

611-EED-001, Rev. 02

EOSDIS Evolution and Development (EED) Contract

Release 8.2 Mission Operation Procedures for the EED Contract

Revision 02

September 2013

Raytheon Company
Riverdale, Maryland

This page intentionally left blank.

Release 8.2 Mission Operation Procedures for the EED Contract

Revision 02

September 2013

Prepared Under Contract NNG10HP02C
CDRL Item # 023

RESPONSIBLE AUTHOR

Lay'wan F. Gamble 9/30/2013
Lay'wan Gamble, Sr. Software Engineer Date
EOSDIS Evolution and Development (EED) Contract

RESPONSIBLE OFFICE

Panda Johnson (for Tim Ortiz) 9/30/13
Timothy W. Ortiz, Program Manager Date
EOSDIS Evolution and Development (EED) Contract

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 EED Contract Office
Raytheon Company
5700 Rivertech Court
Riverdale, Maryland 20737

Revision History

Document Number	Status/Issue	Publication Date	CCR Number
611-EED-001	Original	March 2011	11-0055
611-EED-001	Revision 01	April 2012	12-0096
611-EED-001	Revision 02	September 2013	13-0229

This page intentionally left blank.

Abstract

This document, Release 8.2 Mission Operation Procedures for the EED 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.....	2-2

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	3-3
3.5	Changing Your Passphrase	3-3
3.5.1	Changing Your Passphrase	3-4
3.6	Logging in to System Hosts	3-4
3.6.1	Log in to System Hosts	3-5
3.7	System Startup and Shutdown	3-6
3.7.1	Cold Startup By Subsystem	3-6
3.7.2	Warm Startup	3-7
3.7.3	Normal Shutdown	3-8
3.7.4	Emergency Shutdown	3-9
3.7.5	System Shutdown by Server	3-11
3.8	ECS Assistant	3-11
3.8.1	Starting ECS Assistant	3-11
3.9	Tape Operations	3-13
3.9.1	Networker Administrator Screen	3-14
3.9.2	Labeling Tapes	3-14
3.10	System Backups and Restores	3-16
3.10.1	System Backup	3-16
3.10.2	System Restore	3-17
3.11	User Administration	3-19
3.11.1	Screening Personnel	3-19
3.11.2	Screening Procedures	3-20
3.11.3	Adding a New User	3-21
3.11.4	Deleting a User	3-21
3.11.5	Changing a User's Account Configuration	3-23
3.11.6	Changing User Access Privileges	3-24
3.11.7	Changing a User Password	3-24
3.11.8	Checking a File/Directory Access Privilege Status	3-24
3.11.9	Changing a File/Directory Access Privilege	3-25
3.11.10	Moving a User's Home Directory	3-28
3.12	Commercial Off-the-Shelf (COTS) Software Administration	3-28
3.12.1	Installation	3-28

3.12.2 LOG FILES.....	3-28
3.12.3 COTS Configuration.....	3-28

4. Database Administration

4.1 System Overview	4-1
4.1.1 Information Model	4-1
4.1.2 Subsystems.....	4-3
4.1.3 Databases	4-4
4.1.4 Resident Databases	4-5
4.1.5 Database Directory Locations.....	4-5
4.2 Database Management	4-6
4.2.1 Database Management Model	4-6
4.2.2 Database Management Implementation.....	4-7
4.2.3 Hardware, Software, and Database Mapping	4-7
4.3 Database Administrator	4-7
4.3.1 DBA Tasks and Procedures	4-7
4.4 Starting and Stopping Database Servers.....	4-8
4.4.1 Start PostgreSQL Instance	4-9
4.5 Creating Database Devices- DELETED.....	4-9
4.6 Installing Databases and Patches	4-9
4.6.1 Perform a Database Build Procedure (Example Only).....	4-9
4.6.2 Install a Database Patch (Example)	4-9
4.7 Configuring Databases.....	4-10
4.7.1 Configure the PostgreSQL Server Parameters.....	4-10
4.8 Working with Indexes, Segments, and Caches - DELETED.....	4-11
4.9 Backing Up and Recovering Data	4-11
4.9.1 Perform Manual Backups	4-11
4.9.2 Perform a User Database Recovery (Order of Procedures).....	4-12
4.10 Establishing Database Security - DELETED	4-12
4.11 Copying and Extracting Data - DELETED	4-12
4.12 Bulk Copying - DELETED.....	4-12
4.13 Monitoring - DELETED.....	4-12

4.14	Tuning - DELETED.....	4-12
4.15	Ensuring Database Quality - DELETED	4-12
4.16	Sybase Troubleshooting - DELETED	4-12

5. Security Services

5.1	Scanning Network Vulnerabilities.....	5-1
5.2	2-Factor Authentication	5-1
	5.2.1 RSA SecureID Administration	5-2
	5.2.2 RSA Authentication for PAM.....	5-4
5.3	Aging Passwords.....	5-4
5.4	Secure Access through Secure Shell.....	5-4
	5.4.1 Installation of SSH.....	5-5
	5.4.2 The SSH Encryption Mechanism.....	5-5
	5.4.3 Using Secure Shell.....	5-6
	5.4.4 Multiple Connections.....	5-7
	5.4.5 Secure FTP.....	5-7
	5.4.6 Other Notes	5-7
	5.4.7 Configuration of Secure Shell.....	5-7
	5.4.8 Administration of Secure Shell.....	5-9
5.5	Controlling Requests for Network Services (TCP Wrappers).....	5-10
5.6	Monitoring File and Directory Integrity (OSSEC).....	5-10
	5.6.1 Installation of OSSEC.....	5-11
	5.6.2 Configuring the ossec.conf File	5-11
	5.6.3 Monitoring OSSEC.....	5-11
5.7	Generating Security Reports.....	5-11
	5.7.1 User Activity Data	5-12
5.8	Reporting Security Breaches	5-13
5.9	Initiating Recovery from Security Breaches.....	5-13

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	Juniper Firewall	6-2
6.4.2	Production VLAN Ethernet Switch	6-2
6.4.3	SAN LAN GigE Switch.....	6-3
6.5	Domain Name Service (DNS) Structure.....	6-3
6.6	Host Names.....	6-4
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
7.2.2	Hyperic.....	7-3

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	8-19
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.....	9-14
9.3.1	Purpose.....	9-14
9.3.2	Applicability	9-14
9.3.3	References.....	9-14
9.3.4	Procedures.....	9-15
9.4	Configuration Audits	9-15
9.4.1	Purpose.....	9-15
9.4.2	Applicability	9-16
9.4.3	References.....	9-16
9.4.4	Procedures.....	9-16
9.5	Archiving Procedures for the SW CM Manager (ClearCase)	9-17
9.5.1	Purpose.....	9-17

9.5.2	Applicability	9-17
9.5.3	References.....	9-17
9.5.4	Definitions	9-17
9.5.5	General.....	9-18
9.5.6	Procedures.....	9-18
9.6	Software Delivery and Installation	9-18
9.6.1	Purpose.....	9-18
9.6.2	Applicability	9-19
9.6.3	References.....	9-19
9.6.4	Procedures.....	9-19
9.7	Baseline Manager	9-20
9.7.1	Overview.....	9-20
9.7.2	Baseline Terms and Concepts.....	9-20
9.7.3	Baseline Manager (BLM) Outputs at the Sites.....	9-24
9.7.4	Procedure for Retrieving Baseline Reports	9-25

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	10-3
10.2	Preparation of Earth Science Data Types	10-3
10.2.1	Definitions	10-3
10.2.2	Process	10-4
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.....	10-10

11. Bulk Metadata Generation Tool

11.1	BMGT Overview	11-1
11.2	BMGT GUI.....	11-3
11.2.1	BMGT GUI Functions	11-4
11.2.2	Monitoring System and Verification Status.....	11-6
11.2.3	Monitoring Recent Requests.....	11-8
11.2.4	Cancelling Recent Requests.....	11-13
11.2.5	Reviewing Failed Requests.....	11-15
11.2.6	Reviewing Corrective Export Requisitions	11-18
11.2.7	BMGT Configuration.....	11-19
11.2.8	Error Configurations	11-24
11.2.9	Collection Configurations.....	11-28
11.3	BMGT Manual Mode	11-31
11.3.1	BMGT Manual Mode	11-35
11.4	BMGT ReExport Queue Utility.....	11-36
11.4.1	BMGT ReExport Queue Utility.....	11-39
11.5	BMGT Automatic Mode.....	11-39
11.5.1	BMGT Automatic Mode.....	11-39

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.....	12-5
12.1.4	Request Format	12-6
12.1.5	Update QA Metadata Flags Using QA Update Utility	12-8

13. Data Pool 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.....	13-4
13.3.1	DPL Ingest GUI.....	13-5
13.3.2	Monitoring Requests Status.....	13-12
13.3.3	Viewing Historical Requests.....	13-24
13.3.4	Provider Status.....	13-29
13.3.5	File System Status.....	13-34
13.3.6	Transfer Host Status.....	13-37
13.3.7	Viewing ECS Service Status.....	13-40
13.3.8	Monitoring PDR List.....	13-43
13.4	Interventions & Alerts.....	13-44
13.4.1	Open Intervention.....	13-44
13.4.2	Viewing System Alerts.....	13-55
13.5	DPL Ingest Configuration.....	13-60
13.5.1	Data Provider Configuration.....	13-61
13.5.2	Data Type Configuration.....	13-71
13.5.3	Transfer Host Configuration.....	13-73
13.5.4	File System Configuration.....	13-80
13.5.5	ECS Service Configuration.....	13-82
13.5.6	Global Tuning Configuration.....	13-91
13.5.7	Configure Volume Groups.....	13-98
13.5.8	Operator Configuration.....	13-109
13.6	Reports.....	13-112
13.6.1	Reports.....	13-112
13.6.2	Viewing the Volume Groups History Page.....	13-117
13.7	Help Pages and Context Help.....	13-119
13.8	Data Pool Maintenance GUI.....	13-120
13.8.1	Data Pool Maintenance GUI.....	13-120
13.8.2	Managing Data Pool Collection Groups.....	13-123

14. Archive Management/Data Pool Maintenance

14.1	Archive Management Overview.....	14-1
14.2	Archive Hardware.....	14-1
14.3	Archive Software.....	14-3

14.4	Starting and Stopping StorNext	14-4
14.4.1	Starting the StorNext Application.....	14-4
14.4.2	Stopping the StorNext Application.....	14-7
14.4.3	Rebooting the StorNext Metadata Servers.....	14-8
14.4.4	Avoiding Loss of LUN Labels When Installing Red Hat.....	14-9
14.5	Loading and Removing Archive Media from the Scalar library	14-10
14.5.1	Loading Archive Media	14-11
14.6	Backing Up the StorNext Application	14-17
14.6.1	Executing a StorNext Backup.....	14-19
14.6.2	Scheduling a StorNext Backup	14-22
14.7	Scalar Library	14-23
14.7.1	Scalar I500 library	14-23
14.7.2	Scalar I6000 library	14-26
14.8	LTO Tape Drives	14-32
14.8.1	Cleaning LTO Tape Drives.....	14-33
14.9	Archive Maintenance Tasks - Deleting Granules	14-33
14.9.1	Generating a GeoID File.....	14-35
14.9.2	Deleting Granules, Phase 1: Mark Granules for Deletion (Logical)	14-38
14.9.3	“Undeleting” Granules from the Archive and Inventory	14-40
14.9.4	Deleting Granules, Phase 2: Running the Deletion Cleanup Utility	14-42
14.10	Data Pool Maintenance Tasks.....	14-46
14.10.1	Features of the Data Pool Maintenance GUI.....	14-46
14.10.2	Data Pool File Systems	14-54
14.10.3	Cloud Cover	14-59
14.10.4	Batch Summary.....	14-64
14.10.5	List Insert Queue.....	14-65
14.10.6	Configuration Parameters	14-68
14.10.7	Aging Parameters.....	14-74
14.10.8	Collection Groups	14-76
14.10.9	Themes.....	14-92
14.10.10	Help.....	14-98
14.11	Working with Data Pool Scripts	14-99
14.11.1	Extending the Period of Retention for Granules in the Data Pool.....	14-102

14.11.2	Running the Data Pool Cleanup Utility (DELETED)	14-106
14.11.3	Running the Data Pool Access Statistics Utility.....	14-106
14.11.4	Running the Batch Insert Utility	14-112
14.11.5	Running the Most Recent Data Pool Inserts Utility	14-112
14.11.6	Running the Data Pool Collection-to-Group Remapping Utility	14-114
14.11.7	Running the Data Pool Move Collections Utility	14-115
14.11.8	Running the Data Pool Hidden Scrambler Utility in Rename Mode.....	14-119
14.11.9	Running the Data Pool Cleanup Orphan/Phantom Validation	14-123
14.11.10	Running the Data Pool SoftLink Check Utility	14-127
14.11.11	Running the Data Pool Online Archive Cleanup Utility	14-128
14.11.12	Running the Data Pool Publish Utility	14-131
14.11.13	Running the Data Pool UnPublish Utility.....	14-133
14.11.14	Running the Data Pool Inventory Validation Utility	14-134
14.11.15	Running the Data Pool Checksum Verification Utility (Being replaced by Data Pool Checksum Verification Service (CVS))	14-136
14.11.16	Running the Restore Online Archive from Tape Utility.....	14-140
14.11.17	Running the Restore Tape from Online Archive Utility.....	14-144
14.11.18	Running the Archive Checksum Verification Utility	14-148
14.11.19	Running the XML Check Utility	14-152
14.11.20	Running the Data Pool Band Backfill Utility	14-155
14.11.21	Running the Data Pool Remove Collection Utility [DELETED].....	14-156
14.11.22	Running the Data Pool Cloud Cover Utility [DELETED]	14-156
14.11.23	Running the Data Pool Checksum Verification Service.....	14-156
14.11.24	Running the DPL XML Check Utility.....	14-159

15. Distribution Concepts

15.1	System Overview	15-1
15.2	Order Manager Subsystem (OMS)	15-4
15.3	OM GUI Operator Security	15-4
15.4	Order Manager GUI.....	15-5
	15.4.1 Launching the Order Manager GUI.....	15-6
15.5	Order Manager GUI Operations	15-7

15.6	OM GUI – Request Management	15-9
15.6.1	Request Management Submenu Page – Open Interventions	15-10
15.6.2	Request Management Submenu Page – HEG Interventions.....	15-21
15.6.3	Request Management Submenu Page – Completed Actions and Interventions Filter.....	15-28
15.6.4	Request Management Submenu Page – Distribution Requests [filter].....	15-30
15.6.5	Request Management Submenu Page – FtpPush/SCP Requests Filters and Staging Requests Filters.....	15-35
15.6.6	Request Management Submenu Page – Processing Service Requests [filter].	15-37
15.6.7	Request Management Submenu Page – Operator Alerts.....	15-38
15.6.8	Exiting the OM GUI	15-41
15.7	OM GUI – Destination Monitor	15-41
15.7.1	Destination Monitor Submenu Page – Suspended Destinations.....	15-41
15.8	OM GUI – Archive Data.....	15-46
15.8.1	Archive Data Submenu Page – Historical Distribution Requests Filter.....	15-46
15.8.2	Archive Data Submenu Page – Historical Processing Requests Filter.....	15-48
15.9	OM GUI – OM Status Pages	15-50
15.9.1	OM Status Pages Submenu Page – OM Queue Status	15-50
15.9.2	OM Status Pages Submenu Page – HEG Order Status.....	15-52
15.9.3	OM Status Pages Submenu Page – Staging Status (Media Type, FTP Push Destination and SCP Destination)	15-53
15.9.4	OM Status Pages Submenu Page – Pending HEG Granules	15-55
15.9.5	OM Status Pages Submenu Page – DPL File System Status.....	15-56
15.10	OM GUI – OM Configuration	15-57
15.10.1	OM Configuration Submenu Page – Aging Parameters	15-59
15.10.2	OM Configuration Submenu Page – Server/Database	15-61
15.10.3	OM Configuration Submenu Page – Media.....	15-64
15.10.4	OM Configuration Submenu Page – ODL Metadata Users.....	15-66
15.10.5	OM Configuration Submenu Page – Checksum Users.....	15-68
15.10.6	OM Configuration Submenu Page – External Processing.....	15-69
15.10.7	OM Configuration Submenu Page – FtpPush/SCP Policy	15-71
15.11	OM GUI – Help	15-77
15.11.1	Help Submenu Page – About HelpOnDemand.....	15-78
15.11.2	Help Submenu Page – Help.....	15-78

15.12	OM GUI – View Order Status	15-79
15.12.1	View Order Status Submenu Page – OM GUI Order Status	15-79
15.13	OM GUI – Logs	15-84
15.13.1	Logs Submenu Page – OM GUI Log Viewer	15-84
15.14	OM GUI – Admin Tools	15-86
15.14.1	Admin Tools Submenu Page – Server/Database Parameters	15-87
15.14.2	Admin Tools Submenu Page – Media Parameters	15-87
15.14.3	Admin Tools Submenu Page – Aging Parameters	15-87
15.14.4	Admin Tools Submenu Page – FtpPush Policy	15-87
15.14.5	Admin Tools Submenu Page – Action Pages	15-87
15.14.6	Admin Tools Submenu Page – Profile Management	15-89
15.14.7	Science Command Line Interface (SCLI) in OMS	15-90
15.15	OMS Database Cleanup Guidelines	15-92
15.15.1	Removal of Completed OMS Actions, Interventions and Notifications	15-93
15.15.2	Removal of Order-Tracking Information for Completed Orders	15-93
15.15.3	Fault Handling	15-93
15.16	Troubleshooting a Order Manager GUI Failure	15-94
15.16.1	Checking Log Files	15-108
15.16.2	Checking Database Connections	15-109
15.16.3	Recovering from Order Manager Failures	15-110
15.16.4	Determining the Permissions for Creating an Ftp Pull Subdirectory	15-113
15.16.5	HEG Failures	15-114
15.16.6	Checking HEG Server Log Files	15-132
15.16.7	Checking Files in the HEG Tempfiles Directory	15-143

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	16-5
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 EED Library Administration Overview	17-1
17.1.1 Data Management (DM)	17-2
17.2 Configuration Management (CM) Overview	17-3
17.2.1 Configuration Management (CM)	17-4
17.3 On-Site Documentation Overview	17-5
17.3.1 On-Site COTS Document and Software Maintenance	17-5

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 Configuration Management	18-2
18.2.3 COTS Hardware Maintenance Safety	18-2
18.3 COTS Hardware Maintenance - Contract Information	18-2
18.3.1 COTS Hardware Maintenance Contract	18-2
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	18-3
18.4.2 Hardware Corrective Maintenance Actions	18-4
18.4.3 Contract On-Site Hardware Maintenance	18-5
18.4.4 Return-to-Depot Support	18-7
18.4.5 Return of Failed LRUs	18-7
18.5 Non-Standard Hardware Support	18-8
18.5.1 Escalation of COTS Hardware Support Problem	18-8
18.5.2 Low Cost Equipment – Not Repaired	18-8

19. COTS Software Maintenance

19.1	Introduction.....	19-1
19.2	COTS Software Maintenance Tasks.....	19-2
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 Property Custodian.....	20-3
20.3	Equipment Tagging.....	20-3
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	20-5
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	20-6
20.6	Inventories and Audits	20-6
20.7	Storage	20-7
20.7.1	Segregation Requirements	20-7
20.7.2	Stock Rotation.....	20-7
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. Asset Smart Property Equipment Management System (SMART|PEMS)

23.1	Asset Smart Property Equipment Management System.....	23-1
23.2	Asset Smart User Tool Overview	23-2
	23.2.1 Navigating Asset Smart User Tool	23-2
	23.2.2 Asset Smart System Transactions.....	23-5
23.3	Basic Validation.....	23-14
	23.3.1 Error Messages and Field Status Buttons	23-14
	23.3.2 Blank Out Values with the Not-Code.....	23-15
	23.3.3 All Entered Values Must be Valid Before Committing Your Transaction to the Database.....	23-15
23.4	Handling Errors.....	23-16
23.5	Field Definitions	23-18

24. Maintenance of Configuration Parameters

24.1	Parameter Change Control Procedure.....	24-1
24.2	Overview of Configuration Parameter Files.....	24-2
24.3	Deployment and Baseline Maintenance	24-2
24.3.1	How to Run a Mkcfg.....	24-3

25. EOSDIS Service Interface (DataAccess)

25.1	EOSDIS Service Interface (DataAccess).....	25-1
25.2	Configuring the DataAccess System	25-2
25.2.1	Launching the Data Access GUI	25-2
25.2.2	Adding or Updating a Service	25-4
25.2.3	Creating or Updating a Service to Collection Mapping	25-8
25.3	Monitoring the DataAccess System.....	25-12
25.3.1	Monitoring Recent Requests.....	25-12

List of Figures

Figure 3.8-1.	ECS Assistant GUI Manager Windows	3-12
Figure 3.10-1.	Networker Backup Window.....	3-17
Figure 3.11-1.	/etc/passwd File Fields.....	3-22
Figure 3.11-2.	/etc/group File	3-22
Figure 3.11-3.	Access Permissions	3-26
Figure 4.1.1-1.	Earth Science Information Model.....	4-2
Figure 4.1-2.	An Example of Data Product Levels.....	4-3
Figure 4.5.1-1.	Example of an add_devices.sql File for Creation of a Database Device	4-19
Figure 4.7.1-1.	Example of sp_configure Output	4-25
Figure 4.7.3.1-1.	Configuration Registry.....	4-28
Figure 4.7.3.1-2.	Configuration Registry Attributes Pop-Up Window	4-28
Figure 4.8.2.1-1.	Example of Creation of a Database Segment Template File	4-32

Figure 4.9.4.2-1. Sample template.sql File for Creation of a Database.....	4-41
Figure 4.9.4.2-2. Completed Create Database Script	4-42
Figure 4.10.2.1-1. Sample template.sql File for New Database User Login.....	4-46
Figure 7.2-1. Big Brother Home Page	7-1
Figure 7.2-2. Big Brother Toolbar	7-2
Figure 7.2-3. HQ Homepage.....	7-4
Figure 7.2-4. Alert Definition Schema Diagram	7-7
Figure 7.2-5. Hyperic GUI Administration Tab	7-7
Figure 7.2-6. Hyperic GUI Administration Page.....	7-8
Figure 7.2-7. Business Process Configuration Page	7-9
Figure 7.2-8. Business Processes Group Alert Configuration.....	7-10
Figure 7.2-9. View Business Process Group Alert	7-11
Figure 7.2-10. Update Business Process Group Alert	7-12
Figure 7.2-11. Add new Business Process Group Alert	7-13
Figure 7.2-12. View added Business Process Group Alert.....	7-14
Figure 7.2-13. Business Processes Link	7-14
Figure 7.2-14. View Business Process Page – DPL Ingest Active.....	7-15
Figure 7.2-15. View Business Process - DPL Ingest Down	7-16
Figure 7.2-16. Business Process Mode Tab.....	7-16
Figure 7.2-17. Business Process Status Table	7-17
Figure 7.2-18. Business Process Resource Table	7-18
Figure 7.2-19. Business Process Status Definition	7-19
Figure 7.2-20. Business Process Resource Status.....	7-19
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 (Part 1)	8-14
Figure 8.3-9. Add Trouble Ticket Web Page (Part 2)	8-14
Figure 8.3-10. Add Trouble Ticket GUI (Part 1).....	8-16
Figure 8.3-11. Add Trouble Ticket GUI (Part 2).....	8-17
Figure 8.3-12. Add Trouble Ticket GUI (Part 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 Events 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 Automation 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. EED Configuration Change Request (CCR) Form	9-5
Figure 9.2-3. Workflow Diagram for EED CM Administrator	9-10
Figure 9.2-4. Workflow Diagram for Site-level CM Administrator.....	9-13
Figure 9.7-1. ECS Baseline Concept from a Design (CIL/CAL) View.....	9-22
Figure 9.7-2. ECS Baseline Concept from an Operational (Network) View	9-23
Figure 9.7-3. ECS Baseline Concept from an Operational (Subsystem) View	9-24
Figure 9.7-4. EBIS Home Page.....	9-27
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	10-11
Figure 10.4-5. Installed ESDT Page	10-12
Figure 10.4-6. XML Descriptor Information Page	10-14
Figure 10.4-7. ESDTs to be Installed, Updated, or that Have Failed Page	10-17
Figure 10.4-8. ESDTs Failure Screen.....	10-18
Figure 11.1-1. BMGT Context diagram	11-2
Figure 11.2-1. Home Page and Navigation Panel.....	11-4

