way affect, the EMD operational baseline and baseline documentation. An NCR is required when the technical investigation determines that the operational baseline must be changed in order to correct the problem identified in the trouble ticket. In these cases, the PRB opens the escalated TT in TTPro as an NCR, adding supplemental information as necessary.

EMD's sustaining engineering staff works on resolving NCRs, updating TTPro to document all related activities. TTPro notifies selected EMD staff whenever an NCR changes, and it notifies selected DAAC staff whenever it changes state.

EMD deploys NCR fixes in the form of engineering technical directives, test executables, patches, and releases. Each requires an approved Configuration Change Request as described in the *Configuration Management Plan for the EMD Project* (110-EMD-001).

The PRB closes NCRs after fixes have been installed and verified by the site that submitted them

DAACs close TTs according to local site policies.

8.2 Problem Management Procedures

1. Users and operators having access to TTPro open a trouble ticket. Those without access to TTPro report system problems to their DAAC’s User Services Desk which opens the trouble ticket for them. Trouble tickets can be submitted remotely, via the Internet, using TTPro's web client.

2. The local review board evaluates the severity of the problem and determines assignment of on-site responsibility (???). Trouble tickets that can be resolved locally are assigned and tracked at the local center.

3. The Operations Supervisor reviews each trouble ticket's priority and description, and then assigns it to an appropriate technician or engineer to resolve.

a. For matters that can be resolved locally, technicians and engineers work towards resolving the problems and update the trouble tickets to record their progress. The nominal life cycle of a trouble ticket is Open, Open (Assigned), Solution Proposed, Solution Implemented, then Closed, although tickets may be escalated to the EDF or ECHO and re-opened as well.

b. CM Administrators close trouble tickets upon determining that a problem has been resolved satisfactorily, or after the EMD PRB accepts the problem for tracking as an NCR.

4. Technicians and engineers work towards resolving reported problems and update trouble tickets to record their progress. The nominal lifecycle of a trouble ticket is Open, Open (Assigned), Solution Proposed, Solution Implemented, then Closed, although tickets may be escalated to the EDF (or ECHO) and re-opened as well.

5. Matters that require external or system-level assistance, such as a repair which require changes to the system baseline, are escalated to the EMD PRB for discussion and disposition.

c. TTPro moves the ticket as "forwarded", and creates a trouble ticket at the system level.

d. The EMD PRB reviews the ticket at a PRB telecon telecom to coordinate trouble ticket activities within the EMD organization as well as with development, customer, and user organizations.

e. The DAAC Help Desk assigns the ticket to sustaining engineers for analysis.

f. If the problem can be resolved without changing the operational baseline, engineers at the EDF and the site coordinate to implement the fix, updating the ticket to document the solution. When the problem is resolved, the DAAC Help Desk closes the ticket.

g. If the problem requires a change to the baseline, the DAAC Help Desk uses the ticket to open an NCR, setting its initial severity and category and specifying the ECS product affected.

6. CM Administrators close trouble tickets upon determining that a problem has been resolved satisfactorily, or after the EMD PRB accepts the problem for tracking as an NCR.

8.3 Using the Trouble Ticketing System

ECS' trouble ticketing system is a centralized service located at the EDF. With TestTrack Pro (TTPro) -- a Commercial Off-The-Shelf (COTS) product -- at its core, it provides a common environment and means for classifying, tracking, and reporting operational system problems. Each site's trouble tickets, as well as EMD NCRs, are housed in separate databases called "projects".

TTPro can be accessed over the web or via locally installed Windows, Linux, or Solaris GUI clients. All clients allow users to submit, browse, edit, and query trouble tickets. Predefined and

user-created filters help limit retrievals to records of interest and can be configured to perform detailed trouble tickets searches.

TTPro is configured to notify its users when a trouble ticket is submitted, advanced to a new lifecycle state, or closed. Users can set private options so they receive additional notifications, and they can name specific individuals on any trouble ticket to ensure that they are notified whenever that trouble ticket is updated. In addition, users logged into a project can send email to any other user of the project, and they can have TTPro include a trouble ticket's summary and description data in the message.

Trouble ticketing system users generally perform one or more of the following tasks:

- Access the system by logging onto TTPro.
- Submit a trouble ticket – Users, operators, or User Services personnel, upon discovering a problem with the system (hardware, software, documentation, procedure, etc.) open a trouble ticket in TTPro to document the problem for later resolution. TTPro automatically assigns it a tracking number and places it in the "Open, not assigned" state, and notifies local staff, including the Operations Supervisor.
- Search for a trouble ticket – All trouble ticketing system users rely on search aids to help locate trouble tickets in order to investigate, fix, and maintain status of reported problems.
- Assign trouble ticket – The Operations Supervisor assigns the problem to a Problem Investigator [Resolution Technician] for follow-up.
- Update an open trouble ticket – The Problem Investigator [Resolution Technician] coordinates with problem submitter, developers, vendors, and external organizations to effect local resolution, if possible, and updates the trouble ticket in TTPro to record progress. TTPro notifies affected staff of each change, and may place the ticket in a state (e.g., Solution Implemented) depending on the type of update that the technician entered.
- Change a trouble ticket's lifecycle state – Technicians, engineers, and CM Administrators update trouble tickets to document designated events that mark progress towards resolution of a reported problem, which is reflected in a change of the trouble ticket's lifecycle state.
- Escalate trouble ticket to EDF – The local CM Administrator forwards trouble tickets to the EDF in cases where the problem needs to be elevated to the system-level for advice or resolution, such as when resolution requires a change to the operational baseline. TTPro places the ticket in the Forwarded state and notifies affected staff and EMD PRB members of the change.
- Open an NCR – The DAAC Help Desk opens an ECS NCR in response to an escalated trouble ticket if the operational baseline must be changed in order to correct the problem.

- Close trouble ticket – Local CM Administrators close trouble tickets upon determining that the problem has been resolved satisfactorily, or after the EMD PRB accepts the problem for tracking as an NCR. TTPro places the ticket in the Closed state and notifies staff members of the change.
- Add new users to TTPro's global user database – System-level TT Administrators create user profiles needed for users to log onto the system.
- Grant users access to a Trouble Ticket Project – Local CM Administrators manage users' profiles in trouble ticket projects, controlling access to their trouble tickets and to TTPro features that affect them.
- Reset a user's password – Local CM Administrators set new passwords when users forget them.
- Notifications - System notifications are configured as automation rules by site CM Administrators for the trouble ticket project as a whole.
- Generate reports – Authorized users of a trouble ticket project run pre-built or customized reports available to the project, as desired. All such users can create "private" reports. Trouble ticket system administrators can create reports that can "shared" with others.

Table 8.3-1 identifies where to find the procedures for these tasks in this document.

Table 8.3-1. Trouble Ticket System - Task Checklist (1 of 2)

Order	Role	Task	Section
1	System Users	Logging onto TTPro	8.3.1.1 or 8.3.1.2
2	System Users	Submit a Trouble Ticket	8.3.2.1 or 8.3.2.2
3	System Users	Search for a Trouble Ticket	8.3.3.1 or 8.3.3.2
4	Operations Supervisor	Assign Trouble Ticket	8.3.4.1 or 8.3.4.2
5	Technicians/ Engineers	Update an Open Trouble Ticket	8.3.5.1 or 8.3.5.3
6	Technicians/ Engineers	Change a Trouble Ticket's Lifecycle State	8.3.6.1 or 8.3.6.2
7	CM Administrator	Escalate trouble ticket to EDF	8.3.7.1 or 8.3.7.2
8	DAAC Help Desk	Open an NCR	8.3.8.1 or 8.3.8.2
9	CM Administrator	Close trouble ticket	8.3.9.1 or 8.3.9.2
10	System-level TT Administrator	Add a New User to the Global User Database	8.3.10.1

Table 8.3-1. Trouble Ticket System - Task Checklist (2 of 2)

Order	Role	Task	Section
11	CM Administrator	Grant Users Access to a Trouble Ticket Project	8.3.11.1 or 8.3.11.2
12	CM Administrator	Reset User Password	8.3.12.
13	CM Administrator	Manage Notifications	8.3.13.1 or 8.3.13.2
14	All	Generate Reports	8.3.14.1 or 8.3.14.2

The procedures in the sections below describe how to perform common ECS trouble ticketing tasks. Detailed instructions about how to use specific TTPro features can be found by invoking any client's on-line help.

Table 8.3-2. Trouble Ticket Priority/NCR Severity

As Documented in NASA 420-05-03	As Used/Interpreted by the EMD Project
Category 1: System/Service cannot perform critical function or imposes major safety hazard. (Priority 1) Presents an immediate impact to development, operations, services, or data processing functions; imposes major safety hazard to personnel, systems, or space mission resources; or results in loss of one or more essential mission objectives.	**HIGH (Severity 1)**: An NCR which causes: – Inability to perform a mission-critical function (i.e., Ingest/Pre-Processing/Archiving of Science Data, Planned Processing, Browse/Order/Distribute); – Performance of a mission-critical function to be so degraded that production minimum goals cannot be achieved; – A mission-critical function to be performed improperly, resulting in permanent loss of data; ***and*** for which no workaround exists ***or*** for which no workaround can be accommodated by DAAC operators given a detailed workaround procedure is documented but the procedure is inadequate based upon the complexity of the procedure, the abilities of an adequately trained and experienced operator, or both.
Category 2: System/Service substantially impaired. (Priority 2) Substantially impacts development, operations, services, or data processing functions; fails to operate within critical performance specifications; or cannot effectively or efficiently fulfill baseline requirements.	**MEDIUM (Severity 2)**: An NCR with the consequence that: – The performance of a mission-critical function is degraded and may prevent achieving production minimum goals; – A mission-critical function can be only partially performed, or performs improperly, resulting in temporary loss of data or incorrect data results; – A situation (actually or potentially) severly compromises ECS mission readiness or operational integrity; – A condition exists to produce a severely degraded mission-critical function, but a workaround will allow operations to continue temporarily without permanent loss of data or severely impaired performance/workload/schedules.
Category 3: System/Service slightly impaired. (Priority 3) Causes minor or no substantial impact to development, operations, services, or data processing functions. Support may be degraded, but mission can still be accomplished.	**Severity 3**: An NCR with the consequence that: – A non-critical mission function (e.g., Advertising) cannot be performed, or yields incorrect results; – Unexpected events occur which can be corrected using normal operational procedures with minimal impacts to performance/workloads/schedules – A condition exists to produce a degraded mission-critical function, but a workaround will allow operations to continue indefinitely without severely impaired performance/workload/schedules.
	Severity 4: Improvement (Nuisance; e.g., a typo).
	Severity 5: Enhancement (Identified for next release).

8.3.1 Accessing the Trouble Ticket System

ECS users and operators access TTPro via the web or locally installed Windows, Linux, or Solaris GUI clients. The functionality is largely the same across all the clients, although the look and feel of the web client is necessarily different than the others. In all cases, one must have

access to your site's trouble ticket project, which can be obtained by contacting the local CM Administrator.

8.3.1.1 Logging onto TTPro using the Web Client

1 Launch a supported internet browser. Recommended browsers are Internet Explorer 6.0+, Netscape 7.0+ or Firefox 2.0+.

Note: TTPro works best if pop-ups are enabled for ECS' TTPro website.

2 Enter one of the following URLs:

- **https://links.gsfc.nasa.gov:<*port*>** (for access from outside the EDF)
- **http://links.hitc.com:<port>** (for access from inside the EDF)

3 When the Login to TestTrack Web page appears (Figure 8.3-1), enter your assigned **Username** and your **Password**. Then click **Login**.

Note: First-time users should leave the **Password** field blank. TTPro will prompt you to create a password. Passwords must be a minimum of 8 characters long and include at least one number and one non-alphanumeric (e.g., symbol).

Note: TTPro will prompt you to login again if the **Username** or **Password** you entered is incorrect. If your password has expired, you will be prompted to enter a new one.

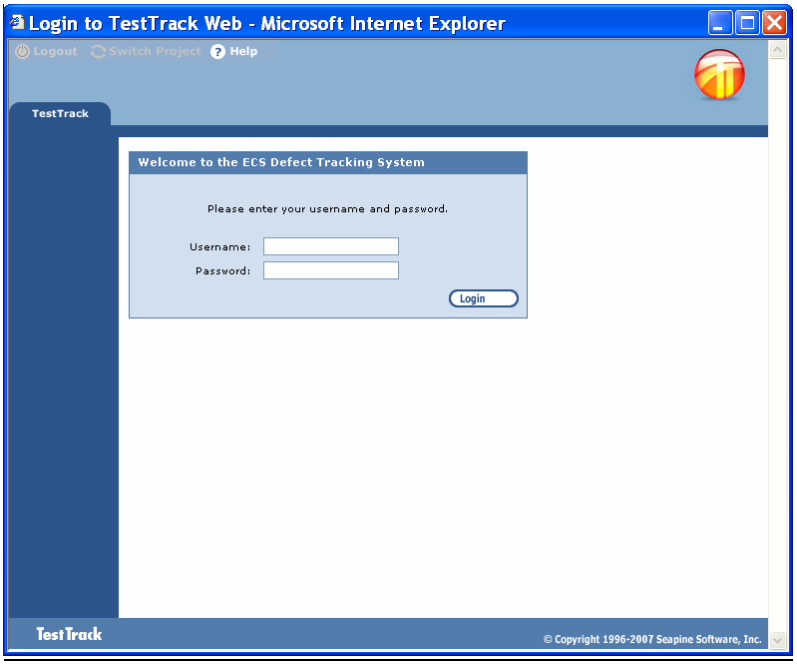


Figure 8.3-1. Login to TestTrack Web Page

4 When the project login page appears (Figure 8.3-2), select the name of the **Project** you want to access (e.g., NSIDC_TTs) and a **Start At** value (e.g., Defect List), and then click **Login**. TTPro will log you into the selected project and display the Work with Trouble Tickets page (Figure 8.3-3), the starting point for working with trouble tickets.

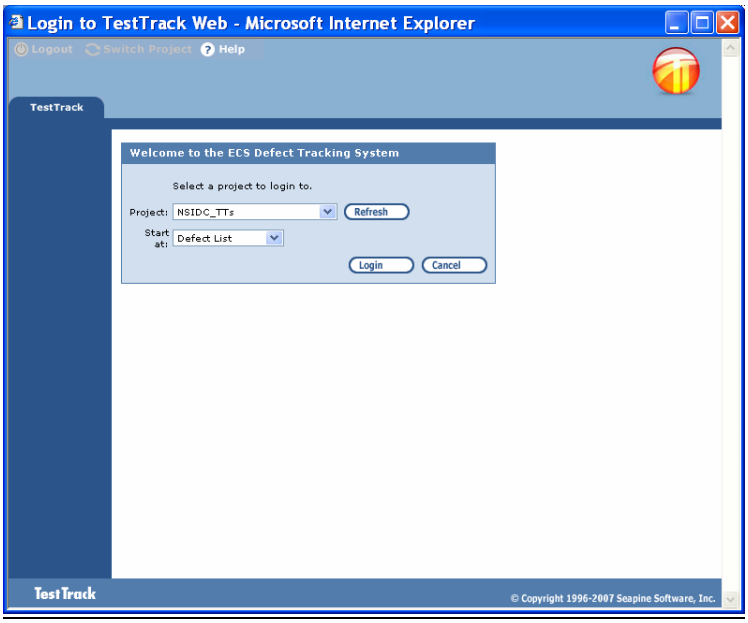


Figure 8.3-2. Login to TestTrack Web Project Page

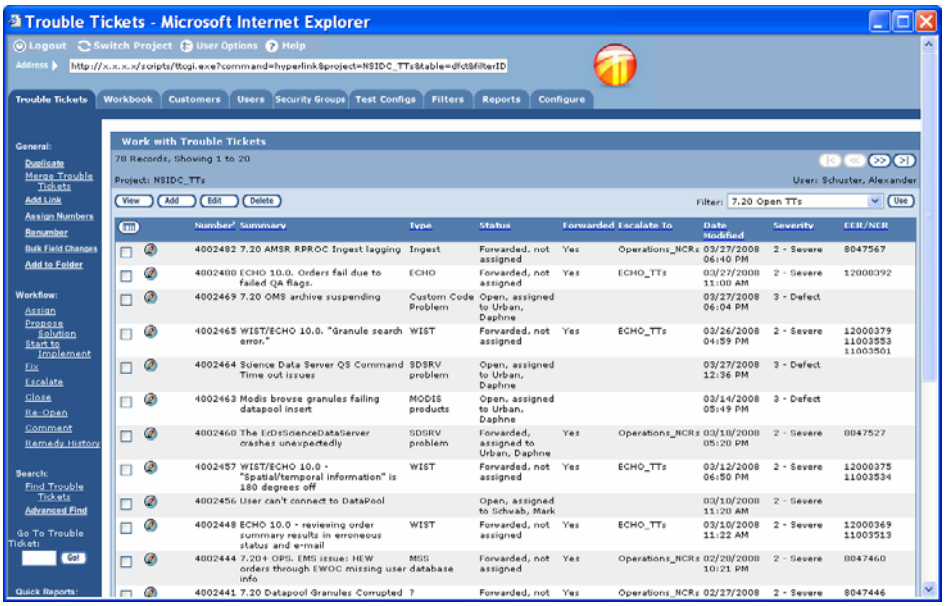


Figure 8.3-3. Work with Trouble Tickets Web Page

8.3.1.2 Logging onto TTPro using the GUI Clients

1 Launch TTPro:

[Windows] Click **Start → Programs → Seapine Software → TestTrack 2008→ TestTrack Client**

[Linux and Solaris]:

a. Logon the workstation on which the TTPro client is installed.

b. Change your working directory to TTPro's application directory (typically, /usr/ecs/OPS/COTS/ttpro/bin).

c. Type `./ttclient &`

2 If using TTPro for the first time, the Add TestTrack Server GUI will appear (Figure 8.3-4) so you can define a TTPro server connection that you can reference when logging into TTPro again. Enter the following:

- **Server Name** – your choice of a name for a TTPro server connection
- **Server Address** – the fully qualified domain name of the machine on which the TTPro server is installed
- **Port** – the baselined tcp port on which the client communicates with ECS' TTPro server.

Your TTPro Administrator can help you set up this connection.

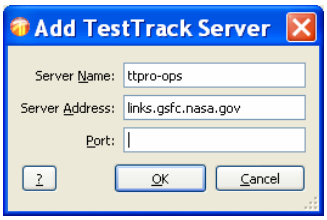


Figure 8.3-4. Add TestTrack Server GUI

3 When the TestTrack Studio Login screen opens (Figure 8.3-5), select the **Server** to which you want to connect, enter your assigned **Username** and your **Password**, and then click **Connect**.

Note: First-time users should leave the **Password** field blank. TTPro will prompt you to create a password. Passwords must be a minimum of 8 characters long and include at least one number and one non-alphanumeric (e.g., symbol).

Figure 8.3-5. TestTrack Studio Login GUI

4 On the TestTrack Project Selection screen (Figure 8.3-6), select the name of the **Project** you want to access (e.g., NSIDC_TTs), and then click **OK**. You can set the **Always login to this project** checkbox to use this project as your default in the future. TTPro will log you into the selected project and display the Trouble Tickets List GUI (Figure 8.3-7), the starting point for working with trouble tickets.

Note: If the **Project** picklist is empty or indicates that projects are loading, click **Refresh** after a few moments to retrieve a new list.

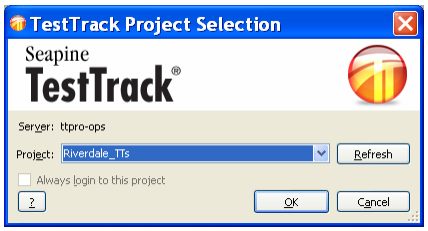


Figure 8.3-6. TestTrack Project Selection GUI

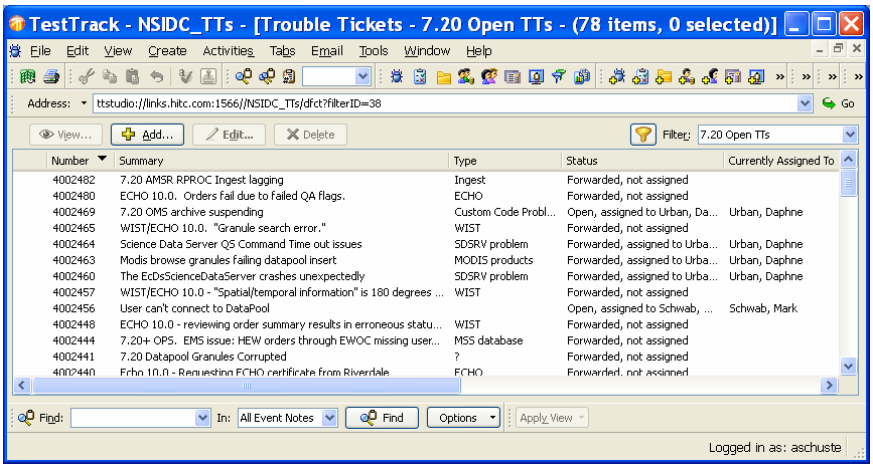


Figure 8.3-7. Trouble Tickets List GUI

8.3.2 Submit a Trouble Ticket

Submit a trouble ticket to document an operational system issue or problem. TTPro emails system notifications automatically to alert designated individuals whenever a new trouble ticket is submitted.

Tables 8.3-3 and 8.3-4 describe the fields and tabs that are viewable when submitting a trouble ticket.

Table 8.3-3. TTPro Trouble Tickets Field Descriptions (1 of 2)

Field Name	Data Type	Size	Entry	Description
Number	Integer	8	System generated	Ticket number, which is set and maintained by the system.
Summary	Character	154	Required	Short description of the problem. Displays as defect listing line in defects project window.
Status	Character	n/a	Automatic	Indicate the assignment and state of transition of defect
Submitter Site	Selection	*	Optional	Home DAAC of the Submitter or defect's originating site.
Type	Selection	30	Optional	Type of problem addressed by this Trouble Ticket (e.g., configuration error, hardware problem, software problem).
Priority	Selection	*	Optional	Priority of trouble ticket assigned at the site (HIGH, MEDIUM, and LOW).

Table 8.3-3. TTPro Trouble Tickets Field Descriptions (2 of 2)

Field Name	Data Type	Size	Entry	Description
Product	Selection	*	Optional	Product exhibiting the problem or issue
Component	Selection	*	Optional	Product's component exhibiting the problem or issue. In legacy (REMEDY) defects, it's the name of the configuration item to which the problem is associated.
Entered by	Character	30	Required	User name of the Submitter or person who created the defect.
Severity	Selection	*	Required	Impact of the problem to the submitter (HIGH, MEDIUM, LOW).
Date Entered	Date	n/a	Optional	Date Trouble Ticket was created at the present site.
Mode	Selection	*	Optional	Run mode in which problem was detected.
Machine Name	Character	60	Optional	Hardware resource on which this problem was detected.
DAAC Trouble Ticket	Character	20	Optional	Unique identifier that is established at the origination site. Legacy identifier of defect (from REMEDY ARS)
CCR/NCR	Character	10	Optional	Identifier of a related CCR or NCR. If more than one, separate each by a space or semicolon for readability.
DAAC POC	Character	n/a	Optional	Name of the issue's point of contact at the DAAC. Used when escalating Trouble Tickets to Landover PRB for advice or resolution.
Duplicate of	Character	10	Optional	The Ticket-ID of the primary Trouble Ticket for the problem reported in this Trouble Ticket and its associated duplicate Trouble Tickets (other tickets reporting the same problem).
Current Report	Selection	*	Optional	Submitter and date of an occurrence of the problem or issue. Helps browse through multiple reports of the same issue.
Found by (Submitter)	Selection	*	Required	Full name of the user who initially reported the problem.
Date	Date	n/a	Optional	Date the problem was encountered.
Version	Selection	*	Optional	Version of the product having the problem.
Description	Character	4060	Optional	Detailed description of the problem
Current Report	Selection	*	Optional	Submitter and date of an occurrence of the problem or issue. Helps browse through multiple reports of the same issue.

*Note, the size of a field with a "selection" data type can vary and the size is automatically adjusted to the size of the item selected from the selection list.

Table 8.3-4. TTPro Tab Descriptions

Tab Name	Description
Detail	Contains the details about one or more occurrences of the problem that was found. Information recorded on this tab include who detected the problem (*Found By* (*Submitter)*), date the problem was detected (*Date)*, *Version* of the version of the product that had the problem *(Version)*, and a description of the problem sufficient for an engineer to perform an analysis *(Description)*.
Workflow	This tab automatically captures identified series of events or activities associated with the trouble ticket's workflow. This listing is populated after the User continues to move through the lifecycle of the defect. Fields displayed data of this tab includes the flow of the *Event*, *Date* of change or input, *Who* activated the event, *Other Information* about the event.
Workaround	This tab contains a description of how to workaround the problem or feature request until a permanent fix can be implemented.
Source Code	Not in use
Email	Optional
Links	Not in use
Folders	Provides access to TTPro folders, a feature to help TTPro users organize their trouble tickets.
History	Displays the trouble ticket's change history

In addition to the fields described in the preceding tables, TestTrack Pro provide a number of dialogue boxes containing fields for documenting notes, dates, and other related information associated with advancing trouble tickets through their lifecycle states. These are discussed elsewhere in this document.

8.3.2.1 Submit a Trouble Ticket using the Web Client

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the **Work with Trouble Tickets** page (Figure 8.3-3). Often this entails simply clicking on the **Trouble Tickets** tab.

2 On the Work with Trouble Tickets page, click **Add** to open the **Add Trouble Ticket** page (Figure 8.3-8 and 8.3-9). **Submitter Site**, **Entered by**, and **Found by (Submitter)** fields are pre-populated with default values.

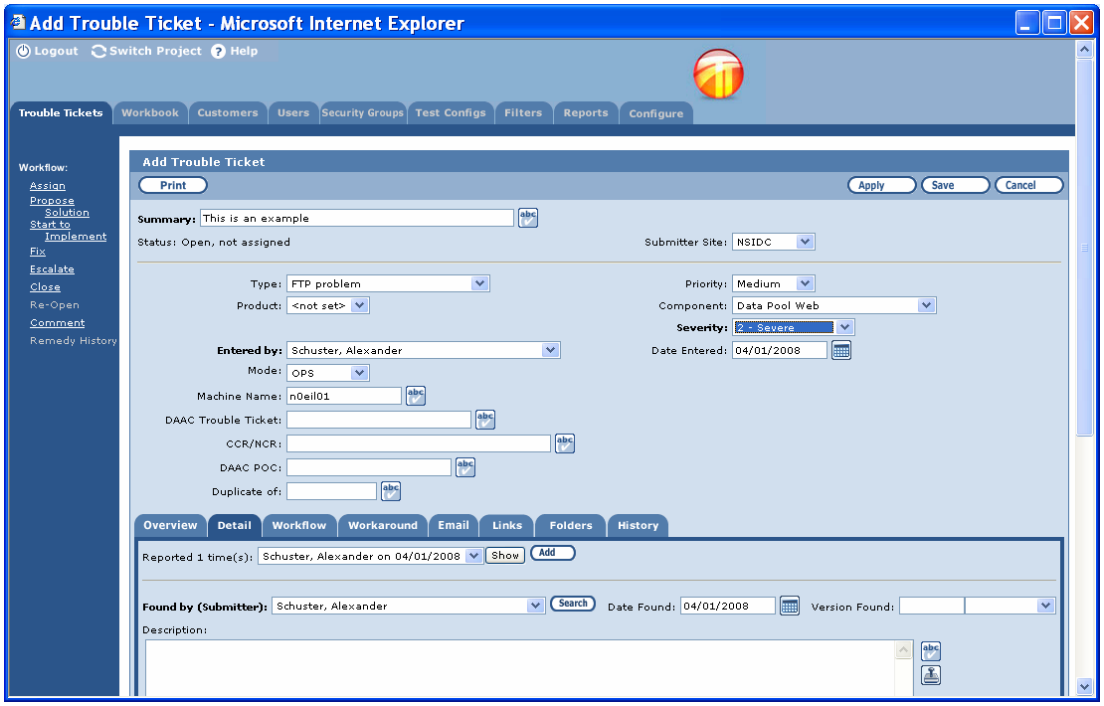


Figure 8.3-8. Add Trouble Ticket Web Page (1 of 2)

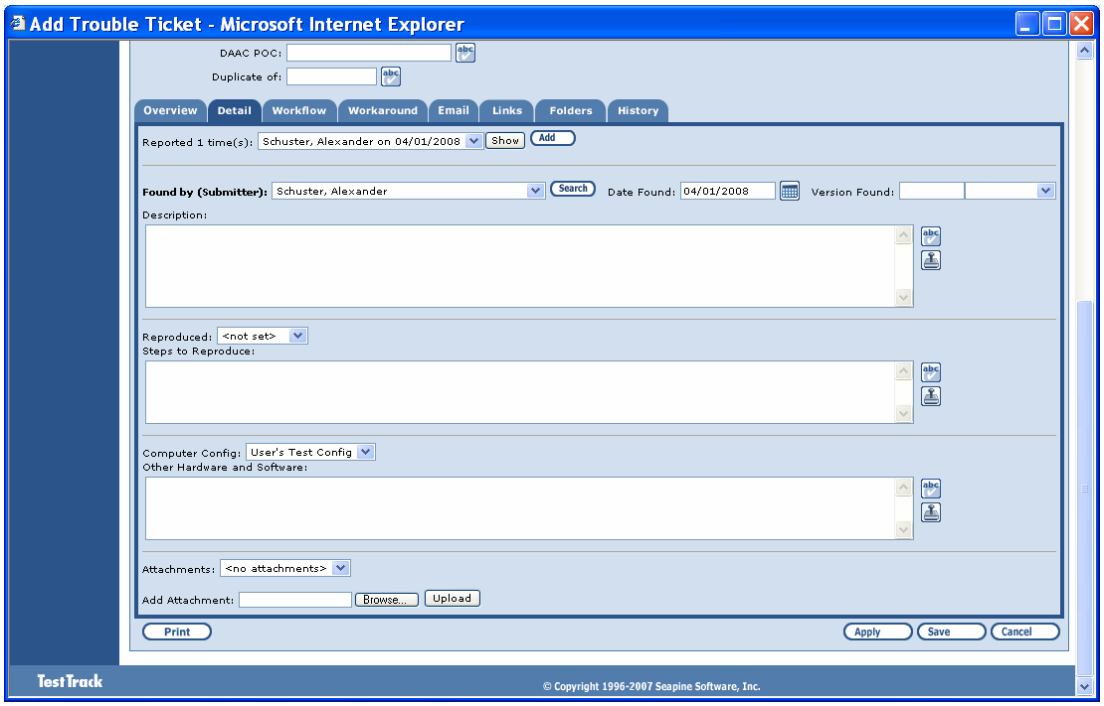


Figure 8.3-9. Add Trouble Ticket Web Page (2 of 2)

3 Enter a concise title for the problem in the **Summary** field.

4 Enter the **Type**, **Priority**, and **Severity** of the problem, choosing values from the fields' picklists.

5 Enter the names of the **Product**, **Component**, **Mode**, and **Machine Affected** by the problem or where the problem occurred, again choosing values from the fields' picklists, where available.

6 If this is a problem documented previously, enter the identifier of the trouble ticket in the **Duplicate of** field.

7 Click on the **Detail** tab to display the fields in which to describe the problem (Figure 8.3-8).

8 Enter the name of the user who found the problem by selecting it from the picklist for the **Found by (Submitter)** field.

9 Enter the date that the problem was detected using the calendar icon next to the **Date Found** field.

10 Describe the problem thoroughly in the **Description** field. Include details sufficient to allow engineers to research, analyze, troubleshoot, or verify the problem adequately,

11 Enter a value in the **Reproduced** field to indicate how readily the problem can be reproduced, then use the **Steps to Reproduce** field to document how.

12 Small, helpful files can be attached to the trouble ticket as follows:

a. Click the Browse button next to the **Add Attachment** field. A file chooser dialog box will appear.

b. Locate and highlight the name of the file, and then click **OK**.

c. Click the **Upload** button to add the file to the trouble ticket.

Note: Attachments must be kept small. Larger files should be placed in the common repository at **XXXXX** instead.

13 Review the trouble ticket for accuracy, then click the **Save** button to submit it. You and others will be notified by e-mail that the trouble ticket has been created.

Note: If, after submitting the ticket, another **Add Trouble Ticket** page appears instead of the **Defect List** page, click the **Cancel** button. Then modify your user options, selecting "Close the Add Trouble Ticket window" option under

Adding multiple trouble tickets..

8.3.2.2 Submit a Trouble Ticket using a GUI Client

1 Login to TTPro (see section 8.3.1.2), choosing your site's trouble ticket project.

2 From the menu bar, select **View → Trouble Tickets…** to navigate to the Trouble Tickets list GUI (Figure 8.3-7).

3 Click **Add…** to open the **Add Trouble Ticket** GUI (Figure 8.3-10, 8.3-11, and 8.3-12). **Submitter Site**, **Entered by**, and **Found by (Submitter)** fields are pre-populated with default values.

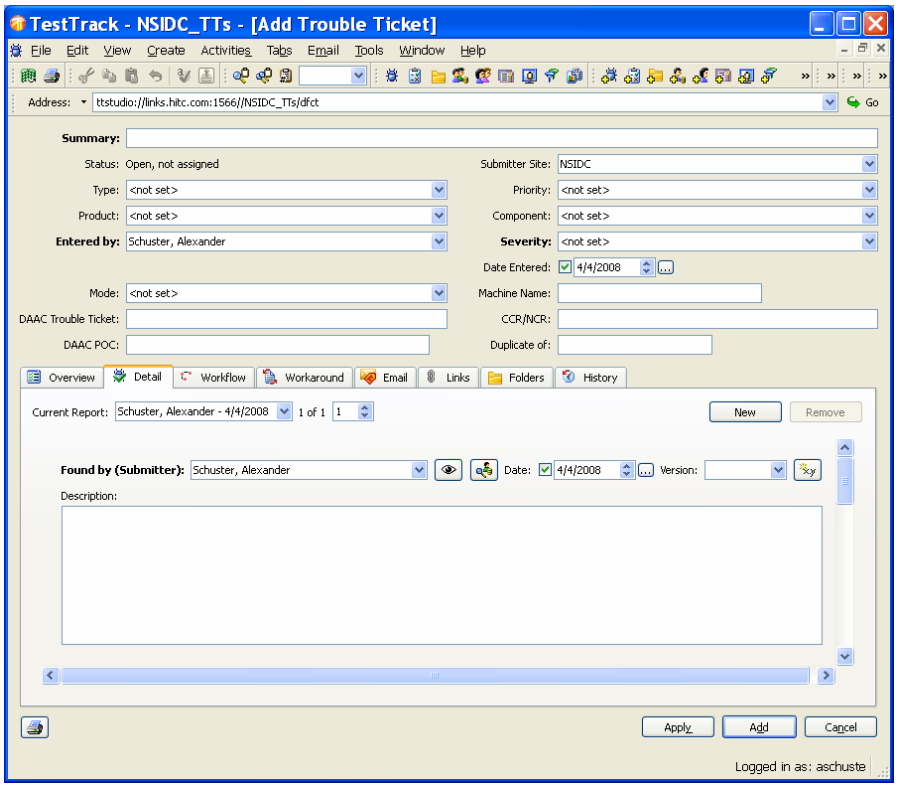


Figure 8.3-10. Add Trouble Ticket GUI (1 of 3)

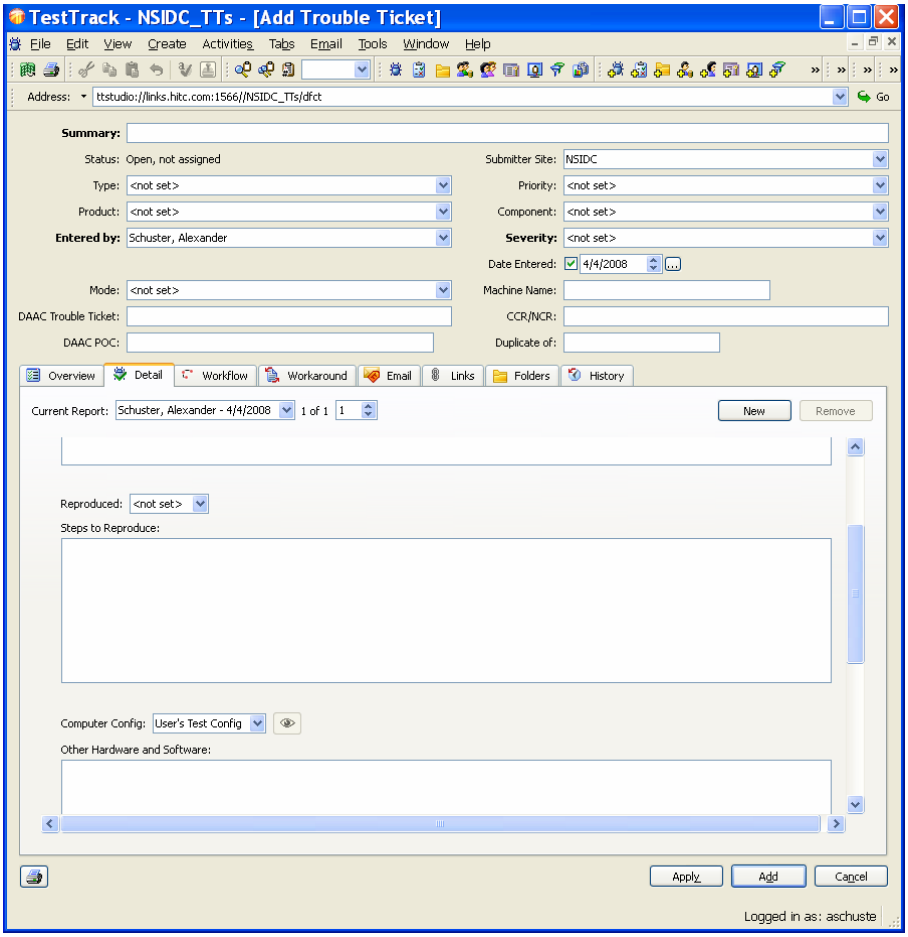


Figure 8.3-11. Add Trouble Ticket GUI (2 of 3)

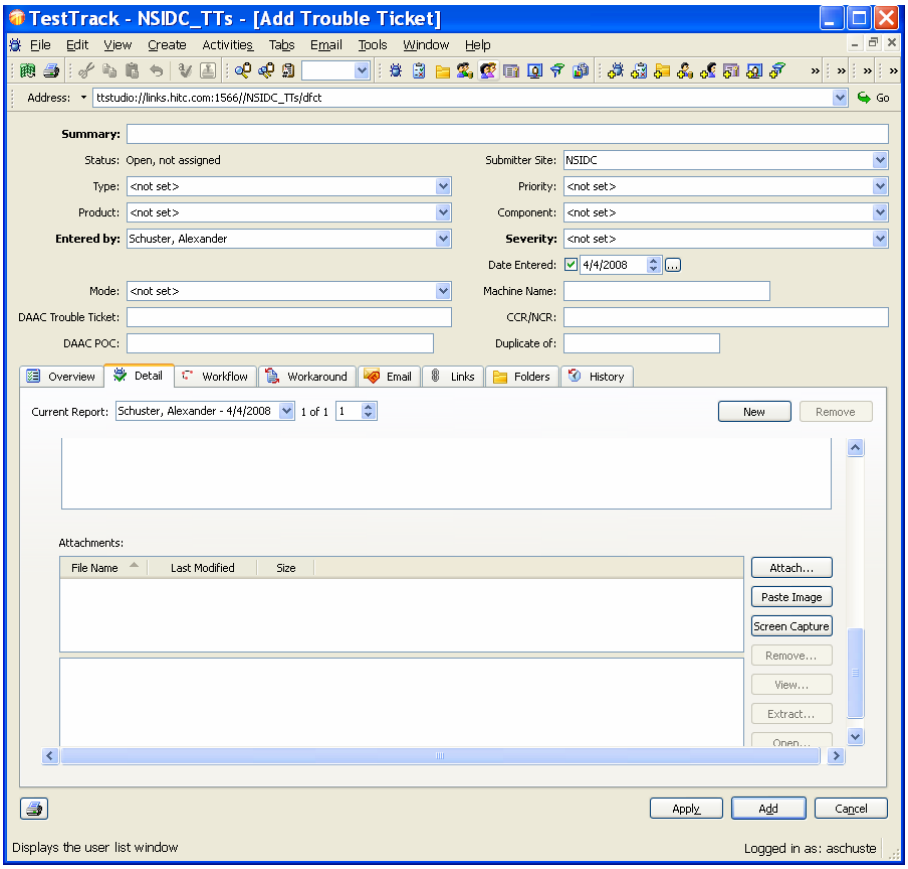


Figure 8.3-12. Add Trouble Ticket GUI (3 of 3)

4 Enter a concise title for the problem in the **Summary** field.

5 Enter the **Type**, **Priority**, and **Severity** of the problem, choosing values from the fields' picklists.

6 Enter the names of the **Product**, **Component**, **Mode**, and **Machine Affected** by the problem or where the problem occurred, again choosing values from the fields' picklists, where available.

7 If this is a problem documented previously, enter the identifier of the trouble ticket in the **Duplicate of** field.

8 Click on the **Detail** tab to display the fields in which to describe the problem (Figure 8.3-11).

9 Enter the name of the user who found the problem by selecting it from the picklist for the **Found by (Submitter)** field.

10 Enter the date that the problem was detected using the calendar icon next to the **Date** field.

11 Describe the problem thoroughly in the **Description** field. Include details sufficient to allow engineers to research, analyze, troubleshoot, or verify the problem adequately.

12 Enter a value in the **Reproduced** field to indicate how readily the problem can be reproduced, then use the **Steps to Reproduce** field to document how.

13 Small, helpful files can be attached to the trouble ticket as follows:

a. Click the Browse button next to the **Attachment** button to the right of the **Attachments** field. The **Attach File** dialog box appears.

b. Locate and highlight the name of the file, and then click **Open**. The name, date of last modification, and size of the file will be added to the **Attachments** field, as well as an icon representing the file.

c. To view an attachment, click on its name or icon and then click the **View…** button.

d. To remove an attachment, click on its name or icon and then click the **Remove…** button.

Note: Attachments must be kept small. Larger files should be placed in the designated common repository, currently `/pub/ecs/hlpdsk/<DAAC>` on host `m0css03.ecs.nasa.gov` instead. Consult your local CM Administrator in case that changes.

14 Review the trouble ticket for accuracy, then click the **Save** button to submit it. You and others will be notified by e-mail that the trouble ticket has been created.

Note: If, after submitting the ticket, another **Add Trouble Ticket** page appears instead of the **Defect List** page, click the **Cancel** button. Then modify your user options, selecting **Close the Add Trouble Ticket window** option under **Adding multiple trouble tickets**.

8.3.3 Search for a Trouble Ticket

A trouble ticket is assigned to one or more users who have access to the site's TTPro project. The same procedure is used to assign and re-assign trouble tickets. Closed trouble tickets cannot be assigned.

8.3.3.1 Search for a Trouble Ticket using the Web Client

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the **Work with Trouble Tickets** page (Figure 8.3-3). Often this entails simply clicking on the **Trouble Tickets** tab.

2 Find the trouble ticket in one of four ways:

a. Select an appropriate record filter from the **Filter** picklist, and then visually scan the list of records returned.

b. If you know the ticket number, type it into the **Go To Trouble Ticket** field in the left pane of the **Work with Trouble Tickets** page (Figure 8.3-3), then click **Go!** TTPro will open the ticket for editing, if it exists.

c. If you know a phrase contained in a text field, click **Find Trouble Tickets** in the left pane of the **Work with Trouble Tickets** page (Figure 8.3-3) to open the **Find Trouble Tickets** page (Figure 8.3-13). Then:

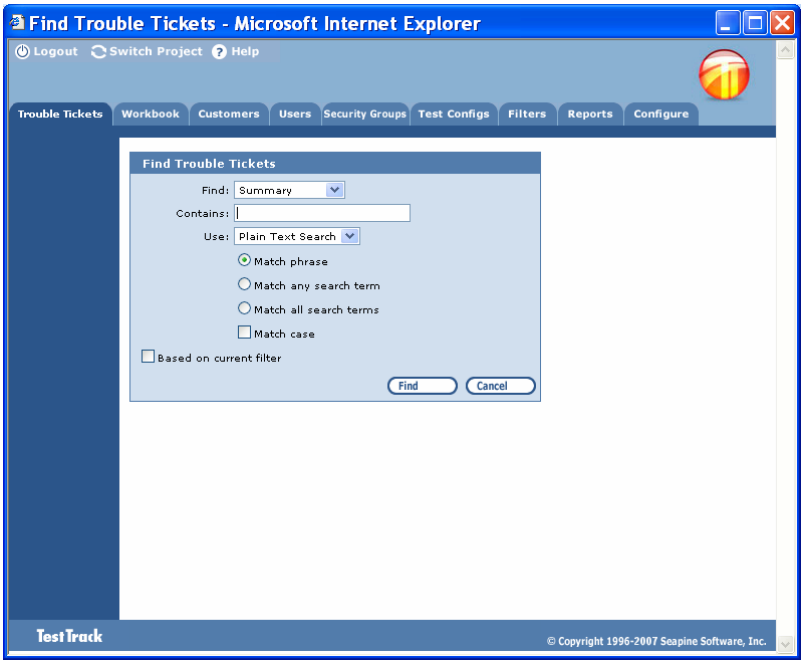


Figure 8.3-13. Find Trouble Tickets Web Page

i. Select the text field to search

ii. Enter a search phrase in the **Contains** field

iii. Choose the phrase matching criteria TTPro is to **Use** when doing the search

iv. Specify whether the search should be limited to trouble tickets accessed **Based on current filter**

v. Click **Find**.

TTPro returns a list of matching tickets.

d. If multiple criteria must be used for the search, click **Advanced Find** in the left pane of the **Work with Trouble Tickets** page (Figure 8.3-14) to open the Advanced Find page. Use the **Insert** and **Add** buttons to define restrictions (i.e., conditions that selected tickets must satisfy). Next, use the **NOT**, **left parens**, **right parens**, and **And/Or** fields to negate, logically relate, and nest restrictions. Click **Find** to start the search.

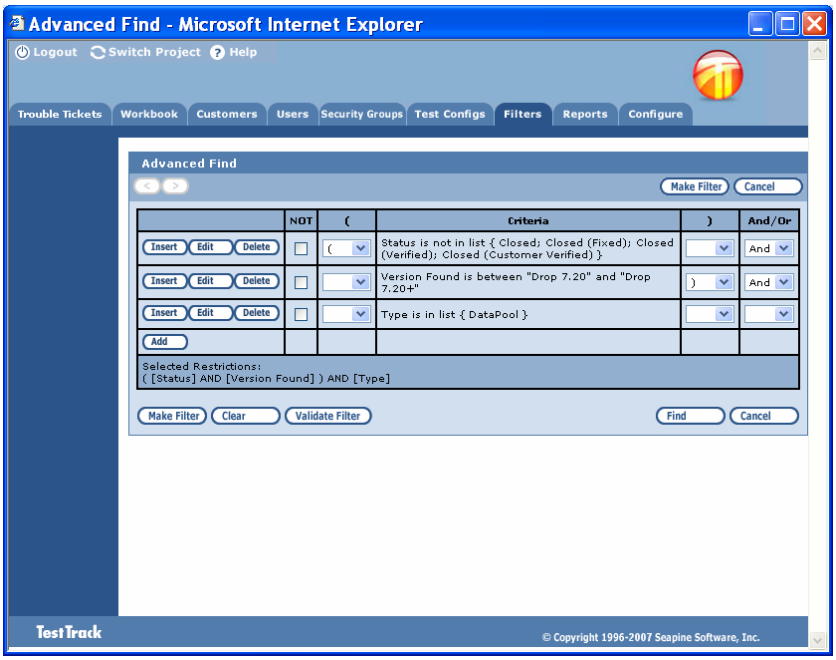


Figure 8.3-14. Advanced Find Web Page

8.3.3.2 Search for a Trouble Ticket using a GUI Client

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 Find the trouble ticket in one of four ways:

a. Select an appropriate record filter from the **Filter** picklist, and then visually scan the list of records returned.

b. If you know the ticket number, on the menu bar click **Edit → Find…** to open the Go To Trouble Ticket dialog box (Figure 8.3-15), type the number into the **Go To Trouble Ticket** field, then click **OK** TTPro will open the ticket for editing, if it exists.

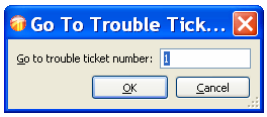


Figure 8.3-15. Find Trouble Ticket GUI

c. If you know a phrase contained in a text field, on the menu bar click **Find…** to open the Find Trouble Ticket dialog box (Figure 8.3-16). Then:

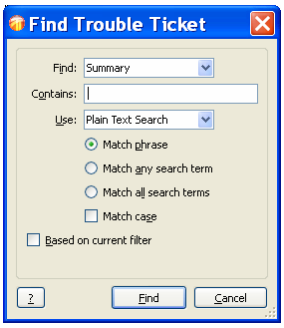


Figure 8.3-16. Find Trouble Ticket GUI

i. Select the text field to search

ii. Enter a search phrase in the **Contains** field

iii. Choose the phrase matching criteria TTPro is to **Use** when doing the search

iv. Specify whether the search should be limited to trouble tickets accessed **Based on current filter**

v. Click **Find**.

TTPro returns a list of matching tickets.

d. If multiple criteria must be used for the search, on the menu bar click **Advanced Find…** to open the Advanced Find dialog box (Figure 8.3-17). Use the **Insert** and **Add** buttons to define restrictions (i.e., conditions that selected tickets must satisfy). Next, use the **NOT**, **left parens**, **right parens**, and **And/Or** fields to negate, logically relate, and nest restrictions. Click **Find** to start the search.

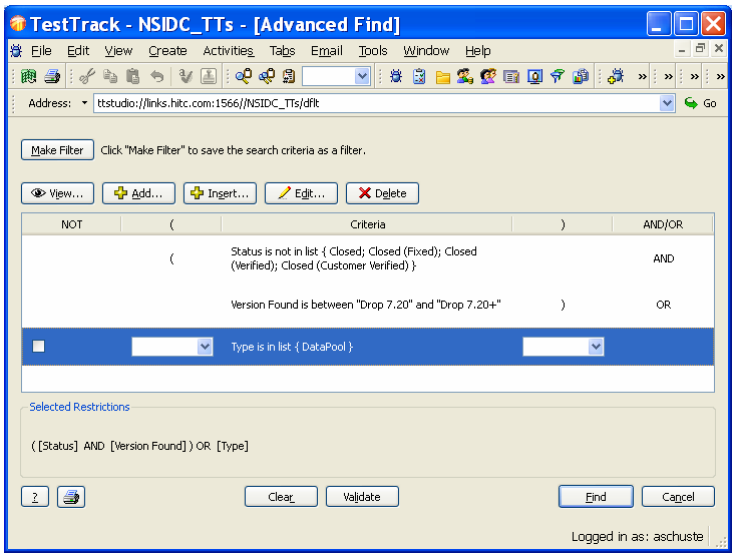


Figure 8.3-17. Advanced Find GUI

8.3.4 Assign Trouble Ticket

A trouble ticket can be assigned to one or more users who have access to the TTPro project in which the ticket was created. The same procedure used for assigning a trouble ticket is used to re-assign it. Closed trouble tickets cannot be assigned.

TTPro emails system notifications automatically to alert assignees whenever a trouble ticket has been assigned to them.

Assigning a trouble ticket does not change its lifecycle state.

8.3.4.1 Assign a Trouble Ticket using the Web Client

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the **Work with Trouble Tickets** page (Figure 8.3-3). Often this entails simply clicking on the **Trouble Tickets** tab.

2 On the **Work with Trouble Tickets** page, search for the trouble ticket (see Section 8.3.3).

3 Click the ticket's checkbox, and then click the **Edit** button atop the list of trouble tickets. This opens the **Edit Trouble Ticket** page.

4 Click **Assign** in the left pane of the **Edit Trouble Ticket** page (Figure 8.3-18). This opens the **Assign** page. The **Assign by** and **Date** fields are pre-populated.

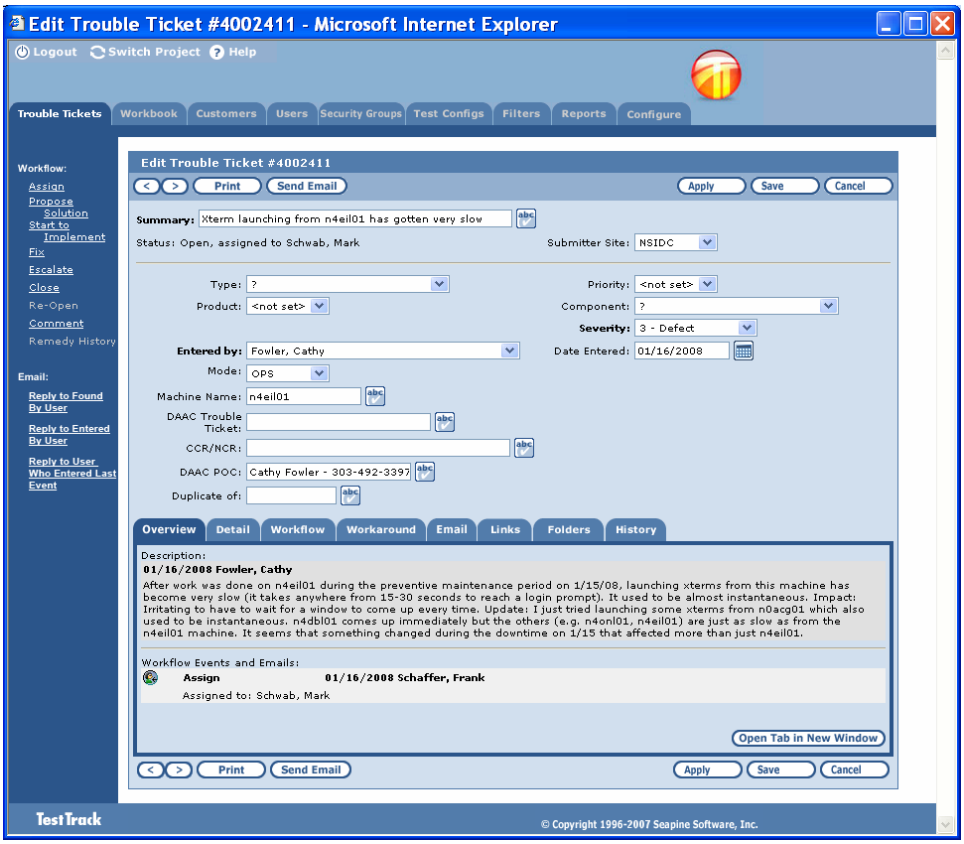


Figure 8.3-18. Edit Trouble Ticket Web Page

5 On the **Assign Web** Page (Figure 8.3-19), click the down arrow next to the **Assign to** field to display its pull-down menu.

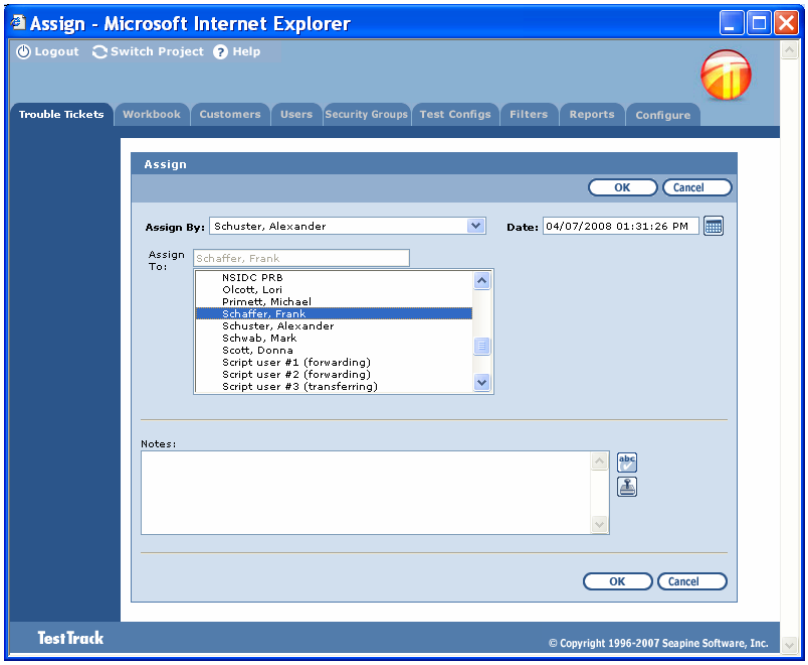


Figure 8.3-19. Assign Web Page

6 Select the names of one or more users from the **Assign to** field's pull-down list, then click **OK**. The **Assign** dialog box closes.

Note: Use the <CTRL> key with your mouse click in order to select multiple names individually. Use the <SHIFT> key to select a series of names.

7 Click **Save** to store the changes and close the **Edit Trouble Ticket** page.

8.3.4.2 Assign a Trouble Ticket using a GUI Client

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 On the Trouble Tickets list GUI, search for the trouble ticket (see Section 8.3.3).

3 Highlight the appropriate trouble ticket, and then click **Edit** to open it.

4 On the menu bar, click **Activities → Assign…** . This opens the Assign dialog box. The **Assign by** and **Date** fields are pre-populated.

5 Click the down arrow next to the **Assign to** field in the **Assign** dialog box (Figure 8.3-20) to display its pull-down menu.

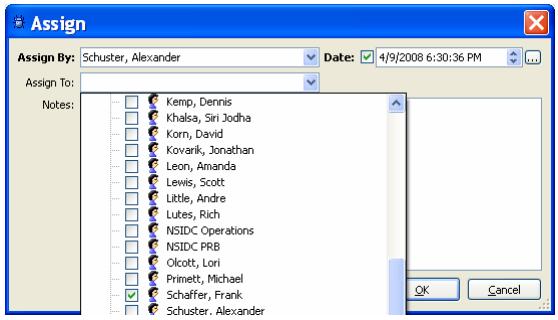


Figure 8.3-20. Assign GUI

6 Select the names of one or more users, and then click **OK**. The **Assign** dialog box closes.

Note: Use the <CTRL> key with your mouse click in order to select multiple names individually. Use the <SHIFT> key In order to select a series of names.

7 Click **OK** to save the changes and close the **Edit Trouble Ticket** GUI.

8.3.5 Update an Open Trouble Ticket

Trouble tickets need updating periodically to clarify or supplement problem statements and to document progress towards resolution, results of analyses, and decisions of the Problem Review Board and Change Control Board.

Note: The procedure for advancing a trouble ticket to a new lifecycle state is covered in Section 8.3.xxx.

8.3.5.1 Update an Open Trouble Ticket using the Web Client

---

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the **Work with Trouble Tickets** page (Figure 8.3-3). Often this entails simply clicking on the **Trouble Tickets** tab.

2 On the **Work with Trouble Tickets** page, search for the trouble ticket (see Section 8.3.3).

3 Open the **Edit Trouble Ticket** page for the desired trouble ticket by clicking the **checkbox** for the trouble ticket and then the **Edit** button atop the list of trouble tickets.

4 Add or modify data, visiting the ticket's **Detail** and **Workaround** tabs as necessary to expose their fields.

Note: When adding information to one the trouble ticket's multi-line text fields, it is often useful to insert a "stamp". A stamp is a pre-defined text string identifying the current date and time. To insert a stamp, click the **Stamp** icon at the right of the field. (Consult your TTPro administrator if stamps are not enabled for your project.)

5 To add another occurrence of the same problem to the trouble ticket:

a. Click the **Detail** tab

b. Click the **Add** button. TTPro creates a new Reported by record and increments the **Reported *n* times** counter by 1. Use the **Reported *n* times** picklist to choose which of the records to view.

c. Add relevant information in the **Found by (Submitter)**, **Date**, **Description**, **Reproduced**, and **Steps to Reproduce** fields.

d. Click **Save**.