Figure 11.2-2. BMGT Login Page.....	11-5
Figure 11.2-3. System Status Tab.....	11-6
Figure 11.2-4. Export-Requests Tab, Requests Listing Table.....	11-8
Figure 11.2-5. Export-Requests – Requests Queue Summary.....	11-9
Figure 11.2-6. Export-Requests – Export Batch Summary	11-10
Figure 11.2-7. Export-Requests – Batch per Collection Summary	11-10
Figure 11.2-8. Export Requests Tab	11-11
Figure 11.2-9. Export Request And Activity State Transition Diagram	11-12
Figure 11.2-10. Export Activity / Errors.....	11-13
Figure 11.2-11. BMGT Configuration.....	11-20
Figure 11.2-12. Collection Configurations Page	11-30
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. Operator Information Panel	13-6
Figure 13.3-2. Built-in Back/Forward Browser Buttons	13-6
Figure 13.3-3. Data Pool Ingest GUI Home Page	13-8
Figure 13.3-4. General Ingest Status/Resume Button.....	13-9
Figure 13.3-5. General Ingest Status/Resume Buttons	13-10
Figure 13.3-6. Ingest GUI Login Screen	13-12
Figure 13.3-7. Active Ingest Request List Filter Panel	13-14
Figure 13.3-8. Ingest Requests Page.....	13-15
Figure 13.3-9. Ingest Request Detail Page	13-17
Figure 13.3-10. Cancel Request/Suspend Requests Buttons	13-21
Figure 13.3-11. Change Priority Dialog Box.....	13-22
Figure 13.3-12. Request Detail Page – Granule List	13-23
Figure 13.3-13. Historical Ingest Requests Page.....	13-26

Figure 13.3-14. Historical Ingest Request Detail Page.....	13-29
Figure 13.3-15. Provider Status Page	13-31
Figure 13.3-16. Provider Status Detail Page.....	13-32
Figure 13.3-17. File System Status Page	13-35
Figure 13.3-18. Transfer Host Status Page	13-38
Figure 13.3-19. ECS Services Status Page	13-41
Figure 13.3-20. PDR List Page	13-43
Figure 13.4-1. Open Interventions Page	13-46
Figure 13.4-2. Interventions Related Configuration Section.....	13-47
Figure 13.4-3. Open Interventions Detail Page	13-51
Figure 13.4-4. Alerts Page	13-56
Figure 13.5-1. Provider Configuration Page.....	13-62
Figure 13.5-2. Edit a Provider Page.....	13-64
Figure 13.5-3. Edit a Polling Location Details Page	13-66
Figure 13.5-4. Add a Provider Page	13-68
Figure 13.5-5. Data Type Configuration Page.....	13-72
Figure 13.5-6. Host Configuration Page	13-75
Figure 13.5-7. FTP (or SCP) Host Configuration Add a New Host Page	13-76
Figure 13.5-8. Host Configuration for [LabelName] Page	13-78
Figure 13.5-9. Host Configuration Details Page.....	13-79
Figure 13.5-10. File System Configuration	13-80
Figure 13.5-11. ECS Services Configuration Page.....	13-82
Figure 13.5-12. ECS Services Configuration: Add Service Host Page.....	13-84
Figure 13.5-13. ECS Services Configuration: Add Service Host Page.....	13-88
Figure 13.5-14. Global Tuning Page	13-97
Figure 13.5-15. Volume Groups Configuration (listing page)	13-99
Figure 13.5-16. Volume Group Configuration: Add Volume Group Page	13-101
Figure 13.5-17. Volume Group Configuration: Add a Volume Group Page.....	13-102

Figure 13.5-18. Operator Configuration Page	13-109
Figure 13.6-1. Detailed Report Page	13-114
Figure 13.6-2. Request Summary Report Page.....	13-115
Figure 13.6-3. Granule Summary Report Page.....	13-116
Figure 13.6-4. Volume Group History Page.....	13-118
Figure 13.7-1. Help – General Topics	13-119
Figure 13.8-1. DPM GUI Home Page	13-122
Figure 13.8-2. Collection Group Page	13-124
Figure 13.8-3. List of Collection	13-125
Figure 13.8-4. Detail Information.....	13-127
Figure 13.8-5. Modify Collection Group.....	13-130
Figure 13.8-6. Add Collection Group.....	13-132
Figure 13.8-7. List of Collections	13-133
Figure 13.8-8. Collections Not In Data Pool Page	13-134
Figure 13.8-9. Add New Collection Page.....	13-134
Figure 13.8-10. Modify Collection Page	13-137
Figure 14.2-1. Online Archive Architecture.....	14-3
Figure 14.4-1. StorNext GUI Home Page.....	14-5
Figure 14.4-2. Admin Pull-Down Menu.....	14-6
Figure 14.4-3. Start/Stop StorNext Page	14-6
Figure 14.4-4. Stop StorNext Page	14-8
Figure 14.5-1. Add Media Page.....	14-12
Figure 14.5-2. Associated Library Page	14-12
Figure 14.5-3. Associated Library Bulk Load Page	14-13
Figure 14.5-4. Complete Add Media Task Page	14-13
Figure 14.5-5. Remove/Move Media Pull Down Menu	14-14
Figure 14.5-6. Remove or Move Media Page.....	14-15
Figure 14.5-7. Select Media Screen.....	14-15

Figure 14.5-8. Complete/Remove Media Task Page.....	14-16
Figure 14.6-1. StorNext Admin Pull- Down Screen.....	14-20
Figure 14.6-2. Backup StorNext Screen	14-21
Figure 14.6-3. Complete Backup Screen	14-21
Figure 14.6-4. Feature Schedules Screen.....	14-22
Figure 14.6-5. Selected Feature Schedules Screen.....	14-23
Figure 14.7-1. Scalar i500 Operator Panel User Interface.....	14-24
Figure 14.7-2. Scalar i500 Web Client User Interface	14-24
Figure 14.7-3. Scalar i500 Login Screen	14-25
Figure 14.7-4. Scalar i6000 Library Management Console.....	14-27
Figure 14.7-5. Scalar i6000 Library Explorer Screen.....	14-28
Figure 14.7-6. Scalar i6000 Control Module Information Screen.....	14-29
Figure 14.7-7. Scalar i6000 Import Media Screen.....	14-31
Figure 14.7-8. Scalar i2000 Export Media Screen.....	14-32
Figure 14.8-1. Clean Drive Screen	14-33
Figure 14.10-1. Security Login Prompt	14-48
Figure 14.10-2. DPM GUI Home Page	14-49
Figure 14.10-3. DPM GUI Home Page	14-51
Figure 14.10-4. Data Pool File System Page	14-55
Figure 14.10-5. Add New File System Page.....	14-56
Figure 14.10-6. Modify File System Information Page.....	14-58
Figure 14.10-7. Cloud Cover Information Page	14-59
Figure 14.10-8. Add New Cloud Cover Information Page.....	14-61
Figure 14.10-9. Modify Source Description Page	14-62
Figure 14.10-10. Batch Summary Page	14-64
Figure 14.10-11. List Insert Queue Page	14-66
Figure 14.10-12. List of Configuration Parameters Page	14-68
Figure 14.10-13. List of Aging Parameters Page.....	14-75

Figure 14.10-14. Collection Groups Page	14-77
Figure 14.10-15. List of Collection Page.....	14-78
Figure 14.10-16. Collection Detail Information Page	14-79
Figure 14.10-17. Modify Collection Page	14-83
Figure 14.10-18. Add Collection Group Page	14-84
Figure 14.10-19. Collections Not in Data Pool Page.....	14-87
Figure 14.10-20. Add New [ECS] Collection Page.....	14-87
Figure 14.10-21. Modify Collection Page	14-90
Figure 14.10-22. Detailed List of Data Pool Themes Page	14-93
Figure 14.10-23. Add New Theme Page	14-93
Figure 14.10-24. Modify Theme Page.....	14-96
Figure 14.10-25. Help Page	14-99
Figure 15.1-1. System Context Diagram	15-2
Figure 15.1-2. Order Manager Subsystem (OMS) Context Diagram for EP requests	15-3
Figure 15.4-1. Security Login Prompt.....	15-6
Figure 15.4-2. Order Manager Home Page.....	15-7
Figure 15.6-1. Open Interventions Page – Fields and Options.....	15-11
Figure 15.6-2. Order Manager GUI Tools: Find (A), Navigation (B), and Refresh (C)	15-11
Figure 15.6-3. Open Interventions Page	15-13
Figure 15.6-4. ECS Order <ID> Details Page	15-14
Figure 15.6-5. Open Intervention for Request <ID> Page	15-14
Figure 15.6-6. Worker Assignment	15-15
Figure 15.6-7. Request Attributes.....	15-17
Figure 15.6-8. Request Level Disposition	15-18
Figure 15.6-9. Close Confirmation for Intervention <ID> with E-Mail.....	15-20
Figure 15.6-10. Intervention Closed.....	15-21
Figure 15.6-11. Open HEG Interventions Page.....	15-22
Figure 15.6-12. Open HEG Interventions – Fields and Options	15-23

Figure 15.6-13. Open HEG Intervention For Request <ID> Detail Page	15-24
Figure 15.6-14. Open HEG Interventions for Request <ID> Detail – Fields and Options ...	15-25
Figure 15.6-15. Processing Instructions Window.....	15-26
Figure 15.6-16. Close Confirmation for Intervention <ID> Page	15-28
Figure 15.6-17. Completed Action and Interventions – Fields and Options (NOTE: Hard Media actions obsolete in 8.1).....	15-29
Figure 15.6-18. Completed Action and Interventions Page (NOTE: only two types of interventions exist post 8.1).....	15-30
Figure 15.6-19. Distribution Requests Page and Filter Window.....	15-31
Figure 15.6-20. Distribution Requests Page – Fields and Options.....	15-32
Figure 15.6-21. Distribution Requests <ID> Profile	15-34
Figure 15.6-22. FtpPush/SCP (A) and Staging (B) Distribution Requests Filters	15-36
Figure 15.6-23. Processing Services Requests Page and Filter	15-38
Figure 15.6-24. Operator Alerts Page (A) and Alert Details Page (B-C).....	15-39
Figure 15.6-25. Operator Alerts Page – Fields and Options.....	15-40
Figure 15.7-1. Suspended Destinations Monitor (A) and Ftp Push Monitor-Suspended Configured Destination (B) Pages	15-43
Figure 15.8-1. Historical Distribution Requests Page (A) and Filter (B).....	15-46
Figure 15.8-2. Historical Distribution Requests Page – Fields and Options	15-47
Figure 15.8-3. Historical Processing Requests Page (A) and Filter (B).....	15-48
Figure 15.8-4. Historical Processing Requests Page – Fields and Options	15-49
Figure 15.9-1. OM Queue Status Page	15-51
Figure 15.9-2. HEG Order Status Page.....	15-52
Figure 15.9-3. Staging Status Pages and Table (Fields).....	15-53
Figure 15.9-4. Pending HEG Granules Page (Frame A) and Tables (Frames 1-2)	15-55
Figure 15.9-5. Data Pool File System Status Page	15-57
Figure 15.10-1. Aging Parameters Page	15-60
Figure 15.10-2. OMS Server and Database Configuration Page.....	15-61
Figure 15.10-3. OM Server/Database Configuration - Parameters	15-63
Figure 15.10-4. Media Configuration Page	15-64

Figure 15.10-5. ODL Metadata File Users Configuration Page	15-67
Figure 15.10-6. Checksum Notification Users Configuration Page	15-68
Figure 15.10-7. External Processing Services Policy Configuration Page.....	15-70
Figure 15.10-8. FtpPush/SCP Policy Configuration Page.....	15-72
Figure 15.10-9. FtpPush/SCP Policy Configuration Page – Fields and Options.....	15-73
Figure 15.10-10. Context-Sensitive Help for Retry Interval Parameter	15-74
Figure 15.10-11. Data Access Services Configuration.....	15-76
Figure 15.11-1. Help Page (A) and HelpOnDemand Example (B)	15-78
Figure 15.12-1. Get Order Status Page	15-79
Figure 15.12-2. Get Order Status Pages Navigation Bars and Fields.....	15-80
Figure 15.12-3. Order Status Pages (A-B2) and Error Prompts (C).....	15-81
Figure 15.12-4. Order Status Details Pages (A-D)	15-83
Figure 15.13-1. OM GUI Log Viewer Page	15-85
Figure 15.14-1. OM GUI Admin Tools Action (Permissions) Pages.....	15-88
Figure 15.14-2. OM GUI Admin Tools Profile Management Page	15-89
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 (Part 1)	16-23
Figure 16.1-12. Manage Bundling Orders Page (Part 2)	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 (Part 1)	16-31
Figure 16.1-17. Configure Completion Criteria Default Values Page (Part 2)	16-33
Figure 16.1-18. List Failed Action Page.....	16-34
Figure 16.1-19. List Statistic Page.....	16-35
Figure 17-1. EDHS and ECS Baseline Information System (EBIS) Homes Pages.....	17-2
Figure 20.3-1. EED Property Tags (Actual Size)	20-4
Figure 23-1. Login Screen	23-2
Figure 23-2. Menu Bar.....	23-2
Figure 23-3. Screen Regions.....	23-3
Figure 23-4. Transaction Headers.....	23-3
Figure 23-5. Direct Navigation	23-4
Figure 23-6. Search Functions	23-6
Figure 23-7. Expanding Search Results.....	23-7
Figure 23-8. Partial Search Results.....	23-8
Figure 23-9. Leading String Search.....	23-9
Figure 23-10. Related Screens Searches.....	23-10
Figure 23-11. Viewing an Asset record	23-11
Figure 23-12. Add and Maintain – Icon Legend	23-12
Figure 23-13. Adding a record.....	23-13
Figure 23-14. Modifying a Record	23-14
Figure 23-15. Error messages	23-14
Figure 23-16. Error messages- Icon Legend.....	23-15
Figure 23-17. Field Validation.....	23-16
Figure 23-18. Correcting Errors.....	23-17
Figure 25.1-1. Architectural Overview of the DataAccess System.....	25-1
Figure 25.2-1. Data Access Login Page	25-3

Figure 25.2-2. Data Access Collection Configuration Tab	25-4
Figure 25.2-3. Service Configuration Tab (with filter applied and context menu visible)	25-5
Figure 25.2-4. Add New Service Dialog Box.....	25-6
Figure 25.2-5. Projection Validates Selection Dialog Box	25-8
Figure 25.2-6. Collection Configuration Tab and Context Menu.....	25-9
Figure 25.2-7. Configure Service for Collection Dialog Box.....	25-10
Figure 25.2-8. Configure Hdf Objects Drop Down Menu.....	25-11
Figure 25.3-1. Monitor Tab	25-13
Figure 25.3-2. Job Information Pop-up for a Complete Job	25-14
Figure 25.3-3. Job Information Pop-up for a Failed Job	25-15

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. ECS Assistant - Activity Checklist	3-11
Table 3.9-1. Tape Operations - Activity Checklist.....	3-13
Table 3.10-1. System Backup and Restores - Activity Checklist.....	3-16
Table 3.11-1. User Administration - Activity Checklist.....	3-19
Table 4.1.1-1. Data Product Level Definitions.....	4-3
Table 4.1.2-1. Subsystem Functions.....	4-4
Table 4.1.3-1. Location of Principal Database Components	4-5
Table 4.1.5-1. Databases.....	4-7
Table 4.3.1-1. DBA Tasks Performed on a Regular Basis	4-8
Table 4.6-1. Installing Databases and Patches - Activity Checklist	4-9
Table 5.4-1. Secure Access through Secure Shell - Activity Checklist.....	5-5
Table 5.7-1. Security – Activity Checklist	5-11
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 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. CCR Form Field Descriptions	9-6
Table 10.4-1. ESDT Maintenance - Activity Checklist.....	10-10
Table 11.1-1. BMGT - Activity Checklist.....	11-3
Table 11.2-1. BMGT Configuration	11-21
Table 11.2-2. BMGT Error Configuration.....	11-25
Table 11.3-1. Manual Export - General Arguments	11-32
Table 11.3-2. Manual Export – Generated Product Arguments	11-32
Table 11.3-3. Manual Export – Run Type Arguments	11-33
Table 11.3-4. Manual Export – Item Selection Arguments	11-34
Table 11.4-1. ReExport Queue Utility Commands.....	11-37
Table 11.4-2. ReExport Queue Utility Options	11-37
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	13-7
Table 13.3-2. Home Page Field Descriptions	13-8
Table 13.3-3. Request Status Page Column Descriptions	13-12
Table 13.3-4. Ingest Request Status Allowed Actions	13-13

Table 13.3-5. Ingest Request Detail Page –Request Info Field Descriptions.....	13-18
Table 13.3-6. Ingest Request Detail Page – Granule Statistics Field Descriptions.....	13-18
Table 13.3-7. Ingest Request Detail Page – Granule List Field Descriptions	13-19
Table 13.3-8. Granule List – Granule Allowable Actions.....	13-20
Table 13.3-9. Historical Ingest Request Detail Page –Field and Column Descriptions.....	13-27
Table 13.4-1. Interventions & Alerts.....	13-44
Table 13.4-2. Open Interventions Detail – Intervention Info	13-52
Table 13.4-3. Open Interventions Detail – Granule List	13-53
Table 13.5-1. Modifying DPL Ingest Configuration	13-61
Table 13.5-2. Edit a Data Provider Configuration Parameter Descriptions	13-62
Table 13.5-3. Polling Location Page Field Descriptions.....	13-65
Table 13.5-4. Data Type Configuration Page Field Descriptions.....	13-71
Table 13.5-5. SCP or FTP Host Page Related Field Descriptions.....	13-74
Table 13.5-6. File Systems Configuration Page – Field Descriptions.....	13-81
Table 13.5-7. ECS Services Configuration Field Description.....	13-83
Table 13.5-8. ECS Services Configuration: Add Service Host - Field Descriptions	13-85
Table 13.5-9. Global Tuning Parameter Descriptions	13-93
Table 13.5-10. Volume Groups Configuration Page Field Descriptions.....	13-100
Table 13.5-11. Add Volume Group Page Field Description	13-102
Table 13.5-12. Volume Group Naming	13-104
Table 13.6-1. Reports.....	13-112
Table 13.6-2. Volume Groups History Page Field Description.....	13-117
Table 13.8-1. Data Pool Maintenance	13-120
Table 14.4-1. Starting and Stopping StorNext.....	14-4
Table 14.5-1. Loading and Removing Archive Media -Activity Checklist.....	14-11
Table 14.6-1. StorNext Backup Procedures - Activity Checklist	14-19
Table 14.7-1. StorNext Backup Procedures - Activity Checklist	14-25
Table 14.7-2. StorNext Backup Procedures - Activity Checklist	14-27

Table 14.8-1. Table Cleaning Procedure - Activity Checklist.....	14-32
Table 14.9-1. Deleting Granules - Activity Checklist	14-35
Table 14.9-2. Command Line Parameters of the EcDsBulkSearch.pl.....	14-35
Table 14.9-3. Command Line Parameters for EcDsBulkDelete.pl.....	14-39
Table 14.9-4. Command Line Parameters for EcDsBulkUndelete.pl.....	14-41
Table 14.9-5. Command Line Parameters for EcDsDeletionCleanup.....	14-43
Table 14.10-1. Data Pool Maintenance Tasks - Activity Checklist	14-47
Table 14.11-1. Data Pool Scripts - Activity Checklist	14-101
Table 14.11-2. Command Line Parameters	14-117
Table 14.11-3. Configuration File Parameters.....	14-118
Table 14.11-4. Command Line Parameters	14-124
Table 14.11-5. Configuration Parameters.....	14-125
Table 14.11-6. Command Line Parameters	14-127
Table 14.11-7. Command Line Parameters	14-129
Table 14.11-8. Configuration Parameters.....	14-130
Table 14.11-9. Command Line Parameters	14-132
Table 14.11-10. Command Line Parameters	14-134
Table 14.11-11. Command Line Parameters	14-135
Table 14.11-12. Command Line Parameter.....	14-137
Table 14.11-13. Configuration Parameters.....	14-138
Table 14.11-14. Command Line Parameters	14-141
Table 14.11-15. Configuration Parameters.....	14-142
Table 14.11-16. Command Line Parameters	14-145
Table 14.11-17. Configuration Parameters.....	14-146
Table 14.11-18. Command Line Parameter.....	14-149
Table 14.11-19. Configuration Parameters.....	14-150
Table 14.11-20. Command Line Parameter.....	14-153
Table 14.11-21. Configuration Parameters.....	14-153

Table 14.11-22. Command Line Parameters	14-156
Table 14.11-26. Command Line Parameter	14-157
Table 14.11-27. Configuration Parameters.....	14-158
Table 14.11-28. Command Line Parameter	14-159
Table 14.11-29. Configuration Parameters.....	14-160
Table 15.3-1. OM GUI Operator Security Capabilities.....	15-5
Table 15.4-1. Launch Order Manager GUI - Activity Checklist.....	15-6
Table 15.5-1. Operator GUI Security Capabilities	15-8
Table 15.6-1. Request Management - Activity Checklist.....	15-9
Table 15.7-1. Destination Monitor - Activity Checklist.....	15-41
Table 15.8-1. Archive Data - Activity Checklist.....	15-46
Table 15.9-1. OM Status Pages - Activity Checklist.....	15-50
Table 15.10-1. OM Configuration - Activity Checklist.....	15-58
Table 15.10-2. External Processing Services Parameters.....	15-70
Table 15.12-1. OM GUI Order Status - Activity Checklist.....	15-80
Table 15.13-1. OM GUI Log Viewer - Activity Checklist.....	15-84
Table 15.14-1. Admin Tools – Activity Checklist.....	15-86
Table 15.14-2. Command Line Parameters of the SCLI Tool.....	15-90
Table 15.16-1. Troubleshooting Order Manager - Activity Checklist	15-94
Table 15.16-2. Order Manager GUI User Messages	15-95
Table 15.16-3. Recovering from Order Manager Failures	15-110
Table 15.16-4. Troubleshooting HEG Problems	15-116
Table 16.1-1. Spatial Subscription Server GUI - Activity Checklist	16-1
Table 18.4-1. DAAC Hardware Problem Reporting Procedure	18-3
Table 18.4-2. Hardware Corrective Maintenance Actions	18-4
Table 18.4-3. Obtaining On-Site Hardware Maintenance Support	18-5
Table 18.4-4. Procedure for Return to Depot (Advance Replacement and Return before Replacement).....	18-7
Table 18.5-1. Procedure for Time and Material Support.....	18-8

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	20-2
Table 20.1-4. Receiving Process Checklist	20-3
Table 20.2-1. The Site Property Engineer Actions for Property Received from the Property Custodian	20-3
Table 21.3-1. Installation Planning Activity Outline.....	21-2
Table 22.1-1. COTS Training – Activity Checklist.....	22-1
Table 25.2-1. Configuring Data Access Systems - Activity Checklist.....	25-2
Table 25.3-1. Configuring Data Access Systems - Activity Checklist.....	25-12

Abbreviations and Acronyms

This page intentionally left blank.

1. Introduction

This document, Release 8.2 Mission Operation Procedures for the Earth Observing System Data and Information System (EOSDIS) Evolution and Development (EED) Contract, 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 NNG10HP02C. This reflects the system as delivered at Release 8.2.

1.2 Scope

The scope of this document is directed to Distributed Active Archive Center (DAAC) operations activities to support Release 8.2 the 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 Microsoft Word format with a master copy forwarded to the following address:

The EED Contract Office
Raytheon Company
5700 Rivertech Court
Riverdale, MD 20737

For specifics on authoring, formatting, importing, exporting and maintenance of procedures and instructions, refer to Chapter 17 Library Administration.

1.3 Purpose

The purpose of this document is to identify the procedures and instructions to operate and maintain Release 8.2 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 be used as a training aid for operations staff that is located at the DAAC 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-EED-001).