6 To advance the trouble ticket to a different lifecycle state or to modify data associated with workflow, use the procedures in Section 8.3.4.

7 Click **Apply** to store the changes and continue editing the trouble ticket, or click **Save** to store the changes and close the **Edit Trouble Ticket** page.

8.3.5.2 Update an Open Trouble Ticket using a GUI Client

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 On the Trouble Tickets list GUI, search for the trouble ticket (see Section 8.3.3).

3 Highlight the appropriate trouble ticket, and then click **Edit** to open it.

4 Add or modify data, visiting the ticket's **Detail** and **Workaround** tabs as necessary to expose their fields.

Note: When adding information to one the trouble ticket's multi-line text fields, it is often useful to insert a "stamp". A stamp is a pre-defined text string identifying the current date and time. To insert a stamp, select **EDIT → Stamp…** from the menu bar. (Consult your TTPro administrator if stamps are not enabled for your project.)

5 To add another occurrence of the same problem to the trouble ticket:

a. Click the **Detail** tab

b. Click the **New** button. TTPro creates a new **Reported by** record and increments the **Current Report** counter by 1. Use the arrow keys next to the **Current Report** field to choose which of the records to view.

c. Add relevant information in the **Found by (Submitter)**, **Date**, **Description**, **Reproduced**, and **Steps to Reproduce** fields.

6 To advance the trouble ticket to a different lifecycle state or to modify data associated with workflow, use the procedures in Section 8.3.4:

7 Click **Apply** to store the changes and continue editing the trouble ticket, or click **OK** to save the changes and close the **Edit Trouble Ticket** GUI.

8.3.6 Change a Trouble Ticket's Lifecycle State

Trouble tickets have a lifecycle, the stages of which are called states. Newly submitted tickets start in the Open state and, when work on them is completed, end up in the Closed state. Although a nominal lifecycle consists of the Open, Solution Implemented, and Closed states, additional lifecycle states exist. A trouble ticket need not advance through all the states or through the states in a particular sequence.

A trouble ticket changes state when a user records certain workflow events. Table 8.3-5 lists the possible workflow events and the lifecycle state and other changes each triggers. Typically, access to the Escalate and Close events is restricted to certain site personnel.

Table 8.3-5. Workflow Events and Corresponding Lifecycle States

Event	Description	Resulting State	Data That Can Be Added to Defect	Assignment Change
Assign	Assign ticket to one or more team members	No Change	Assigned to	New
Propose Solution	Identify fix	Solution Proposed	Due date; Version; Effort to fix	None
Escalate	Elevate ticket to PRB or ECHO for advice or resolution	Forwarded	Requested Category	None
ON HOLD	Work put on hold regarding fix	ON HOLD	None	None
Fix	Move trouble ticket to fixed state and capture resolution	Fixed	Effort, Affects Documentation, Affects Test Plan, Resolution, Version	None
Close	Move ticket into Closed state	Closed	Resolution	Clears
Re-Open	Re-open currently closed Trouble Ticket	Open (Re-Opened)	None	New
Comment	Add a comment to a Trouble Ticket	No change	Comment	None

TTPro emails system notifications automatically to alert designated team members whenever a trouble ticket's state changes.

8.3.6.1 Change a Trouble Ticket's Lifecycle State using the Web Client

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the **Work with Trouble Tickets** page (Figure 8.3-3). Often this entails simply clicking on the Trouble Tickets tab.

2 On the **Work with Trouble Tickets** page, search for the trouble ticket (see Section 8.3.3).

3 Open the Edit Trouble Ticket page for the desired trouble ticket by clicking the **checkbox** for the trouble ticket and then the **Edit** button atop the list of trouble tickets.

4 Click the desired workflow event from the list of those available under **Workflow:** in the left pane of the **Edit Trouble Ticket** page. The event's dialog page opens.

5 Record details in the fields provided (Figure 8.3-21), particularly the fields having labels in boldface as these require an entry.

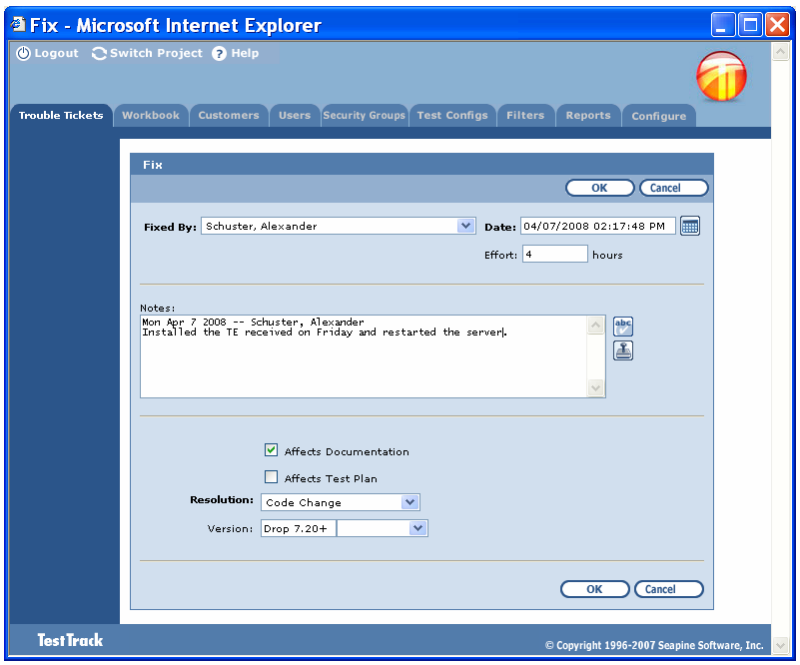


Figure 8.3-21. Fix Event's Web Page

6 Click **OK** to save your changes. The event's dialog page closes and returns you to the **Edit Trouble Ticket** page.

7 Click **Save** on the **Edit Trouble Ticket** page. The page closes and the **Trouble Tickets list** page is displayed.

8.3.6.2 Change a Trouble Ticket's Lifecycle State using a GUI Client

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 On the **Trouble Tickets list** GUI, search for the trouble ticket (see Section 8.3.3)

3 Highlight the appropriate trouble ticket, and then click **Edit** to open it.

4 On the menu bar, click **Activities**, and then click on the desired workflow event. The event's dialog box opens. Figure 8.3-22 is an example.

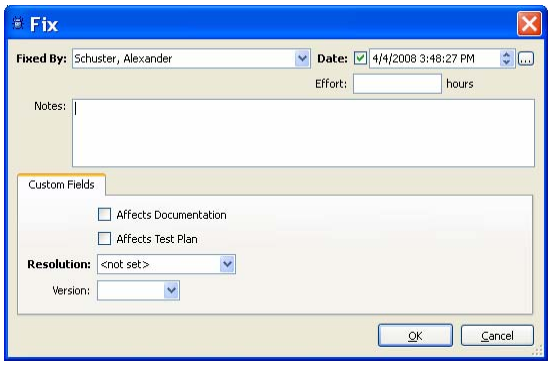


Figure 8.3-22. Fix Events GUI

5 Record details in the fields provided, particularly the fields having labels in boldface as these require an entry.

6 Click **OK** to save your changes. The event's dialog box closes and TTPro returns you to the Edit Trouble Ticket GUI.

7 Click **OK** on the **Edit Trouble Ticket** GUI. The GUI closes and returns you to the **Trouble Tickets list** GUI.

8.3.7 Escalate a Trouble Ticket

Sites escalate trouble tickets when system-level advice or baseline changes are required. Escalated tickets are forwarded to the specified system-level project, and selected individuals are notified. The new ticket's number is placed in the original trouble ticket's **DAAC Trouble Ticket** field.

8.3.7.1 Escalate a Trouble Ticket using the Web Client

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the Work with Trouble Tickets page (Figure 8.3-3). Often this entails simply clicking on the **Trouble Tickets** tab.

2 On the **Work with Trouble Tickets** page, search for the trouble ticket (see Section 8.3.3).

3 Open the **Edit Trouble Ticket** page for the desired trouble ticket by clicking the **checkbox** for the trouble ticket and then the **Edit** button atop the list of trouble tickets.

4 Click **Escalate…** from the list of events available under **Workflow:** in the left pane of the Edit Trouble Ticket page. The event's dialog page opens with the Escalate by and Date fields pre-populated.

5 On the **Escalate** page (Figure 8.3-23):

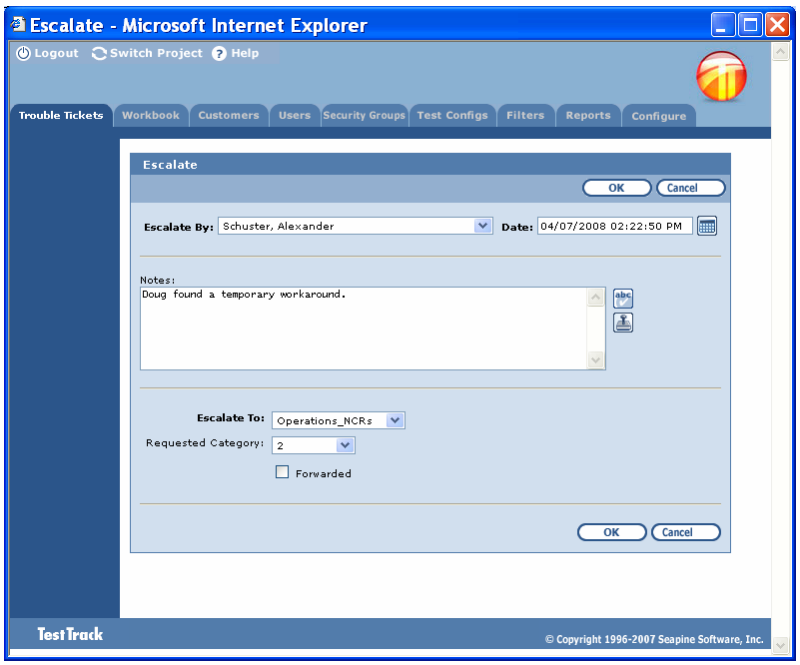


Figure 8.3-23. Escalate Page

a. Add to the **Notes** field any pertinent details not already included in the trouble ticket.

b. In the **Escalate to** field, choose the project to which the trouble ticket is to be forwarded: : This field requires an entry.

- Select **ECHO_TTs** if the problem is related to ECHO

- Select **Operations_NCRs** if the problem is related to ECS.

c. Update the **Requested Category** field with a value from its picklist, if desired. Categories reflect how urgently a solution is needed.

d. Do NOT update the **Forwarded** field. (It should be greyed out.) This field is set by automated tools to indicate that a trouble ticket has been forwarded successfully.

e. Click **OK** to save your changes. The **Escalate** page closes and the **Edit Trouble Ticket** page displays.

6 Enter the name and/or phone number of a point-of-contact in the trouble ticket's **DAAC POC** field.

7 Click **Save** on the **Edit Trouble Ticket** page. The page closes, and TTPro updates the database and displays the Trouble Tickets list page.

8.3.7.2 Escalate a Trouble Ticket using a GUI Client

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 On the Trouble Tickets list GUI, search for the trouble ticket (see Section 8.3.3)

3 Highlight the appropriate trouble ticket, and then click **Edit** to open it.

4 On the menu bar, click **Activities → Escalate…**. The event's dialog box opens with the Escalate by and Date fields pre-populated.

5 On the **Escalate** GUI (Figure 8.3-24),

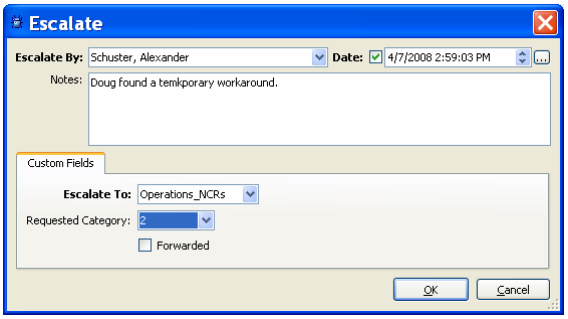


Figure 8.3-24. Escalate GUI

a. Add to the **Notes** field any pertinent details not already included in the trouble ticket.

b. In the **Escalate to** field, choose the project to which the trouble ticket is to be forwarded: This field requires an entry.

- Select **ECHO_TTs** if the problem is related to ECHO.
- Select **Operations_NCRs** if the problem is related to ECS.

c. Update the **Requested Category** field with a value from its picklist, if desired. Categories reflect how urgently a solution is needed.

d. Do NOT update the **Forwarded** field. (It should appear greyed out.) This field is set by automated tools to indicate that a trouble ticket has been forwarded successfully.

e. Click **OK** to save your changes. The event's dialog box closes, and TTPro returns you to the **Edit Trouble Ticket** GUI.

6 Enter the name and/or phone number of a point-of-contact in the trouble ticket's **DAAC POC** field.

7 Click **OK** on the **Edit Trouble Ticket** GUI. The GUI closes, and TTPro updates the database and returns you to the Trouble Tickets list GUI.

8.3.8 Open an NCR

When the EMD PRB determines that a system-level trouble ticket should be made an NCR, a member of the DAAC Help Desk advances the ticket from the Pending PRB Review state to the Open state in the Operations NCRs project.

8.3.8.1 Open an NCR using the Web Client

---

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page of the Operations_NCR project. If already logged in, navigate to the Work with NCRs page (Figure 8.3-3). Often this entails simply clicking on the NCRs tab.

2 On the **Work with NCRs** page (Figure 8.3-3), search for the ticket -- it would be in the Pending PRB (review) state. Click the **checkbox** for the NCR then the **Edit** button atop the list of trouble tickets to open the **Edit NCR** page.

Note: Your web page may have different columns that what is shown in Figure 8.3-25.

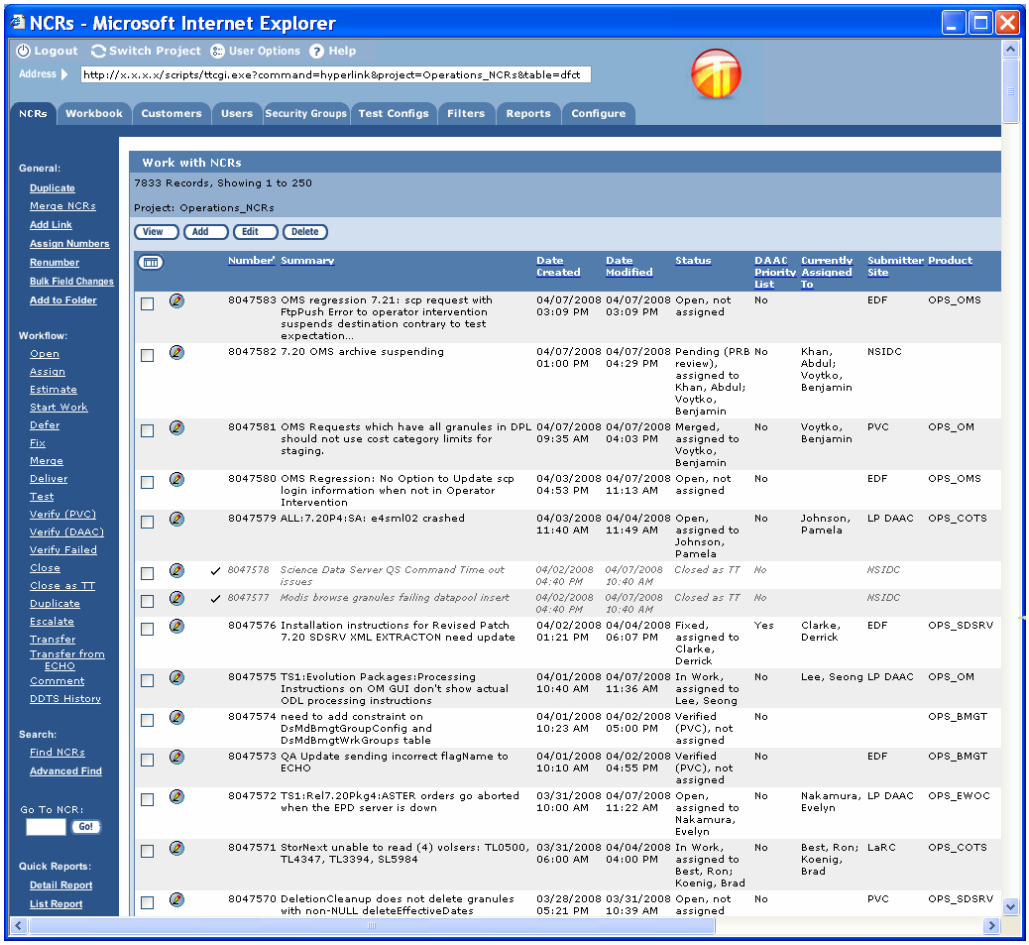


Figure 8.3-25. Work with NCRs Web Page

3 Click **Open…** from the list of events available under **Workflow:** in the left pane of the **Edit NCR** page (Figure 8.3-26). The event's dialog page opens with the **Open by** and **Date** fields pre-populated.

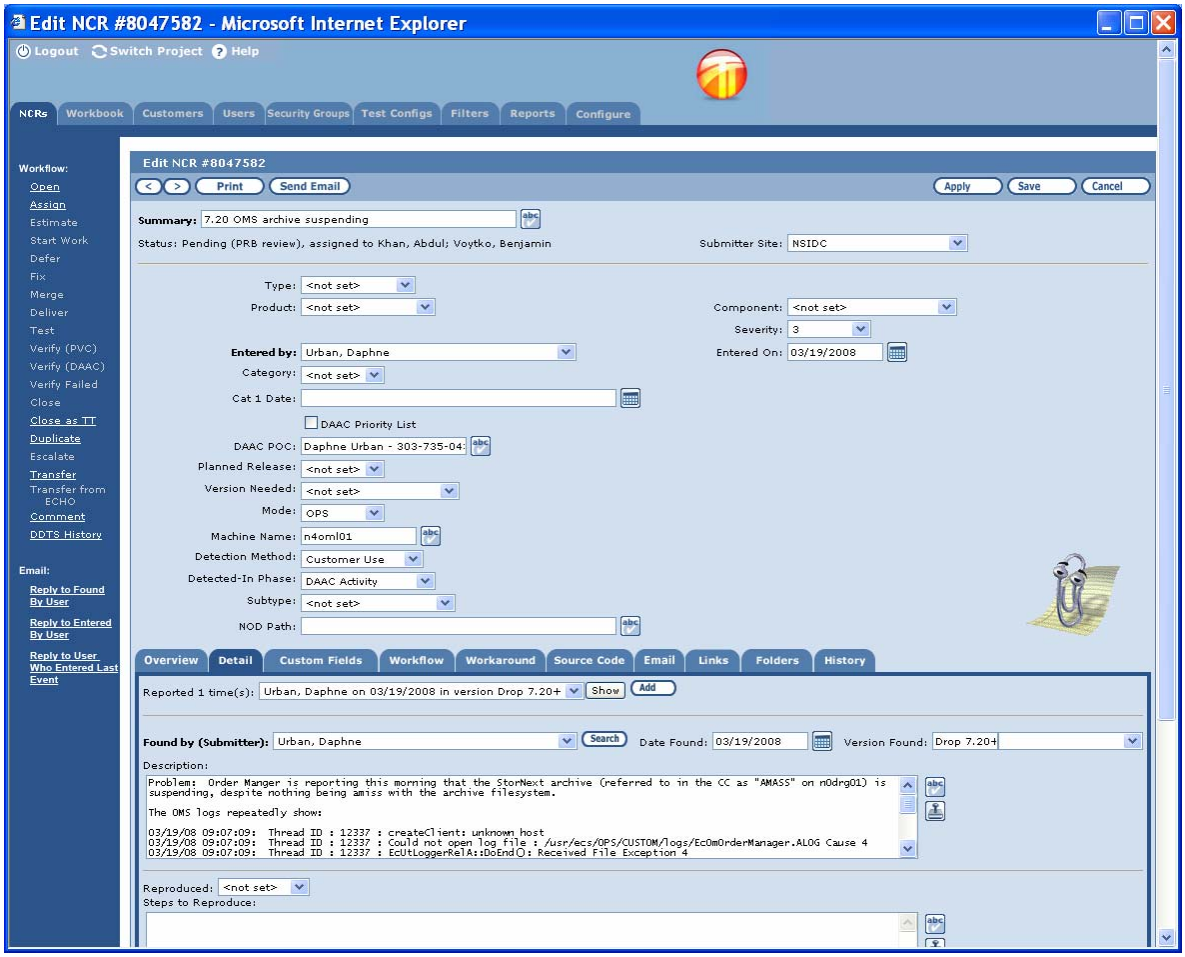


Figure 8.3-26. Edit NCR Web Page

4 On the **Open web** page (Figure 8.3-27):

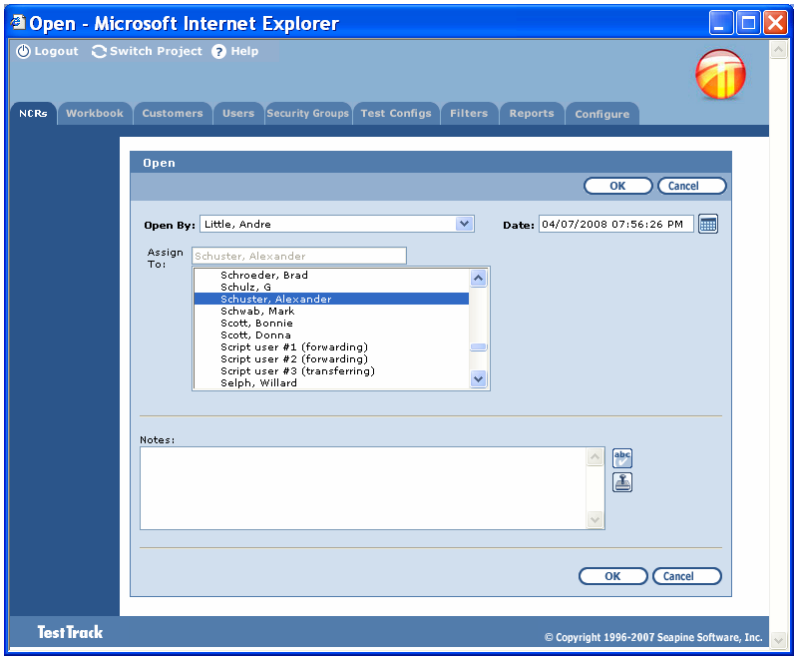


Figure 8.3-27. Open Web Page

a. Assign the NCR to one (or more) engineers by clicking the down arrow next to the **Assign to** field and selecting one (or more) users.

b. Add to the **Notes** field any pertinent details not included in the trouble ticket.

c. Click **OK** to save your changes. The **Open** page closes and the **Edit NCR** page returns.

5 On the **Edit NCR** page:

a. Fill in appropriate values in the NCR's **Product**, **Component**, **Severity**, and **Category** fields.

b. Click **Save**. The page closes, and TTPro updates the database and returns to the **NCRs list** page.

8.3.8.2 Open an NCR using a GUI Client

---

1 Login to TTPro (see section 8.3.1.1), choosing the Operations_NCRs project.

2 On the Operations_NCRs GUI (Figure 8.3-28), search for the ticket. It would be in the Pending PRB (review) state. Highlight it, and then click **Edit** to open it. The **Edit NCRs** GUI appears.

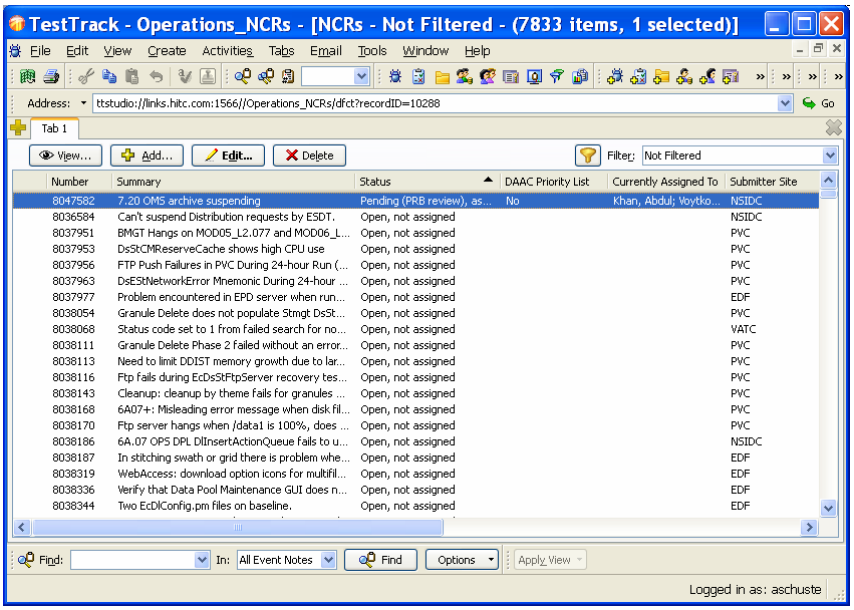


Figure 8.3-28. Operations_NCRs GUI

3 On the menu bar for the Edit NCR GUI (Figure 8.3-29), click **Activities → Open…**. The event's dialog box opens with the **Open by** and **Date** fields pre-populated.

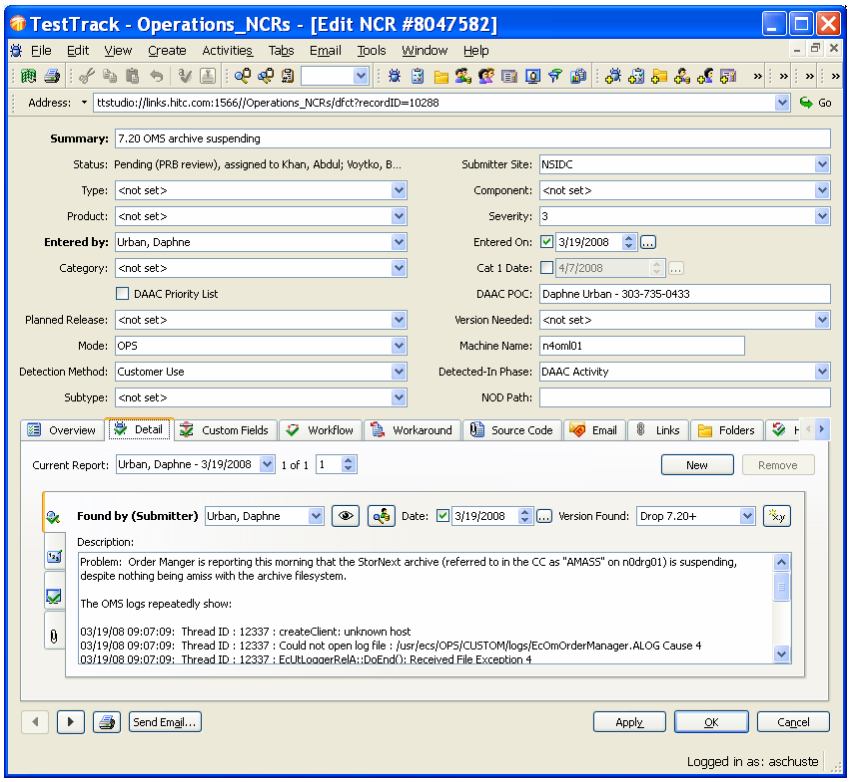


Figure 8.3-29. Edit NCRs GUI

4 On the Open GUI (Figure 8.3-30):

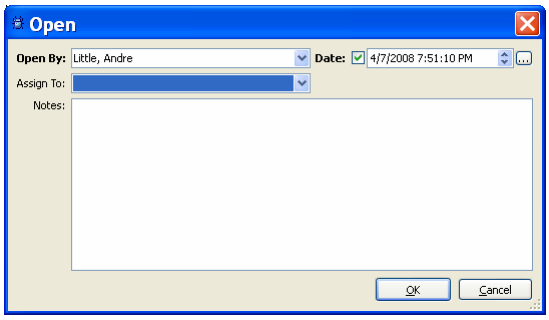


Figure 8.3-30. Open GUI

a. Assign the NCR to one (or more) engineers by clicking the down arrow next to the **Assign to** field and selecting one (or more) users.

b. Add to the **Notes** field any pertinent details not included in the trouble ticket.

c. Click **OK** to save your changes. The event's dialog box closes, and TTPro returns you to the **Edit NCR** GUI.

5 On the **Edit NCR** GUI:

a. Fill in appropriate values in the NCR's **Product**, **Component**, **Severity**, and **Category** fields.

b. Click **OK**. The GUI closes, and TTPro updates the database and returns you to the **NCRs list** GUI.

8.3.9 Close a Trouble Ticket

Trouble tickets can be closed for a variety of reasons, such as when the problem has been resolved and verified, a solution is no longer needed, or the issue can not be duplicated. Closing a trouble ticket clears all assignments and renders the ticket read-only for all but the site's TTPro administrators. Selected staff are notified whenever a trouble ticket is closed.

8.3.9.1 Close a Trouble Ticket using the Web Client

---

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the **Work with Trouble Tickets** page (Figure 8.3-3). Often this entails simply clicking on the Trouble Tickets tab.

2 On the Work with Trouble Tickets page, search for the trouble ticket (see Section 8.3.3).

3 Open the **Edit Trouble Ticket** page for the desired trouble ticket by clicking the **checkbox** for the trouble ticket and then the **Edit** button atop the list of trouble tickets.

4 Click **Close…** from the list of events available under **Workflow:** in the left pane of the **Edit Trouble Ticket** page. The event's dialog page (Figure 8.3-31) opens with the **Close by** and **Date** fields pre-populated.