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 secure shell, system startup and shutdown, system monitoring, tape operations, system backup and restore, log maintenance, user administration, and COTS software administration.
- 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 and system monitoring, password protection, file modification and logging system access monitoring, detection and reporting of security breaches .
- Section 6 **Network Administration.** Identifies the operations procedures and/or operations instructions for network administration activities, such as network and system configuration monitoring, and control and monitoring of the system network capabilities.
- 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 monitoring and controlling problems reporting and

resolution. This is handled through submitting, processing, tracking 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 ECS component used for generation of the external metadata representation of ECS holdings. The distinct data products generated by BMGT are exported to the EOSDIS ClearingHouse (ECHO) and ingested into the ECHO database where they are made available to ECHO clients such as Reverb.
- Section 12 **Quality Assurance.** Identifies the operations procedures and/or operations instructions to perform management of Quality Assurance (QA) metadata, the QA Update utility (QAUU), consolidation of the QAMUT utility from SDSRV into a single utility, and identifying input file data format updates.
- Section 13 **Data Pool Ingest.** Identifies the operations procedures and/or operations instructions to support data acquisition.
- Section 14 **Archive Management/Data Pool Maintenance.** Identifies the operations procedures and/or operations instructions for archiving activities, such as archive repository maintenance, fault monitoring and notification, and temporary data storage. Providing a persistent data store for all science and ancillary data; all browse data files; and all XML metadata, ESDT definition, and XML schema files.
- Section 15 **Distribution Concepts.** Identifies the operations procedures and/or operations instructions to support data distribution activities, order management, 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 and data subscriptions insertion.
- 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 EED project.
- Section 19 **COTS 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 EED 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 point of contract, training scheduling, and training record maintenance.
- Section 23 **Inventory Logistical Management (ILM).** The Asset Smart ILM helps the operations staff at EDF 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.
- 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.
- Section 25 **EOSDIS Service Interface (DataAccess).** Identifies the operations procedures and/or instructions for configuring and operating the EOSDIS Service Interface.
- **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.

	Statement of Work for EED Contract
423-CDRD-001	Contract Data Requirements Document for EED Task 02 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.

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 EED Project.

105-EED-001	Property Management Plan for the EED Project
110-EED-001	Configuration Management Plan for the EED Project
170-EMD-003	A Data Formatting Toolkit for Extended Data Providers to NASA's Earth Observing System Data and Information System
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-EED-001, Rev. 02	Release 8.2 Operations Tools Manual for the EED Contract
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-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 EED 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-EED-001, Rev. 02	Release 8.2 Segment/Design Specifications for the EED Contract
311-EED-001, Rev. 02	Release 8.2 INGEST (INS) Database Design and Schema Specifications for the EED Contract
311-EED-002, Rev. 02	Release 8.2 Order Manager (OMS) Database Design and Database Schema Specifications for the EED Contract
311-EED-003, Rev. 02	Release 8.2 Spatial Subscription Server (SSS) Database Design and Schema Specifications for the EED Contract
311-EED-005, Rev. 02	Release 8.2 Archive Inventory Management (AIM) Database Design and Schema Specifications for the EED Contract
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-TD _x -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

This page intentionally left blank.

3. System Administration

3.1 Overview

The following sections define step by step procedures for the routine tasks performed by ECS System Administrators. Topics covered are as follows: ssh, system startup, and shutdown, system monitoring, tape operations, system backup and restore, user administration, and Commercial Off The Shelf (COTS) software administration.

3.2 Secure Access to DAACs

The Local Area Network (LAN) at the DAACs is more secure than most other LANs. There is a set of hosts that are externally advertised to the Internet. Access to these hosts requires the use of SSH and 2-Factor Authentication. 2-Factor Authentication is covered in section 5.2 of this document.

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.

3.3 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 LINUX 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 12 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 environment 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 12 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 environment 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 LP DAAC
4 ASDC 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 environment 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 12 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 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 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 *x5dpl01* as user *cmops* enter:
ssh -l jdoe x5dpl01
 - 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 x5dpl01
- or -
ssh -l cmops x5dpl01
 - Examples of Linux host names include **e5dpl01**, **l5oml01**, **n5eil01** and **p5oml01**.
 - 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	Performing Normal Shutdown	(P) 3.7.3.1	
4	SA	Performing Emergency Shutdown	(P) 3.7.4.1	

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
 - PostgreSQL Server
- 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 PostgreSQL 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
 - PostgreSQL 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 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.

3.7.3.1 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 Linux prompt type **shutdown -g0 -i0** or **init 0** 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
 - PostgreSQL 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 PostgreSQL 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.
-

3.7.4 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.

3.7.4.1 Performing Emergency Shutdown

- 1 Log in to the server as root.
- 2 Type *root_password* at the Linux prompt then press the **Return/Enter** key.
- 3 Type **init 0** at the Linux prompt then press the **Return/Enter** key.
- 5 Shutdown all client workstations.
- 7 Determine which machines perform the following functions (some machines may perform multiple functions).
 - PostgreSQL
 - Mail Hub
 - NFS/ClearCase
 - DNS/NIS
- 8 Power off the PostgreSQL/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).
-

3.7.5 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 ECS Assistant

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 3.8-1 shows the ECS Assistant GUI for access to manager functions, the ECS Assistant subsystem manager GUI, and an example of a confirmation dialog.

Table 3.8-1 contains the activity checklist for ECSAssistant.

Table 3.8-1. ECS Assistant - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Starting ECS Assistant	(P) 3.8.1	

3.8.1 Starting ECS Assistant

- 1 Log in to one of the host machines.
- 2 At the Linux 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 Linux 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.

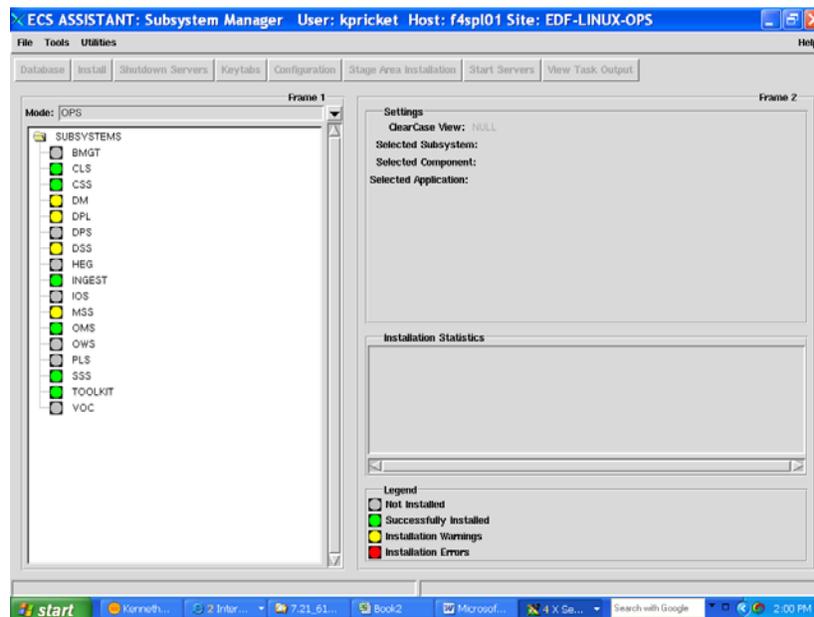


Figure 3.8-1. ECS Assistant GUI Manager Windows

- 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.
-

3.9 Tape Operations

In this document you will learn how Networker Administrative software, the Quantum DXi7500 appliance, and the Scalar 50 tape library work together to administer the use of virtual and physical 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 3.9-1 contains the activity checklist for Tape Operations.

Table 3.9-1. Tape Operations - Activity Checklist

Role	Task	Section	Complete?
SA	Networker Login Procedures	3.9.1.1	
SA	DXi7500 Login Procedure	3.9.1.2	
SA	Performing Tape Labeling For DXi7500	3.9.2.1	
SA	Tape Rotation Procedures for Scalar 50 When Reusing Tapes in Library	3.9.2.2	

Key Terms:

- **Cartridge** – We use LTO4 tapes and they can hold up to 800GB of data in uncompressed mode and up to 1.6 TB when compressed.
- **Drive** - Hardware device into which the tape or tape cartridge is inserted that performs the actual recording of data. We are using LTO4 drives.
- **Inventory** - The action of making an index.
- **Virtual Tape Library (VTL)** – disk storage is configured as tape to allow faster backups and restore with existing [backup software](#) and existing backup and recovery processes and policies.
- **De-Duplication** – The process of reducing data storage by storing data once. If the data shows up again, pointers to the first occurrence are used which takes less space then storing the data again.
- **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 50 is attached directly to the backup server by a fibre cable. It has 2 LTO4 tape drives and can hold up to 38 LTO4 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.

3.9.1 Networker Administrator Screen

3.9.1.1 Networker Login Procedures

- 1 Login to <*Backup Server*> as root.
 - 2 Start Mozilla firefox. .
 - 3 Browse to Networker NMC (URL <http://<Backup Server>:9000>).
 - 4 Login to Networker
 - 5 Choose enterprise at the top.
 - 6 Left click <servername> in left pane.
 - 7 Double click Networker in right pane (launches Networker application).
 - Backup Servers by DAAC:
 - NSIDC n4msl21
 - LP e4msl21
 - ASDC l4msl21
-

3.9.1.2 DXi7500 Login Procedure

- 1 Login to <*Backup Server*> as root
 - 2 Start Mozilla firefox. .
 - 3 Browse to Admin page (URL <http://<DXi7500 Appliance IP>>).
 - 4 Login to *DXi7500*.
 - Username: admin Password: <*Password set by System Admin*>.
-

3.9.2 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 DXi7500 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.

3.9.2.1 Performing Tape Labeling For Scalar 50

Blank Tape Rotation Procedures for Scalar

*Note: These steps assume the tape being newly labeled is brand new or does not have a label. If it is an old tape being reused see the section titled “Tape Rotation Procedures for Scalar 50 When Reusing Tapes Already in Library”.

- 1 Stop all backups (if running) and unmount all 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 From the Networker GUI, label the 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 <Scalar 50>.
 - You should now see unused labeled tape in its slot.
-

3.9.2.2 Tape Rotation Procedures for Scalar 50 When Reusing Tapes in Library

When a used tape is inserted into the library, the library will reinventory the slots and you will see that tape in the Networker GUI

From the Networker GUI, label the physical tape:

- Right click the <unlabeled> or <labeled> tape and choose Label.

- Make the following choices:
- Select Pools: Put the new tape in the desired pool.
- Press OK.

You should now see the tape loaded into a drive labeled and put back in the jukebox slot.

3.10 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 either the VTL or the backup tapes.

Table 3.10-1 contains the activity checklist for System Backup and Restores.

Table 3.10-1. 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	

3.10.1 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 in the VTL and 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.

3.10.1.1 Performing System Backup

-
- 1 Login to *<Backup Server>* as root.
 - 2 Start Mozilla firefox /tools/firefox/firefox.
 - 3 Browse to Networker NMC (URL http://*<Backup Server>*:9000).
 - 4 Login to Networker
 - 5 Choose enterprise at the top.
 - 6 Left click *<servername>* in left pane.
 - 7 Double click Networker in right pane (launches Networker application).
 - 8 Select the monitoring button
 - 9 Right click the group and select start or click the start button
-

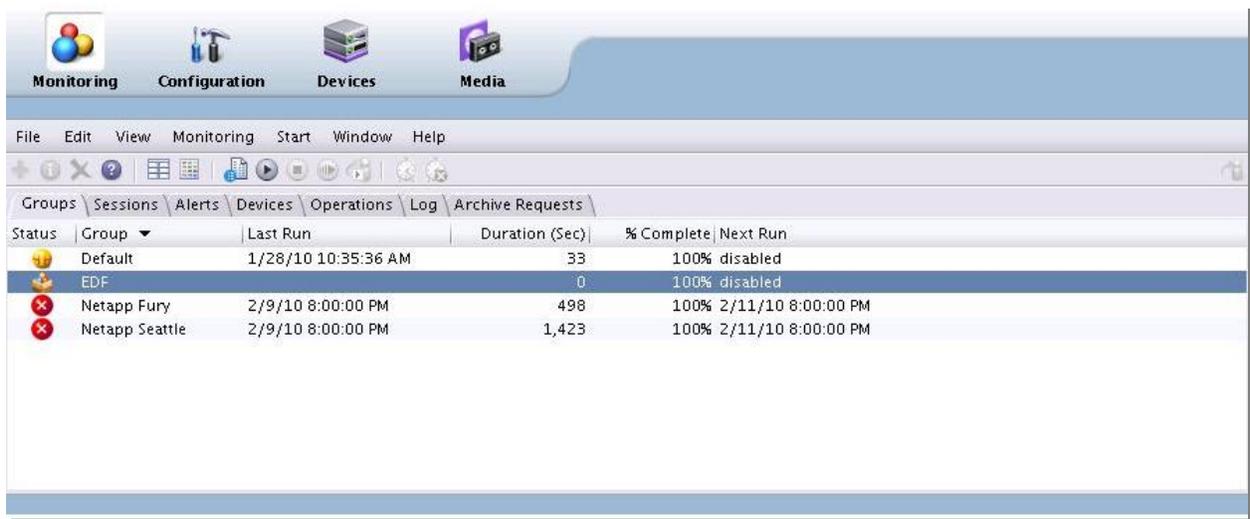


Figure 3.10-1. Networker Backup Window

3.10.2 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

3.10.2.1 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 5.
 - 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 6.
- 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 Linux 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. You are now able to restore files.
- 10 Select **file(s) to be restored**.
 - 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 User Administration

3.11.1 Screening Personnel

Table 3.11-1 contains the activity checklist for User Administration.

Table 3.11-1. 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	

3.11.1.1 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 2810.1A 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 1600.1A 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.

3.11.2 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.

3.11.3 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 Linux text editor and the files **/etc/passwd** (Figure 3.11-1), **/etc/group** (Figure 3.11-2) and **/etc/auto.master**.

The System Administrator (SA) creates a new user account with command-line/script entries. As an example, The EDF uses 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.

3.11.4 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.

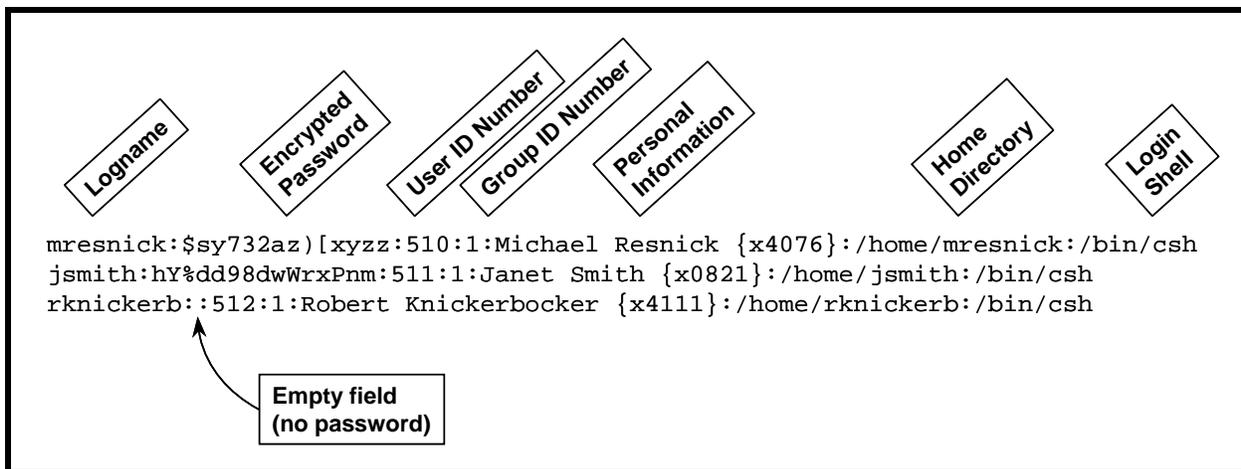


Figure 3.11-1. /etc/passwd File Fields

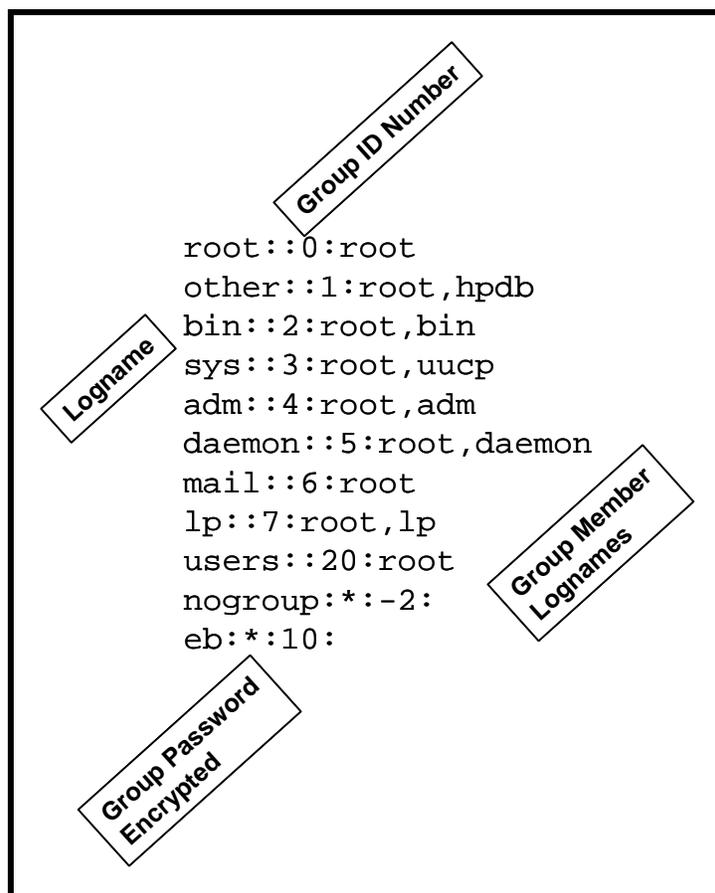


Figure 3.11-2. /etc/group File

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:

- **Linux 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 EDF uses 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.

3.11.5 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 Linux Group
 - New Login Shell
- Current Linux Login of the User

3.11.6 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
- System login of the user

3.11.7 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:

- System 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.

3.11.8 Checking a File/Directory Access Privilege Status

3.11.8.1 Checking File/Directory Access Privileges

- 1 At a system 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 system 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.

3.11.9 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)

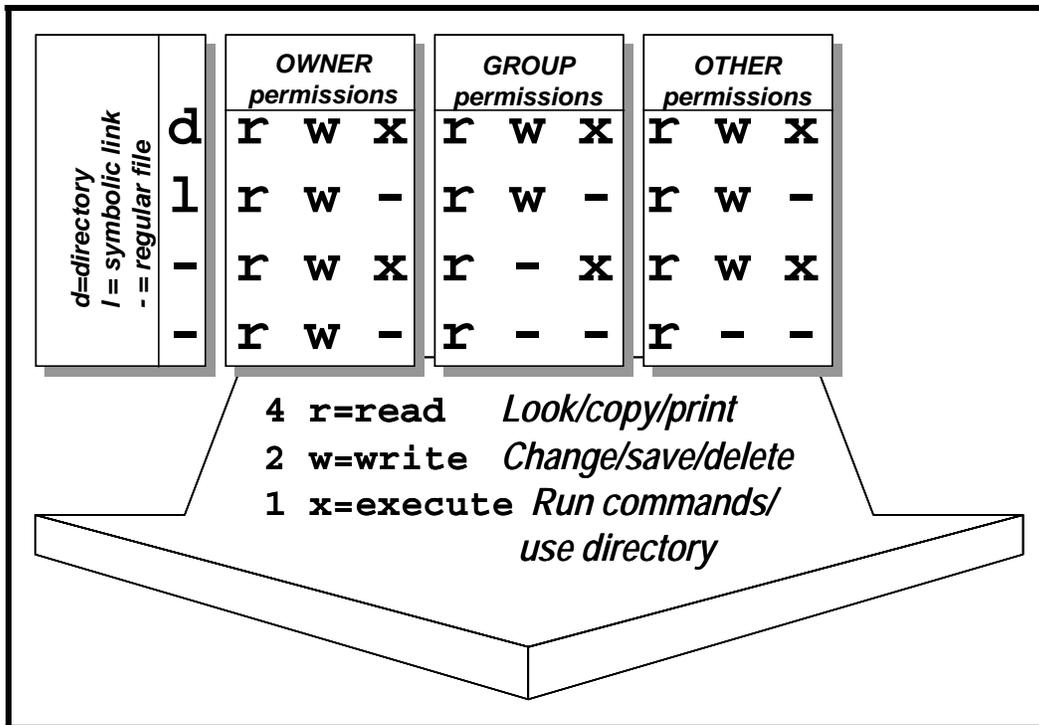


Figure 3.11-3. Access Permissions

3.11.9.1 Changing a File/Directory Access Privilege

- 1 At the system 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.
-

3.11.10 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.

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

The ECS organization provides maintenance for ECS hardware, software, and firmware systems delivered under the ECS contract to the ECS sites. The project maintenance philosophy for software is to provide ECS centralized support for developed items and vendor support for COTS software.

3.12.1 Installation

ECS 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 ECS management.

3.12.2 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.

3.12.3 COTS Configuration

The COTS software upgrades are subject to CCB approval before they may be loaded on any platform. ECS 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.

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 4.1.1-1. 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-EED-001, Implementation Earth Science Data Model for the EED 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.

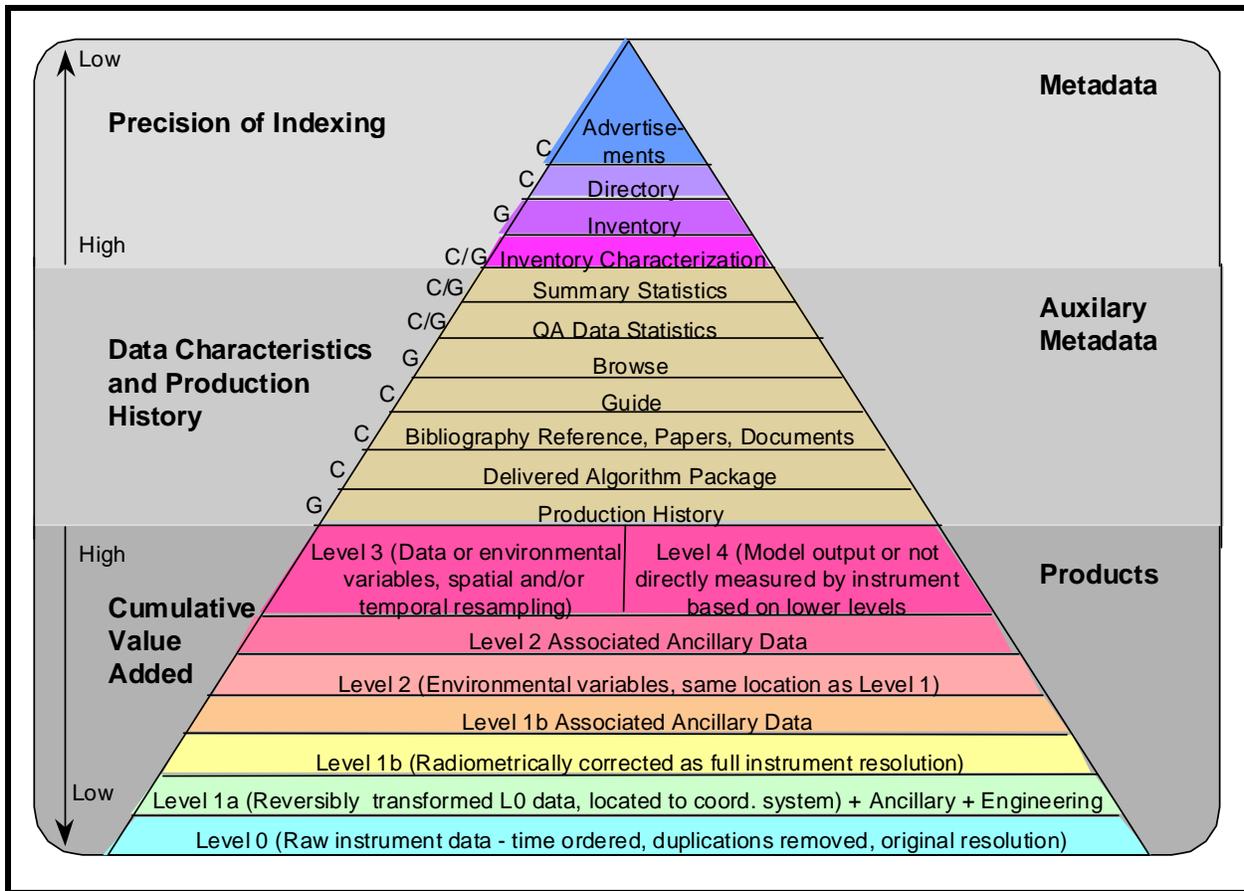


Figure 4.1.1-1. Earth Science Information Model

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 4.1.1-2 and described in Table 4.1.1-1.

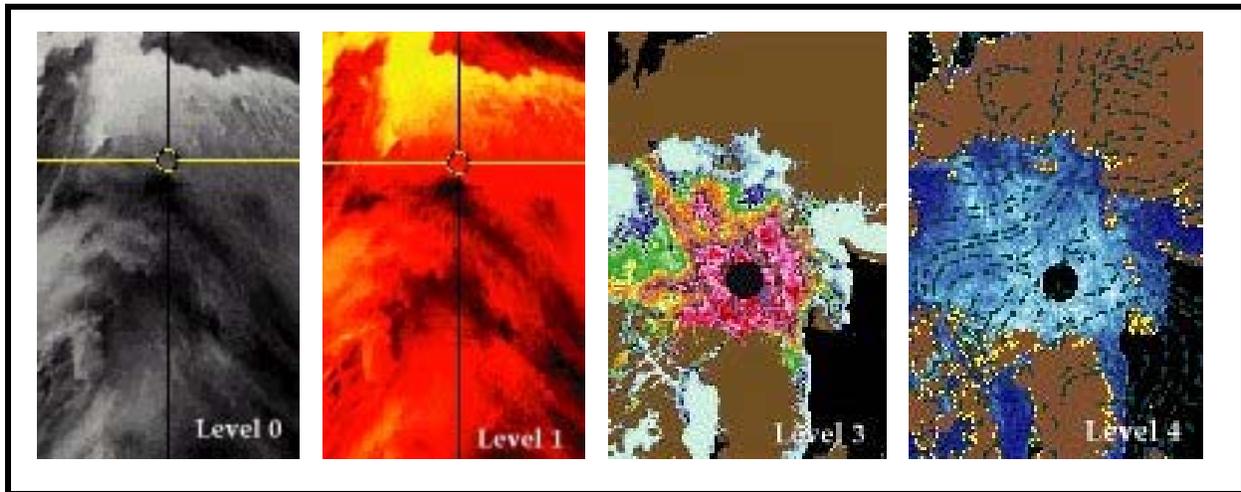


Figure 4.1.1-2. An Example of Data Product Levels

Table 4.1.1-1. 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 4.1.2-1. More detailed information can be found in the *Segment/Design Specification for the EED Contract (305-EED-001)*. 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. 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.
- **Spatial Subscription Server.** Provides the capability to register “subscriptions” to data collections based upon several different granule level metadata attributes (including spatial coverage attributes). Also evaluates ingested granules against existing Subscriptions and carries out associated actions.
- **Order Manager.** Provides both “push” and “pull” order processing for granules within the archives.

Table 4.1.2-1. Subsystem Functions

Subsystem		Functions
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 <i>ad hoc</i> or scheduled basis and deals with external system interfaces
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)

4.1.3 Databases

Custom Databases. The SDPS RDBMS model utilizes a single database per instance. The site can create an instance for each mode or the site can use a single instance for the OPS mode and combine multiple test modes into another single instance. Each mode is made up of several RDBMS schema/name spaces; these schema hold the persistent data (tables) for the subsystem.

Table 4.1.3-1 lists these schema and describes the type of data stored. Other data requirements are met through the use of flat files, which are described below. All custom databases are implemented using PostgreSQL.

Table 4.1.3-1. Custom Databases

Database Name	Document Number	DB Software	Logical Categories
Archive Inventory Management Subsystem (AIM)	311-EED-005	PostgreS QL	Database Version Information
			System Management Data
			Collection, Granule Metadata
			DAP Metadata
			Spatial Metadata
			Granule Metadata
			Collection Metadata
			Temporal Metadata
			Data Processing Data
Ingest Subsystem (ingest)	311-EED-001	PostgreS QL	Database Version Information
			Datatype Information
			Configuration Data
			Active Requests
			Validation Data
			Table Locking Information
Common Tools (common)	N/A	PostgreS QL	Functions used by other subsystems
Order Manager Server (oms)	311-EED-002	PostgreS QL	Queue/Status Information
			Request Information
			Intervention Information
Spatial Subscription Server (sss)	311-EED-003	PostgreS QL	Database Version Information
			Subscription Information
			Event Information
			Action Information

4.1.4 Resident Databases - DELETED

4.1.5 Database Directory Locations

Locations of principal database components are shown in Table 4.1.5-1.

Table 4.1.5-1. Location of Principal Database Components

Name	Variant	Vendor	Principal Directory	Comments
Software Developer's Kit (postgres client tools)	LINUX	Postgres	/tools/postgres	Contains client programs as well as shared libraries

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 EED 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. EED 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 PostgreSQL software. Primary components include:

PostgreSQL server PostgreSQL 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 PostgreSQL's client/server architecture.

4.2.3 Hardware, Software, and Database Mapping

Currently, RDBMS instances reside on Linux machines. The hardware layout diagrams are available in documents 920-TDx-001, *Hardware-Design Diagram*. Hardware to software mappings are available in documents 920-TDx-002 *Hardware-Software Map*. The hardware database mappings are available in document 920-TDx-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 .
- Maintaining user accounts for the users from the external system.
- Working with EED 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 4.3.1-1 shows DBA tasks that have to be done on a regular basis and the section where they are addressed in this document.

Table 4.3.1-1. DBA Tasks Performed on a Regular Basis

Time Period	Task	Importance	Found In ...
	Remove old backup files.	Keeping track of seven (7) days worth of retrievable data or can specify another value.	The pgbackup.pl utility does this automatically. This utility should be executed via a cron entry.
Weekly	Monitor PostgreSQL disk usage		Monitoring and Tuning Databases
	Reclaim Disk Space	Improves performance by compacting tables into fewer disk blocks	This should be done during the weekly preventative maintenance period.
Monthly	Reboot		Starting and Stopping Servers

4.4 Starting and Stopping Database Servers

The PostgreSQL RDBMS was delivered with a custom code script for starting and stopping an instance called “postgres_start_stop.” This script should be copied to the postgres user’s script directory and renamed to add a suffix for the instance (for example: postgres_start_stop_ops). This process should be repeated for each instance of PostgreSQL running at the DAAC. The script for each instance must also be modified to specify the correct values for the following two variables:

POSTGRES_HOME=/usr/ecs/OPS/COTS/postgres/current_ops

DATA_HOME=/pg_data/ops/current/data

4.4.1 Start a PostgreSQL Instance

An instance can be started by the postgres linux user with the following command:

```
> postgres_start_stop_<instance> start
```

4.4.1.1 Stop the PostgreSQL instance

The instance can be stopped by the postgres linux user by issuing the following command:

```
> postgres_start_stop<instance> stop
```

4.5 Creating Database Devices - DELETED

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 Patch 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-EED-001, Revision 02 *Release 8.2 Operations Tools Manual for the EED Contract*.

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/postgres/<SUBSYSTEM>` directory.

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.

```
# psql -h <server_name> -d ecs -U <db_user_name> -p <port_number>
#
# select * from <subsystem_schema>.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 than 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**.

4.7 Configuring Databases

4.7.1 Configure the PostgreSQL Server Parameters

The PostgreSQL server parameters are stored in the postgresql.conf file within the instances data directory. The PostgreSQL RDBMS was delivered with three different postgresql.conf files (postgresql.conf.test, postgresql.conf.maintenance, postgresql.conf.oltp). Each of these files contains the server parameter values that are appropriate for its named purpose. For example: if a test instance needs to be configured the postgresql.conf entry in the data directory should be a symbolic link to postgresql.conf.test. If a large maintenance operation is required on an instance then it would be appropriate to change the symbolic link to postgresql.conf.maintenance. All of these sample configuration files are located in the data directory and the server should be stopped and started whenever the symbolic link to the postgres.conf file is changed. The start utility can be used to bounce the server using the following command:

```
>postgres_start_stop_<instance> restart
```

4.8 Working with Indexes, Segments, and Caches - DELETED

4.9 Backing Up and Recovering Data

The PostgreSQL RDBMS within SDPS utilizes two file systems on the database server. The first file system is used to store the data files and transaction logs; it is mounted as /pg_data. The second file system is used to store backups of the data files and transaction logs; it is mounted as /pg_backup. Each of these file systems has separate directories for managing each RDBMS instance running on the server.

A backup utility called pgbakup.pl was provided to perform “online” backups of the instance. The utility uses a PostgreSQL utility called pg_base_backup to perform the actual online backup. The SDPS pgbakup.pl adds the knowledge of the SDPS architecture to the pg_base_backup and it also adds the ability to specify a retention parameter for the number of backups to keep in the /pg_backup file system. The pgbakup.pl utility will remove old backups up to the number of backup copies specified for retention.

A crontab entry should be created for the postgres linux user to perform a nightly backup. An example cron entry might look like:

```
#--- Nightly backup -----
```

```
00 03 * * * /usr/ecs/OPS/COTS/postgres/scripts/pgbakup.pl --instances=ops,test --retain=10 -  
-mail
```

This crontab entry performs a full backup of the “ops” and “test” instances, retains 10 backup copies of each instance. It also sends out an email to notify all interested parties that the backup is complete. The script utilizes a pgbakup.cfg file which allows the configuration of email addresses for notification, the instances that are available for backup, and for each instance the host name and port number that is supporting the instance. This configuration file should be updated before the first use of pgbakup.pl; it can also be updated as needed to add or remove email addresses or if a host name or port number changes.

4.9.1 Perform Manual Backups

The pgbakup.pl utility can also be run from the command line, however PostgreSQL provides utilities to export or import data that can also be useful. These utilities are called pg_dump and pg_restore and they can be used to export an entire database, a schema, or even just a single table. It is important to note that these dump files represent a point in time “snapshot” of the data and they can’t be used with the pgbakup.pl backups. Please refer to the PostgreSQL documentation for a full description of these utilities.

Both the **dump database** and **dump transaction**

4.9.2 Perform a User Database Recovery (Order of Procedures)

Database recovery is described in the PostgreSQL documentation (chapter 24.3.4). The only thing specific to SDPS is the knowledge of where the data files and backups are stored. As mentioned before, data files are stored in the /pg_data file system and backups are stored in /pg_backup. Also note that SDPS does not use tablespaces. Database recovery can start as far back and the number of backups that are configured in the retention parameter to pgbackup.pl and can be restored to a specific point in time.

4.10 Establishing Database Security – DELETED

4.11 Copying and Extracting Data – DELETED

4.12 Bulk Copying – DELETED

4.13 Monitoring – DELETED

4.14 Tuning – DELETED

4.15 Ensuring Database Quality – DELETED

4.16 Sybase Troubleshooting - DELETED

5. Security Services

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS 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 – OSSEC Host Based Intrusion Detection System (HIDS), RSA SecurID, RSA Authentication Agent for PAM, and Attachmate Reflections for Secure IT (RSIT). OSSEC monitors for intruders by logging system access and changes to files. Attachmate Reflections for Secure IT (RSIT) Secure Shell (ssh) provides strong authentication access and session encryption from external, non-trusted networks as well as internally within a DAAC. RSA Authentication Agent for PAM and RSA SecurID work in conjunction with RSIT SSH to provide 2-Factor Authentication for host access from external sources. Security Services also supports detection of, reporting, and recovery from security breaches. Security scans of each system are performed monthly 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 sections define step-by-step procedures for Security 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 ECS contract 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 ECS 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. The software and the keys must be obtained through ESDIS CSO.

5.2 2-Factor Authentication

All NASA programs have a Headquarters-mandated requirement to implement 2-factor authentication for external interactive access. 2-factor authentication is combined use of:

- A **shared secret** that can be synchronized between a local device such as a token and server-based software,

- A Personal Identification Number (PIN) or other numeric **user secret** known only to the user. This is generated the first time the user attempts to login.

To support GSFC requirements as specified in the Shana Dale memo of July, 2006, both trusted (root) and untrusted (normal user) **external** interactive access must authenticate using 2-factor. Password and even passphrase authentication are not adequate. External access is generally defined as access from the Internet. On-campus access is considered local. The EMC/RSA SecurID product has been selected by NASA as well as ECS as the standard 2-Factor Authentication product until the government smart card-based system becomes available.

In addition, the Federal Information Security Management Act (FISMA) based Certification and Authorization (C&A) rules also require remote access to be POSIX-standard login control. This augments Secure Shell (SSH) capabilities to be the same or better than what POSIX standard operating systems provide for console access.

5.2.1 RSA SecureID Administration

5.2.1.1 Accessing the RSA SecurID Remote Administration Utility

1. Secure shell into any linux blade in production.

```
$ ssh p4wg101
```

2. Use the rdp program to access the appliance:

```
$ rdesktop <applianceIPAddress>:8198
```

3. A login window should popup. Login with an administrative account/token:

Username: *administrator*

Password: <PIN> + <TOKENCODE>

4. This will bring up a MS Windows desktop. To administer the appliance, select the following:

“Start” -> “All Programs” -> “Administrative Tools” -> “Web Interface for Remote Administration”

5. Login with an administrative account/token.

5.2.1.2 Add a User and Assign a Token

From the RSA SecureID Remote Administration Utility **Home** screen:

1. Select the **Users** tab or click **Add Users and Assign Tokens**
2. Click the **New...** button
3. Enter the **First Name** in the ‘First name:’ box

4. Enter the **Last Name** in the ‘Last name:’ box
 5. Enter the **User ID** in the ‘User ID:’ box
- Note:** The user ID must be the same as their UNIX login ID.
6. From the ‘Token serial number:’ pull down menu, select a token serial number
 7. Click **OK**

5.2.1.3 Clear a PIN

You may need to clear a user’s PIN if they are not able to connect using their current PIN. It is also a good idea to do this when issuing a new token.

From the RSA SecureID Remote Administration Utility **Users** tab:

1. Find the user and click the radio button next to their User ID
2. Click **View Tokens**
3. Click the **Clear PIN** button on the right side of the screen
4. Click **OK** at the ‘Clear PIN Confirmation’ screen

5.2.1.4 Enable a Token

If a user incorrectly enters their PIN more than 3 times, it will disable their token. From the RSA SecureID Remote Administration Utility **Users** tab:

1. Find the user and click the radio button next to their User ID
2. Click **View Tokens**
3. Click the **Edit Token Status** button on the right side of the screen
4. Check the box next to ‘Enabled:’
5. Click **OK**

5.2.1.5 Import New Tokens

When new tokens are received, the token seed file must be imported into the RSA appliance. The seed file is downloaded from RSA by following the directions that come with the tokens. In some instances, the seed file will be downloaded from Riverdale. Once you have obtained the seed files and the password that goes with them, you will need to sftp them to the appliance. After the seeds are transferred to the appliance, go to the **Tokens** tab in the RSA SecureID Remote Administration Utility:

1. Click the **Import New Tokens** sub-tab
2. Click the **Browse...** button

3. Navigate to the location of the seed file and select the file
4. Click **Open**
5. Click the **Upload File** button
6. Enter the **File Password** in the 'File password:' box
7. Click **OK**

5.2.2 RSA Authentication Agent for PAM

Both SecurID and RSA Authentication Agent for PAM use a subsystem called Pluggable Authentication Modules or PAM. RSA Authentication Agent for PAM enables an integrated access control mechanism that limits or enables access to ECS hosts externally by user, group, date, day and/or time. Once installed by following the Release Notes, RSA Authentication Agent for PAM does not require further administration.

5.3 Aging Passwords

Password aging is required by NPR 2810.1, *NASA Procedural Requirements: Security of Information Technology*. There are various methods for implementing password aging, dependant upon the architecture of the environment. If NIS is in use, password aging can be achieved via scripting. If NIS is not in use, it can be done manually on each system. There are also software packages that will provide this feature. The DAACs use different methods based on their environments.

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 Attachmate Reflections for Secure IT (RSIT).

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	Configuration of Secure Shell	(P) 5.4.7	

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://pete.edf.rvl.us.ray.com>

5.4.2 The SSH Encryption Mechanism¹

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 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 EED 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,

¹ From the *sshd* man page

RSA challenge-response authentication, or password-based authentication. (NOTE: In the EED 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

1 To login, use the command:

```
% ssh 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 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.