5 On the **Close** page:

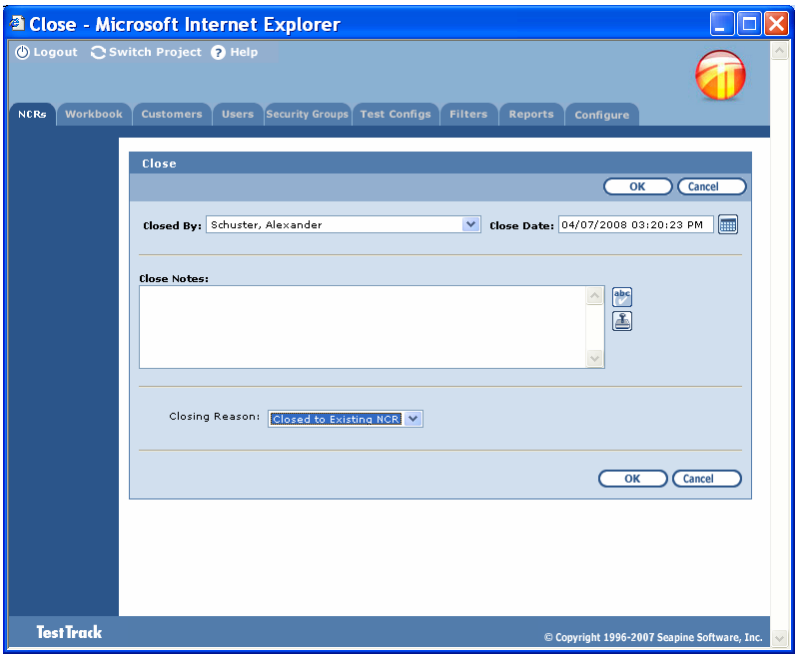


Figure 8.3-31. Close Page

a. Add to the **Notes** field any pertinent details not already included in the trouble ticket.

b. Update the **Resolution** field with a value from its picklist.

c. Click **OK** to save your changes. The event's dialog page closes and returns you to the **Edit Trouble Ticket** page.

6 Click **Save** on the **Edit Trouble Ticket** page. The page closes and the **Trouble Tickets list** page is displayed.

8.3.9.2 Close a Trouble Ticket using a GUI Client

---

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 On the **Trouble Tickets** list GUI, search for the trouble ticket (see Section 8.3.3)

3 Highlight the appropriate trouble ticket, and then click **Edit** to open it.

4 On the menu bar, click **Activities → Close…**. The event's dialog box (Figure 8.3-32) opens with the Close by and Date fields pre-populated.

5 On the Close GUI:

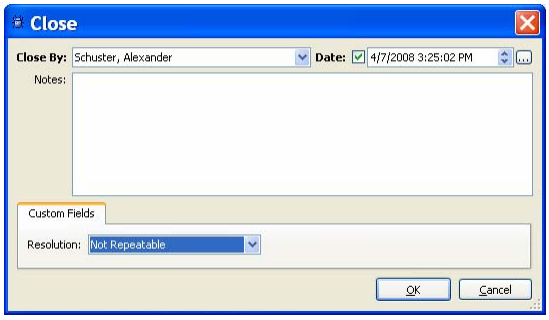


Figure 8.3-32. Close GUI

a. Add to the **Notes** field any pertinent details not already included in the trouble ticket.

b. Update the **Resolution** field with a value from its picklist.

c. Click **OK** to save your changes. The event's dialog box closes, and TTPro returns you to the Edit Trouble Ticket GUI.

6 Click **OK** on the Edit Trouble Ticket GUI. The GUI closes, and TTPro updates the database and returns you to the Trouble Tickets list GUI.

8.3.10 Add a New User to the Global User Database

Every TTPro user must have a user profile defined for them in the Seapine License Server's global user database at the EDF. User profiles contain the user's name, username (i.e., login id), e-mail address, phone number, site id, type of product license used, and license server access privileges. Other information can be recorded as well. These profiles are created by system-level TTPro Administrators upon request by the local CM Administrators using the License Server Admin utility, a tool that can be started only from the TTPro server machine.

8.3.10.1 Add a New User to the Global User Database Using the GUI Client

---

1 Local CM Administrator notifies the system-level TTPro Administrator via email that a new user requires access and provides the following information:

- Full name – first name and last name; middle initial is optional. No two TTPro users can have the same full names.
- Username –the preferred character string that the user will enter as their logon id. No two TTPro users can have the same Username.
- E-mail address – address to which system and personal trouble ticket notifications will be sent.

- Phone Number – number at which the individual can best be reached.
- Type of license needed (floating or named) – **Floating Licenses** are available on a first-come, first-served basis to any user having an active, registered login id in TTPro. Whenever all the licenses in this pool are in use, new login requests will be denied. **Named Licenses** are assigned to individual users and are always available for those users. Named licenses are assigned to those who need frequent, prolonged or unencumbered access to TTPro. The number of licenses -- both floating and named -- are limited.
- Level of license server access required – most users need no access to the license server. Others such as the local CM Administrators, however, need to be able to retrieve user profiles in order to add users to their projects. See Section xxx for more details.

2 System-level TTPro Administrator logs onto the TTPro License Server host and, as a privileged user, launches the License Server Utility from the command line as follows:

```
# /usr/ecs/OPS/COTS/ttpro/splicsvr/bin/lsadmin &
```

3 On the License Server Admin Utility GUI (Figure 8.3-33), click the **Global Users** button to access the list of global user profiles.

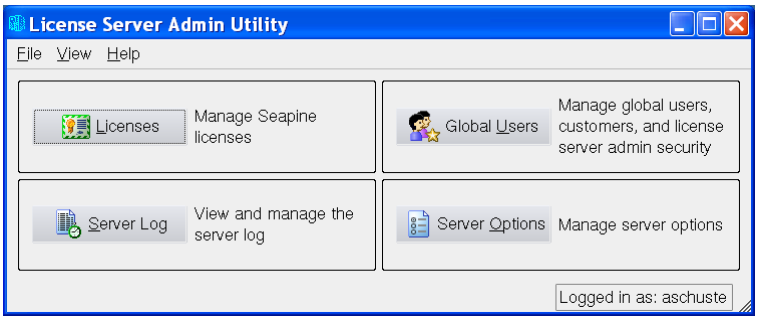


Figure 8.3-33. License Server Admin Utility GUI

4 Click **Add** on the **Global Users** GUI (Figure 8.3-34).

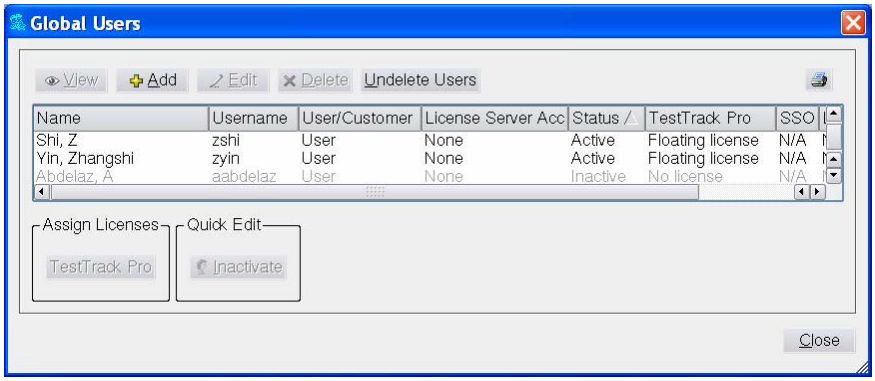


Figure 8.3-34. Global Users GUI

5 On the **Add User** GUI (Figure 8.3-35):

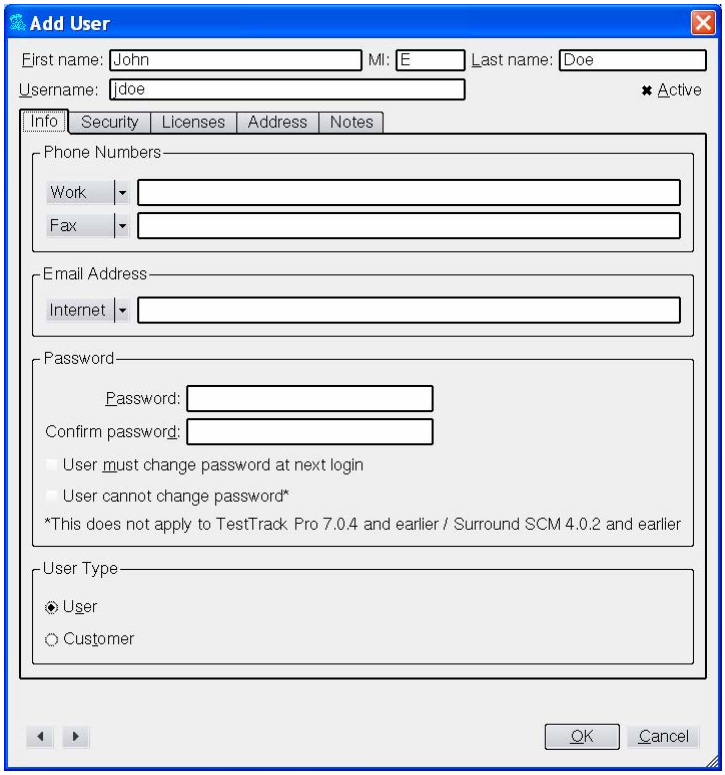


Figure 8.3-35. Add User GUI

a. Fill in the **First name**, **MI**, **Last name**, and **Username** fields.

b. Ensure that the **Active** checkbox is set. Inactive users cannot access TTPro or receive notifications; they exist to preserve the names of former users in trouble tickets that reference them.

6 On the **Info** tab:

a. Fill in the user's **Work** telephone number and **Internet** email address.

b. Click the **User must change password at next login** checkbox so that TTPro prompts the user to enter a new password the next time they log in.

c. Ensure that the **User** checkbox is set. Customers cannot logon to TTPro.

7 If the new user needs to be able to add user profiles to a trouble ticket project, click the **Security** tab (Figure 8.3-35), and then click the **User can retrieve global users, but cannot login to the license server admin utility** radio button (Figure 8.3-36).

Note: The default license server privilege, **Users cannot login to the license server admin utility**, precludes license server access and is appropriate for almost all TTPro users.

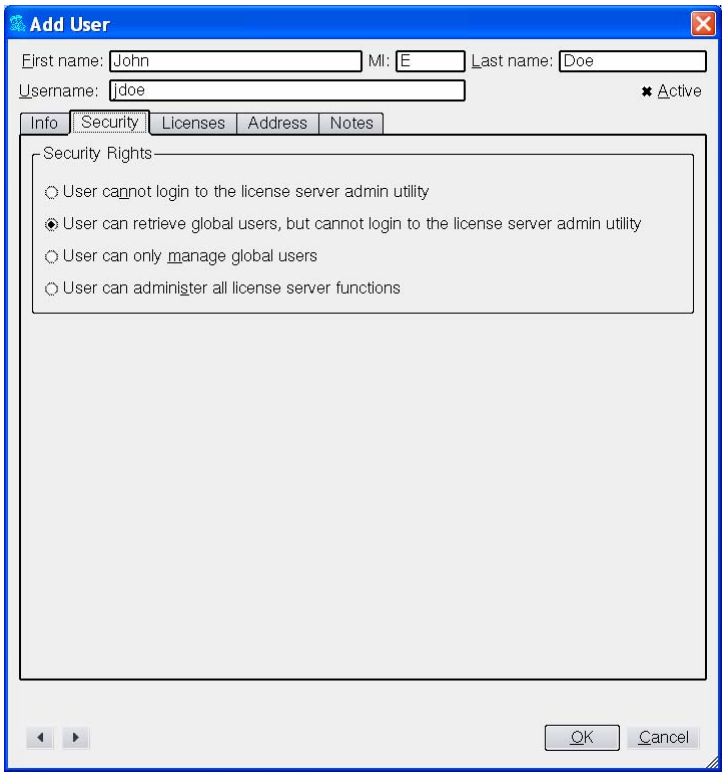


Figure 8.3-36. Add User GUI (Security tab)

8 On the Licenses tab (Figure 8.3-37):

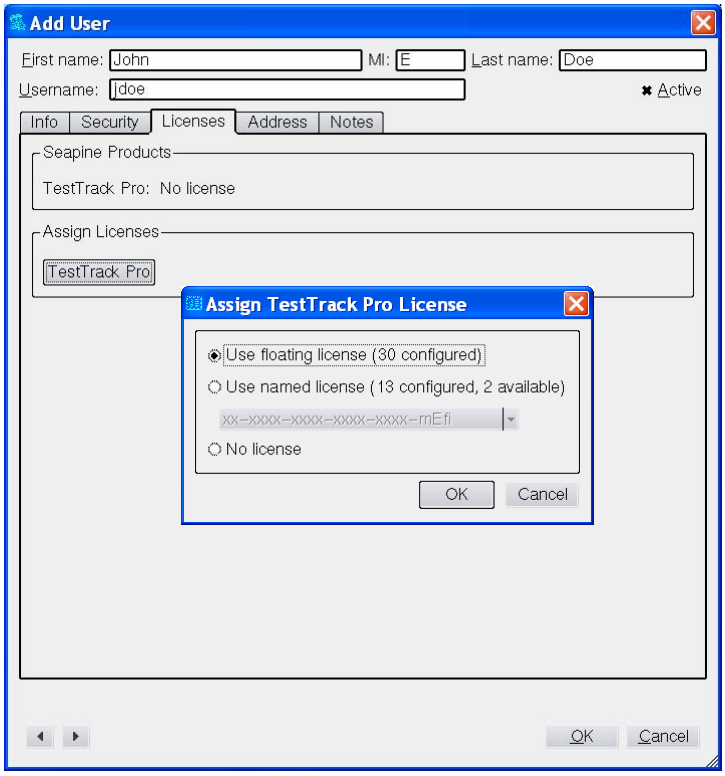


Figure 8.3-37. Add User GUI (Licenses tab)

a. Click the **TestTrack Pro** button.

b. When the **Assign TestTrack Pro License** GUI appears, click **Use floating license** or **Use named license**, as appropriate.

c. If assigning a named license, use the associated pull-down menu to choose which license to assign.

9 On the **Address** tab (Figure 8.3-38), enter the acronym for the user's site in the **Company** field.

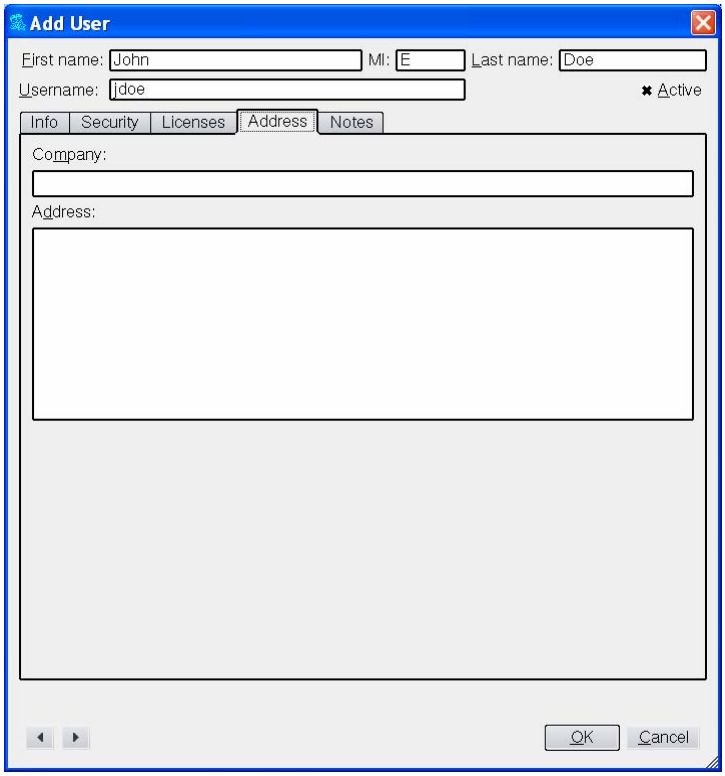


Figure 8.3-38. Add User GUI (Address tab)

10 Click **OK** to save the data.

11 Click **Close** to dismiss the Global Users GUI.

8.3.11 Grant a User Access to a Trouble Ticket Project

Anyone needing access to a site's trouble tickets must be assigned to one of the project's security groups. A security group is a collection of users who share responsibilities and perform similar tasks. Access to TestTrack Pro functions, such as assigning a trouble ticket or closing it, is controlled by group security. Table 8-3.6 lists role-based security groups found in all sites' project and summarizes the trouble ticketing privileges each group's members have.

Site CM Administrators grant users access to the site's trouble ticket project. Adding a new user to a project entails copying the individual's global user profile into the project, and then mapping it to a security group. Changing an existing user's privileges entails re-mapping the profile to a different group.

Note: Site CM Administrators require at least **User can retrieve global users, but cannot login to the license server admin utility** privileges on the Seapine License Server.

Table 8.3-6. Trouble Ticket Security Groups

Security Group	Description of Privileges
Administrator	Project file administration. Adds security groups and user profiles. Changes permissions. Escalates trouble tickets. Sets menu items. Etc.
Browser	Read only permission. View records only, but can not update records.
Customer	Not used. Example of possible customer configuration
DAACHELP	Can view site's escalated trouble tickets and update the Forwarded checkbox in Escalate events.
Engineers/Developers	All permissions except for admin commands and selected others considered admin commands. Attempts to resolve problem.
Inactive	For inactive users so you do not have to delete the user. No user rights!
Operations Supervisor	All permissions except for admin commands and others considered admin commands. Typically assigns problem priority and resolution responsibility.
Operator	All permissions except for admin and event commands and selected others treated as admin commands; cannot update closing code, assignments or fix event data.
TT Review Board Chair	All permissions except for admin commands and selected others considered admin commands. Reviews proposed solutions.
Resolution Technician	All permissions except for admin commands and selected others considered admin commands. Attempts to resolve problem.
Resource Manager	All permissions except for admin commands and selected others considered admin commands; Assigns problem priority and resolution responsibility. Can forward trouble ticket to another site.
Restricted View	Example of a user group using a filter to limit the viewing rights.
User Services	All permissions except for admin commands and selected others considered admin commands. Submits trouble ticket internally for user.

8.3.11.1 Grant a User Access to a Trouble Ticket Project using the Web Client

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page. If already logged in, navigate to the **Work with Trouble Tickets** page (Figure 8.3-3). Often this entails simply clicking on the Trouble Tickets tab.

2 Click the **Users** tab on the **Work with Trouble Tickets** page (Figure 8.3-3). The **Work with Users** page displays.

3 Click the **Retrieve Global** button on the **Work with Users** page (Figure 8.3-39) to access the list of global user profiles.

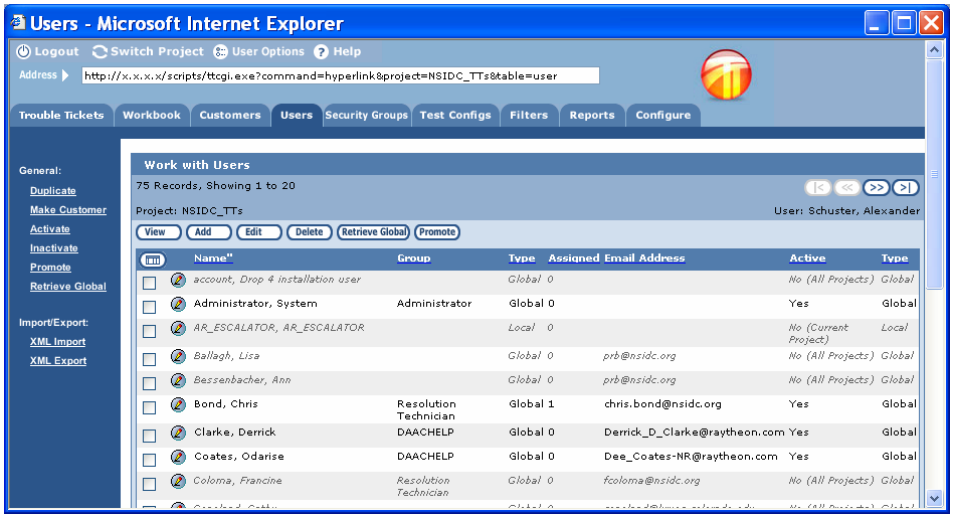


Figure 8.3-39. Users Web Page

4 Click on one (or more) of the names listed on the **Retrieve Global User** page (Figure 8.3-40), and then click **OK**. TTPro will import the profile(s) from the global user database.

Note: Type the first character of a user's last name to help find the user in the list.

Note: Use the <CTRL> key with your mouse click in order to select multiple names individually. Use the <SHIFT> key to select a series of names.

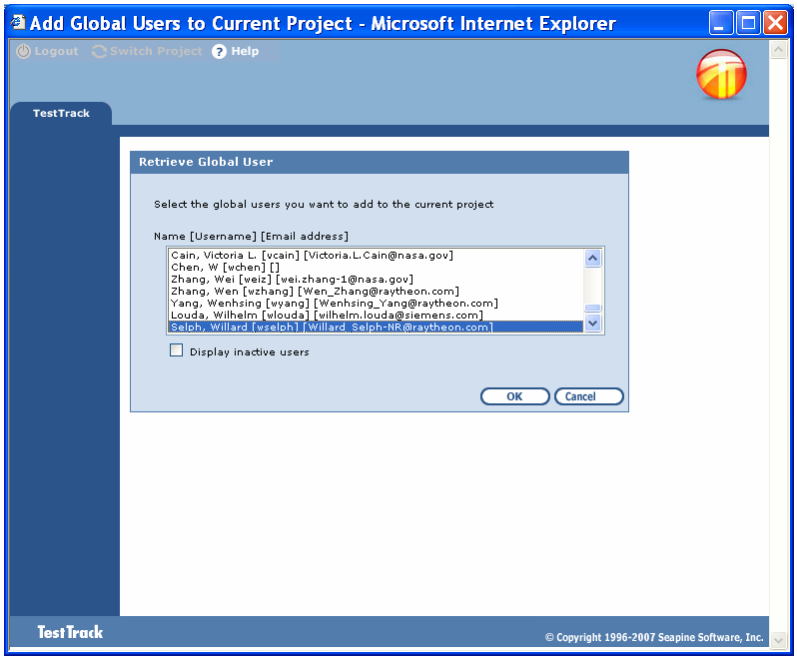


Figure 8.3-40. Retrieve Global User GUI

5 Click the user's **checkbox** on the **Work with Users web** page, and then click the **Edit** button atop the list of users.

6 On the **Edit User web** page that opens (Figure 8.3-41), map the user to a **Security Group** using the picklist for that field.

Note: To change an existing user's privileges, simply re-map the profile to another group.

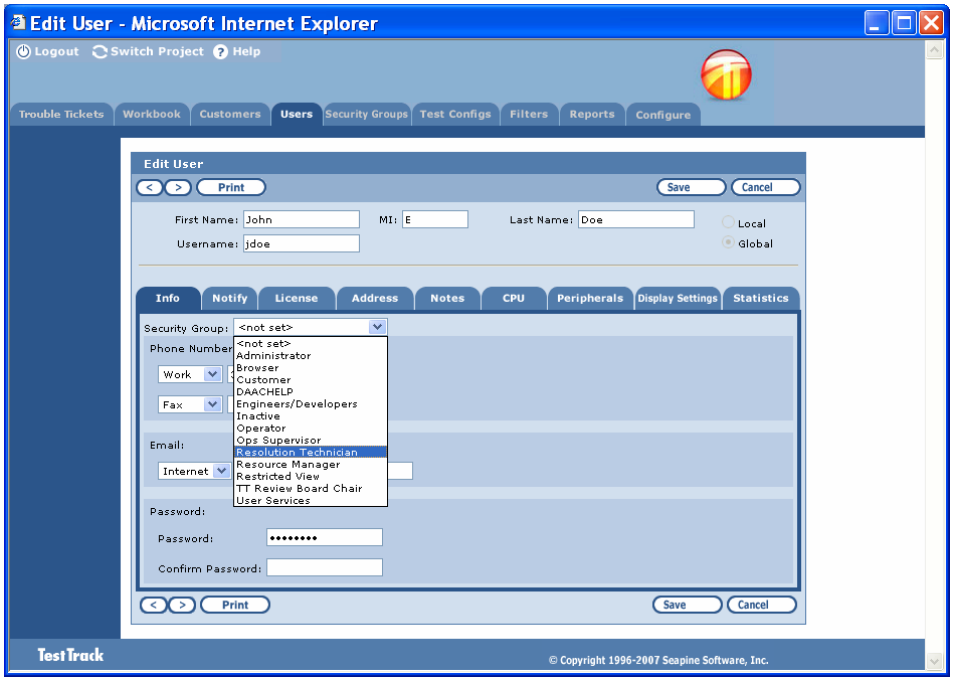


Figure 8.3-41. Edit Users Web Page

7 Click **Save**. TTPro saves the change and returns to the **Work with Users web** page. The user will now be able to access the project.

8.3.11.2 Grant a User Access to a Trouble Ticket Project using a GUI Client

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 Click **View → Users…** from the menu bar to open the **Users** GUI.

3 Click the **Retrieve Global User…** button on the **Users** GUI (Figure 8.3-42) to access the list of global user profiles.

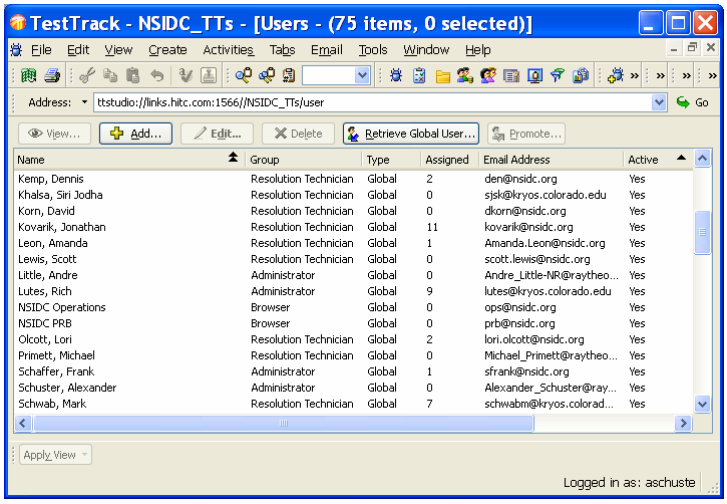


Figure 8.3-42. Users GUI

4 Click on one (or more) of the names listed on the **Retrieve Global User** GUI (Figure 8.3-43), and then click **Add**. TTPro will import the users' profiles from the global user database.

Note: Use the <CTRL> key with your mouse click in order to select multiple names individually. Use the <SHIFT> key to select a series of names.

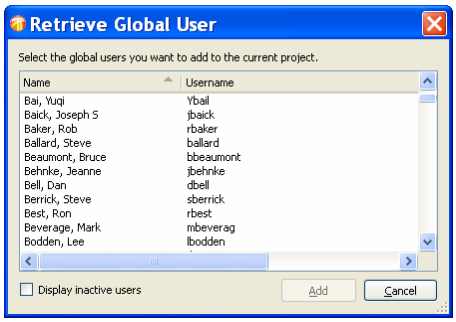


Figure 8.3-43. Retrieve Global User GUI

5 Select the user's profile and click the **Edit** button on the **Users GUI** to open the **Edit Users** GUI.

6 On the **Edit User** GUI that opens, map the user to a **Security Group** using the picklist for that field (Figure 8.3-44).

Note: To change an existing user's privileges, simply re-map the profile to another group.

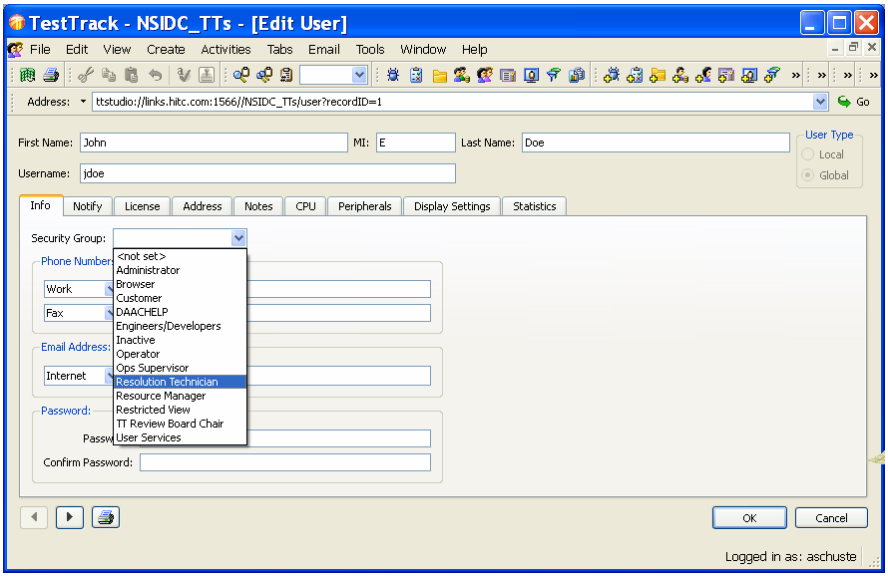


Figure 8.3-44. Edit User GUI

7 Click **OK**. TTPro saves the change and the **Edit User** GUI closes. The user will now be able to access the project.

8.3.12 Reset a User's Password

Occasionally users forget their TTPro passwords. Site CM Administrators can reset the password for a user of their projects by creating a TTPro Password Reset trouble ticket. When the ticket is submitted, TTPro changes the password if it can and emails the new password to the user. It moves the trouble ticket to the Fixed state if the password was changed successfully; and it notifies the administrator who created the ticket if an error occurs.

A valid TTPro Password Reset trouble ticket:

- Is created by a member of the project's Administrator security group
- Is in the Open state
- Has "TTPro Password Reset" in its **Type** field
- Has the name of the target user in its **Found by (Submitter)** field, and it is different than that of who created the ticket to preclude changing Administrators' passwords inadvertently.

Refer to Section 8.3-2 for the procedures for submitting a trouble ticket.

Note: If an attempt to reset a password fails because the trouble ticket was in error, edit the trouble ticket to correct the error rather than submit a new trouble ticket, and leave it in the Open state.

8.3.13 Manage Notifications

Notifications inform individuals when a trouble ticket changes. The system sends them via email in response to a variety of actions and under conditions specified in advance. System notifications are configured as automation rules by site CM Administrators for the trouble ticket project as a whole. User notifications are configured as user options by individual users who want to receive notices under additional circumstances. Trouble ticket notices are configured by individual users when editing a trouble ticket to ensure other, specific individuals are notified whenever that particular ticket changes.

Notifications are sent after records are saved in the database, typically when tickets are submitted, are assigned, or change state. They contain information from the trouble ticket in formats prescribed by pre-defined email templates. Site CM Administrators can modify the templates or define others.