5.4.5 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 thisisfilename ↵
sftp> put thisotherfilename ↵
sftp> quit ↵
```

5.4.6 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!

5.4.7 Configuration of Secure Shell

5.4.7.1 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.

5.4.7.2 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!

%

5.4.7.3 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!

5.4.8 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: The only DAACs that still use TCP Wrappers are NSIDC and ASDC. The EDF and other DAACs use Juniper firewalls, which are covered under section 6.7 of this document.

5.6 Monitoring File and Directory Integrity (OSSEC)

OSSEC is a tool that aids in the detection of unauthorized modification of files resident on UNIX systems. One important application of OSSEC is its use as the first and most fundamental layer of intrusion detection for an organization. OSSEC 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. OSSEC flags and logs any differences, including added or deleted entries. When run against system files regularly, OSSEC 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 OSSEC, system administrators can conclude with a high degree of certainty that a given set of files remain free of unauthorized modifications if OSSEC reports no changes. OSSEC works in conjunction with these other solutions to provide a "Defense in Depth"(trademark) security solution.

The system administrator should install OSSEC 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 OSSEC 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. OSSEC should be configured to mail the system administrator any output that it generates.

5.6.1 Installation of OSSEC

Use the procedures provided in the Release Notes for the relevant version of OSSEC. Release Notes are available through the “Release Notes” link at the following URL:

<http://pete.edf.rvl.us.ray.com>

5.6.2 Configuring the ossec.conf File

There are several configuration options for OSSEC. These are contained in the ossec.conf file, located in the ../ossec/etc directory on each host. All the rules, decoders and major configuration options are stored centrally in the manager, making it easy to administer even a large number of agents. Detailed information for configuring the various options can be found at <http://www.ossec.net/doc>.

5.6.3 Monitoring OSSEC

OSSEC monitoring is done through the OSSEC Web User Interface (WUI). The URL to access the WUI is <http://x4msl10:8001>. This is the address for your local OSSEC management server.

5.7 Generating Security Reports

Table 5.7-1 contains the activity checklist for Security.

Table 5.7-1. Security - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	User Activity Data	(P) 5.7.1	

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.

5.7.1 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 `tty`s can be abbreviated, thus `last 0` is the same as `last tty0`.
-

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.

5.8 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.

5.9 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.

This page intentionally left blank.

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

EED Network Administration requires access to restricted documents that are posted on the ECS 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 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-EED-001, Revision 02 Release 8.2 Operations Tools Manual for the EED Contract.

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.

There are few common and uniquely designed network features implemented in each of the DAACs

- The Production Network at each Distributed Active Archive Center (DAAC) consists of an Ethernet Virtual Local Area Network (VLAN) supported by Ethernet 100-Mb/s and Gigabit Ethernet (GigE) connections and a SAN LAN GigE switch.
- The VLAN Ethernet switch is connected to a Juniper Firewall by a Gigabit Ethernet connection with the exception of ASDC which connects directly to the Langley NASA campus core network..
- NSIDC network is connected through Colorado University Campus. With a netflow router managed by EED
- LP DAAC Primary ISP is campus their firewall provides access to both M&O, and Production Campus. The DMZ High speed subnet is accessible with a separate 10G/s interface on public facing host. Public DMZ is design to allow uninterrupted service for data downloads that over 1Gb/s accumulatively.

System hosts within a DAAC are connected to the Production VLAN Ethernet switch. The switch is used to connect hosts at 100/1000 Mb/s. The VLAN Ethernet switch is connected to the Juniper Firewall via a 1000-Mb/s (GigE) connection.

Each of DAACs have HP Flex Ethernet module in place with 3 Gb/s redundant aggregated links. The primary NSIDC, LP DAAC and PVC are trunking three VLANs over these uplinks for Management, Metadata and Production network. ASDC Management and Metadata VLANs are handled by their Cisco Catalyst 3750X Layer 3 Metadata switch. All of the StorNext SAN clients and MetaData servers are connected to the Metadata LAN GigE switch across the DAACs

6.4 Network Hardware Components

The DAAC LANs consist of the following major hardware components:

- Juniper Firewall (NSIDC controlled and LP DAAC which is USGS controlled)
- Production VLAN Ethernet Switch.
- Metadata LAN GigE Switch.
- HP Flex10 10G Network modules (integrated in HP Blade c7000 Chassis)

6.4.1 Juniper Firewall

The Juniper Firewall hardware consists of Juniper SRX 650 appliance running JUNOS 10.x operating system. It contains a routing engine and packet forwarding, as well as a pair of redundant power supplies.

6.4.2 Production VLAN Ethernet Switch

The Ethernet switch at each DAAC is a Cisco Catalyst 6506E, which provides a large number of 100 and 1000-Mb/s interfaces. The VLAN1 Ethernet switch interfaces with all Production hosts

and the Juniper Firewall. The VLAN10 Ethernet switch interfaces with the Juniper 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 EED.

6.4.3 Metadata SAN LAN GigE Switch

The GigE Switch is Cisco Catalyst 3560G module and is placed at LP DAAC, NSIDC and PVC. It connects the StorNext SAN clients and MetaData servers to a high-speed private network. LaRC is utilizing Cisco 3750X switch, which is a newer module of its predecessor.

Maintenance and configuration of the SAN LAN GigE Switch are considered non-trivial functions. Such tasks are addressed in special technical training provided by the vendor and supplemental training provided by EED.

6.5 Domain Name Service (DNS) Structure

The parent DNS domain for the system is **ecs.nasa.gov**. These DNS servers reside within IONet at GSFC. In this domain are the User and Production hosts for all DAACs.

The ecs.nasa.gov Authoritative DNS servers are:

NASA External

- ns1.nasa.gov
- ns2.nasa.gov
- ns3.nasa.gov

NASA EBnet-Open

- ns1.ipam.eosdis.nasa.gov
- ns2.ipam.eosdis.nasa.gov
- ns3.ipam.eosdis.nasa.gov

NASA EBnet-Split

- ns5.ipam.eosdis.nasa.gov
- ns6.ipam.eosdis.nasa.gov
- ns7.ipam.eosdis.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)
- NSIDC Production network:
 - n4nsl01.nsidcb.ecs.nasa.gov (internal)

- n4nsl02.nsidcb.ecs.nasa.gov (internal)

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:
 - ns1.nasa.gov (external)
 - ns2..nasa.gov (external)
 - ns3.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 e4eil01.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. This is achieved through the use of a stateful firewall at each site. Access to a DAAC's Production network is controlled by Juniper firewalls either under the direct control of the DAAC or via the campus network administrator (note: ASDC has production network is controlled by the NASA Langley campus network team and thus uses a different firewall). See your local firewall administrator for information on how the firewalls are configured. 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:

- Determining whether the Domain Name Service (DNS) is resolving host name and IP addresses correctly.
- Actively testing the connectivity using the ping function.
- Ensuring connectivity is authorized (See your local firewall administrator for information on what remote connectivity is allowed)

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.gsfc.nasa.gov
Address: xxx.xxx.xxx.xx
Name: g0spg01.gsfc.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.gsfc.nasa.gov
Address: xxx.xxx.xxx.xx
Name: g0css02.gsfc.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.gsfc. 9182666 1 8103032 0 0
hip0 65280 xxx.xxx.xg0spg01h.gsfc. 5554524 0 6776651 0 0
xpi0 4352 xxx.xxx.xxx.xg0spg01u.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 0xfffff00 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.gsfc.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.gsfc.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.gsfc.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.gsfc.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 Juniper firewall implementation. 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.xg0spg01u.	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 implementation. See your local firewall administrator for assistance when troubleshooting connectivity issues with hosts outside of the Production network.

This page intentionally left blank.

7. System Monitoring

7.1 Overview

This chapter covers procedures for the management operations that monitor the network and server applications. The graphical tool available to monitor system status include **Big Brother Better Than Free Edition (BTF)** and **Hyperic HQ Enterprise v4.3 (HQ)**. These programs provide system monitoring 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/host monitoring and notification COTS application. DAAC network administrators use it to monitor network devices, hosts 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, hosts and services on the EED Production LANs. (URL Example; <http://f4msl10.hitc.com>). Big Brother capabilities are executed through the use of GUIs. Figure 7.2-1 Big Brother Home Page is an example of the standard or default view of the homepage.

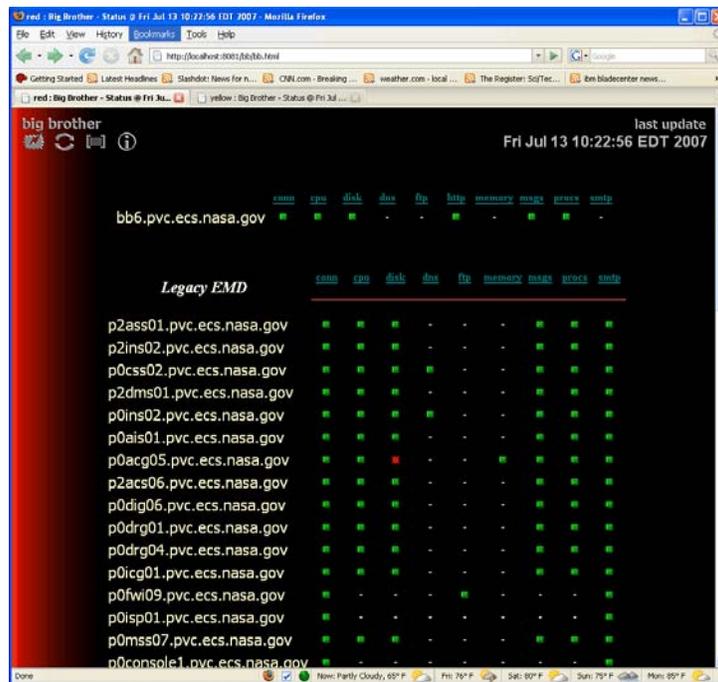


Figure 7.2-1. Big Brother Home Page

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, hosts and services status	View icon color and on web GUI; view quick status dialog box.	Icon color indicates the status of network devices, hosts and services.	To verify that all network devices, hosts and services on the devices are operational. To ascertain network devices and services that is not operating properly.