8.3.13.1 Manage Notifications using the Web Client

1 Login to TTPro (see section 8.3.1.1), choosing to start at the **Defect List** page.

2 To create a system notification:

a. Click the **Configure** tab, and then **Automation Rules** in the left pane of the Project Configuration page (Figure 8.3-45). The **Configure Automation Rules** page displays with the Notifications tab selected.

Figure 8.3-45. Project Configuration Web Page

b. On the **Notifications** tab (Figure 8.3-46), click **Add** to add a rule. The **Add Notification Rule** page is displayed with the Precondition tab selected.

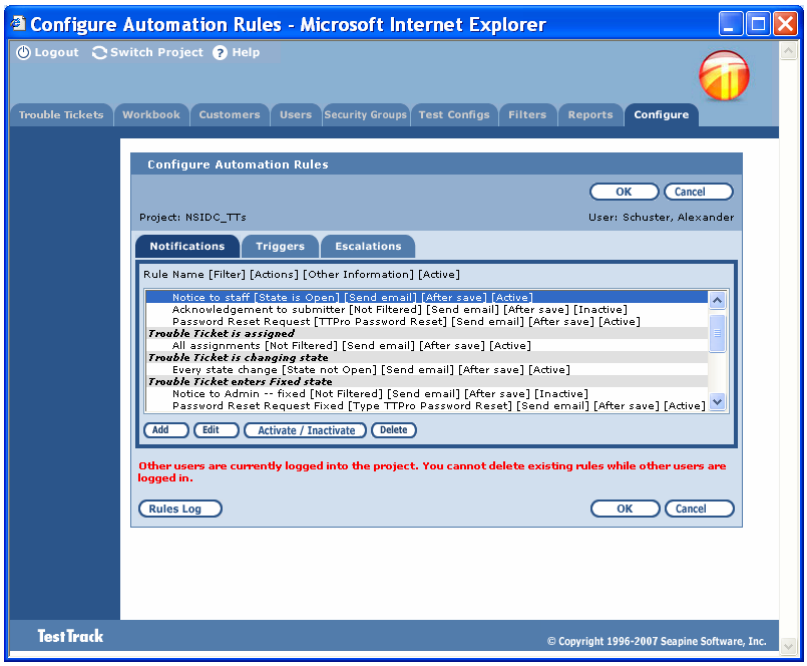


Figure 8.3-46. Configure Automation Rules Web Page

c. On the **Precondition** tab (Figure 8.3-47):

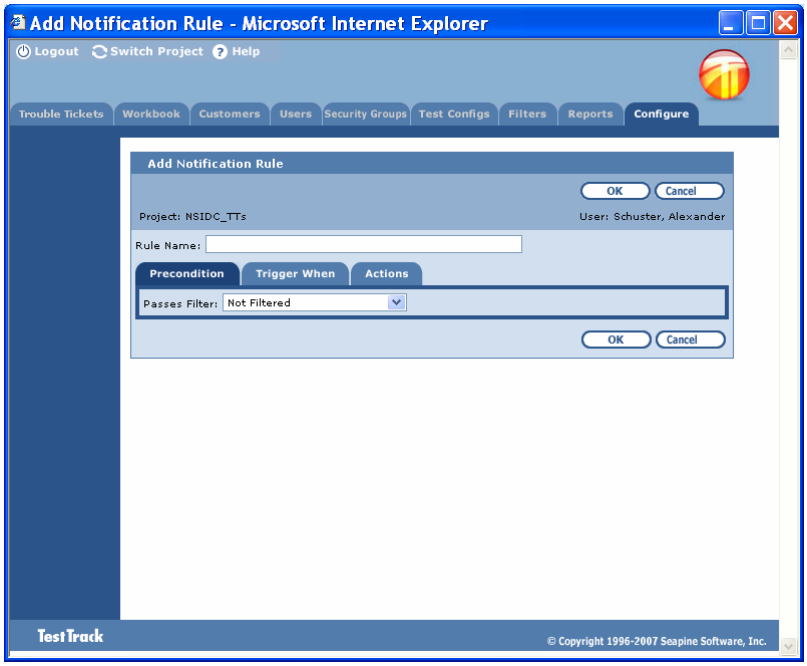


Figure 8.3-47. Add Notification Rule (Precondition tab) Web Page

i. Enter a **Rule Name.**

ii. Optionally select a **Passes Filter**. You may want to select a filter if the project contains a large number of records.

d. Click the **Trigger When** tab (Figure 8.3-48), and then select the activity that causes the notification to be sent.

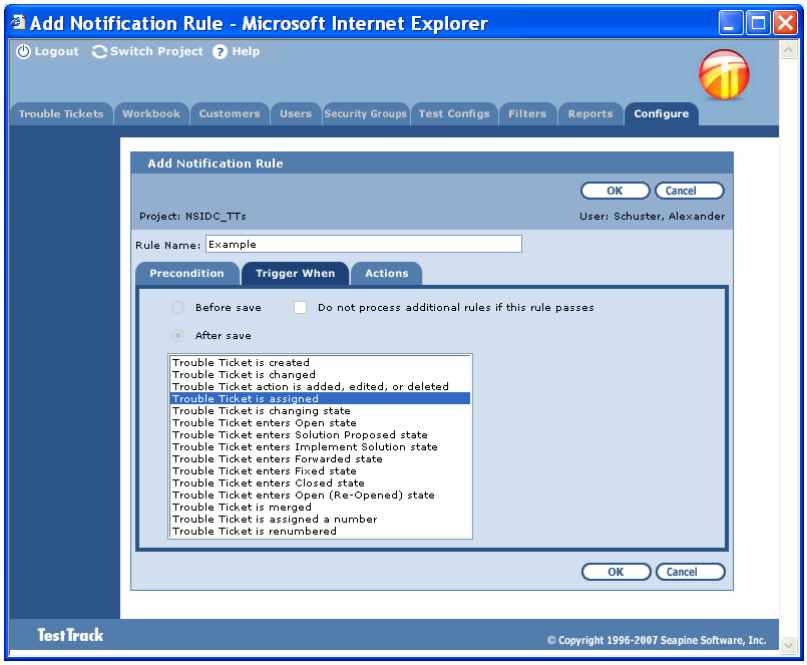


Figure 8.3-48. Add Notification Rule (Trigger When tab) Web Page

e. Click the **Actions** tab (Figure 8.3-49) and then click **Add** to to configure the send email action. (Click **Edit** or **Delete** to change or delete one, respectively.) The **Add Rule Action** page displays.

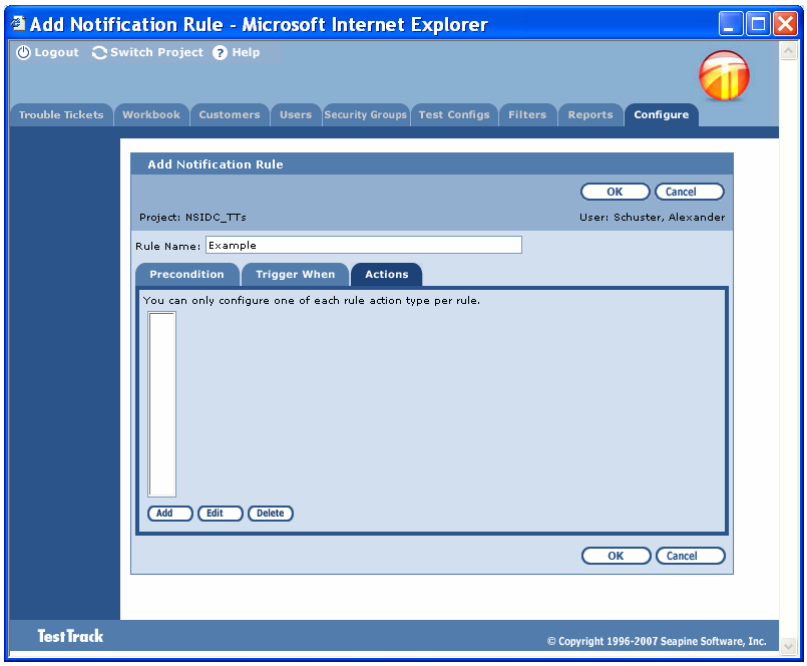


Figure 8.3-49. Add Notification Rule (Actions tab) Web Page

f. On the **Add Rule Action** page (Figure 8.3-50):

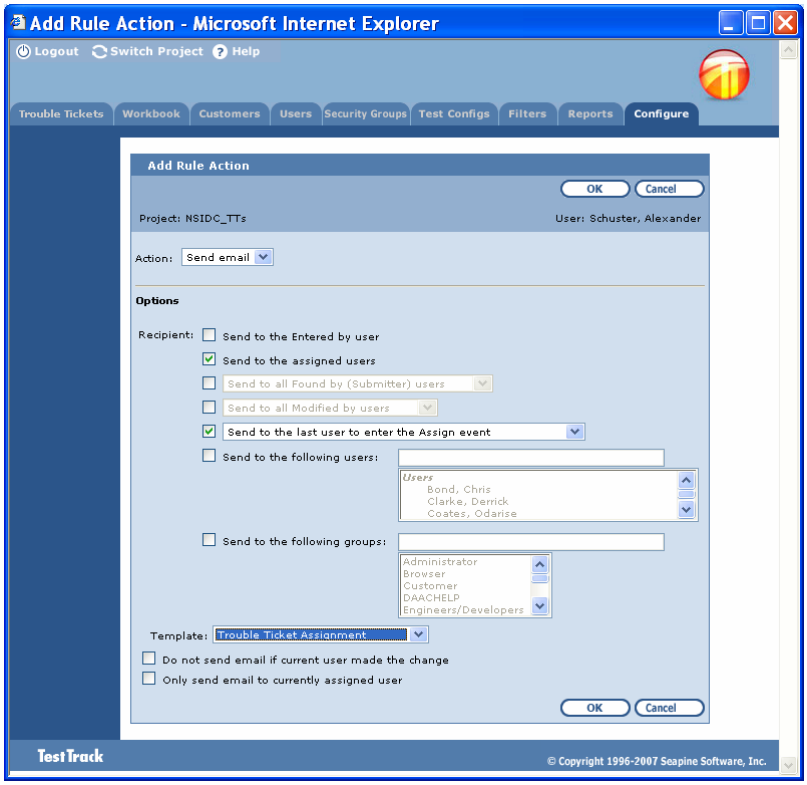


Figure 8.3-50. Add Rule Action Web Page

i. Use the checkboxes and picklists to select one or more recipients.

ii. Select an email **Template**. (To create a new template, see the on-line help for procedures.)

iii. Select **Do not send email if I made the change** if you do not want to receive an email when you change a record.

iv. Select **Only send email if item is assigned to me** to only receive email when you are the assigned user.

v. Click **OK** to add the rule action and return to the **Add Notification Rule** page.

g. Click **OK** on the **Add Notification Rule** page. The rule is added.

h. Click **OK** on the **Configure Automation Rules** page to return to the **Project Configuration** page

3 To create a user notification:

a. Click **User Options** at the top of the **Trouble Tickets list** page.

b. When the **User Options** page displays (Figure 8.3-51), click **Add** in the **Notifications** category to add a rule. The **Add Notification Rule** page is displayed with the **Precondition** tab selected.

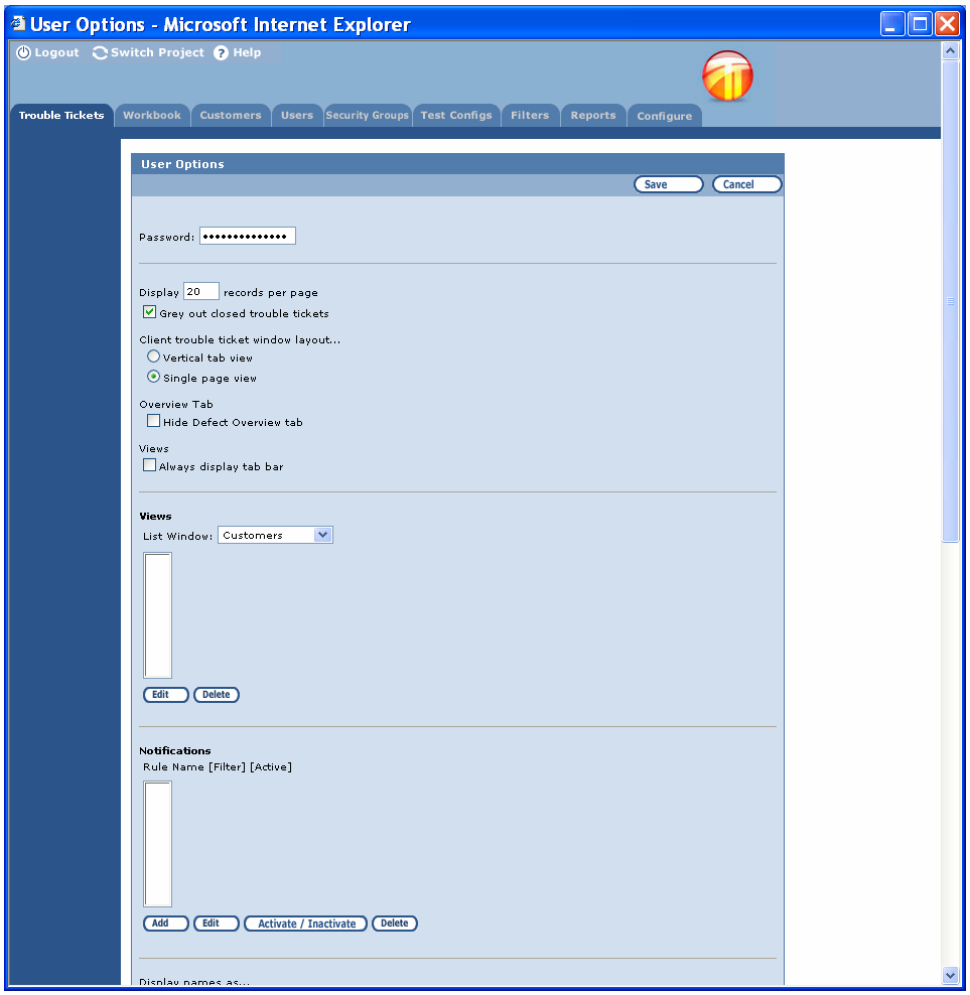


Figure 8.3-51. User Options Web Page

c. .On the **Precondition** tab (Figure 8.3.52):

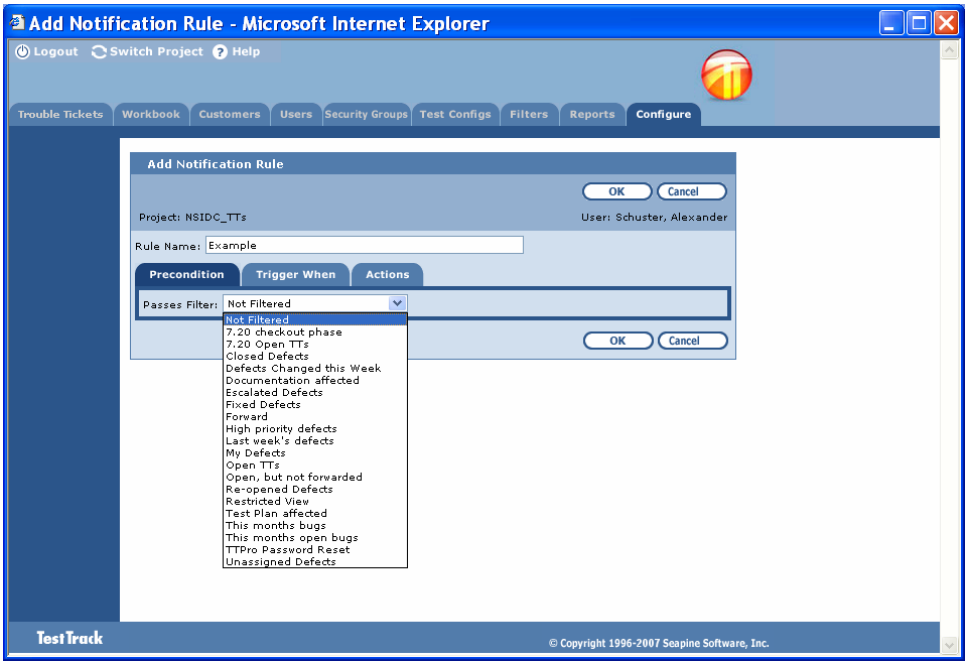


Figure 8.3-52. Add Notification Rule (Precondition Tab) Web Page

i. Enter a **Rule Name**.

ii. Optionally select a **Passes Filter**. You may want to select a filter if the project contains a large number of records.

d. Click the **Trigger When** tab (Figure 8.3-53), and select an activity to specify when the notification is sent.

Figure 8.3-53. Add Notification Rule (Trigger When Tab) Web Page

e. Click the **Actions** tab (Figure 8.3-54).

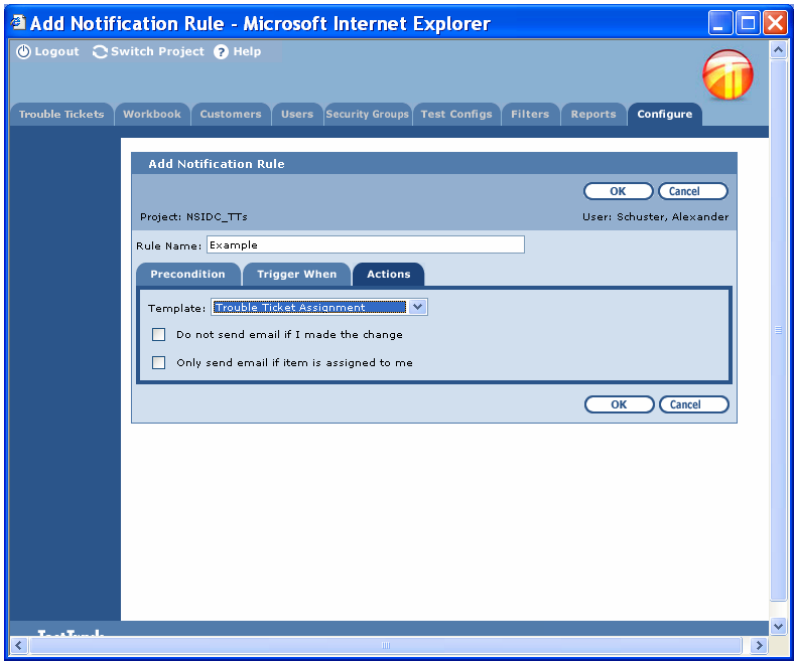


Figure 8.3-54. Add Notification Rule (Actions Tab) Web Page

i. Select an email **Template**. (To create a new template, see the on-line help for procedures.)

ii. Select **Do not send email if I made the change** if you do not want to receive an email when you change a record.

iii. Select **Only send email if item is assigned to me** to only receive email when you are the assigned user.

f. Click **OK**. The rule is added and the **Add Notification Rule** GUI closes.

g. Click **Save** to store the changes and exit **User Options**.

4 To notify users when a specific trouble ticket changes:

a. On the **Work with Trouble Tickets** page (Figure 8.3-55):

i. Search for the trouble ticket in which to add the notification (see Section 8.3.3).

ii. Click the **checkbox** next to the trouble ticket, and then click the **Edit** button atop the list of trouble tickets. The **Edit Trouble Ticket** page displays.

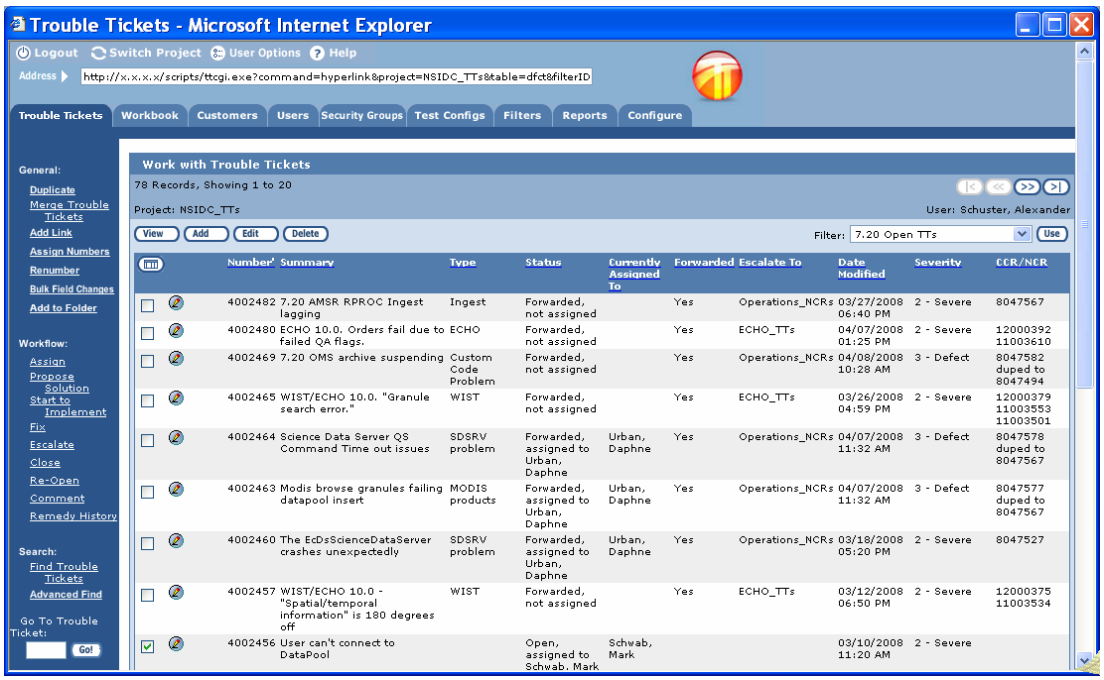


Figure 8.3-55. Work with Trouble Tickets Web Page

b. Click the **Email** tab on the **Edit Trouble Tickets** page (Figure 8.3-56).

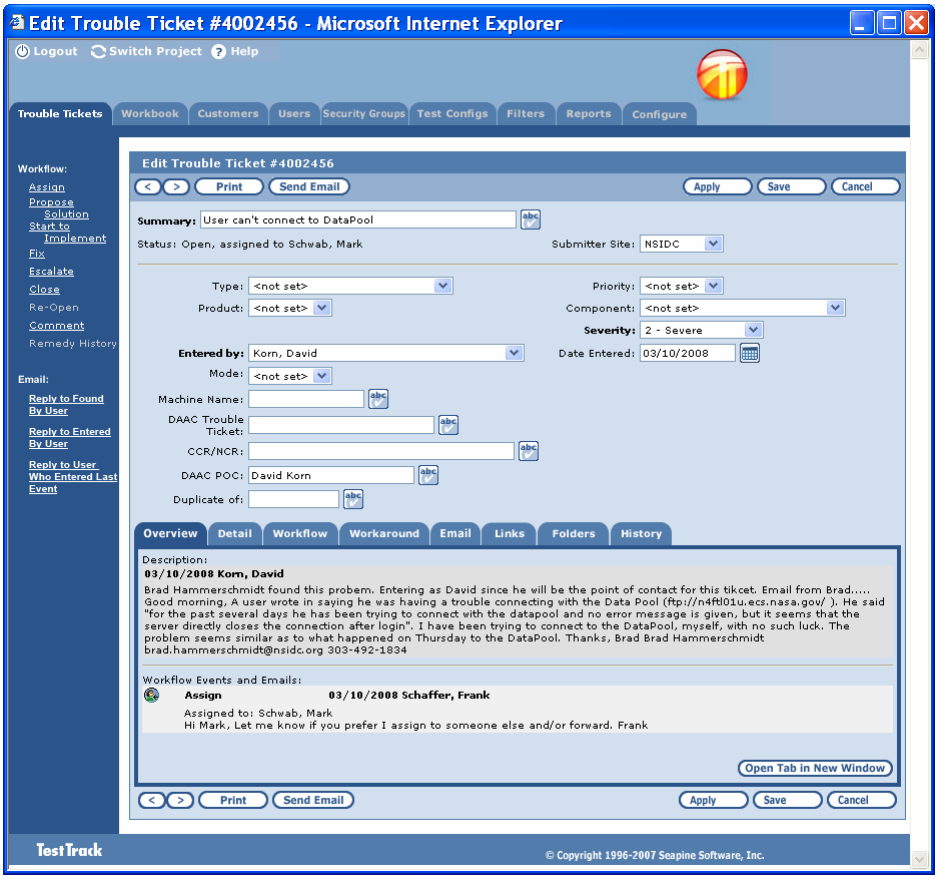


Figure 8.3-56. Work with Trouble Tickets (Detail Tab) Web Page

c. On the **Email** tab (Figure 8.3.57):

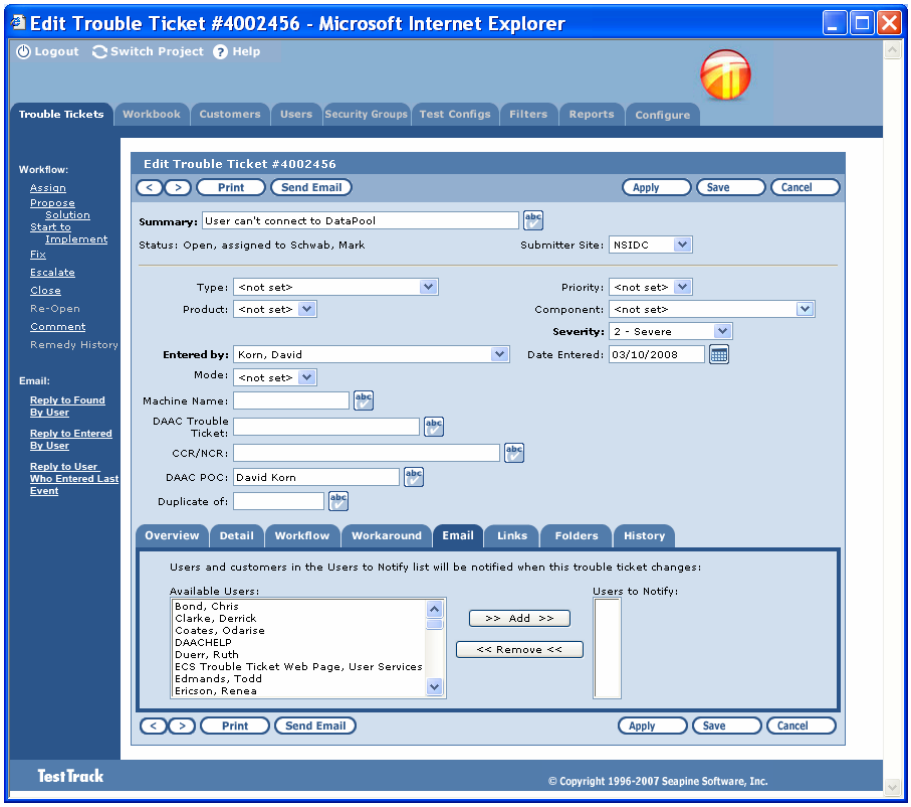


Figure 8.3-57. Edit Trouble Ticket (Email Tab) Web Page

i. Select the users you want to notify when the ticket changes.

ii. Click **Add**, select the users from the **Add Mail Recipients** dialog box, and click **Add**.

Note: You can only add recipients when you are adding or editing a defect.

d. Click **Apply** or **Save** to save the changes and return to the **Work with Trouble Tickets** page.

8.3.13.2 Manage Notifications using a GUI Client

1 Login to TTPro (see section 8.3.1.1), choosing your site's trouble ticket project.

2 To create a system notification:

a. Choose **Tools → Administration → Automation Rules** from the menu bar The **Configure Automation Rules** dialog box opens with the **Notifications** tab selected.

b. On the **Notifications** tab (Figure 8.3-58), click **Add** to add a rule. The **Add Notification Rule** page is displayed with the **Precondition** tab selected. The **Summary** field displays a rule summary that changes as you configure the rule.

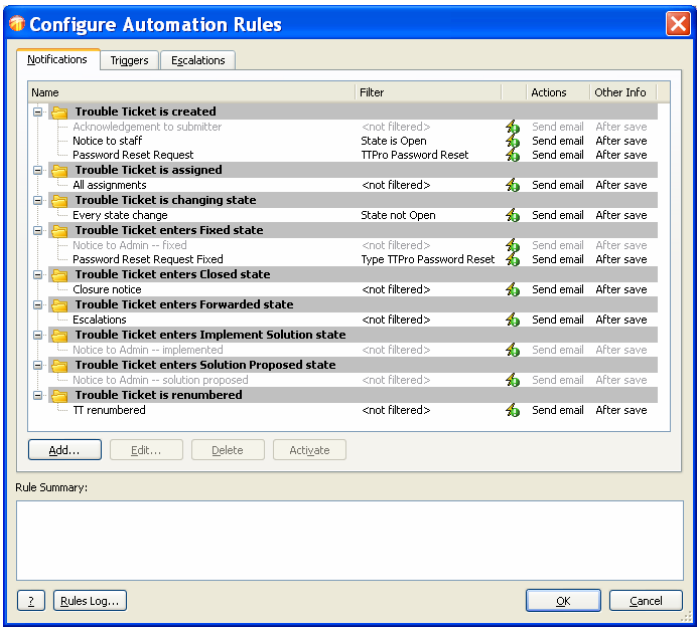


Figure 8.3-58. Configure Automations Rules GUI

c. On the **Preconditions** tab (Figure 8.3-59):

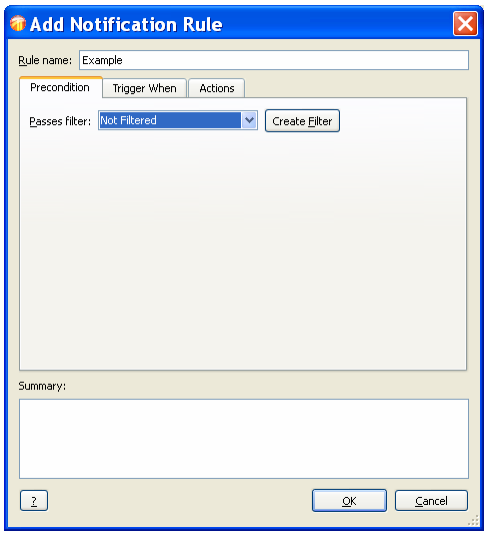


Figure 8.3-59. Add Notification Rule (Precondition Tab) GUI

i. Enter a **Rule Name**.

ii. Optionally select a **Passes** filter. You may want to select a filter if the project contains a large number of records. You can create a new filter by clicking **Create Filter**.

d. Click the **Trigger When** tab (Figure 8.3-60), and then select the activity that causes the notification to be sent.