View network devices, hosts and 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.

7.2.1.1 Menu Toolbar

The Big Brother Server Display web page has a “Toolbar” at the upper left portion of the main page and sub-pages. The toolbar has four icons which are explained in detail and is represented in 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.

Figure 7.2-2. Big Brother Toolbar

7.2.1.2 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 it is service impaired beyond preset thresholds, the color of this device's service changes from green or yellow to a red animated starburst shape as shown in Figure 7.2-1. The color codes are shown in Table 7.2-2. *Color Codes by Order of Severity*. 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.
	Aked - A current event has been acknowledged by one or many recipients. The acknowledgement is valid until the longest delay has expired

7.2.2 Hyperic

HQ is a web based (URL Example; <http://f4iil01.hitc.com:7080>) system monitoring and management tool. This comprehensive system monitoring solution effectively manages and monitors infrastructures through automatic discovery of software and network resources; automatic reporting of the key indicators of application health and well-being; a rich database of your software inventory and its operating history; remote control and administration of software resources; alerting, notification, escalation, and corrective action; and powerful facilities for analysis, visualization, and reporting.

Figure 7.2-3 is an example of the HQ home page.

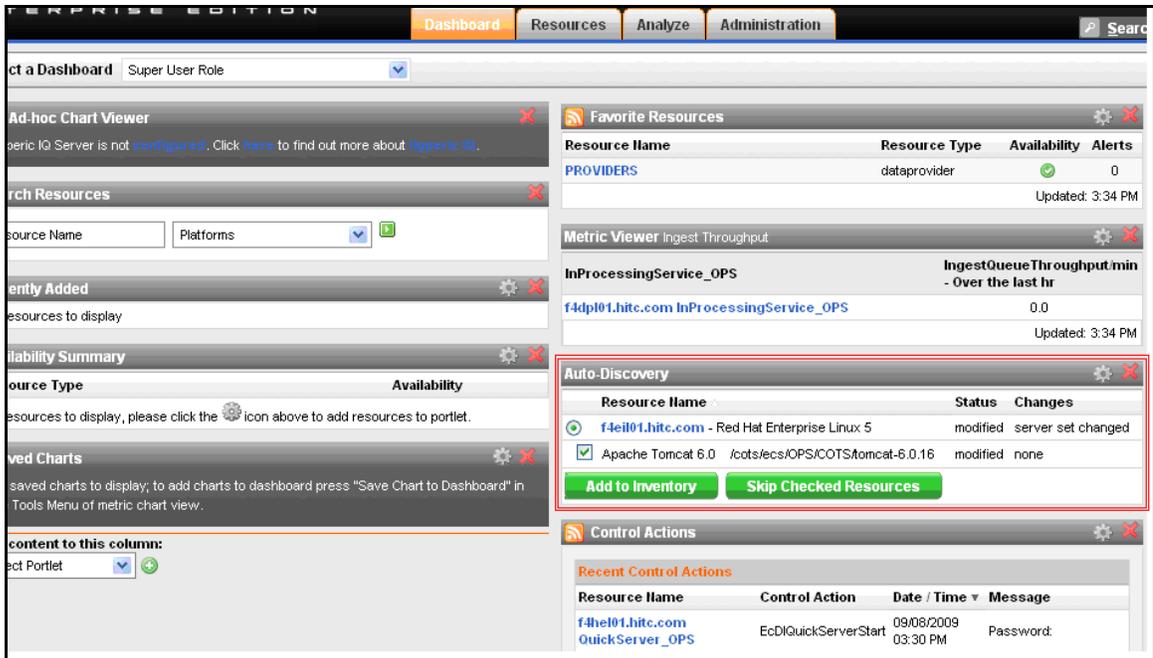


Figure 7.2-3. HQ Homepage

The following items are Hyperic HQ Enterprise monitoring tool features used by EED:

Auto-Discovery

An HQ Agent scans its host machine, finds the software and services running on it, and adds it all to the HQ database.

Real-Time Monitoring

HQ's default metric collection provides immediate visibility into [availability](#), [performance](#), [utilization](#), and throughput. HQ metric collection is the foundation for automated alerting and action. You can set alerts for individual resources, groups of resources, resources of the same type, and at the application level. Based on the type and severity of the condition that triggers an alert, you can kick off a variety of automatic responses, for instance, an email notification, a server restart, or a message to your ticketing system. HQ provides multiple views and tools for monitoring and analyzing performance and availability. The metric collection choices you make are reflected in the tabular and chart views that are automatically presented in the HQ user interface. You can adjust chart views on-the-fly to correlate multiple metrics, and understand relationships and ripple effects.

Controls and Actions

Using HQ operators can perform remote control actions on the platforms and services under management. For example, you can start, stop, and run garbage collection on an

application server, or perform analysis or housekeeping functions on a database server. You can use HQ control actions to streamline day-to-day operations, reduce the risk of human error or oversight, and respond rapidly when remote control is necessary.

Reporting and Analysis

The metrics that HQ collects provide a rich basis for analyzing and understanding service levels, utilization, chronically problematic resources, best practices compliance and other aspects of your infrastructure. HQ features that enable analysis and interpretation of performance and availability include use of the report center. HQ's reports provide easy visibility into performance and service-level activity across your network. The HQ-provided reports show availability, alerts, inventory, resource utilization, and resources for which there are no metrics. In addition, you can create your own report templates to satisfy enterprise-specific needs. Reports can be driven by user-input parameters and can be generated in several formats: PDF, HTML, Excel, and CSV.

7.2.2.1 Business Processes

7.2.2.1.1 Overview

Business Processes are a way of organizing resources to quickly recognize problems and to assess the operational impact of individual component failures. A custom Hyperic HQ User Interface plugin will be developed to extend the standard COTS GUI to provide the operator with a mechanism to configure and view their business processes.

Business processes can have one of four statuses:

- Active – There is work to do and the work is being completed as expected
- Inactive – All of the components appear to be functional, but there is not any work to complete.
- Degraded – The business process is functioning but not at the required capacity
- Down – The business process is unable to complete any work.

Each business process contains a collection of resources and the resources can have one of three statuses:

- Available – The resource is currently up
- Unavailable – The resource is currently down
- Alert Pending – There is at least one alert pending for the resource

7.2.2.1.2 Configuring Business Processes

The Hyperic grouping feature will be used to define a business process. All resources related to a business process will be mapped to a group. The business process group name must follow the naming convention BP_<MODE>_<Business Process Name>. This will allow the custom Hyperic HQ User Interface plugin a way to identify a business process group from one that is not.

The information of resource state and metrics are conveyed to the business process through alerts. For example, if we decided that the status of the DPL Ingest business process should be 'Down' if the EcDIProcessingService resource is unavailable, an alert must be configured to occur when the processing service is down. Then the Ingest business process can be configured to be 'Down' based on the alert.

In order to determine which resource alert has an impact on the overall business process status and to what degree, each business process has an alert definition configuration file named <business_process_name>_AlertDefinitionConfig.xml. The files are located under /usr/ecs/OPS/CUSTOM/cfg directory. This xml file holds the configuration information of the business processes within the mode and the mapping of the relevant alert definition to the status (down, inactive, degraded, active) category of the business process. Not all alerts need to be defined in this configuration file, only those that impact the status of the business process. For alerts that are raised within a business process that are not defined in the configuration file, the priority of the alert is examined and the status of the business process will be defaulted to 'Degraded' if the alert has a priority of 'Medium' or 'High'. This gives the operator the capability to handle newly created alert definitions.

See Figure 7.2-4 below for the xml schema diagram of the business process alert definition configuration file.

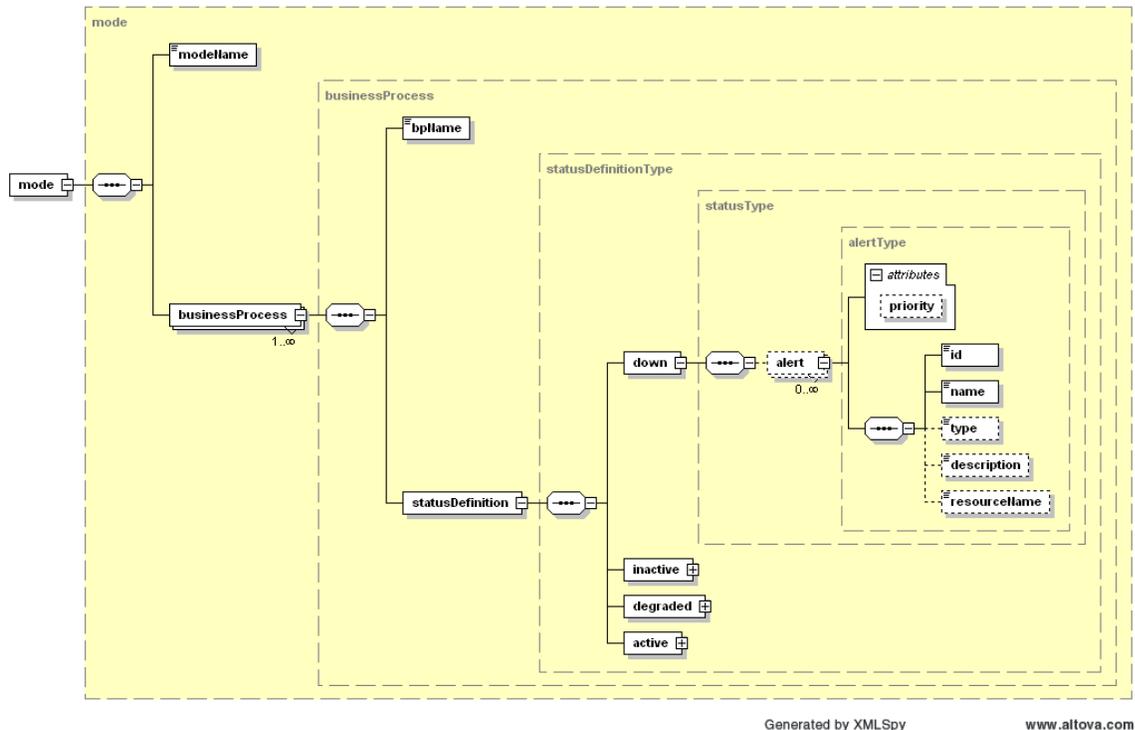


Figure 7.2-4. Alert Definition Schema Diagram

Sometime we may want to change the status of a business process when a combination of different alerts on different resources happens at the same time. For example, we may want to mark the Data Access business process as “degraded” when either WIST or WebAccess is down; but when both of them are down, we want to mark the Data Access business process as “down”. Since hyperic does not provide the functionality to configure alerts on incompatible groups, we added a custom group alert capability in our Business Process configuration and view pages.

Operator can configure group alert to be any combination of resource alerts and define how the group alert would impact the overall business process status. Each business process could have a group alert definition configuration file. If one exists, it is named `<business_process_name>_GroupAlertDefinitionConfig.xml`. The configuration files are located under `/usr/ecs/OPS/CUSTOM/cfg` directory. Operator should not manually update the configuration files. All update should be done through the hyperic GUI.

We created a custom HQU Business Process Configuration page to let operators view and configure the existing resource alert and group alert definitions with in the system. See Figures 7.2-5, 7.2-6, and 7.2-7 below:

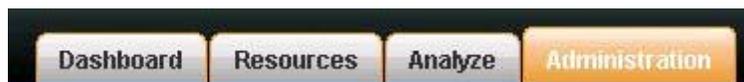


Figure 7.2-5. Hyperic GUI Administration Tab

The Business Process Configuration page will be located under the Administration tab.

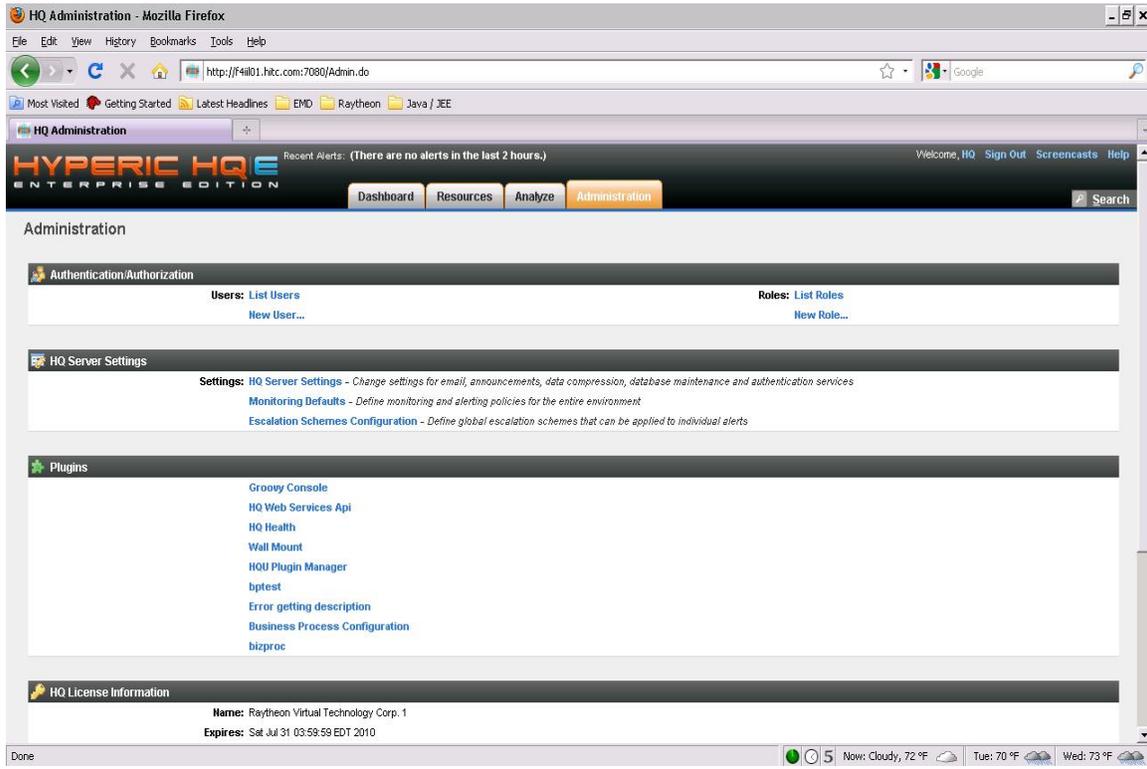


Figure 7.2-6. Hyperic GUI Administration Page

After clicking on the tab, the administration page is loaded. The business process configuration link, “Business Process Configuration” is located under the Plugin section. Click on the link to load the page.

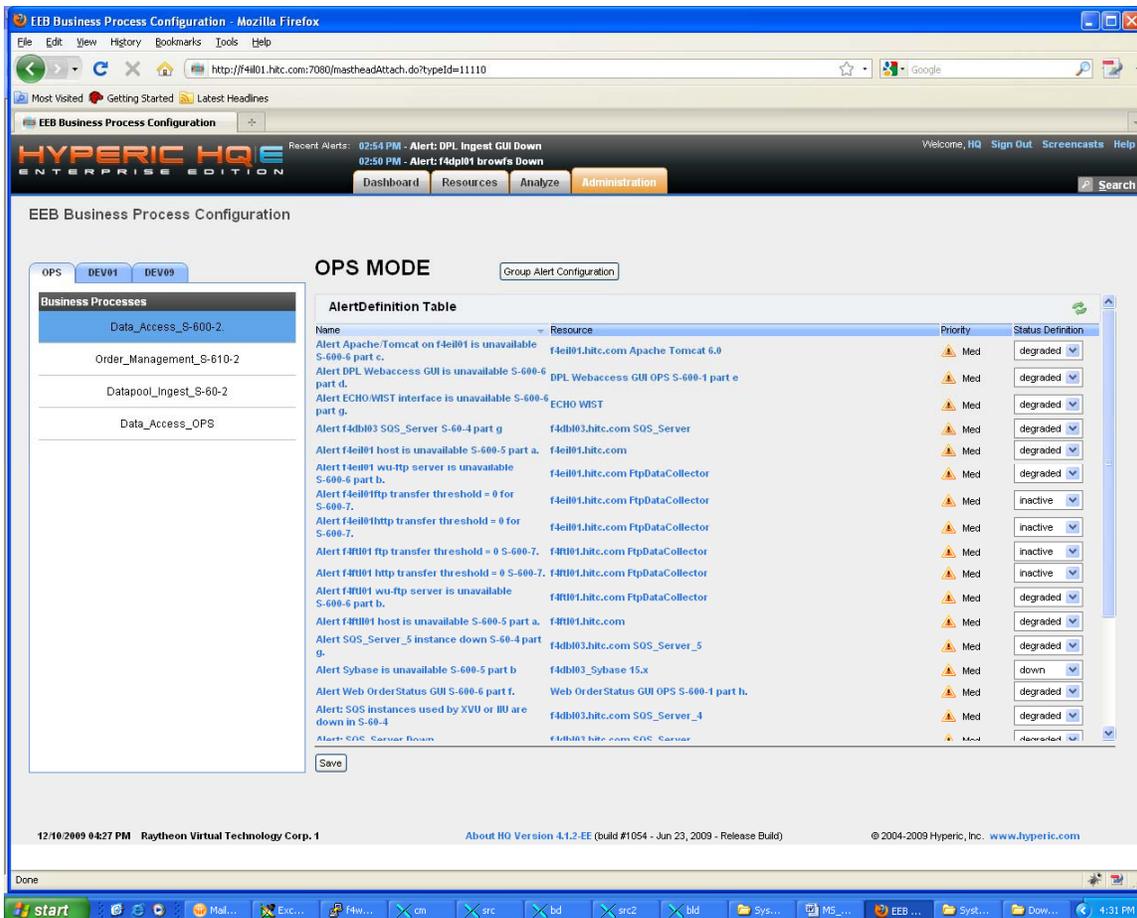


Figure 7.2-7. Business Process Configuration Page

The Business Process Configuration page contains a tab container. Each tab represents an ECS mode. Each mode container is divided into two panes and will display mode specific business process configuration. The left pane contains a list of business processes. The business process highlighted represents the current selection. Selecting a business process in the left pane will update the information on the right pane. The right pane contains a list of alert definitions for the selected business process. For each item in the list, the alert definition name, the resource name, the priority and the status definition is displayed. The alert definition name is a link to the configuration page of the alert definition. The resource name indicates which resource the alert definition is associated with and is a link to the detail page of the resource. The priority column shows the severity of the alert definition. It can have one of three values - low, medium, or high. The status definition shows the mapping of the alert definition to a business process status category. It can have one of four values - “Active”, “Inactive”, “Degraded”, or “Down”.

The alert definition configuration files will be loaded for all modes when the Business Process Configuration page is loaded or refreshed. An operator with admin privileges can configure the

status definition field of each alert to its desired category. Once the operator clicks the “save” button at the bottom of the page, the xml configuration file will be updated with the new configuration values on the page.

Operator can configure group alerts by clicking on the “Group Alert Configuration” button on the top of the right pane. This will bring up the group alert configuration page, see Figure 7.2-8 below:

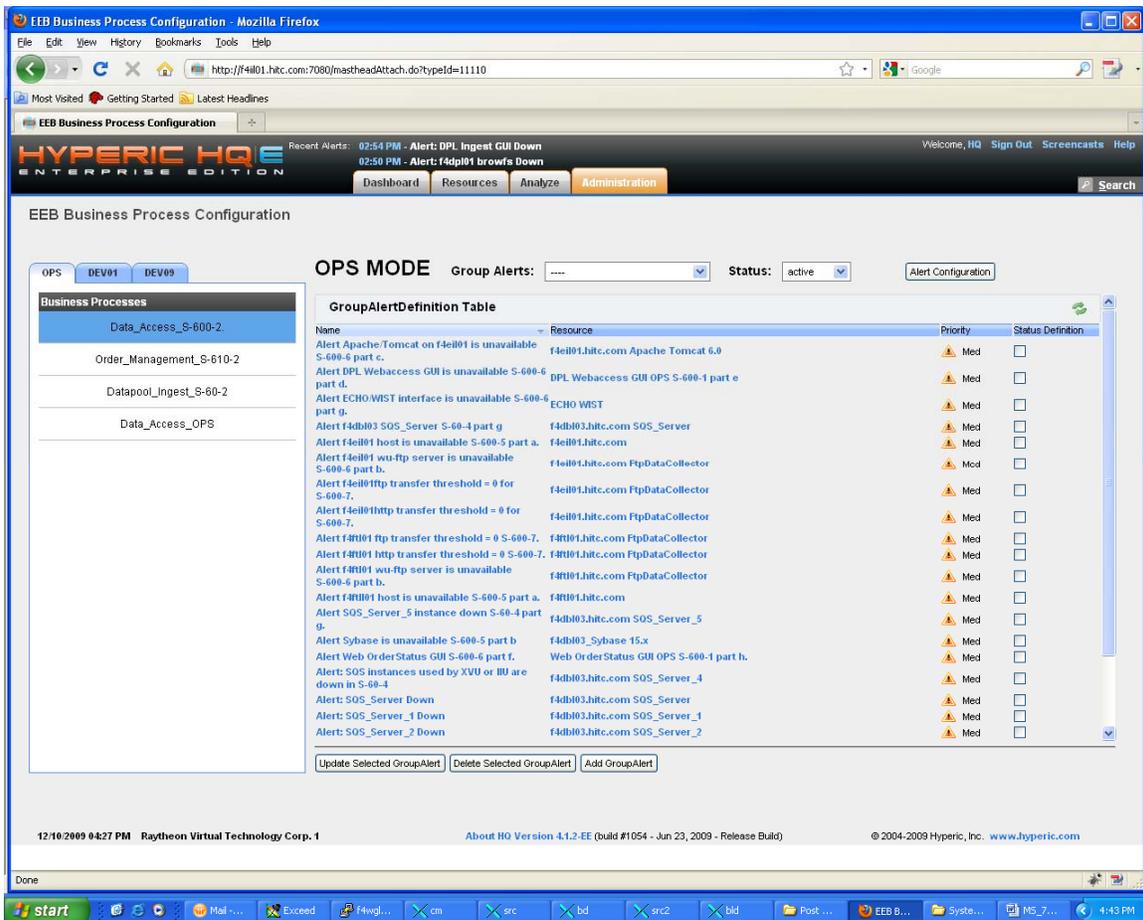


Figure 7.2-8. Business Processes Group Alert Configuration

“Alert Configuration” button will lead operator back to the Alert definition page. Operator can view existing group alerts, updated group alerts, delete group alerts and create new group alerts through the buttons on the page.

To view an existing group alert, operator can click the drop down list on the top of the page next to the MODE. When clicked, the drop down list will list all existing group alerts. Once operator makes a selection, the group alert configuration will be displayed in the GroupAlertDefinition table below. See Figure 7.2-9 *View Business Process Group Alert* below:

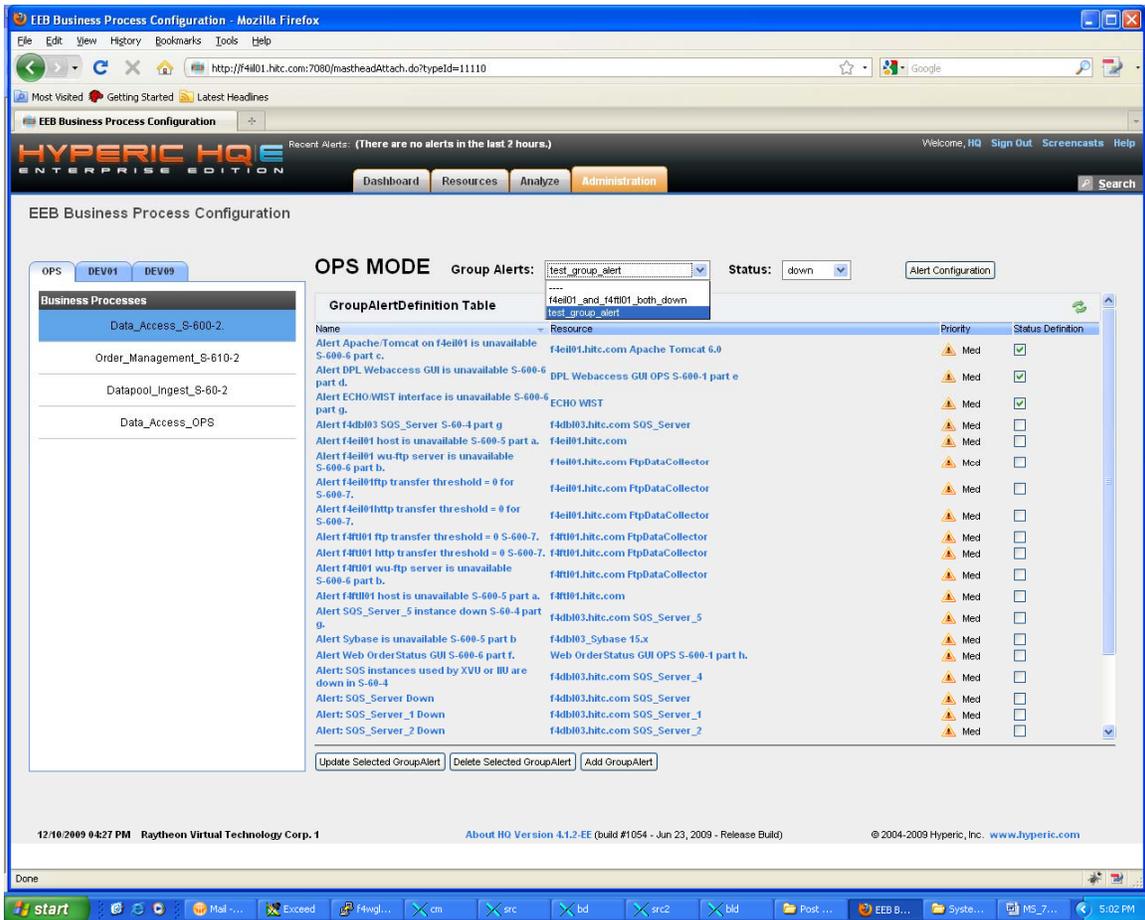


Figure 7.2-9. View Business Process Group Alert

Operator can delete the selected group alert by clicking on the “Delete Selected GroupAlert” button.

Operator can modify the group alert definition by selecting a different status definition of the business process on the status drop down list next to the Group Alert name on the top of the page; or/and check/uncheck the checkboxes in the GroupAlertDefinition table, then click the “Update Selected GroupAlert” button to update the group alert definition. See Figure 7.2-10 below:

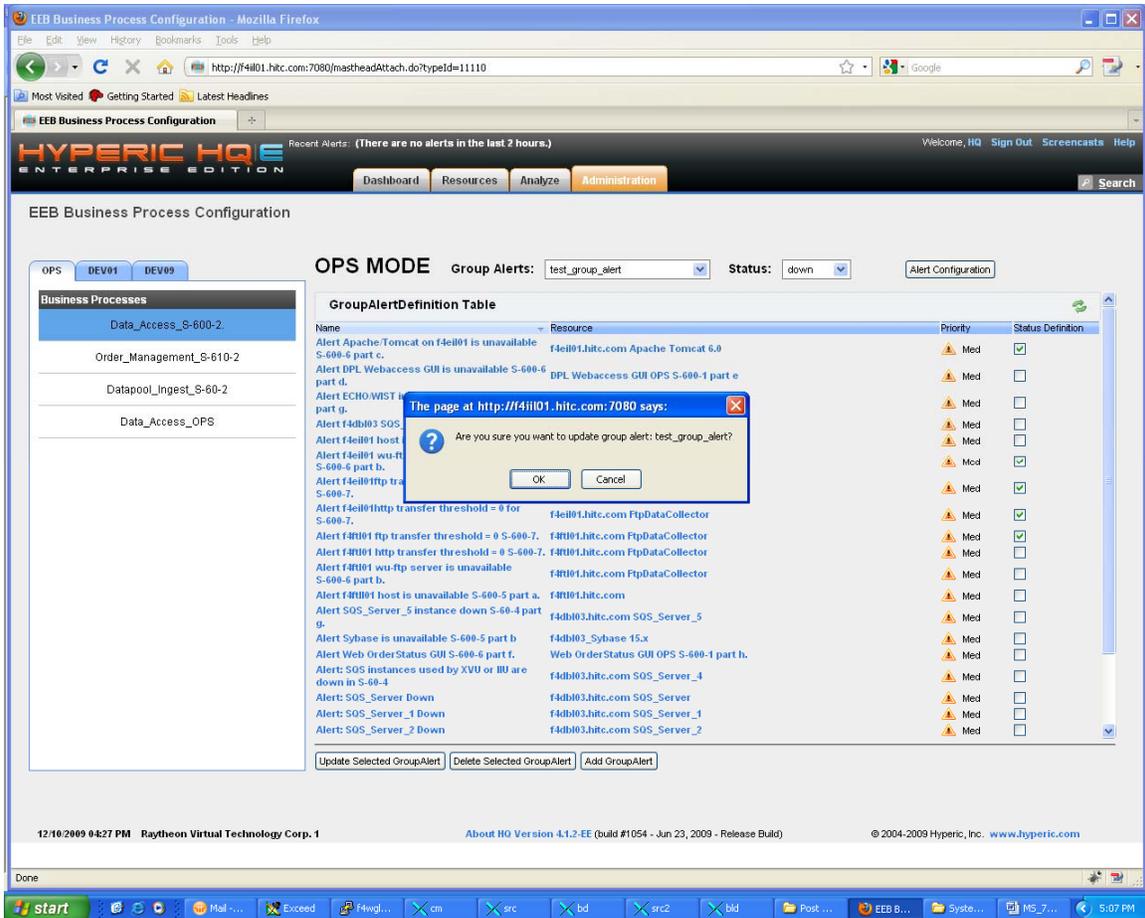


Figure 7.2-10. Update Business Process Group Alert

Operator can add a new group alert by clicking on the “Add GroupAlert” button. See Figure 7.2-11 below:

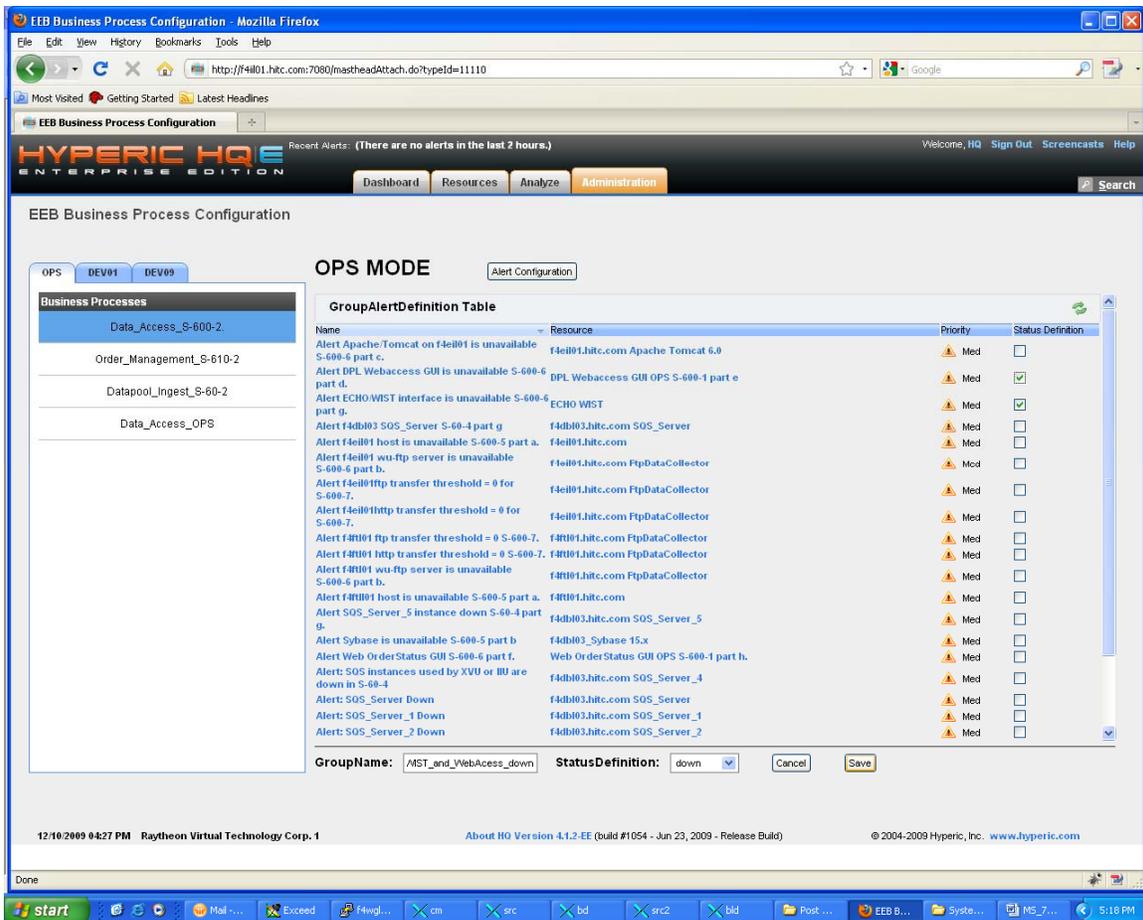


Figure 7.2-11. Add new Business Process Group Alert

Operator can type in the group alert name in the GroupName text box, select the status definition of the group alert via the StatusDefinition drop down list and check/uncheck the checkboxes in the GroupAlertDefinition table to add selected individual resource alerts in the group alert definition. Operator can cancel the add operation by clicking the “Cancel” button. Once operator click the “Save” button and confirm through the confirmation popup window. A new group alert will be added and become visible through the Group Alerts drop down list on the group alert configuration page. See Figure 7.2-12 below:

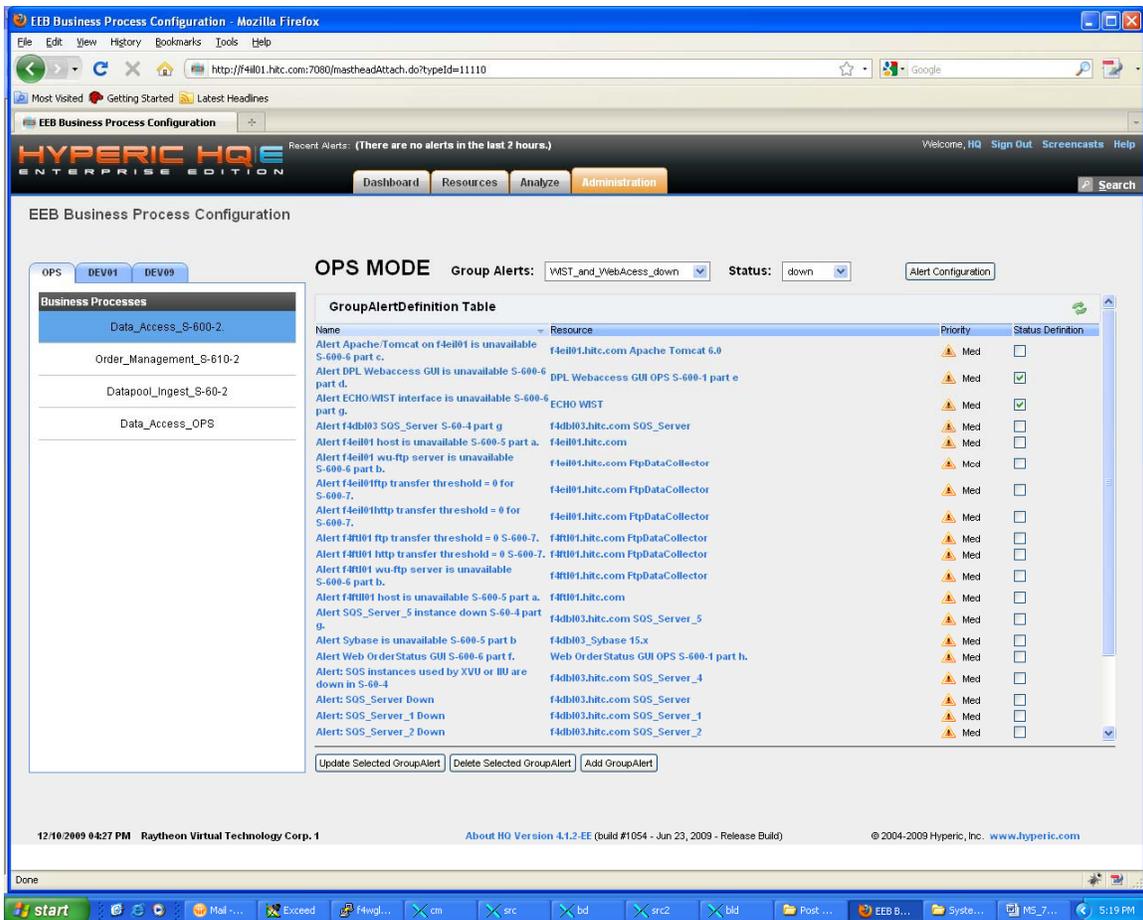


Figure 7.2-12. View added Business Process Group Alert

7.2.2.1.3 View Business Process

With the custom HQU plugin, an operator can use the Hyperic HQ GUI to get a quick overview of the status of all business processes. The business process page can be navigated to via the Resource tab and clicking on the 'Business Processes' link as shown below in Figure 7.2-13.



Figure 7.2-13. Business Processes Link

Business Process Status Page

The Business Process Status page is divided into two panes. The left pane contains a list of business processes. It shows the name and the business process status. The business process that is currently selected is highlighted in blue. The right pane contains a list of resources for the selected business process. It shows the resource name, the status of the resource, and the reason explaining why a resource is not available. Clicking on the resource name will take the operator to a detailed page of the resource. Selecting another business process will update the resource list in the right pane. Figure 7.2-14 shows Business Process Page for DPL Ingest Archive as well as Figure 7.2-15 that shows the bottom of the page.

The screenshot displays the 'Business Processes Status' interface. It features a top navigation bar with tabs for 'OPS', 'TS1', 'TS2', and 'OTHER'. The main content is divided into two panes. The left pane, titled 'Business Processes', contains a table with columns for 'Business Processes' and 'Status'. The 'DataPool_Ingest' process is highlighted in blue and has a green status icon. Below this table is a legend for 'Business Process Status Definition' with icons for ACTIVE (green circle), INACTIVE (blue circle), DOWN (red X), and DEGRADED (yellow triangle). The right pane contains a table with columns for 'Name', 'Priority', and 'Alert Definition'. This table lists various resources, all of which have a green status icon. Below this table is a legend for 'Resource Status Definition' with icons for AVAILABLE (green circle), UNAVAILABLE (red X), and ALERT (yellow triangle).

Business Processes	Status
DataPool_Ingest	ACTIVE
DATA_ARCHIVE [private to hqadmin]	INACTIVE
TEST	INACTIVE

Name	Priority	Alert Definition
f4db03.hitc.com f4db03_sqs_srvr_1	AVAILABLE	
f4db03.hitc.com f4db03_sqs_srvr_4	AVAILABLE	
f4db03.hitc.com Sybase 15.x	AVAILABLE	
f4dp01.hitc.com	AVAILABLE	
f4dp01.hitc.com Apache Tomcat 6.0	AVAILABLE	
f4dp01.hitc.com DPIU_OPS	AVAILABLE	
f4dp01.hitc.com IIU_OPS	AVAILABLE	
f4dp01.hitc.com InNotificationService_OPS	AVAILABLE	
f4dp01.hitc.com InProcessingService_OPS	AVAILABLE	
f4dp01.hitc.com XVU_OPS	AVAILABLE	
f4ei01.hitc.com QuickServer_OPS	AVAILABLE	
f4ft01.hitc.com QuickServer_OPS	AVAILABLE	
f4om01.hitc.com QuickServer_OPS	AVAILABLE	
f4sp01.hitc.com QuickServer_OPS	AVAILABLE	

Figure 7.2-14. View Business Process Page – DPL Ingest Active

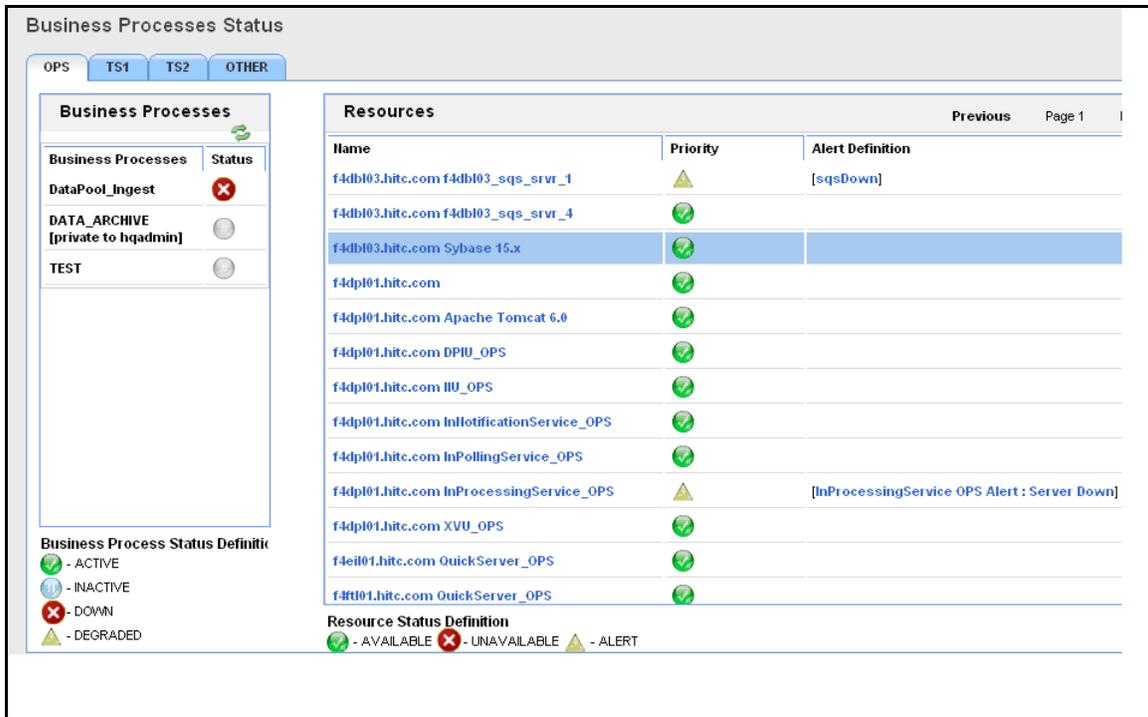


Figure 7.2-15. View Business Process - DPL Ingest Down

Mode Tabs

The Mode Tabs renders a different view of the Business Process filtered by mode. All business processes are defined within a specified mode thus the specified mode tab will display only those business process defined within the current mode as shown in Figure 7.2-16.



Figure 7.2-16. Business Process Mode Tab

Business Process Status Table

The Business Process Status Table provides a quick view of the overall health of a business process. The “Business Processes” column provides the name of all the business processes within the specified mode. The “Status” column provides the overall status of the business process. The status of the business process is determined by the alerts that correspond to the resources that are members of the business process. An xml configuration file will hold the definitions of the impact an alert has on the overall state of a business process. The Business

Process Status Table controls the Business Process Resource Table located to the left of it. When the cursor is placed over the name of a particular business process within the Business Process Status Table it is highlighted and the Business Process Resource Table will refresh to display information on the resources that are members of the selected business process as shown in Figure 7.2-17.

Business Processes	
Business Processes	Status
DataPool_Ingest	

Figure 7.2-17. Business Process Status Table

Business Process Resource Table

The Business Process Resource Table provides a view of the resources that are members of the current business process selected in the Business Process Status Table. Besides the resources defined in the hyperic system, custom group alerts are also displayed as a type of resource. This gives user a better view when the business process status is determined by a custom group alert.

The “Name” column contains the name of a resource. The resource name can be clicked on for a detailed view of the resource. The “Priority” column defines the status of a resource. If any alerts have fired that pertain to a resource, the column will display the status change. The “Alert Definition” column will display the names of any alerts related to the resource that have fired and have not been fixed. The alert name can be clicked on for a detailed view of the alert definition.

Figure 7.2-18 shows the Business Process Resource Table.

Mode[OPS] Business Process[DataPool_Ingest] Resources			Previous	Page 1	Next
Name	Priority	Alert Definition			
f4db103.hitc.com f4db103_sqs_srvr_1					
f4db103.hitc.com f4db103_sqs_srvr_4					
f4db103.hitc.com Sybase 15.x					
f4dpl01.hitc.com					
f4dpl01.hitc.com Apache Tomcat 6.0					
f4dpl01.hitc.com DPIU_OPS					
f4dpl01.hitc.com IIU_OPS					
f4dpl01.hitc.com InNotificationService_OPS					
f4dpl01.hitc.com InPollingService_OPS					
f4dpl01.hitc.com InProcessingService_OPS					
f4dpl01.hitc.com XVU_OPS					
f4eil01.hitc.com QuickServer_OPS					
f4ftl01.hitc.com QuickServer_OPS					

Figure 7.2-18. Business Process Resource Table

Business Process Status Definition

The Business Process Status Definition legend, shown in Figure 7.2-19, defines the meaning of each icon displayed in the Business Process Status Table.

- Active – There is work to do and the work is being completed as expected
- Inactive – All of the components appear to be functional, but there is no work to complete
- Degraded – The service is functioning but not at the required capacity
- Down – The service is unable to complete any work

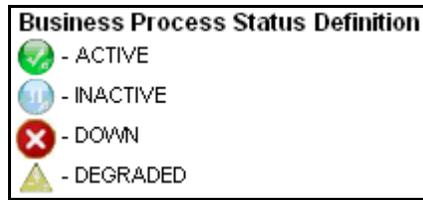


Figure 7.2-19. Business Process Status Definition

Resource Status

The Resource Status legend, shown in Figure 7.2-20, defines the meaning of each icon displayed in the Business Process Resource Table.

- Available – The resource is currently up
- Unavailable – The resource is currently down
- Alert Pending – There is at least one alert pending for the resource



Figure 7.2-20. Business Process Resource Status

This page intentionally left blank.

8. Problem Management

Problem management is the practice of monitoring and controlling problem reporting and resolution. EED 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 EED'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 EED staff when problems rated "critical" are reported, and forwards the tickets to the EDF for review by the EED 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 EED'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 EED 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.

EED's sustaining engineering staff works on resolving NCRs, updating TTPro to document all related activities. TTPro notifies selected EED staff whenever an NCR changes, and it notifies selected DAAC staff whenever it changes state.

EED 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 EED Project* (110-EED-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.
 - b. CM Administrators close trouble tickets upon determining that a problem has been resolved satisfactorily, or after the EED PRB accepts the problem for tracking as an NCR. Closed tickets may be re-opened, if necessary.
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 EED PRB for discussion and disposition.
 - a. TTPro moves the ticket as "forwarded", and creates a trouble ticket at the system level.