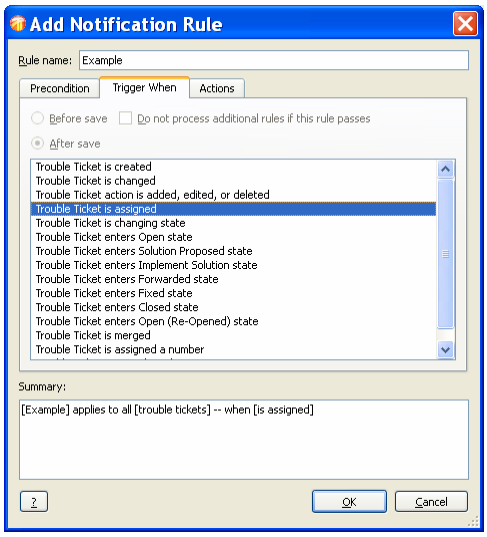


Figure 8.3-60. Add Notification Rule (Trigger When Tab) GUI

e. Click the **Actions** tab (Figure 8.3-61) and then click **Add** to to configure the send email action. (Click **Edit** or **Delete** to change or delete one, respectively.) The **Add Rule Action** page (Figure 8.3-62) displays.

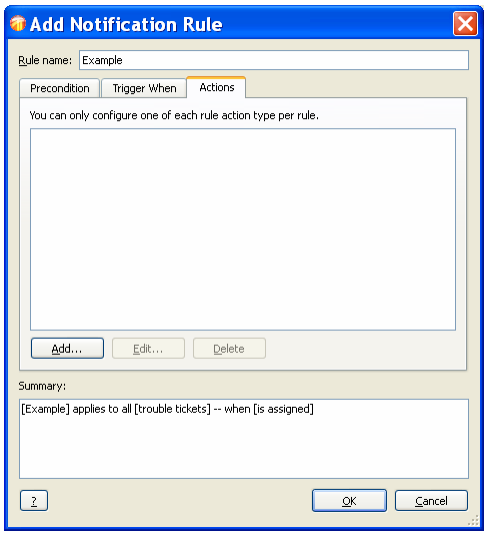


Figure 8.3-61. Add Notification Rule (Actions Tab) GUI

f. On the **Add Rule Action** GUI (Figure 8.3-62):

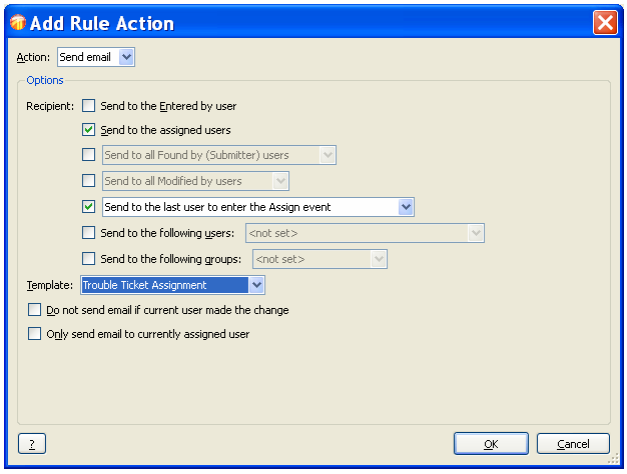


Figure 8.3-62. Add Rule Action GUI

i. Use the checkboxes and picklists to select one or more recipients.

ii. Select an email **Template**. (To create a new template, see the on-line help for procedures.)

iii. Select **Do not send email if I made the change** if you do not want to receive an email when you change a record.

iv. Select **Only send email if item is assigned to me** to only receive email when you are the assigned user.

v. Click **OK** to add the rule action.

g. Click **OK** on the **Add Notification Rule** GUI. The rule is added.

h. Click **OK** on the **Configure Automation Rules** GUI to close it.

3 To create a user notification:

a. Choose **Tools > User Options** from the menu bar.

b. When the **User Options** GUI appears, select the **Notifications** category (Figure 8.3-63), and then click **Add** to add a rule. The **Add Notification Rule** dialog box opens with the **Precondition** tab selected.

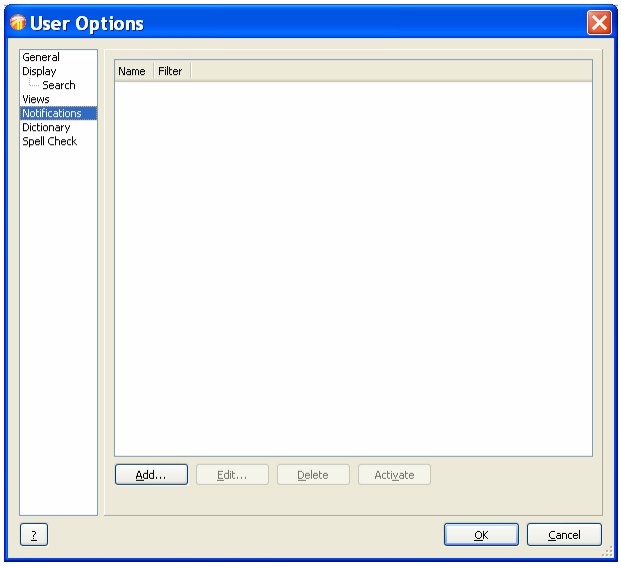


Figure 8.3-63. User Options (Notification Category) GUI

c. On the **Precondition** tab (Figure 8.3.64):

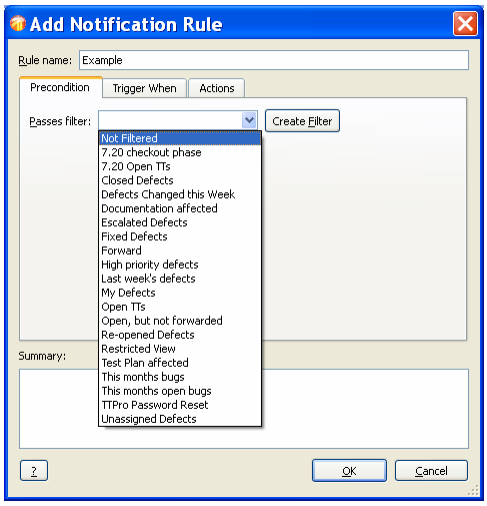


Figure 8.3-64. Add Notification Rule (Precondition Tab) GUI

i. Enter a **Rule name**.

ii. Optionally select a **Passes filter**. You may want to select a filter if the project contains a large number of records. You can create a new filter by clicking **Create** Filter.

d. Click the **Trigger When** tab (Figure 8.3.65), and select an activity to specify when the notification is sent.

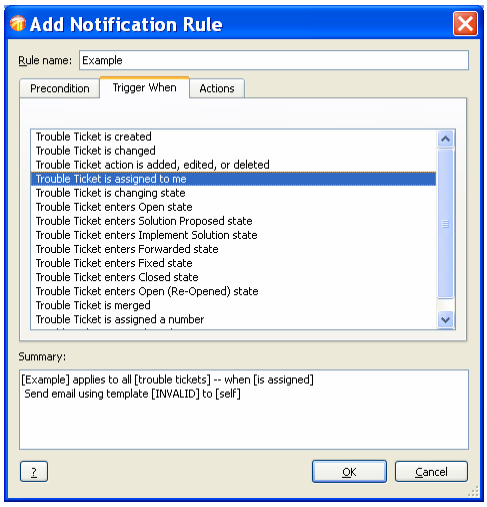


Figure 8.3-65. Add Notification Rule (Trigger When Tab) GUI

e. Click the **Actions** tab (Figure 8.3-66).

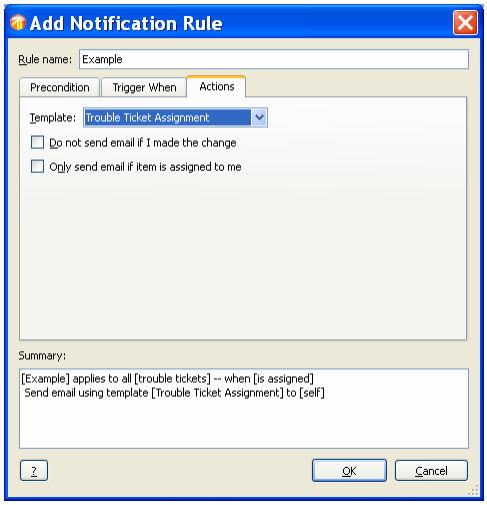


Figure 8.3-66. Add Notification Rule (Actions Tab) GUI

i. Select an email Template. (To create a new template, see the on-line help for procedures.)

ii. Select **Do not send email if I made the change** if you do not want to receive an email when you change a record.

iii. Select **Only send email if item is assigned to me** to only receive email when you are the assigned user.

f. Click **OK**. The rule is added and the **Add Notification Rule** GUI closes.

g. Click **OK** to exit User Options.

4 To notify users when a specific trouble ticket changes:

a. On the **Trouble Tickets List** GUI (Figure 8.3-67):

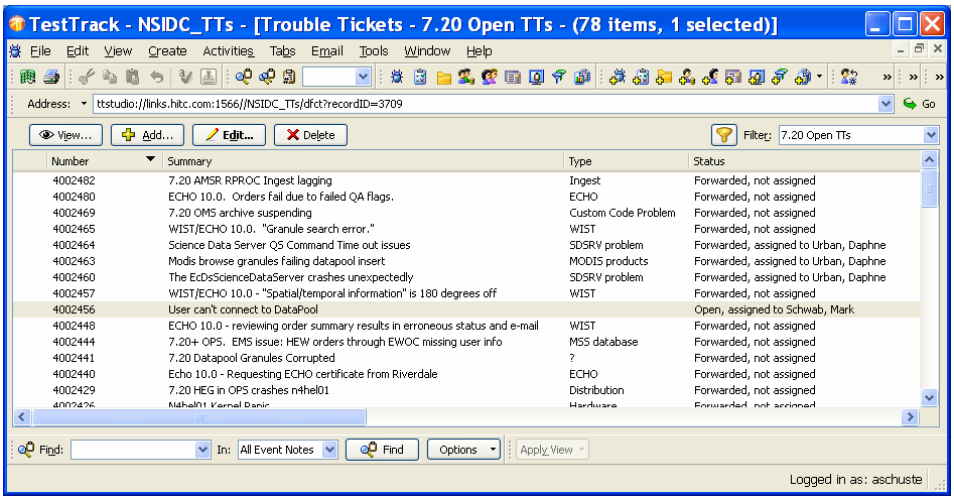


Figure 8.3-67. Trouble Tickets GUI

i. Search for the trouble ticket (see Section xxx).

ii. Highlight the appropriate trouble ticket, and then click **Edit** to open it. The **Edit Trouble Ticket** GUI appears.

b. Click the **Email** tab on the **Edit Trouble Tickets** GUI. On the **Email** tab (Figure 8.3-68):

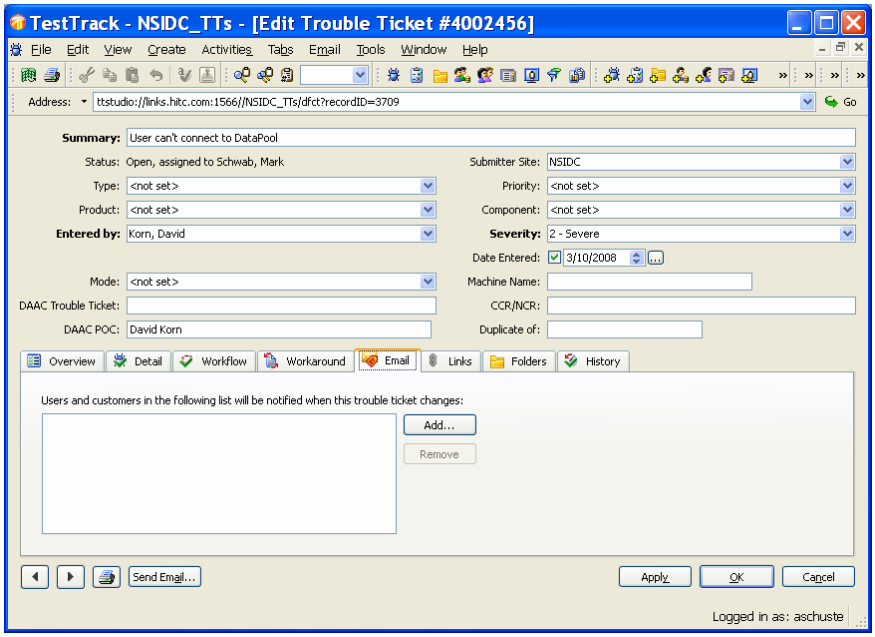


Figure 8.3-68. Edit Trouble Ticket (Email Tab) GUI

i. Select the users you want to notify when the ticket changes.

ii. Click **Add**, select the users from the **Add Mail Recipients** dialog box, and click **Add**.

Note: You can only add recipients when you are adding or editing a defect.

c. Click **Add** or **OK** to save the changes, or click another tab.

8.3.14 Generating Trouble Ticket Reports

Each TTPro project is equipped with numerous general-purpose, predefined reports. These reports can be run as-is, customized, or used as templates by anyone wishing to create their own reports.

Reports are used to analyze the data collected in a TestTrack project. You can use filters to build reports that focus on the data you need. You can also share reports with other users or keep them private. Table 8.3-7 describes one each of TTPro's four types of reports: Detail, List, Distribution, and Trend.

Table 8.3-7. Sample Reports in TestTrack Pro

Report Type	Report Description	When and Why Used
Detail – Display of Open Defects	A full report of every Trouble Ticket not in a Closed state, sorted by Trouble Ticket number.	When and if someone wants a copy of all open Trouble Tickets.
List – Summary of Problems	A list of the Trouble Tickets found or modified during the week prior to the report, containing only key details and sorted by Trouble Ticket number.	When and if someone wants a list of the Trouble Tickets opened or updated during the past week.
Distribution – Team Assignment Report	A distribution report identifying the Trouble Tickets found or modified during the week prior to the report, containing only key details and sorted by Trouble Ticket number.	When and if someone wants to know how evenly work is distributed among the staff.
Trend – Trend of Open Defects and Types	A trend report identifying the number of Trouble Tickets of each problem type in the Open state over time, grouped and ordered by month.	When and if someone wants to review (or forecast) trends among the types of problems reported.

The procedures below focus on how to run a report. Complete instructions for creating custom reports can be found in the TTPro Users Manual or the on-line, context sensitve help.

8.3.14.1 Generate Reports using the Web Client

1 From the TestTrack Pro menu, click **View → Reports….** The Reports – All Types

2 Select **Report**, then select **Detail** (or Distributed, List, Trend) to display of open TTs.

8.3.14.2 Generate Reports using a GUI Client

1 You can view, add, edit, delete, or print reports from the Reports list window.

a. From the TTPro menu, click **View → Reports…**. The Reports list window opens. (Figure 8.3-69).

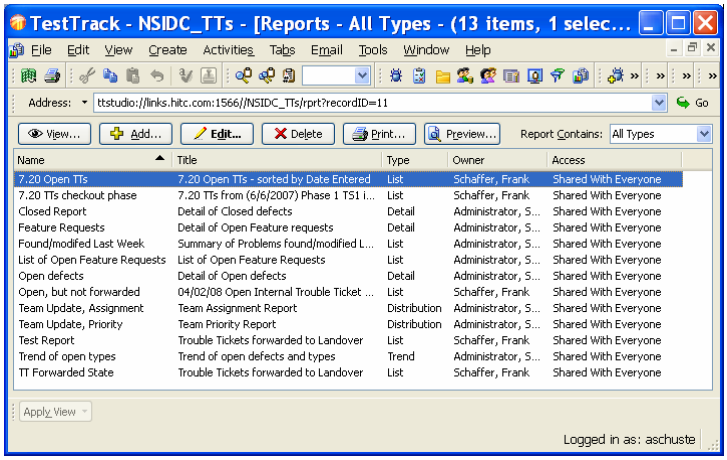


Figure 8.3-69. Reports List GUI

b. Optionally select a record type from the Report Contains list to filter the list window.

c. Select a report and click View to view its settings. All fields are read-only.

d. Click Add to create a new report.

e. Select a report and click Edit to change an existing report's settings.

f. Select a report and click Delete to delete it.

g. Select a report and click Print to print it. TTPro will open a print dialog box. Modify or verify print settings, and then click Print. When printing completes, TTPro returns you to the Reports list window.

h. Select a report and click Preview to preview a report before printing. TTPro opens the report in your default browser. Use the browser's print facility to print the report, then close your browser window.

2 Alternatively, you can print a detail or list report of one or more records selected from the trouble tickets list window.

a. On the **Trouble Tickets** list window, click on the trouble tickets to include in the report, using the <CTRL> and <SHIFT> keys to select multiple records, as desired.

b. Click **File → Print…** from the TTPro menu. The **Print Options** dialog box opens (Figure 8.3-70).

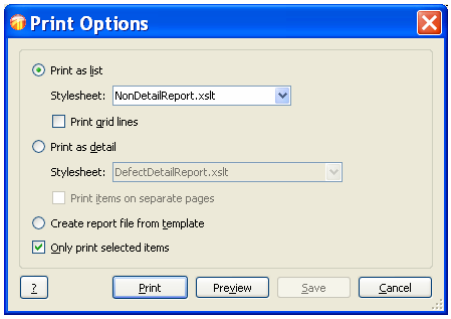


Figure 8.3-70. Print Options GUI

i. To print a list report, click Print as list, choose a preferred stylesheet, and click Print grid lines if you want item separators in the report.

ii. .To print a detail report, click Print as detail, choose a preferred stylesheet, and click Print items on separate pages if you want each trouble ticket to begin on a new page.

c. Click Only print selected items unless you want to print all trouble tickets from the list window.

d. Click Print to print the report. TTPro will open a print dialog box. Modify or verify print settings, and then click Print. When printing completes, TTPro returns you to the Reports list window.

e. Click Preview to preview a report before printing. TTPro opens the report in your default browser. Use the browser's print facility to print the report, then close your browser window.

3 You can also print a detail report from within a trouble ticket that is already open for viewing or editing.

a. On the View (or Edit) Trouble Ticket GUI, click the Generate a detail report of the open item icon at the lower left side of the screen. TTPro opens the report in your default browser.

b. Use the browser's print facility to print the report, then close your browser window.

8.4 Emergency Fixes

Emergencies may be in real time with the understanding that the trouble ticket system must be brought up-to-date as soon as possible after implementing the repair. The example presented below, involves a hardware failure. The problem needs to be resolved quickly to bring a system back into operation. The resolution requires emergency replacement of a component that is of a later version than is contained in the original equipment. The scenario is summarized in Table 8.4-1.

It is 7:00 on a Saturday evening. The DAAC operator detects a problem with the automated tape library (ATL) and reports the problem to the trouble ticket system. The trouble ticket is routed to the System Administrator, who confirms that the system will not operate and notifies the site Maintenance Engineer. After running further diagnostics, the Maintenance Engineer reports the problem and symptoms to the OEM's maintenance desk. The original equipment manufacturer (OEM) maintenance representative arrives and concludes that a controller card has failed. The only card the OEM has immediately available is of a later version and no spares are available on site. It will be Monday at the earliest before a replacement board of the same revision level can be located. The site maintenance engineer reports this to the operations Crew Chief (i.e., shift leader) for a decision.

The DAAC cannot afford to have the ATL down until Monday. The Crew Chief calls the DAAC manager at home, apprises him of the situation, and obtains approval to replace the board with the later version if tests conclude that it works properly. The OEM's maintenance representative installs the board. The site's sustaining engineer tests the new controller board, finds that it works properly, and brings the ATL back on-line. The sustaining engineer updates the trouble ticket to document the configuration change and the authority for the change, and forwards it to the site CMA. The site Maintenance Engineer updates the property record with the model, version, and serial number of the new board.

The site CM Administrator reviews the trouble ticket, and presents it to the local CCB for approval. The CMA then updates the Baseline Manager with the new configuration and TT number authorizing the change. At this point, the site is operational at variance from the system baseline (i.e., site unique) and is at risk of losing maintenance support from OPS Deployment.

The site CMA forwards the trouble ticket to the SMC, presented to the PRB for priority review and is solved or translated into an NCR. The PRB reviews all emergency TTs to assess whether there may be impacts to the system and/or applicability to other sites. The SCDV CCB monitors all open NCR promotion and approves them for closure.

In the event that it is later discovered that the new version controller board has adverse impacts when operating in the system configuration, a board of the original version will have to be obtained to replace the newer version. In such cases, the action will be recorded on a new trouble ticket, citing the previous CCR.

Table 8.4-1 summarizes emergency procedures that might be taken during an after-hours, over-the-weekend emergency hardware failure.

Table 8.4-1. Example of Emergency Change Procedure

Operator/User	System
Operator prepares trouble ticket to report ATL controller failure.	Trouble ticket recorded.
System Administrator and Maintenance Engineer confirm ATL controller failure, call ATL maintenance vendor, report call and time in Trouble ticket.	Diagnosis and vendor call recorded in trouble ticket.
Maintenance vendor isolates failure to the controller card. The later version card is the only card available.	
Crew Chief notified of situation and decision needed to bring ATL up to full operating capability. Approves use of the newer version card, records decision in the trouble ticket, forwards trouble ticket to Sustaining Engineer.	
Maintenance vendor installs card, tests using hardware diagnostics. Crew Chief authorizes controller to be brought back on-line.	
Maintenance Engineer records card installation by model/version into the trouble ticket.	Trouble ticket action recorded.
Sustaining Engineer reads trouble ticket and prepares for discussion at 8:30 am meeting. Updates the TT.	Install action recorded in TT. TT routed to the CMA.
CMA updates site baseline, forwards TT to the CCB. When CCB approves the action, CMA forwards to SMC.	Site ATL baseline updated in Baseline Manager.
PRB reviews emergency NCR, checks for applicability to other sites.	

9. Configuration Management Procedures

The prepared procedures are applicable to all EMD hardware, software, and firmware components of systems or subsystems developed and acquired by the EMD contract and/or delegated to configuration management control by the operational site-level organizations. The procedures are applicable to all items maintained by the EMD Sustaining Engineering Organization in support of EMD mission-specific projects and multiple mission-specific institutional facilities. The procedures are not applicable to those entities controlled by higher level ESDIS Project Office CM Plans. CM procedures already in place may be used by the contractor subject to direction from the Change Control Board (CCB) chairperson.

Some major features of the approach being described here include:

- Customers participate in establishing the procedures;
- The SCDV CCB performs a support role for ESDIS and its designated on-site CCBs by processing system-level CCRs & Trouble Tickets (also known as defects);
- Prioritization, automated tools, and procedures are used for handling change requests;
- Diverse/Strategic representation at hierarchical CCBs facilitates a path for speedy escalation/resolution of problems/issues;
- Local organizations have the needed autonomy to accomplish their mission with the minimum necessary outside intervention to promote timely resolution of local problems and enable timely production of data products;
- Proper use and deployment of CM database assets to support all CCBs allows management monitoring, control, and analysis of activities;
- Coordination with the Failure Review Board allows coordinated response to problems and filtering of prioritized issues; and
- Common CM tools will be used in all elements of the EMD Project during operations.

The procedures are organized into seven major sections that address the EMD system-level flow-down of procedures to the site-level which references applicable site-tailored procedures. The topics include:

- (Section 9.1) Configuration Identification
- (Section 9.2) Change Control Procedures
- (Section 9.3) Configuration Status Accounting
- (Section 9.4) Configuration Audits
- (Sections 9.5 and 9.6) Software CM Manager (ClearCase)

- (Section 9.7) Baseline Manager (ClearCase).

9.1 Configuration Identification Procedure

9.1.1 Purpose

The purpose of configuration identification during sustaining engineering is to incrementally establish and maintain the definitive basis of control and status accounting for the EMD control items. To accomplish configuration identification for both hardware and software, the configuration management (CM) administrator (CMA) will ensure the maintenance of each EMD configuration controlled item in an operational baseline by executing the following tasks:

a. Assign identifiers to configuration items (CIs) and their component parts and associated configuration documentation, including revision and version number where appropriate. Assign serial and lot numbers, as necessary, to establish the CI effectivity of each configuration of each item of hardware and software.

b. Follow EMD developer guidelines as referenced below in Section 9.1.3.

c. Use vendor nomenclature for COTS items.

d. Follow author-designated version control and nomenclature for documents and follow the EMD Library guidelines (cf. Chapter 17, *Library Administration*) administered by the EMD Librarian.

e. Support the EMD Librarian's efforts to maintain linkage of the EMD documentation to EMD configuration items in the Baseline Manager tool (cf. Section 9.7). Ensure that the marking and labeling of items and documentation with their applicable identifiers enables correlation between the item, configuration documentation, and other associated data.

f. Maintain a release system for configuration changes (cf. Section 9.2, *Configuration Change Control Procedures).*

g. Maintain views of operational baselines using the Baseline Manager tool.

9.1.2 Applicability

All EMD CM Administrators and support personnel.

9.1.3 References

ESDIS CM Plan

Configuration Management Plan for the EMD Project	110-EMD-001
EMD Software Build Process	CM-1-045
Data Identification Numbering	DM-002

DoD MIL-STD-973

9.2 Configuration Change Control Procedures

9.2.1 Purpose

The ESDIS CCB chartered Change Control Boards (CCBs) shall apply configuration control measures to all the EMD configuration items and the associated documentation prior to the time it is baselined for operations. The CCBs shall apply configuration control measures to accomplish the following objectives:

a. Ensure effective control of all CIs and their approved documentation.

b. Provide effective means, as applicable, for (1) proposing engineering changes to CIs, (2) requesting deviations and waivers pertaining to such items, (3) preparing notices of revision, and (4) preparing Specification Change Notices.

c. Ensure the implementation of approved changes.

9.2.2 Applicability

All ESDIS chartered EMD CCBs.

9.2.3 References

ESDIS CM Plan

EMD Configuration Management Plan	110-EMD-001
CCB Change Control Process	CM-004

9.2.4 Procedures

9.2.4.1 Configuration Change Request Preparation

The Configuration Change Request (CCR) form in Figure 9.2-2 has been developed as a medium for the drafting of CCRs throughout the EMD Operations Deployment environment for changes processed locally at EMD site-level chartered CCBs at the SMC and DAACs (GSFC (GES), LaRC (ASDC), EDC (LP DAAC) and NSIDC). For changes processed by the ESDIS Change Control Board (CCB), use ESDIS forms (Figure 9.2-1). For EMD CCBs, use the new EMD Electronic CCR Tool. There are numbered items on the form that correspond exactly to the data entry required to be performed by the respective originator of the CCR. Each CCB will have unique CCR identification sequence numbers. Each CCB can forward CCRs and reports from the Change Request Manager to SMC, which processes system-level CCRs for ESDIS CCB. The ESDIS CM Plan will determine the charter of the respective CCBs and thus the scope of CCR issues to be addressed by the site CCBs.

Earth Observing System Data and Information System (EOSDIS)
Core System (ECS)
Configuration Change Request (CCR)

1. **Configuration Control Board (CCB)**
ESDIS:___ ECS:___ SMC:___ DAAC: GSFC___, LaRC___, EDC___, NSIDC___,

2. CCR No.

3. Submitted Date:

4. Revision

5. Priority
Emergency ☐
Urgent ☐
Routine ☐

6. Change Class

7. Status

8. CCR Title:

9. Originator: Org: e-mail: phone:

10. Approval:_____ _____
signature date

11. Reason for Change

(indicate attachment ___)

12. Description of Change

(indicate attachment ___)

13. Impact Analysis:
Cost: ☐ None ☐ Small (Not exceeding $100,000) ☐ Medium ($100,000 to $500,000) ☐ Large (Over $500,000)
Evaluation Engineer: Org: e-mail: phone:
Impact Evaluators: ESDIS___; ECS Dev___; SEO___; SMC___; DAACs: GSFC___, LaRC___, EDC___, NSIDC___, EOC___;
Others_____ (indicate attachment ___)

14. Comments: (Indicate Sites/ Organizations Affected)

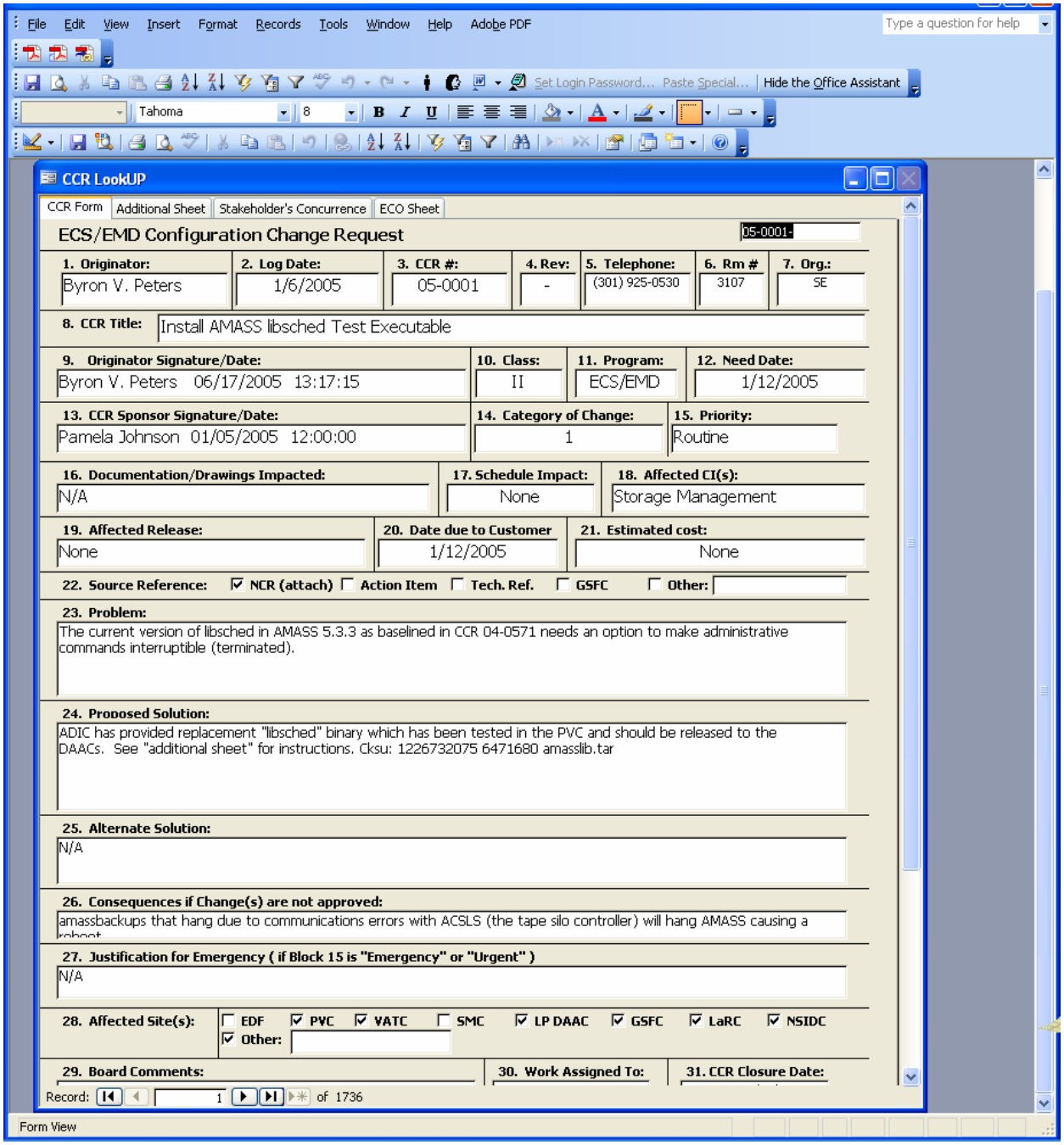
(indicate attachment ___)

15. Board Action: ☐ Approved ☐ Withdrawn ☐ Disapproved ☐ Deferred Until_____
date
Further Action Required: ☐ ECP ☐ Waiver ☐ Deviation ☐ Tech Direction ☐ Contract Mod. ☐ DCN Other:_____

16. CCB Approval
Chair:_____ _____
signature date

17. CCR Implemented
CM Admin. signature:_____ date:_____

Figure 9.2-1. ESDIS Configuration Change Request (CCR) Form



CCR LookUP

CCR Form | Additional Sheet | Stakeholder's Concurrence | ECO Sheet

ECS/EMD Configuration Change Request 05-0001-

1. Originator:	2. Log Date:	3. CCR #:	4. Rev:	5. Telephone:	6. Rm #	7. Org.:
Byron V. Peters	1/6/2005	05-0001	-	(301) 925-0530	3107	SE

8. CCR Title: Install AMASS libsched Test Executable

9. Originator Signature/Date:	10. Class:	11. Program:	12. Need Date:
Byron V. Peters 06/17/2005 13:17:15	II	ECS/EMD	1/12/2005

13. CCR Sponsor Signature/Date:	14. Category of Change:	15. Priority:
Pamela Johnson 01/05/2005 12:00:00	1	Routine

16. Documentation/Drawings Impacted:	17. Schedule Impact:	18. Affected CI(s):
N/A	None	Storage Management

19. Affected Release:	20. Date due to Customer	21. Estimated cost:
None	1/12/2005	None

22. Source Reference: ☑ NCR (attach) ☐ Action Item ☐ Tech. Ref. ☐ GSFC ☐ Other:

23. Problem:
The current version of libsched in AMASS 5.3.3 as baselined in CCR 04-0571 needs an option to make administrative commands interruptible (terminated).

24. Proposed Solution:
ADIC has provided replacement "libsched" binary which has been tested in the PVC and should be released to the DAACs. See "additional sheet" for instructions. Cksu: 1226732075 6471680 amasslib.tar

25. Alternate Solution:
N/A

26. Consequences if Change(s) are not approved:
amassbackups that hang due to communications errors with ACSLS (the tape silo controller) will hang AMASS causing a reboot

27. Justification for Emergency (if Block 15 is "Emergency" or "Urgent")
N/A

28. Affected Site(s): ☐ EDF ☑ PVC ☑ VATC ☐ SMC ☑ LP DAAC ☑ GSFC ☑ LaRC ☑ NSIDC ☑ Other:

29. Board Comments:	30. Work Assigned To:	31. CCR Closure Date:

Record: 1 of 1736

Form View

Figure 9.2-2. EMD Configuration Change Request (CCR) Form

The following enumerated text corresponds to the numbered items on the CCR form:

(1) **Change Control Board (CCB) --** The designated CCB is checked-off for changes processed by the ESDIS Change Control Board (CCB) and its EMD site-level chartered

CCBs at the SMC, EOC, and DAACs (GSFC(GES), LaRC (ASDC), EDC (LP DAAC) and NSIDC).

(2) **CCR Number --** The unique serialized CCR number is applied at each site.

(3) **Submitted Date --** The date that the CCR was prepared is documented.

(4) **Revision --** The current revision is designated for tracking changed versions of original CCR.

(5) **Priority --** The priority level of the CCR is assigned. Emergency CCRs may have already been implemented on a temporary basis by the Trouble Ticket Review Board (TTRB) with concurrence from the CCB Chair who later receives the CCR to document /implement the permanent change. Urgent items will be reviewed by the next CCB meeting. Routine items will be reviewed as soon as the schedule permits.

(6) **Change Class --** Change Classes are either I or II. Class I will be handled by ESDIS-only because of cost, schedule, and/or mission impacts that may require requirements changes. Class II items do not affect mission requirements, but may have cost and/or schedule implications which affect maintenance, operations, procedures, documentation, site-tailored items, COTS implementation, site installations of core system changes, science SW changes, etc.

(7) **Status --** Table 9.2-1 is a summary of the workflow of events (Figure 9.2-3) of the CCR states as defined in the TestTrack Pro defect tracking database tool (which implements the Change Request Manager). Note that the hard copy form will not be updated chronically, but will be kept in the master suspense file of the CM Administrator until stamped closed-out (item #7 & 15) and appropriate signatures (viz., items 16, & 17) are acquired.

Table 9.2-1. State Table Composition in TestTrack Pro Format

State	Event
Open	Open – Initial Escalation from DAACs
Assigned	Assign
Estimate	Estimate
Start Work	Start Work
Fix	Fix
Merged	Merge
Tested (Integration)	Test
Verified (PVC/DAAC)	Verify (PVC/DAAC)
Verified (Failed) as Open	Assign, Open, Defer, Close
Verified (PVC/DAAC) as Closed	Close, Deliver

Transition (NCR State)	Transition (NCR Event)	Action or Allowed Next Events
Pending (PRB review) ⇒ **Open**	Initial state of NCR escalated from DAACs– Open	Perform initial review
Open ⇒ **Assigned**	Assign	Problem assigned to engineer(s) for technical assessment; cost/schedule/impact
Open (assigned) ⇒ **Estimate**	Estimate	Determined/Enter workaround information, if applicable; record cost, schedule and impact information; Technical Assessment Approval
Open (assigned) ⇒ **Start Work**	Start Work	Work on fix has begun
Open (assigned) ⇒ **Fix**	Fix	Fix has been built, installed and is ready for testing
Fixed ⇒ **Merged**	Merge	After merge approved, maintenance engineer merge code (to Baseline(s) 1, 2, 3)
Merged ⇒ **Tested (integration)**	Test	Product has undergone integration testing in test environment (PVC, VATC, EDF); ready for verification testing
Tested (integration) **Verified (PVC/DAAC)**	Verify (PVC/DAAC)	Fix was verified by Test; added test procedure (results of a fix verification); Quality verification of fix; delivery and closure recommended
*Verified (Failed) ⇒ **Open***	*Assign, open, defer, close*	*Fix failed verification testing and can be re-worked, deferred, or closed*
Verified (PVC/DAAC) ⇒ **Closed**	Close, Deliver	With PRB/DAAC Approval –directed that problem be closed

Figure 9.2-3. TestTrack Pro Workflow of Events

Explanations of DDTS' State Table Content:

Uppercase character in the 1st column is the character stored in the change request record to indicate what state a change request is in. DDTS uses this character to go into the table and extract the descriptive name for display in reports.

Names in the second column are the state in the present tense. They are shown on the DDTS list of states that are available for selection during input. It's also used by some of DDTS' query and report code. It facilitates querying based on descriptive names opposed to a single letter.

Names in the third column are the state in the past tense. They are shown on the DDTS change request record. It's also used by some of DDTS query and report code. It facilitates querying based on descriptive names opposed to a single letter.

Definitions (a state is the stage that a proposed change has reached in its life cycle.):

New - the initial state for all newly entered change requests.

Assign-Eval- state entered when the change request is being assigned to an engineer for evaluation/analysis.

Assign-Implement- state entered when the change request is being assigned to an engineer for development.

Implement-state entered when the proposed change has been developed.

Assign-Verify-state entered when the developed change is being assigned to an engineer for verification testing.

Verify- state entered when a developed change has been tested and verified that it functions properly.

Close- state entered when all activity specified in the change request has been completed or that the approval authority has decided to close it prior to completion of all activity.

Duplicate-state entered when a change request is determined to be a duplicate of an existing change request. Duplicate change request identifies change request being duplicated.

Forward-state entered when a change request needs to be forwarded to another DDTS defined project (In DDTS terminology, a project is a grouping of change requests. For example, a change request from a site project can be forwarded to an EMD project.).

Defer- state entered when activity on a change proposal has to be postponed.

(8) **CCR Title --** The CCR title is supplied by the originator.

(9) **Originator --** The originator name, organization, e-mail address, and phone number is given.

(10) **Approval --** The CCR is approved by the designated management authority that is assigned by the CCB. This sponsorship requirement acts as a primary filter to eliminate from consideration those CCRs that cannot be implemented or which have no EMD site management support.

(11) **Reason for Change --** The reason for the change is narrated on the form and/or the designated attachment.

(12) **Description of Change --** The proposed implementation of the change is narrated along with any known impacts, resources, and expenses to be incurred.

(13) **Impact Analysis --** Impact analysis is documented in the form of Figure 9.2-4 and Figure 9.2-5. The impact analysis is collected by the CCB Chair appointed Evaluation Engineer in coordination with the CM Administrator who maintains the CM records and assembles the review package for the CCB. The Evaluation Engineer documents the list of Impact Evaluators and derives and/ or verifies cost, technical, and schedule impact of the proposed change based on all inputs received. The results of the coordinated CCR Impact Analysis inputs are presented in the CCR Impact Summary form shown in Figure 9.2-4 part of the CCR review package.

(14) **Comments** -- Comments are added to the CCR to summarize sites and/ or organizations affected by the CCR. Additional comments may address proposed CCB dispositions and recommendations to be indicated by resolutions in item #15.

(15) **Board Action --** CCB actions and follow-up actions that will be facilitated and tracked by the CM Administrator are indicated. Possible CCB dispositions are given as

approved, withdrawn, disapproved, and deferred (pending follow-up activities by the indicated schedule date). Further actions are indicated as:

- Engineering Change Proposal (ECP)- changed scope of contract requirements
- Waiver-- declaration that certain contract requirements no longer apply
- Deviation-- change of contract terms or substitution of terms or deliverable requirements
- Technical Direction-- order by Contracting Officer's Technical Representative (COTR) to perform certain tasks within the scope of the contract
- Contract Modification-- changes to the terms of a contract
- Document Change Notice (DCN)- notification of changes to published documents
- Others-- Engineering Change Notice, Change Order, Escalate to higher CCB authority, etc.

(16) **CCB Approval --** CCB approval signature authority by CCB Chair or designate.

(17) **CCR Implemented --** This signature and close-out stamp (item #7) are executed by the CM Administrator witnessing the completion of the CCR implementation process which is tracked in the Change Request Manager automated tool DDTS and updated in Baseline Manager for affected version control status changes.

CCR Impact Analysis

Responder Request Number: ____
Responder:_____
Responder Point of Contact:
address:_____
_____
phone:_____
e-mail:_____
CCB Schedule Date:_____
CCR Number:_____
CCR Log Date:_____
CCR Originator:_____
CCR Originator Point of Contact:
address:_____
_____
phone:_____
e-mail:_____

Evaluation Engineer:_____
Evaluation Engineer Point of Contact:
address:_____
_____
phone:_____
e-mail:_____
Requested Return Date:_____

Rough Order of Magnitude (ROM) Impact Analysis

Basis of Estimate:

Technical Assumptions and Comments:

Cost Impact:
None [ ]
Small [ ] < $ 100, 000
Medium [ ] $100,000 < x < $500,000
Large [ ] > $500,000

Schedule Impact:

Technical Assessment: (Your impact analysis should consider the implementation approach; interfaces affected; HW or SW changes required; documentation changes required-- change from/to pages; suggested alternatives, if any; and impact to security features. If your system is not impacted, please provide that information to the CM Administrator.)

Comments:

Signed:_____
(Responder)

Date:_____

Figure 9.2-4. EMD CCR Impact Analysis (Part 1)

CCR Impact Summary

Evaluation Engineer:_____
Evaluation Engineer Point of Contact:
address:_____
_____
phone:_____
e-mail:_____
CCR Board Date:_____

Resources Summarized:

Technical Summary:

ROM Summary (BOE, Cost, and Schedule):

Recommendation:

Signed:_____
(Evaluator)

Date:_____

Figure 9.2-5. EMD CCR Impact Summary (Part 2)

9.2.4.2 Change Control Board Process (System and Site-level CCBs)

The EMD organization will provide administrative and technical support services for the CCB at each site. Each site's CCB is controlled by the host site organization and provides the authority and direction for the EMD contractor to modify the operational baseline. The ESDIS CCB has chartered an EMD Review Board to coordinate EMD system-level changes and problem management via the EMD contractor and on-site Review Boards that also act as site CCBs. This is illustrated using the CM Administrator's workflow for the sustaining engineering support of the EMD Review Board in Figure 9.2-6 and the On-Site CM Administrator's workflow for sustaining engineering support of the on-site CCB in Figure 9.2-7. The problem management process was discussed in detail in Chapter 8 of this document. Both diagrams illustrate the flow of CCRs through the respective CCBs with inputs from the review boards and evaluators that determine the disposition of proposed changes. Details of this process are given below:

System-level Change Control Procedures

(The enumeration corresponds to the diagram of Figure 9.2-6)

(1) Configuration Change Requests are received by the EMD CM Administrator from all sources with regard to the operational EMD Core System as described in Section 9.2.4.1. These changes designated as from other sources could involve system enhancements, procedures, interfaces (both external and internal), documentation changes, etc. that are not the subject of contemporaneous problem reports which would be first deliberated by the Trouble Ticket Review Board (TTRB) and/or Failure Review Board as explained below.

(2) Proposed common baseline changes will be proposed based on Trouble Ticket (TT) resolutions obtained from the respective review boards (see Chapter 8 for details). The respective TT would be closed via a corresponding CCR to either ratify, i.e., to make permanent the prior temporary/emergency action taken by the TTRB or to consider normal priority (scheduled) changes for incorporation into future change releases.

(3) The EMD CM Administrator is responsible for logging the CCR into the Change Request Manager.

(4) The CCB chair assigns an evaluator and the EMD CM Administrator coordinates impact assessment.

(5) Class I change requests (proposed changes that affect controlled milestones, schedules, budget, cost and requirements) are forwarded to the ESDIS CCB for consideration with recommendations from the EMD Review Board.

(6) Class II change requests (proposed changes affecting documentation, hardware [alternative use of], software [correction of errors], and COTS substitution without a Class I impact) are considered by EMD Review Board deliberations.

(7) Notice of proposed changes is distributed to affected parties and review board members to obtain and coordinate impact assessment and optimize the approach to implement proposed changes.

(8) The results of EMD Review Board deliberations are factored into review board resolutions which determine whether, when, or where the system changes will be implemented.

(9) Approved changes are processed by the EMD CM Administrator to the support activities, i.e., site CCBs, support personnel (EMD), vendors, etc. who are provided with change orders, schedule, and implementation instructions.

(10) Disapproved changes are processed by the EMD CM Administrator via official notifications, memo to the file, and update of the Change Request Manager (CRM).

(11) The EMD CM Administrator tracks implementation and closure of CCRs via directions to implementing organizations and their acknowledgements using the CRM tracking and statusing features.

(12) New versions and/or maintenance updates are annotated in Baseline Manager at the SMC and at the affected sites by following the procedures for configuration identification, activation dates, deactivations dates, and issuing version description documents.

(13) Simultaneously, the SW Change Manager (ClearCase) is updated with directory trees, installation files, and software as required by SW maintenance.

(14) Status of this activity to implement changes and assigned responsibilities is tracked through closure in the CRM at SMC and at the sites.

(15) The databases are synchronized by manual checking between applications Baseline Manager vs. CRM vs. SW Change Manager) and automated verification by the SW CM Manager for purposes of SW distribution and maintenance.

(16) The TT Review Board is empowered to make emergency fixes without common baseline changes and update these changes directly to Baseline Manager with documentation to follow via the CCR submitted to the appropriate CCB. Proposed common baseline changes must be submitted by CCR to the EMD Review Board.

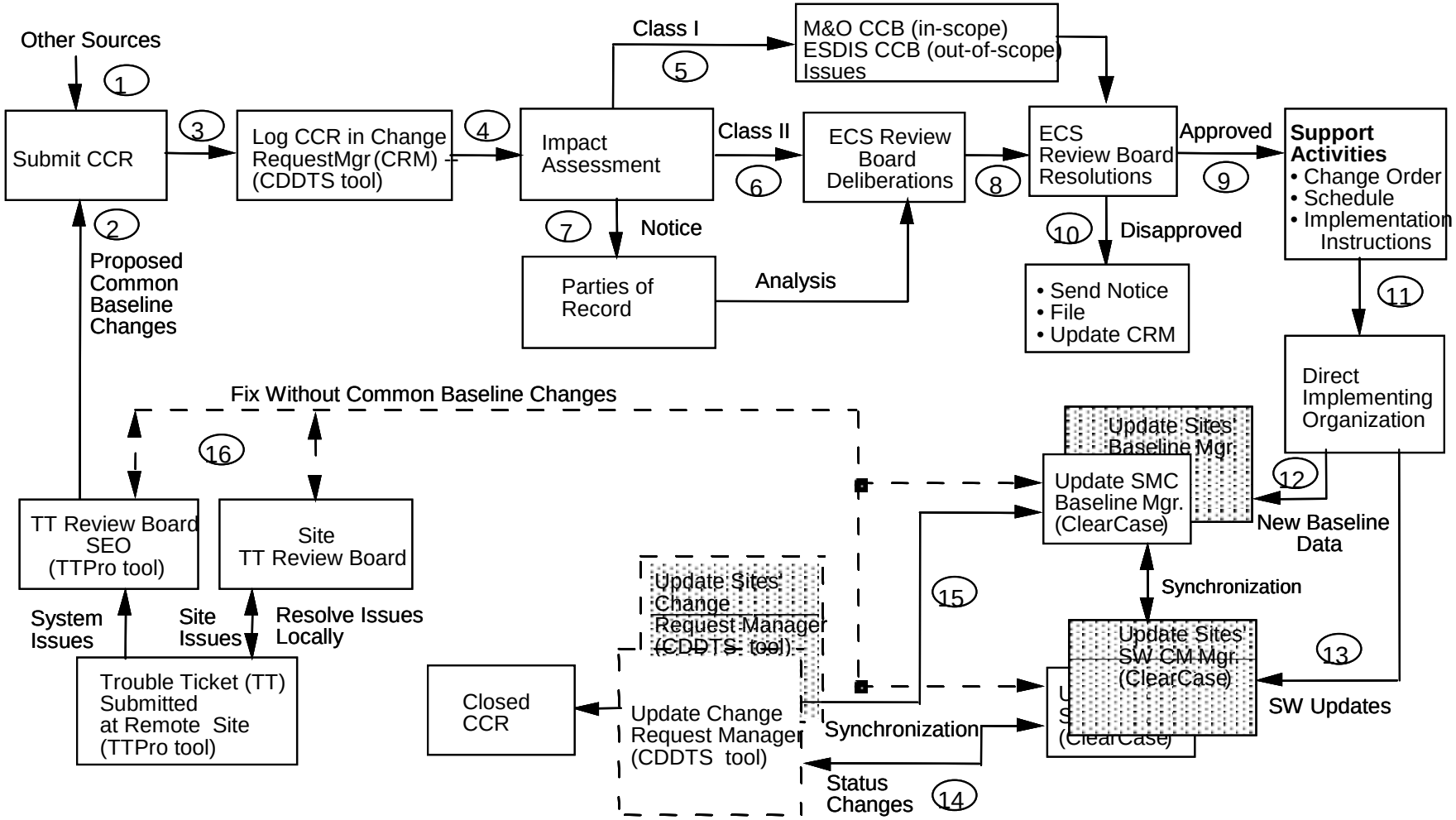


Figure 9.2-6. Workflow Diagram for EMD CM Administrator

Site-level Change Control Procedures

(The enumeration corresponds to the diagram of Figure 9.2-7)

(1) Configuration Change Requests are received by the Site CM Administrator from all sources with regard to the **site unique extensions** to the operational EMD Core System as described in Section 9.2.4.1. These changes designated as from other sources could involve system enhancements, procedures, interfaces (both external and internal), documentation changes, etc. that are not the subject of contemporaneous problem reports which would be first deliberated by the Site/ EMD Trouble Ticket Review Board (TTRB) and/or Failure Review Board as explained below.

(2) Proposed site baseline changes will be proposed based on Trouble Ticket (TT) resolutions obtained from the respective review boards (see Chapter 8 for details). The respective TT would be closed via a corresponding CCR to either ratify, i.e., to make permanent the prior temporary/emergency action taken by the TTRB or to consider normal priority (scheduled) changes for incorporation into future change releases.

(3) The Site CM Administrator is responsible for logging the CCR into the Change Request Manager.

(4) The CCB chair assigns an evaluator and the Site CM Administrator coordinates impact assessment.

(5) Class I/System Issues change requests (proposed changes that affect controlled milestones, schedules, budget, cost and requirements) are forwarded to the EMD Review Board for consideration with recommendations from the Site CCB. Class I issues are further forwarded with recommendations by the EMD Review Board to the SCDV CCB for in-scope issues and to the ESDIS CCB for consideration of out-of scope issues with respect to the SOW of the EMD Contract.

(6) Class II change requests (proposed changes affecting documentation, hardware [alternative use of], software [correction of errors], and COTS substitution without a Class I impact) are considered by Site CCB deliberations.

(7) Notice of proposed changes is distributed to affected parties and review board members to obtain and coordinate impact assessment and optimize the approach to implement proposed changes.

(8) The results of Site CCB deliberations are factored into CCB resolutions which determine whether, when, or where the system changes will be implemented.

(9) Approved changes are processed by the Site CM Administrator to the support activities, i.e., other CCBs, support personnel vendors, etc. who are provided with change orders, schedule, and implementation instructions.

(10) Disapproved changes are processed by the Site CM Administrator via official notifications, memo to the file, and update of the Change Request Manager (CRM).

(11) The Site CM Administrator tracks implementation and closure of CCRs via directions to implementing organizations and their acknowledgements using the CRM tracking and statusing features.

(12) New versions and/ or maintenance updates are annotated in Baseline Manager at the affected sites and the SMC by following the procedures for configuration identification, activation dates, deactivations dates, and issuing version description documents.

(13) Simultaneously, the SW Change Manager (ClearCase) is updated with directory trees, installation files, and software as required by SW maintenance.

(14) Status of this activity to implement changes and assigned responsibilities is tracked through closure in the CRM at the sites.

(15) The databases are synchronized by manual checking between applications Baseline Manager vs. CRM vs. SW Change Manager) and automated verification by the SW CM Manager for purposes of SW distribution and maintenance.

(16) The on-site TT Review Board is empowered to make emergency fixes without common baseline changes and update these changes directly to Baseline Manager with documentation to follow via the CCR submitted to the appropriate CCB. Proposed common baseline changes must be submitted by CCR to the EMD Review Board.

Each site's CCB accepts initial release or updates from the ESDIS CCB. Similarly, the Distributed Active Archive Center (DAAC) CCBs will accept product generation software from an ESDIS authority. Local tailoring and installation decisions are determined by the site CCB.

In the case of Evaluation Package (EP) and Prototype deliveries, the EMD CCB as directed by ESDIS will provide a configured, documented, executable with supporting files. Again, installation decisions are determined by the site CCB.

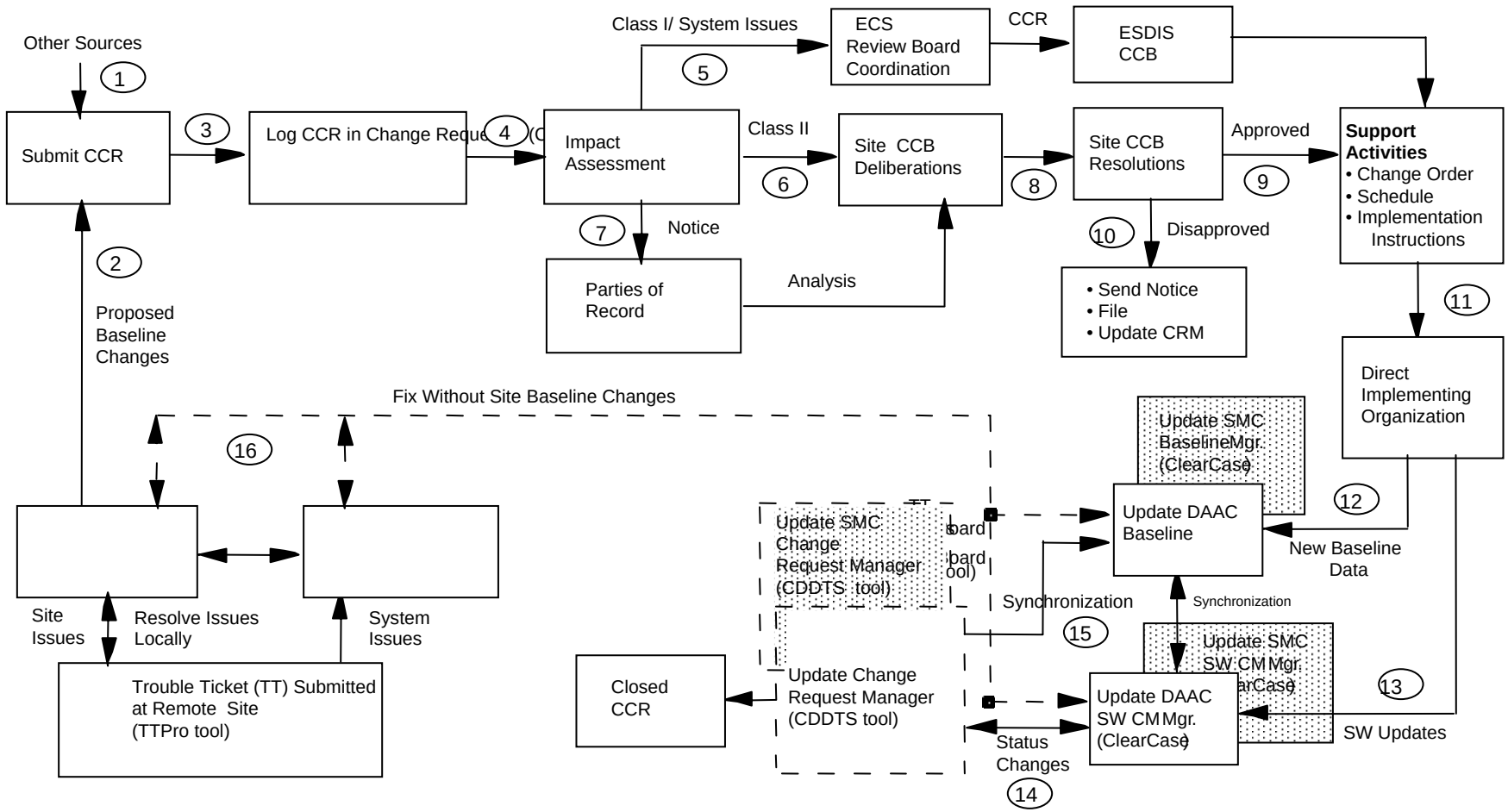


Figure 9.2-7. Workflow Diagram for Site-level CM Administrator

Each Science Computing Facility (SCF) is assumed to have a configuration control function. For commonality with other sites, it is assumed that this function will be performed by a CCB. A major difference, though, is the EMD contractor does not have an active role in the support of this CCB.

The SCF CCB will provide two types of configuration control:

(1) Configuration control of software and databases that are to be executed in another site's environment. In this mode, it operates very much as the EMD CCB does to establish a product baseline.

(2) Configuration control of SCF resources that are made available to the EOSDIS community. In this mode, its functions are the same as a DAAC CCB.

The EMD CM function at each DAAC will accept science SW and data items from the SCF CCB. These items will be incorporated into the DAAC's operational baseline as directed by the DAAC CCB.

The EOC CCB will control the operational configuration of the required EOC operational baseline. EMD CM will provide services as directed by the CCB.

The EMD Review Board will be charged with the responsibility for centralized coordination and control of EMD CM activities to ensure:

- EMD integrity and quality of service
- Successful coordination with both internal and external networks, systems, and on-site facilities
- Timely ESDIS CCB visibility into and oversight of EMD operations
- Convenient user administrative services

9.3 Configuration Status Accounting Procedures

9.3.1 Purpose

Operational phase configuration status accounting (CSA) consists of recording and reporting information about the configuration status of the EMD Project's documentation, hardware and software throughout the Project life cycle. Periodic and ad hoc reports keep ESDIS informed of configuration status as the operational mission evolves. Reports to support reviews and audits will be extracted as needed starting from the RRR.

The Baseline Manager tool described in Section 9.7 records and tracks as-built products designated as EMD control items (i.e., custom, COTS, science, toolkit, etc.) SW and HW items along with their associated documentation and records) and historical versions of EMD operational configurations. Baseline Manager, which is updated with the acceptance tested version of the EMD baseline at RRR, records and reports EMD document change status and histories, mission milestone baselines, and change status.

CSA entails maintaining version histories of delivered and maintained products as well as histories of operational baselines and changes made to each baseline. Additionally, CSA tracks the status of proposed changes from initial CCR submission to ultimate disposition and/or implementation. CSA also maintains historical records of CCRs.

9.3.2 Applicability

All ESDIS chartered CCBs

9.3.3 References

ESDIS CM Plan

EMD Configuration Management Plan 110-EMD-001

9.3.4 Procedures

The following are topical items subject to periodic or ad hoc reporting on behalf of the respective CCB or a system-level summary of information that will be reported by the CM Administrator representing the operational baseline for all the EMD sites.

(a) **New CCRs and Revisions.** This is a standard Change Request Manager report. This report will be issued monthly and summarized annually.

(b) **CCB Review.** Distribute CCR copies for review (and Impact Analysis forms if applicable). Print the agenda and distribute prior to the meeting.

(c) **Open Action Items.** Open action items should be statused regularly between meetings. The CCR tool provides reports of Open Action Items (ECOs) for the DAACs and Riverdale.

(d) **CCB Meeting.** Record the CCB's disposition of each CCR. CCB meetings are no longer held. All CCR information is accessible from the CCR tool.

(e) **Record Action Items.** Record actions, assignments, and due dates.

(f) **CM Librarian Maintained Document Changes.** When all authorized document changes have been accomplished prepares DCN, post the final version on the EMD Document Data Server and distribute hardcopy as required.

(g) **Minutes Distribution.** CCR approvals are performed with email from the CCR tool.

(h) **CCR Implementation Status.**

- After CCB disposition, regularly status opens CCRs until closure.
- Class I events include: CCR to EMD Review Board for review/approval; Technical Review Board; and ESDIS Disposition
- Further events are as follows for implementation status: Consent Obtained; Item Received; Installed; Document Completed; etc.

- CCR CLOSED: A Class I CCR is not closed until the ESDIS contract officer's authorization is received or the reference CCR has been withdrawn.
- Class II document change CCRs may be closed with the CM Administrator's issuance of the DCN.
- Other non-document change CCRs may be closed when the originator verifies to the CM Administrator that all specified changes have been implemented.

9.4 Configuration Audits

9.4.1 Purpose

EMD will support Physical Configuration Audits (PCAs). EMD will also support audits by ESDIS and our own Quality Office functions. Internal CM self-audits will be conducted by EMD. Self-audits evaluate the Project's compliance with the Configuration Management Plan for the EMD Project and the ESDIS CMP. The CM self-audits will verify:

- That CM policies, procedures, and practices are being followed.
- That approved changes to documentation, and to software and hardware products are properly implemented.
- That the baseline documentation of each CI agrees with the as-deployed configuration and that adequate records of differences are available at all times.

A post-audit report is written outlining the specific items audited, audit findings, and corrective actions to be taken. All action items are tracked to closure.

In addition, EMD supports formal audits scheduled and conducted by ESDIS. These audits are conducted to validate that each EMD CI is in conformance with its functional and performance requirements defined in the technical documentation. The audits validate that:

- The as-built configuration compares directly with the documented configuration identification represented by the detailed CI specifications.
- Test results verify that each EMD product meets its specified performance requirements to the extent determinable by testing.
- The as-built configuration being shipped compares with the final tested configuration. Any differences between the audited configuration and the final tested configuration are documented.
- When not verified by test, the compatibility of EMD products with interfacing products or equipment is established by comparison of documentation with the interface specifications that apply.
- COTS products are included in audits as integral parts of the EMD baseline.

9.4.2 Applicability

All ESDIS chartered CCBs

9.4.3 References

Configuration Management Plan for the EMD Project 110-EMD-001

9.4.4 Procedures

The audits are standardized for a limited set of issues that drive the process for which the audit is taken, FCA/PCA, Security Issues, General Accounting, Test Readiness Review, or Operational Certifications. The baseline references for the audits will be maintained by the ClearCase Baseline Manager tool (cf. Section 9.7). Release Notes documents will be used to document auditable changes to configured articles that are issued at the EMD configuration item (CI) level. Audit processes, including Project Instruction documentation, are discussed in the *Configuration Management Plan for the EMD Project*, 110-EMD-001.

The release notes will contain the prioritized current status summary of any Trouble Tickets/Discrepancy Reports against the CI that is being issued per the change request.

Some general guidelines and/or items that must be tailored for the specific size and scope of configuration audit to be conducted include:

(a) Audit Plan;

(b) Conference Agenda;

(c) Location to collect and analyze data; conduct meetings;

(d) Applicable specifications, drawings, manuals, schedules, design and test data;

(e) Test Results Analysis;

(f) Meeting minutes including resulting audit action items;

(g) Tools and inspection equipment necessary for evaluation and verification;

(h) Unencumbered access to the areas and facilities of incoming inspection, fabrication, production, and testing;

(i) Personnel from each engineering, production, and quality department to be available for discussion of their respective areas;

(j) Copies of inspection reports, process sheets, data sheets, and other documentation deemed necessary by the Government FCA/ PCA teams; and

(k) Isolation of the item(s) and detailed parts to be reviewed.

9.5 Archiving Procedures for the SW CM Manager (ClearCase)

9.5.1 Purpose

This section details the concerns and procedures used by Configuration Management for the backup of ClearCase Version Object Base, public storage area for files (VOB) data.

9.5.2 Applicability

All EMD CM Administrators, SW Maintenance Engineers, and Sustaining Engineers

9.5.3 References

EMD Configuration Management Plan 110-EMD-001

9.5.4 Definitions

Build - an assemblage of threads to produce a gradual buildup of system capabilities.

EMD Development Facility (EDF) - the software development environment including data, hardware, software, networks, facilities and procedures used to support EMD software development and testing.

Software - for the purposes of this instruction, software includes all EMD-developed application software, COTS software, build and environmental instructions, and databases used in the execution of these products.

System-level - for the purpose of this instruction, system-level includes all EMD integration and test activities beginning with installation of software.

Software Development File - a repository for a collection of material pertinent to the development or support of software.

Thread - a set of components (software, hardware, and data) and operational procedures that implement a scenario, portion of a scenario, or multiple scenarios.

View - a unique workspace (operator private storage) management or “sandbox management” that provides developers with transparent, file-level access to any version of any element through the use of dynamically-evaluated, user-specified version selection rules.

VOB - Versioned Object Base. Secure, permanent, virtual file system that is mountable. Repository for public area storage of version-controlled data/files.

9.5.5 General

1. IT Infrastructure maintains a backup for all EMD systems. This procedure documents the additional steps CM has taken to ensure that the Infrastructure backups include the nightly backup of the ClearCase Versioned Object Base (VOB) Data. These VOBs store all versions of all of all custom software developed for the EMD project. In the event of a catastrophic failure, everything can be restored from the VOB data.

2. There is a cron job that runs on each VOB server (sweat, tears, nelix, janeway and triton) at 11:55 pm as the user id "vobadm" to lock down the individual VOBs (necessary to flush the database caches back to disk, in order to obtain a valid file for backup), tar up important VOB storage directories (the entire source pool, and the local copies of the VOB storage directories, which includes the VOB databases), and copy that data across the network to a staging area (located in /tools/ccbackup) along with log files of the backup process. This process takes approximately 55 minutes.
3. The staging area is then backed up by IT Infrastructure using their standard backup procedures. IT Infrastructure maintains it's own process of offsite storage for the EMD systems backups.
4. For EMD Evolution, the ClearCase view servers and VOB servers have been moved from Solaris 8 hosts to Linux hosts. A noted benefit of the porting of ClearCase has been speed. ClearCase functions now execute between 40-80 times faster, due to the host network interface improvements (x10) and the much faster processors. This primarily covers compilations and file preparations.

9.5.6 Procedures

No additional procedures are needed on Configuration Management's part.

9.6 Software Delivery and Installation

9.6.1 Purpose

This section describes the delivery of Sustaining Engineer Organization-developed software from the Landover facility to a remote site (a DAAC), and subsequent installation of the software onto target hosts, in accordance with configuration management controlled processes. The process begins with an approved CCR. The CCR precisely defines the software to be released to the remote sites. Software is prepared and delivered using the *DeliveryTool*. The *DeliveryTool* is a custom ClearCase tool that was developed to ensure accurate and controlled release of software. Software installation is controlled by each sites' Configuration Change Board (CCB). Landover CSG prepares and releases the software to the DAACs, but the DAACs control the installation of the software into their operational modes.

9.6.2 Applicability

All EMD sites' Sustaining Engineers, System Administrators, CM Administrators, and Maintenance Engineers

9.6.3 References

Configuration Management Plan for the EMD Project	110-EMD-001
COTS and Custom Software Preparation and Delivery	CM-1-032-1

9.6.4 Procedures

9.6.4.1 Overview

This section describes the release of CM controlled software under the authority of the SCDV CCB's approved CCRs.

Assumptions:

- CM maintains records of software preparations and deliveries.
- Baseline records are maintained in the Baseline Manager (ClearCase tool)
- Electronic Delivery is performed via Secure Copy (scp) to target DAACs.
- Resource Planning, Mode Management, and other issues are not addressed in this scenario.

Summary of Procedures:

- Software is prepared delivered using a CM operated DeliveryTool. An approved CCR specifies which previously prepared software is to delivered and to which sites. Refer to CM-1-032-1, COTS and Custom Software Preparation and Delivery
- DAAC CCB Approves the Installation of the delivered software into a DAAC Operational Baseline (e.g., a mode, "OPS", "TS1", etc.)
- Software is installed in accordance with CCR installation instructions, and in accordance with local DAAC procedures/processes
- Delivery Tracking pages are maintained by EMD CM, located at:

http://pete.hitc.com/baseline/

LPDAAC	http://e0ins01.edcb.ecs.nasa.gov:10160/baseline/
GES	http://g0ins01.gsfcb.ecs.nasa.gov:10160/baseline/
LaRC	http://l0ins01.larc.ecs.nasa.gov:10160/baseline/
NSIDC	http://n0ins02u.ecs.nasa.gov:10160/baseline/
SMC	http://m0mss16.ecs.nasa.gov:10160/baseline/

9.6.4.2 Functional Roles

EMD CM Administrator--Ensures that changes to the hardware, software, and procedures are properly documented and coordinated. Recommends configuration of all EMD configured hardware and software.

DAAC/SMC CM Administrator--Ensures that changes to the hardware, software, and procedures are properly documented and coordinated. Maintains control of all configured hardware and software. Assists in the development and administration of the library with respect to local configuration management procedures.

DAAC Sustaining Engineering--SW Maintainer--Produces, delivers, and documents the corrections, modifications, and enhancements made to EMD software (including COTS), and/or adaptations or incorporations of EMD COTS software.

9.7 Baseline Manager

9.7.1 Overview

The EMD provides a *ClearCase* Baseline Manager (BLM) tool to assist in documenting changes to the baseline, and to maintain a historical record of those changes. The tool is used by CM Personnel to manage baseline data about resources deployed to all external ECS sites, including the DAACs and the SMC, as well as the three internal ECS sites, the PVC, and the EDF2 string (Evolution). The BLM tool is used at the EMD Development Facility to maintain system-level records and site-level records; baseline reports are accessible at the operational sites by accessing the URL http://pete.hitc.com/baseline/. This is the EMD Baseline Information System (EBIS). Each site has a replicated EBIS that is served locally. Selection of the "Technical Documents" button provides detailed reports regarding the EMD baseline. As part of Evolution, the Solaris 8 host "pete.hitc.com" has been replaced by Linux host "c4cbl02.hitc.com". To maintain transparency to the EDF users, an alias was created so that the usual EBIS URL could be used. The EDF EBIS though is now served from Linux host "c4cbl02.hitc.com".

9.7.2 Baseline Terms and Concepts

Baseline management is a process to identify and control versions of hardware and software, to provide a standard configuration of systems throughout all sites, and allow unique site-configured systems and baselines. It identifies interdependencies between hardware and software items, and permits maintenance of a complete history of baseline changes throughout the life of the project. For EMD baseline management and BLM tools, certain terms and concepts are key to understanding how data on the system baseline are stored and tracked.

Control Item –	any EMD item under version control by Configuration Management.
Configuration Item –	an aggregation of hardware, firmware, software, or any discrete component or portion, which satisfies and end user function and is designated for configuration control.
Baseline –	a configuration identification document or set of such documents formally designated by the Government at a specific time during the life cycle of a configuration item (CI).
Configured Article –	a control item reportable as part of the Configured Articles List (CAL).
CIL –	a Configuration Items List (CIL) identifies the approved set of CIs that are subject to CM requirements and procedures.

CAL – a Configured Articles List (CAL) describes all CIs, critical item hardware and software, and supporting documentation by which the exact configuration definition of the hardware and software can be determined.

Additional terms, some of which address specific entries in the BLM tool, further define how data on the system baseline items and structure are tracked.

Assembly – An item made up of other items.

Bill of Material – The list of items that comprise an assembly.

Product Structure – The parent-child pairings that define the bill of material for an assembly; each product structure record specifies the effective dates and quantities for a single component of a parent for each engineering change.

Active Date – The date a component becomes effective in an assembly's bill of material. This date is the CCR approval date.

Inactive Date – The date a component is no longer effective in an assembly's bill of material. This date is when a new CCR displaces or affects the item.

Engineering Change – A mechanism for grouping, reporting, and controlling product changes collectively.

Revision – The sequence number of a product structure change to an assembly; it signifies a change to the configuration of an assembly that does not alter its form, fit, or function.

Implementation Status – A record describing the deployment of a control item to a site and the current state and associated date of its implementation; each control item has one record for each site to which it is deployed.

Exporting Data – Creating a formatted file or records extracted from the BLM database; control item engineering change, product structure, and interdependency records may be extracted and sent to other application software at any site.

Importing Data – Loading BLM data from a formatted file.

At the lowest level, the baseline is composed of configured articles that are the specific types of items that make up EMD and are tracked using the BLM tool. It is important to recognize, however, that we impose a conceptual structure on those configured articles to help us think about the system. In fact, it is possible to conceptualize the structure of the system in a number of different ways, and we may select a different conceptual structure based on the requirements of the situation. The EMD baseline management approach and the BLM tool permit recording and tracking these different conceptual baselines, which can be related to the same records of the configured articles.

For example, system designers may conceptualize the system in terms that will help them track subsystems and the configuration items for which each subsystem team is responsible. This may produce a baseline structured according to a design view, such as that shown in Figure 9.7-1.

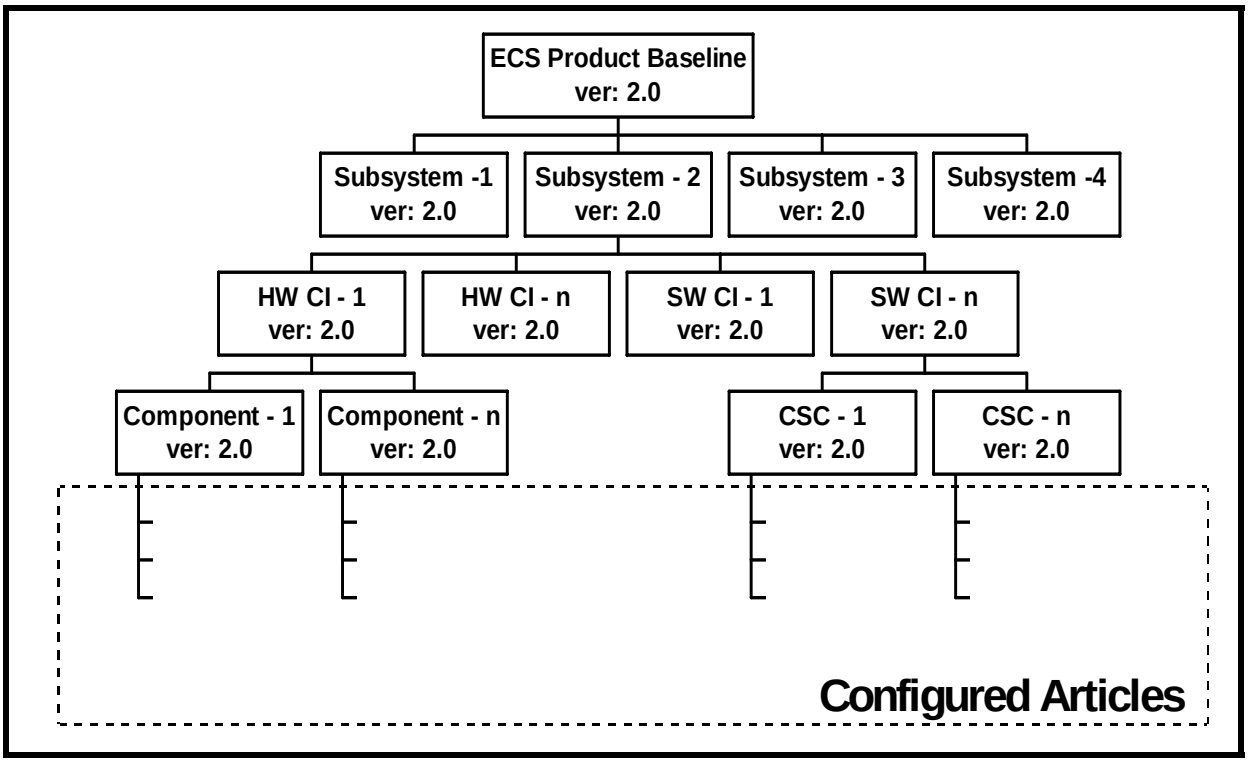


Figure 9.7-1. EMD Baseline Concept from a Design (CIL/CAL) View

At an operations site, the concept reflected in the upper layers of the Design View baseline structure may not be particularly useful. Although the same configured articles are involved, it may be desirable, for instance, to track items from the viewpoint of network administration. The resulting baseline product structure may reflect that shown in Figure 9.7-2.

Even if an operations site is to view EMD product structure as composed of subsystems, it is likely that the concept of CIs will be of little use. Instead, the site is likely to be focused on what hosts make up the subsystems. Therefore, the subsystem view at an operations site may be similar to that illustrated in Figure 9.7-3.

The Baseline Manager database implemented at the EMD Development Facility reflects EMD-developed product structures, and site personnel may not normally need all the data necessary to define these product structures. Instead, BLM tasks are likely to be limited to areas such as noting system changes, perhaps in the context of site-unique requirements and data. However, an understanding of the different ways of conceptualizing the system will help in interpreting baseline data reflected in the BLM.

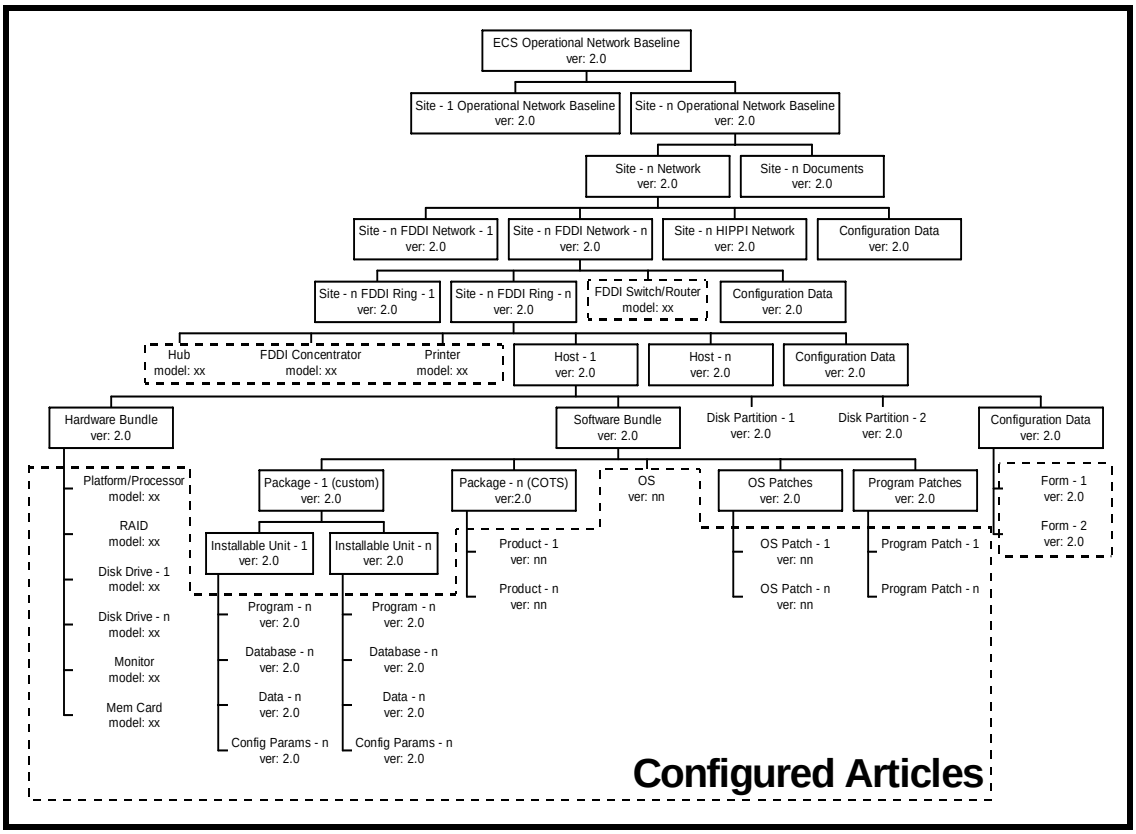


Figure 9.7-2. EMD Baseline Concept from an Operational (Network) View

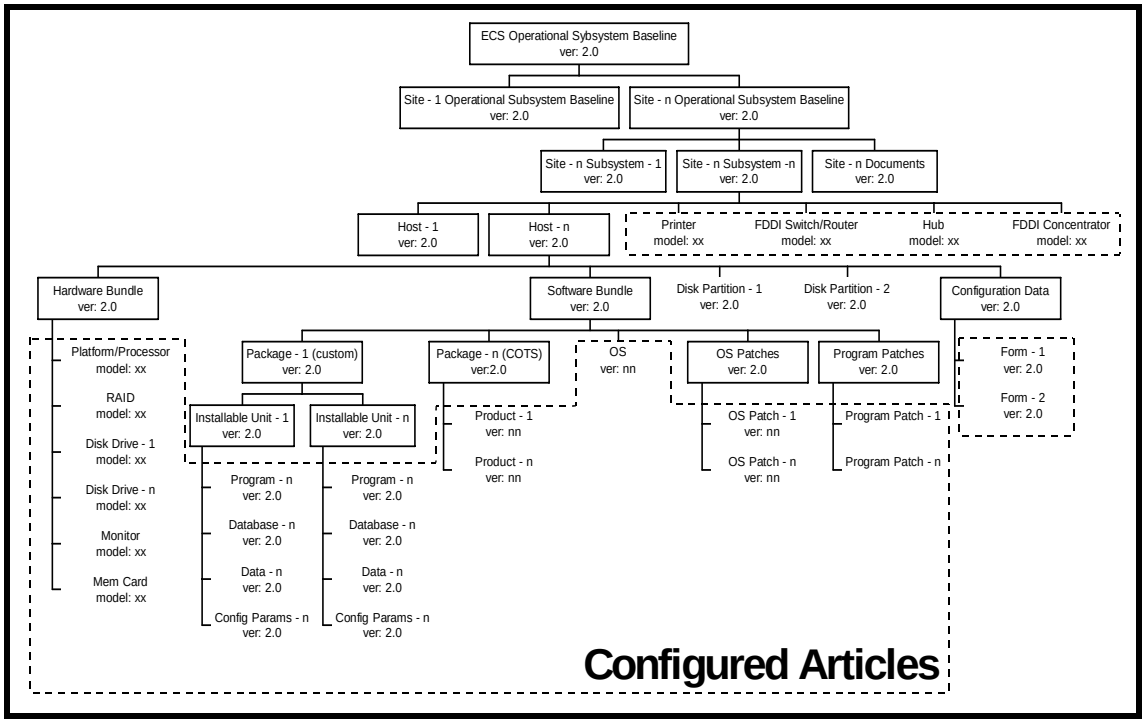


Figure 9.7-3. EMD Baseline Concept from an Operational (Subsystem) View

9.7.3 Baseline Manager (BLM) Outputs Useful at the Sites

The BLM manages the COTS software, operating system patches, and COTS software patch baselines. The BLM records, including information on all scripts, data, and GUIs, are maintained and managed at the EMD Development Facility using ClearCase. The BLM tool produces some of the 910/920 Technical Document reports, with automated posting to EMD Baseline Information System (EBIS) and replication to mirror sites at each DAAC. The reports include the following documents that affect all sites:

- COTS Software Versions 910-TDA-003.
- Site-Host Map 910-TDA-005.
- Critical COTS Software List 910-TDA-023.
- COTS S/W Where-Used Reports 910-TDA-030.

The reports also include the following documents that are site specific:

- Hardware-Software Maps 920-TD(*x*)-002.

  (*Note*: The *x* represents a letter designating specific DAACs. *e.g*, e = LP DAAC, s = SMC, p = PVC, and n = NSIDC.)

- O/S and COTS S/W Patch Maps 920-TD(*x*)-014.

All BLM records are related to approved Configuration Change Requests (CCR) and Release Notes documents (i.e., series 914-TDA-xxx).

The Configuration Management (CM) organization is the principal user of the BLM tool, using it to implement changes to the baseline. The system is used daily to describe CCB-approved system components and to track sites and machines where version-controlled items are configuration controlled. In addition BLM supports other functions such as configuration audits, system engineering and deployment activities. The BLM records describe the hosts for each site. The sites are the operational Distributed Active Archive Centers (DAACs), and Performance Verification Center (PVC). The system also tracks the COTS software and patches that are mapped to their respective hosts. EBIS accommodates the identification of all configuration-controlled items such as documents, and disk partitions.

The BLM capabilities are used to:

- Maintain records that identify what items comprise individual, baselined, system configurations
- Identify the versions and variants of hardware and software items that are currently baselined together with the assemblies (e.g., hosts, subsystems, and networks) that use them
- Record item interdependencies and the sites to which baselined items are deployed
- Keep chronological histories of baseline changes and traceability of items to predecessor versions and system releases

9.7.4 Procedure for Retrieving Baseline Reports

When the EMD software baseline is changed (e.g., addition of a script, update or replacement of a Graphical User Interface (GUI) package), the change must be reflected in the collection, or "catalog," of control items that make up the affected Computer Software Component (CSC) assembly in the EMD product structure. In the BLM software at the EDF, to document the change it is necessary to add the new element to the catalog of version-controlled items, define an engineering change for the CSC assembly, and include the element in the list of items that will now make up that assembly. Once the change is documented, baseline reports reflect the new information. These reports may be accessed through the EMD CMDM server for the EMD Baseline Information System (EBIS). See Figure 9.7-4.

The EBIS page is obtained by a click on the **EMD Baseline** button at the end of the Tools line near the top of the EMD CMDM Server page. On the EBIS page, the EMD Baseline Information Technical Documentation is accessible through use of the **Technical Documents** button at the top of the row of buttons on the left side.

The resulting **EMD Baseline Technical Documentation** page lists the document series, title, and document number. The document numbers are links that provide access to the listed documents. The titles of some documents indicate BLM origin by inclusion of the parenthetical notation **(ClearCase)**.

9.7.4.1 Retrieving Baseline Reports

1. At the UNIX command shell prompt, type **setenv DISPLAY *clientname*:0.0** and then press the **Return/Enter** key.
   - For ***clientname***, use either the local terminal/workstation IP address or its machine name.
2. Start the log-in to a Netscape host by typing **/tools/bin/ssh *hostname*** *(e.g., x4oml01*) at the UNIX command shell prompt, and press the **Return/Enter** key.
   - If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** ("**y**" alone does not work).
   - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
   - If you have not previously set up a secure shell passphrase; go to Step 4.
3. If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 5.
4. At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.
   - You are logged in and a UNIX command shell prompt is displayed.
5. Type **netscape &** and then press the **Return/Enter** key.
   - The Netscape web browser is displayed.

6. Click in the **Netsite:** field.
   - The field is highlighted.
7. Type the Universal Resource Locator (URL) for the EMD Baseline Information Server (**http://pete.hitc.com/baseline/**) and then press the **Return/Enter** key.
   - The **EMD CMDM Server** home page is displayed, offering access to EMD Baseline information as well as a number of tools, EMD web sites, and NASA EOS web sites.
8. On the Tools line click on the **EMD Baseline** button.
   - The **EMD Baseline Information System** page is displayed
9. Click on the **Technical Documents** button.
   - The **EMD Baseline Technical Documentation** page is displayed.
10. Locate the desired report, scrolling down as necessary.
    - Reports derived from the BLM may be indicated with a parenthetical notation **(ClearCase)** in the title entry.
11. Click on the link for the document to be accessed.
    - A directory is displayed with one or more document numbers and versions indicated as links.
12. Click on the link for the document and version desired.

    The document is displayed, and can be printed and searched.

    A sample of the EBIS page is shown in Figure 9.7.4.

EMD Baseline Information System (EBIS)

Tools

Number of hits on this site since 11/01/98: 38739

EBIS Bulletin:

1. Added a year 2006 CCRs button.

Technical Documents	EMD Baseline Technical Documentation
Custom S/W Tracking	Detail Information on Release 7: 7.00, 7.01, 7.02, 7.03, and 7.10 Custom Code CCRs, Deliveries, and Installation Status
Engineering S/W	Engineering Software (/tools/HOTSHELF) delivery information
COTS S/W Tracking	Detail Information on COTS S/W CCRs, Deliveries, and Installation Status
Technical Directives	Engineering Technical Directives, and authorizing CCRs
Release Notes	914-TDA-XXX's, EMD Release Notes and authorizing CCRs
Pre-Ship Reviews	PSR documents- Installation instructions
2006 eCCRs	Approved 2006 CCRs (except Procurement type CCRs)
2005 eCCRs	Approved 2005 CCRs (except Procurement type CCRs)

Figure 9.7-4. Sample EBIS Page