 - b. The EED PRB reviews the ticket at a PRB telecon to coordinate trouble ticket activities within the EED organization as well as with development, customer, and user organizations.
 - c. The DAAC Help Desk assigns the ticket to sustaining engineers for analysis.
 - d. 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.
 - e. 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 EED 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 ECS NCRs, are housed in separate databases called "projects".

TTPro can be accessed over the web or via locally installed Windows, Linux, or Mac OS 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 EED 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 EED PRB accepts the problem for tracking as an NCR. TPro places the ticket in the Closed state and notifies staff members of the change.
- Add new users to TPro’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 TPro 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 TPro	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 describes the Trouble Ticket Priority/Severity levels.

Table 8.3-2. Trouble Ticket Priority/NCR Severity

As Documented in NASA 420-05-03	As Used/Interpreted by the EMD Project
<p>Category 1: System/Service cannot perform critical function or imposes major safety hazard. (Priority 1)</p> <p>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.</p>	<p>HIGH (Severity 1): An NCR which causes:</p> <ul style="list-style-type: none"> - 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.
<p>Category 2: System/Service substantially impaired. (Priority 2)</p> <p>Substantially impacts development, operations, services, or data processing functions; fails to operate within critical performance specifications; or cannot effectively or efficiently fulfill baseline requirements.</p>	<p>MEDIUM (Severity 2): An NCR with the consequence that:</p> <ul style="list-style-type: none"> - 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) severely 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.
<p>Category 3: System/Service slightly impaired. (Priority 3)</p> <p>Causes minor or no substantial impact to development, operations, services, or data processing functions. Support may be degraded, but mission can still be accomplished.</p>	<p>Severity 3: An NCR with the consequence that:</p> <ul style="list-style-type: none"> - 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 Mac OS 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 9.0, 10.0 and Firefox 12.x-23.x. At present, TestTrack also supports Safari 6.x and Google Chrome 21 and later.

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:<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.

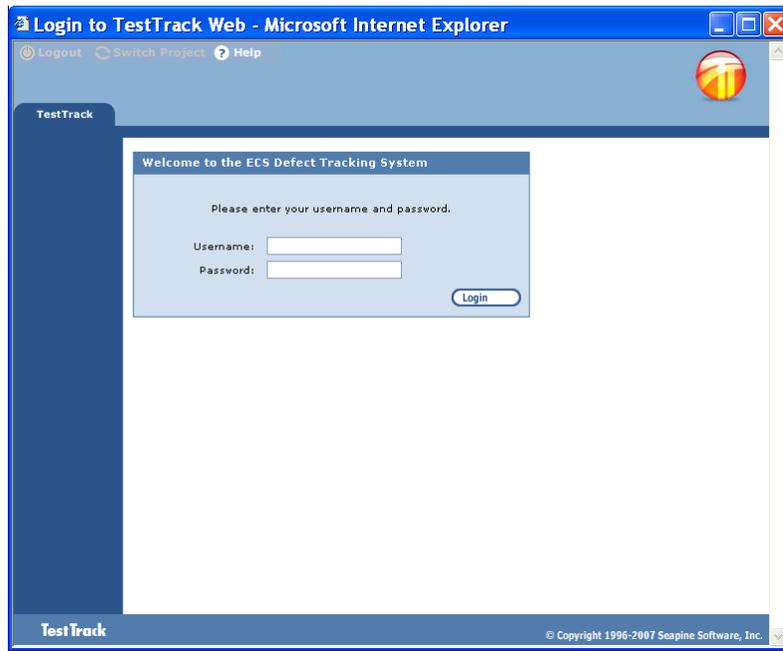


Figure 8.3-1. Login to TestTrack Web Page

- 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.

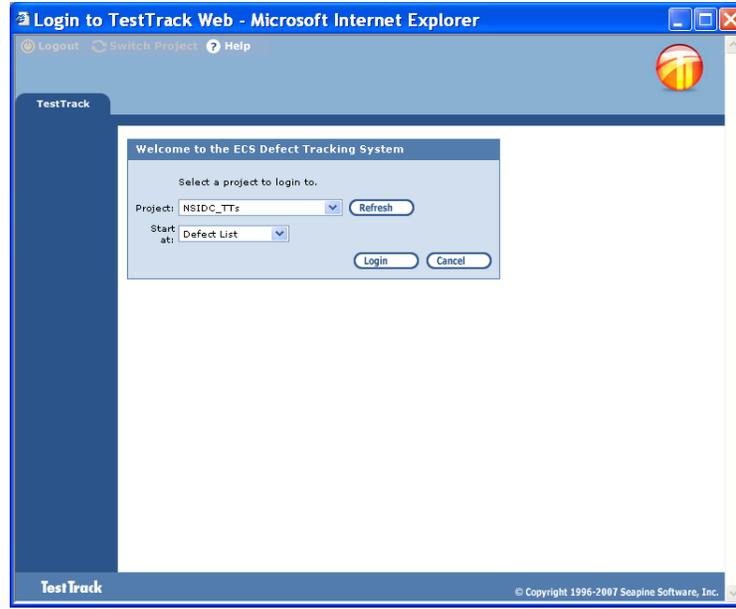


Figure 8.3-2. Login to TestTrack Web Project Page

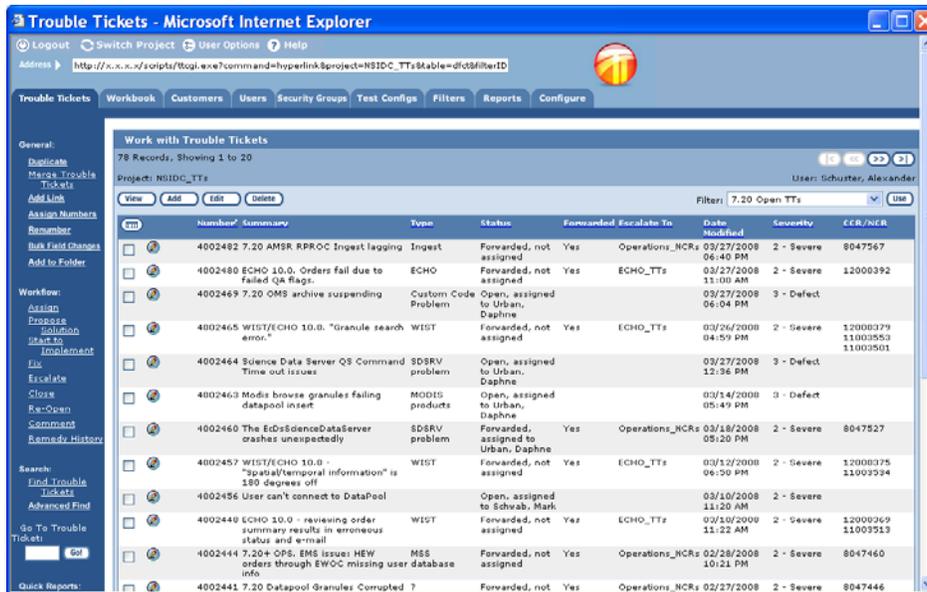


Figure 8.3-3. Work with Trouble Tickets Web Page

8.3.1.2 Logging onto TTPro using the GUI Clients

1 Launch TTPro:

[Windows] Click **Start** → **All Programs** → **Seapine Software** → **TestTrack** → **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 &`

[Mac OS]: Double-click the **TestTrack Client** icon in the Applications/TestTrack folder.

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), click **Login with TestTrack Pro access** (if available), 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** pick list is empty or indicates that projects are loading, click **Refresh** after a few moments to retrieve a new list.

Note: To conserve licenses, do not request a type of access your session will not need.

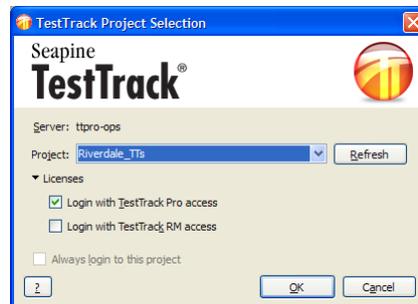


Figure 8.3-6. TestTrack Project Selection GUI

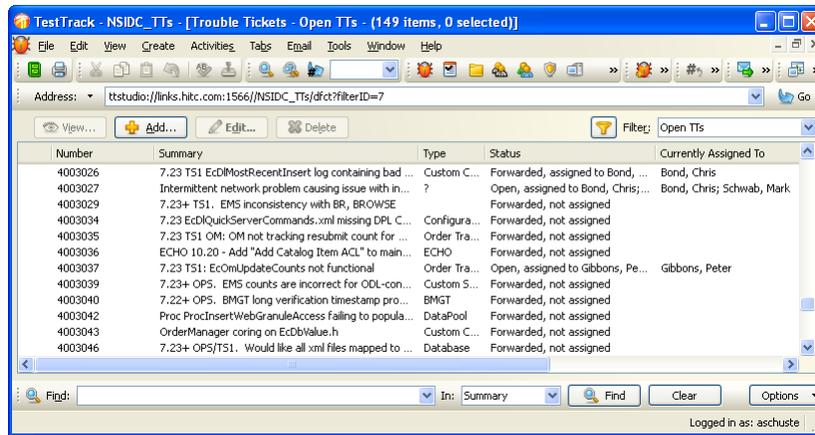


Figure 8.3-7. Trouble Tickets List GUI

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, 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)

Entered by	Character	30	Required	User name of the Submitter or person who created the defect.
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.
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 EED 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 (<i>Found By (Submitter)</i>), date the problem was detected (<i>Date</i>), <i>Version</i> of the version of the product that had the problem (<i>Version</i>), and a description of the problem sufficient for an engineer to perform an analysis (<i>Description</i>).
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 <i>Event</i> , <i>Date</i> of change or input, <i>Who</i> activated the event, <i>Other Information</i> 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.

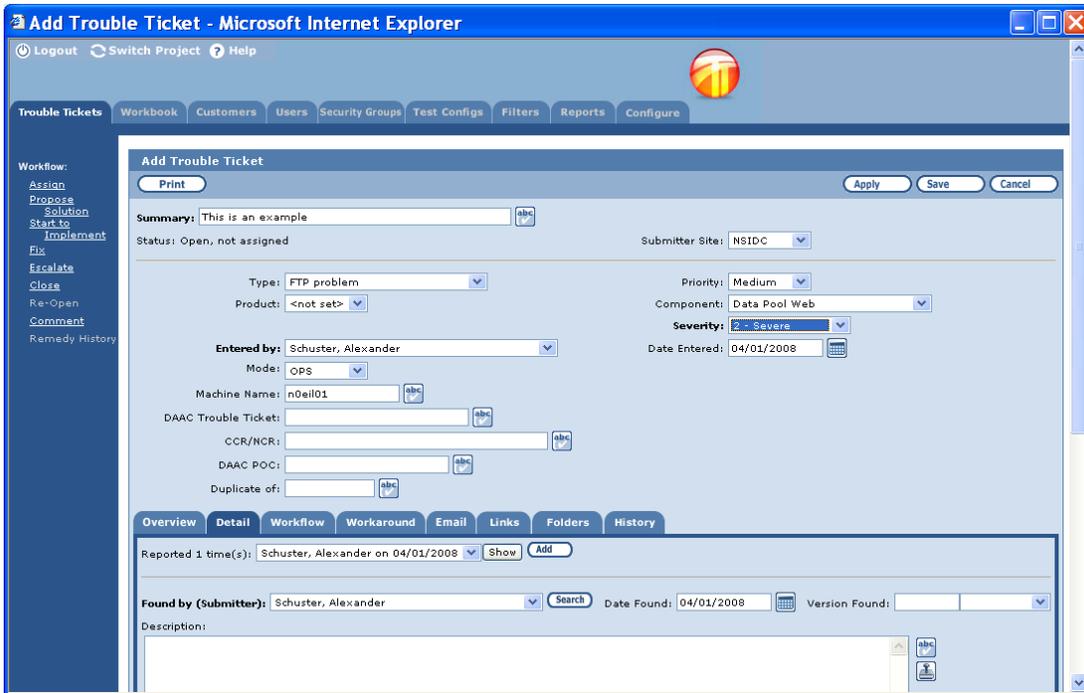


Figure 8.3-8. Add Trouble Ticket Web Page (1 of 2)

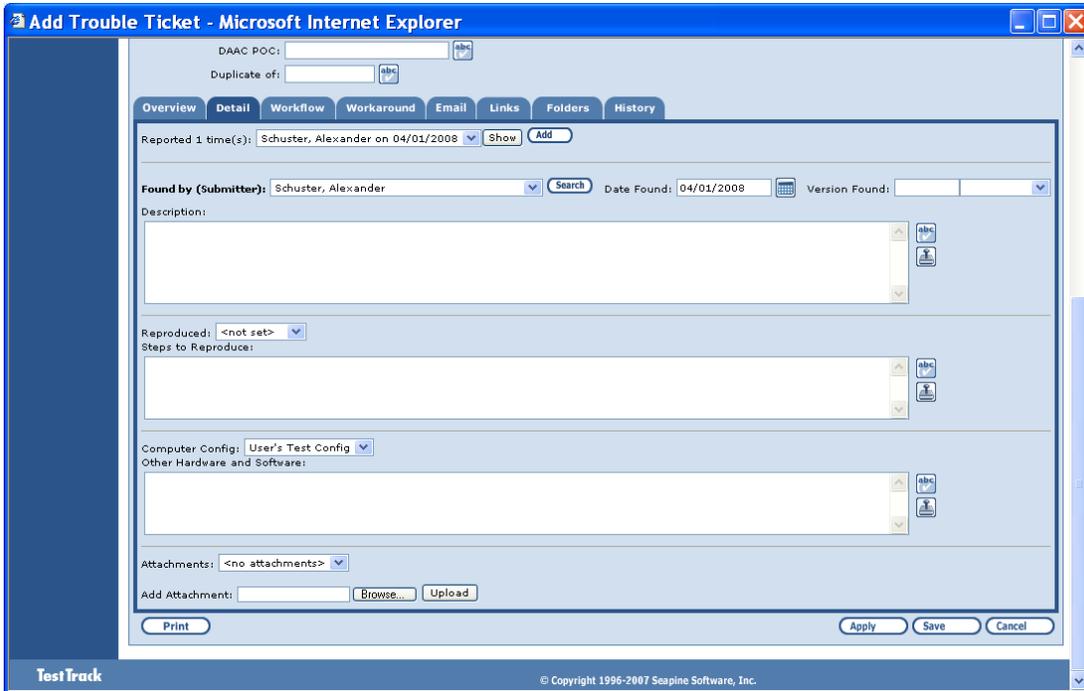


Figure 8.3-9. Add Trouble Ticket Web Page (2 of 2)

- 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' pick lists.
- 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' pick lists, 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 pick list 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, and 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 some common repository instead.

- 13 Review the trouble ticket for accuracy, and 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.

The screenshot displays the 'Add Trouble Ticket' GUI in a web browser. The window title is 'TestTrack - NSIDC_TTs - [Add Trouble Ticket]'. The address bar shows the URL 'ttstudio://links.hitc.com:1566/NSIDC_TTs/dfct'. The form contains several fields: Summary (empty), Status (Open, not assigned), Type (<not set>), Product (<not set>), Entered by (Schuster, Alexander), Mode (<not set>), DAAC Trouble Ticket (empty), DAAC POC (empty), Submitter Site (NSIDC), Priority (<not set>), Component (<not set>), Severity (<not set>), Date Entered (3/18/2010), Machine Name (empty), CCR/NCR (empty), Duplicate of (empty). Below the form is a navigation bar with tabs: Overview, Detail (selected), Workflow, Workaround, Email, Links, Folders, History. The 'Current Report' section shows 'Schuster, Alexander - 3/18/2010' with '1 of 1' reports. The 'Found by (Submitter)' field is pre-populated with 'Schuster, Alexander' and the date is '3/18/2010'. The 'Description' field is empty. At the bottom right, there are 'Apply', 'Add', and 'Cancel' buttons. The status bar at the bottom right shows 'Logged in as: aschuste'.

Figure 8.3-10. Add Trouble Ticket GUI (Part 1)

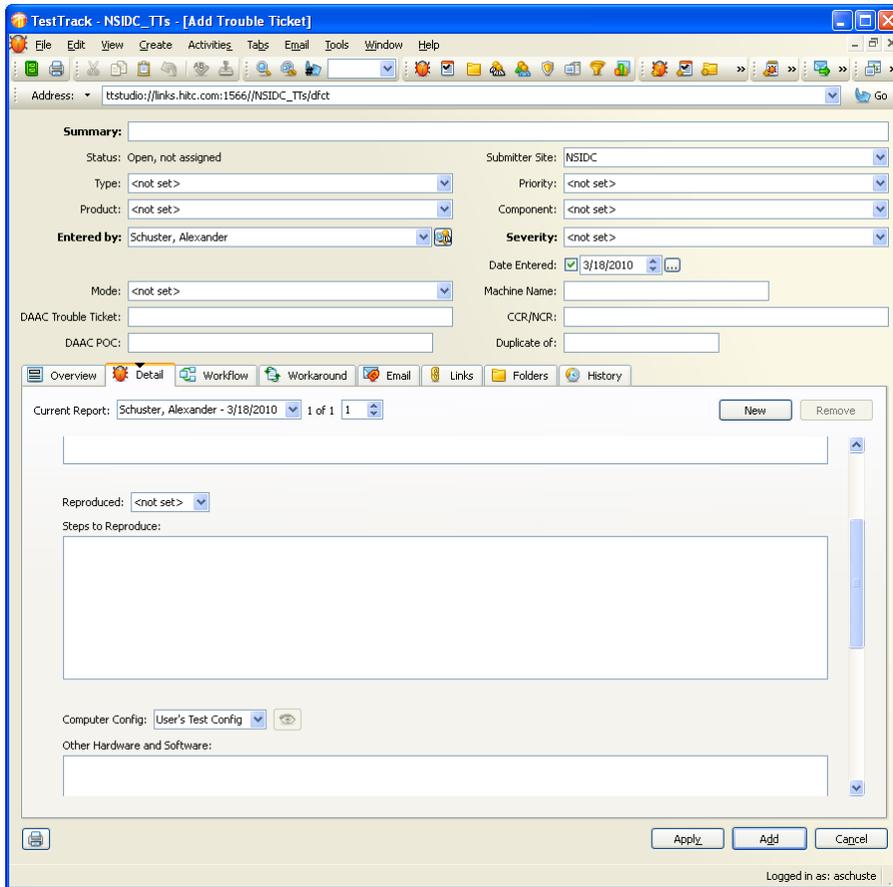


Figure 8.3-11. Add Trouble Ticket GUI (Part 2)

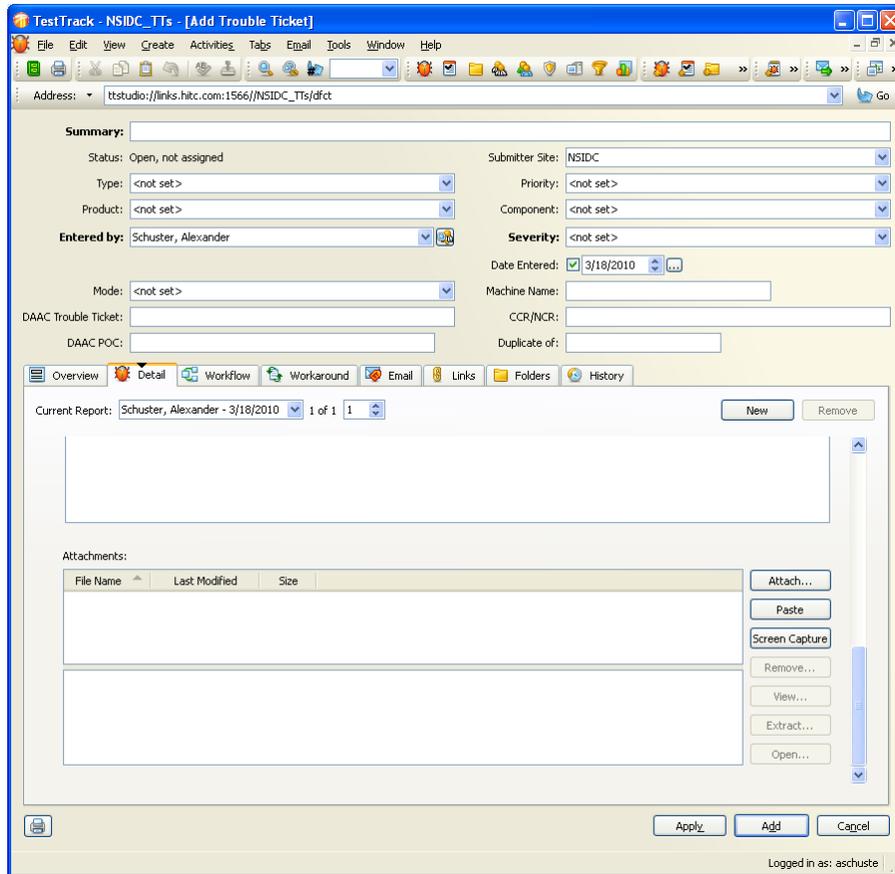


Figure 8.3-12. Add Trouble Ticket GUI (Part 3)

- 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' pick lists.
- 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' pick lists, 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 pick list 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, and 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/h1pdsk/<DAAC>` on host `m0css03.ecs.nasa.gov` instead. Consult your local CM Administrator in case that changes.

- 14 Review the trouble ticket for accuracy, and 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** pick list, 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), and 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:

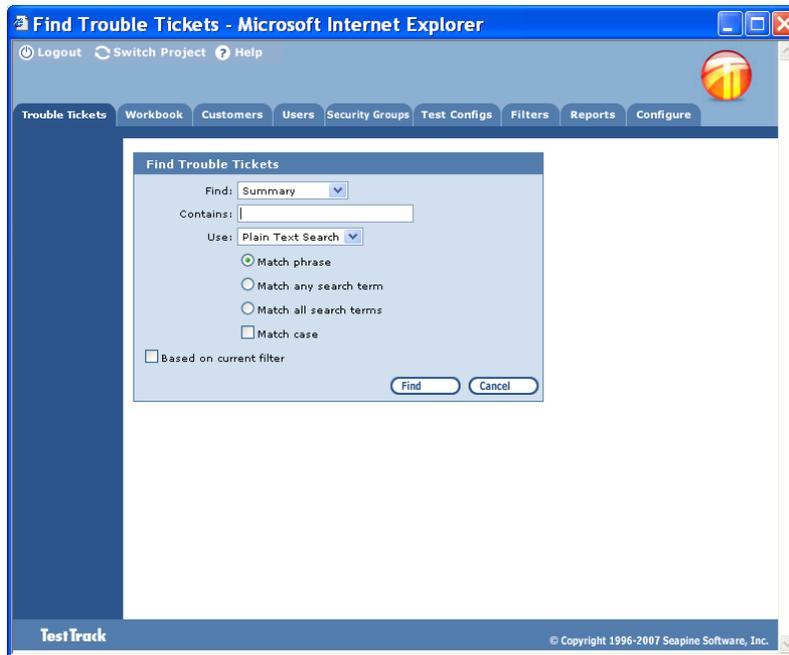


Figure 8.3-13. Find Trouble Tickets Web Page

- 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.

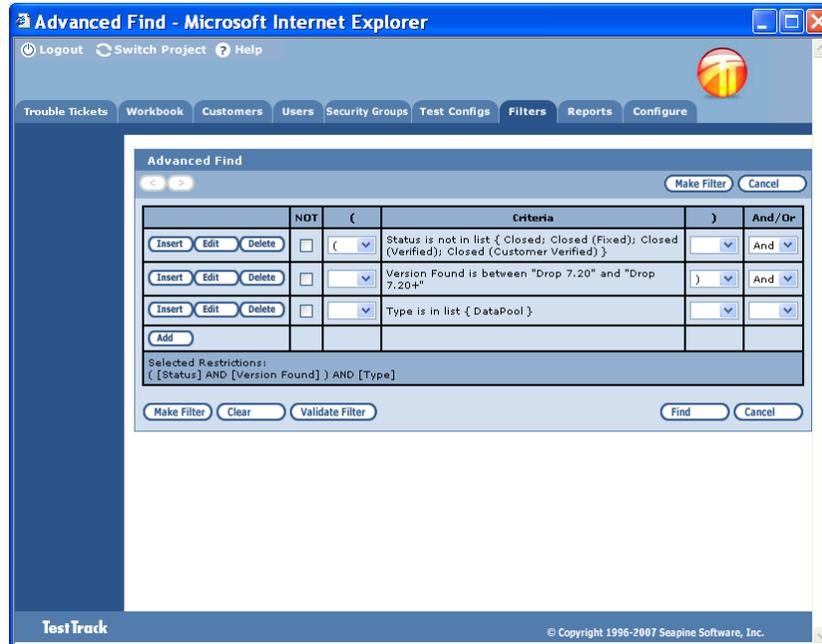


Figure 8.3-14. Advanced Find Web Page

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** pick list, 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, and 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:

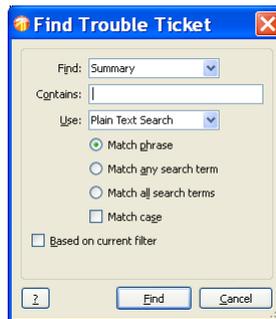


Figure 8.3-16. Find Trouble Ticket GUI

- 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.

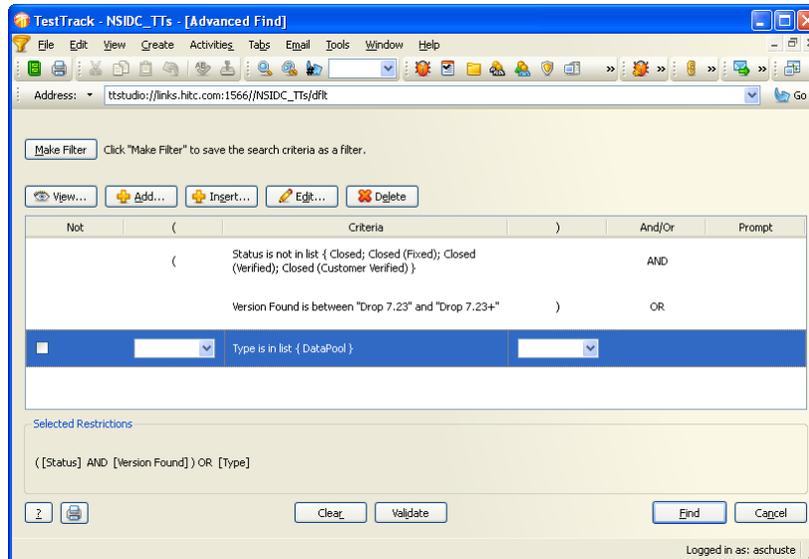


Figure 8.3-17. Advanced Find GUI

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.

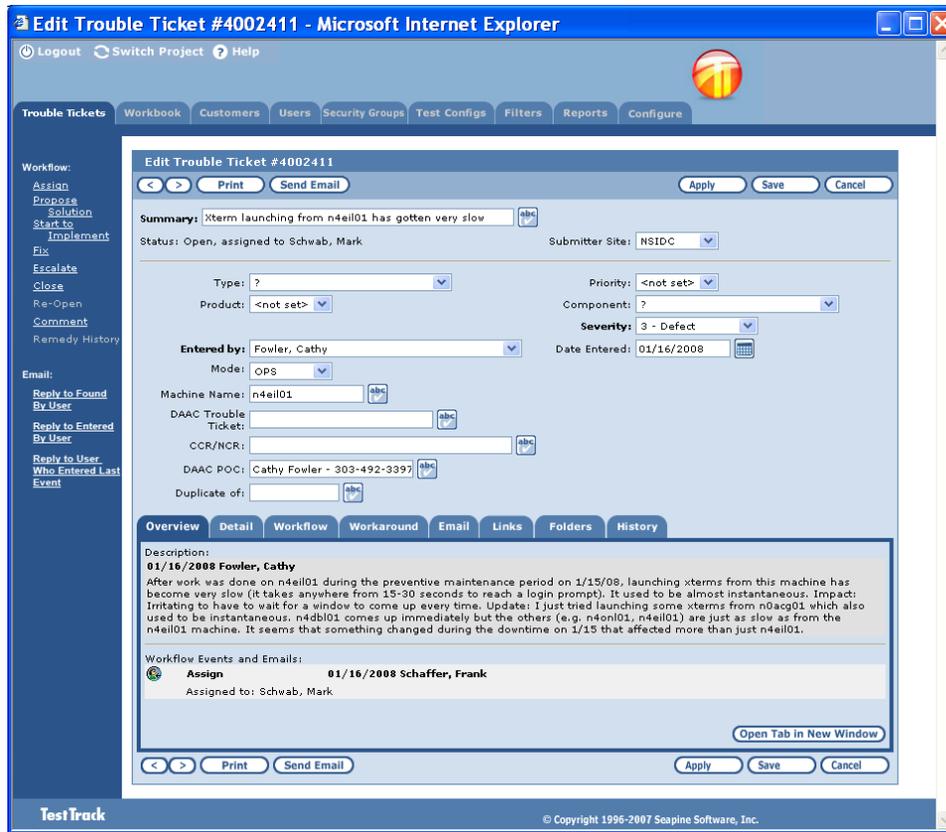


Figure 8.3-18. Edit Trouble Ticket Web Page

- 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.

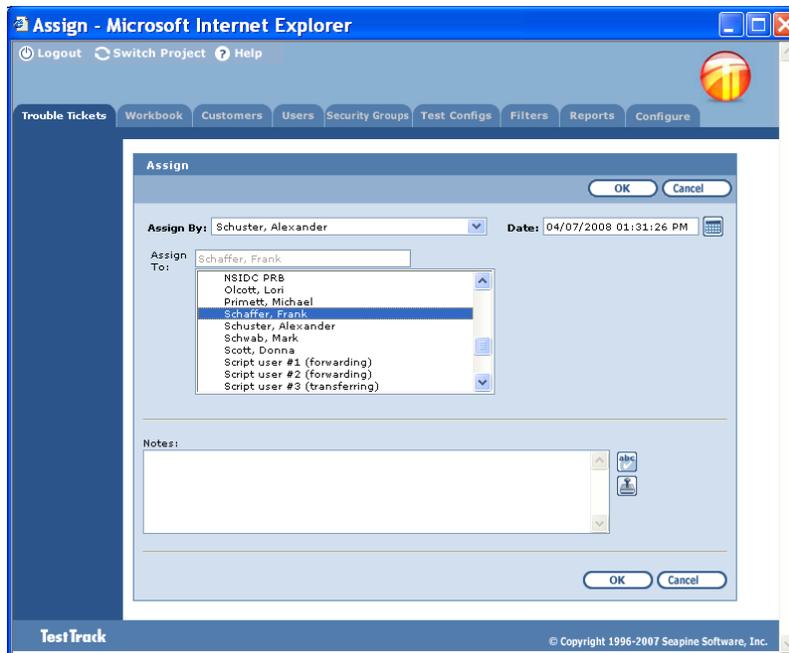


Figure 8.3-19. Assign Web Page

- 6 Select the names of one or more users from the **Assign to** field's pull-down list, 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 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.

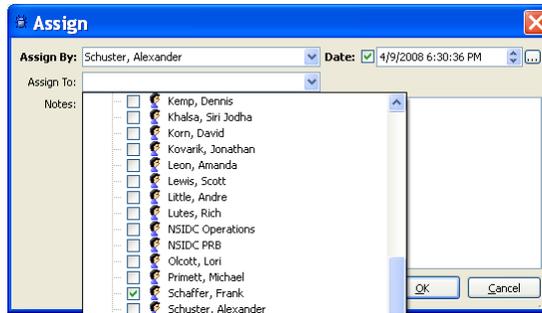


Figure 8.3-20. Assign GUI

- 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 of 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** pick list 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
Start to Implement	Notify submitter and others that work on fix has begun	Implement Solution	Work start date	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.

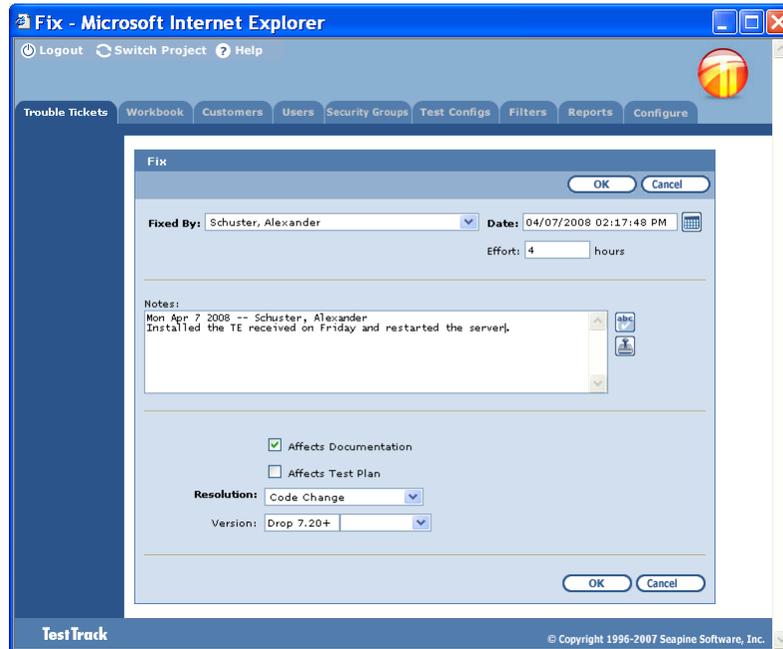


Figure 8.3-21. Fix Event's Web Page

- 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.

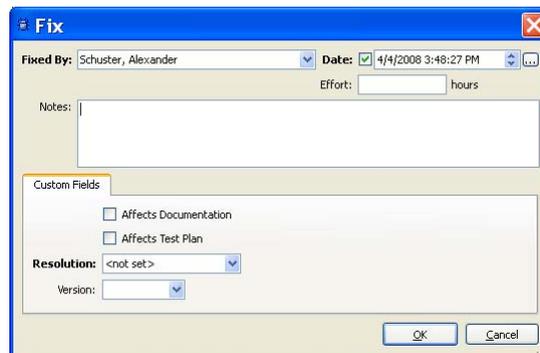


Figure 8.3-22. Fix Events GUI

- 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):

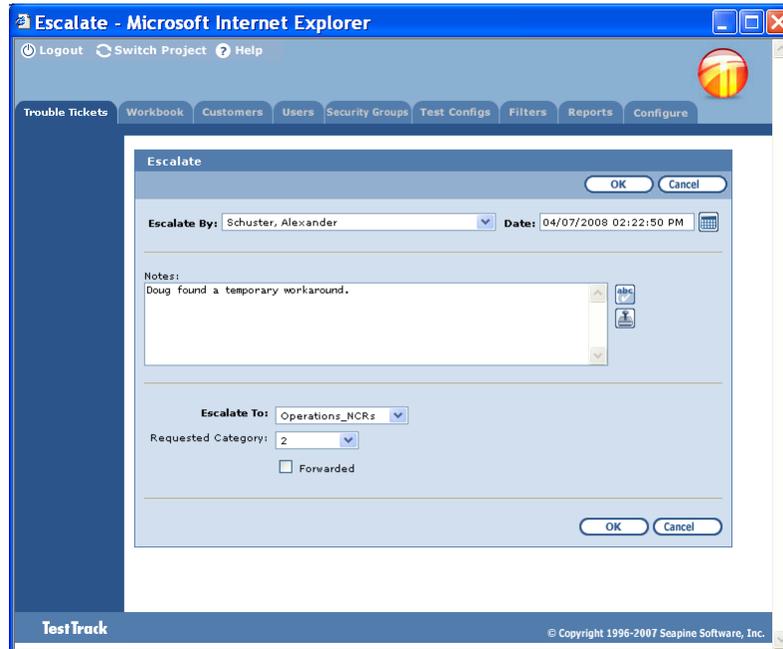


Figure 8.3-23. Escalate Page

- 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 pick list, if desired. Categories reflect how urgently a solution is needed.
 - d. Do NOT update the **Forwarded** field. (It should be grayed 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),

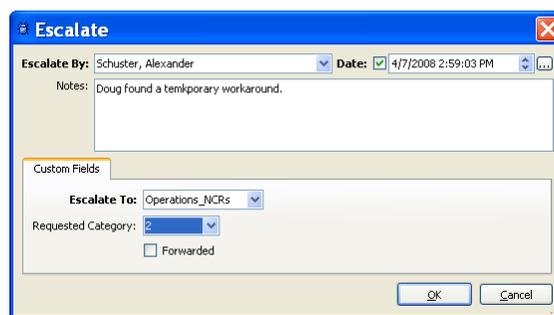


Figure 8.3-24. Escalate GUI

- 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 pick list, if desired. Categories reflect how urgently a solution is needed.
 - d. Do NOT update the **Forwarded** field. (It should appear grayed 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 EED PRB determines that a system-level trouble ticket should be made an NCR, the PRB Chairperson or designee 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_NCRs 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 (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 than what is shown in Figure 8.3-25.

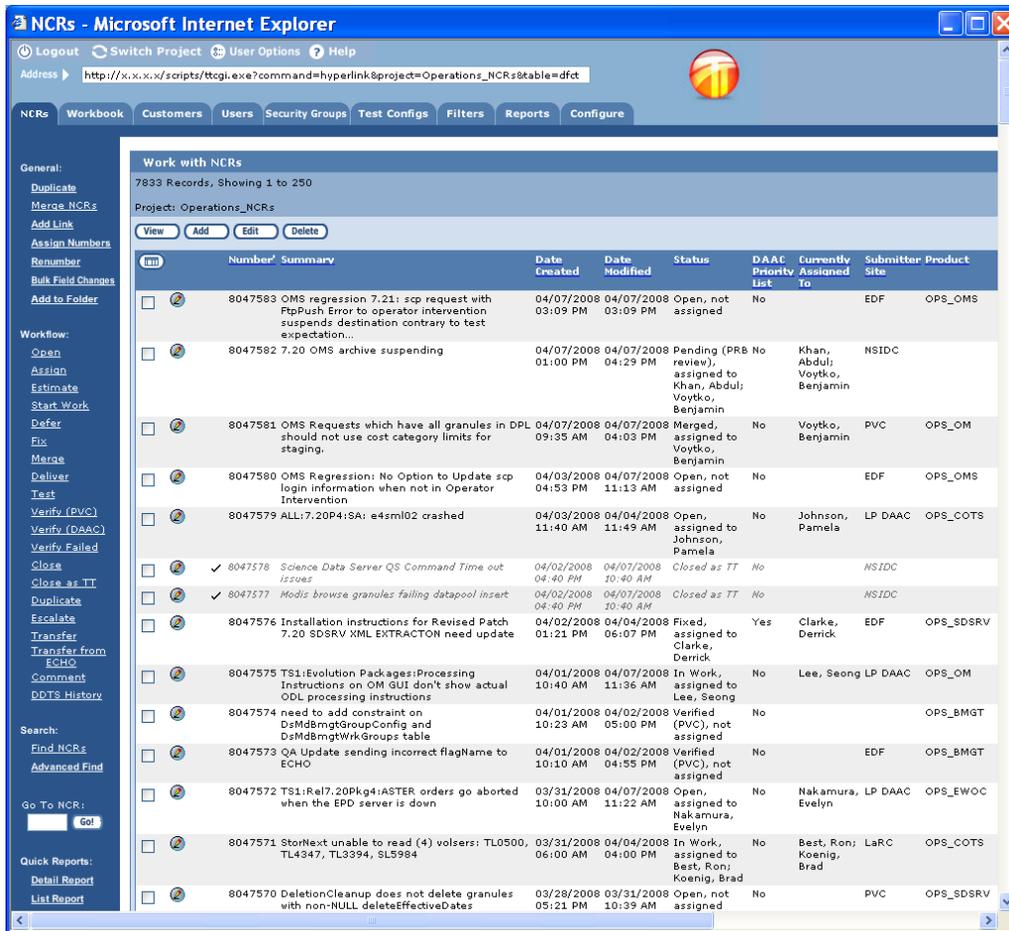


Figure 8.3-25. Work with NCRs Web Page

- 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.

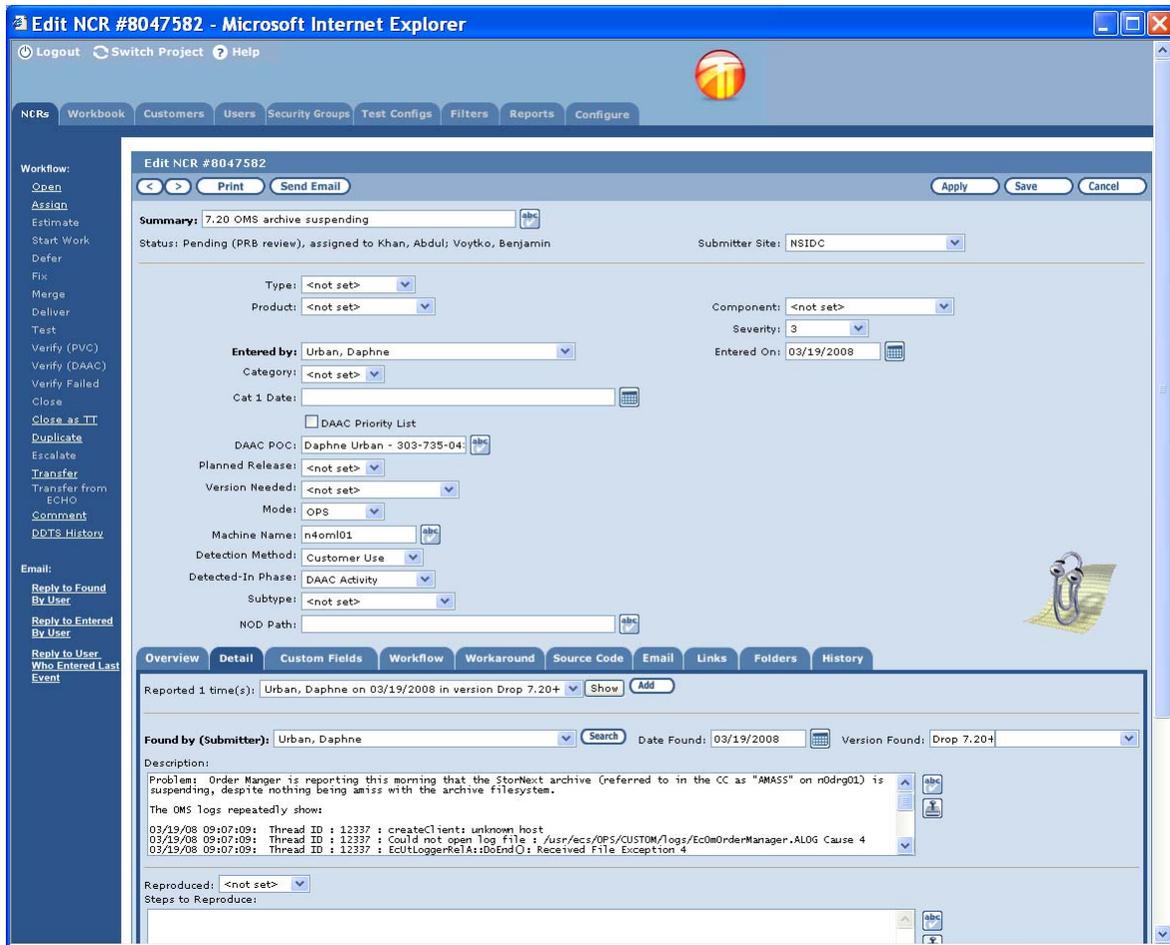


Figure 8.3-26. Edit NCR Web Page

4 On the **Open** web page (Figure 8.3-27):

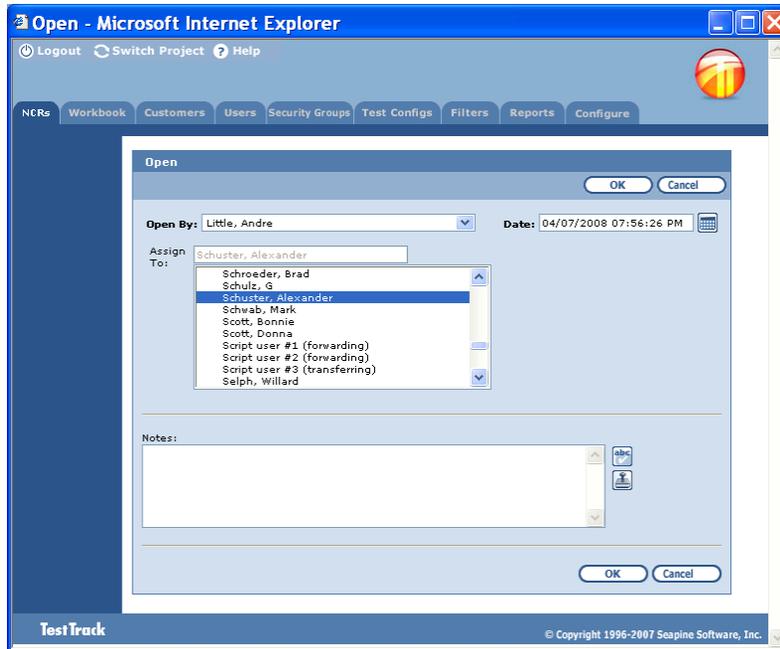


Figure 8.3-27. Open Web Page

- 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.

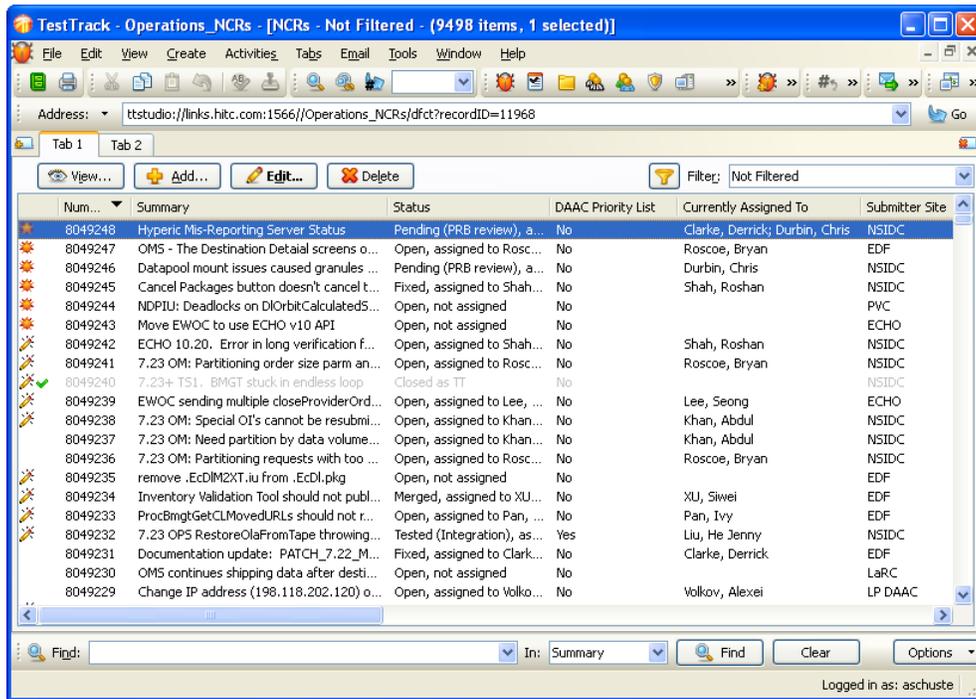


Figure 8.3-28. Operations_NCRs GUI

- 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.

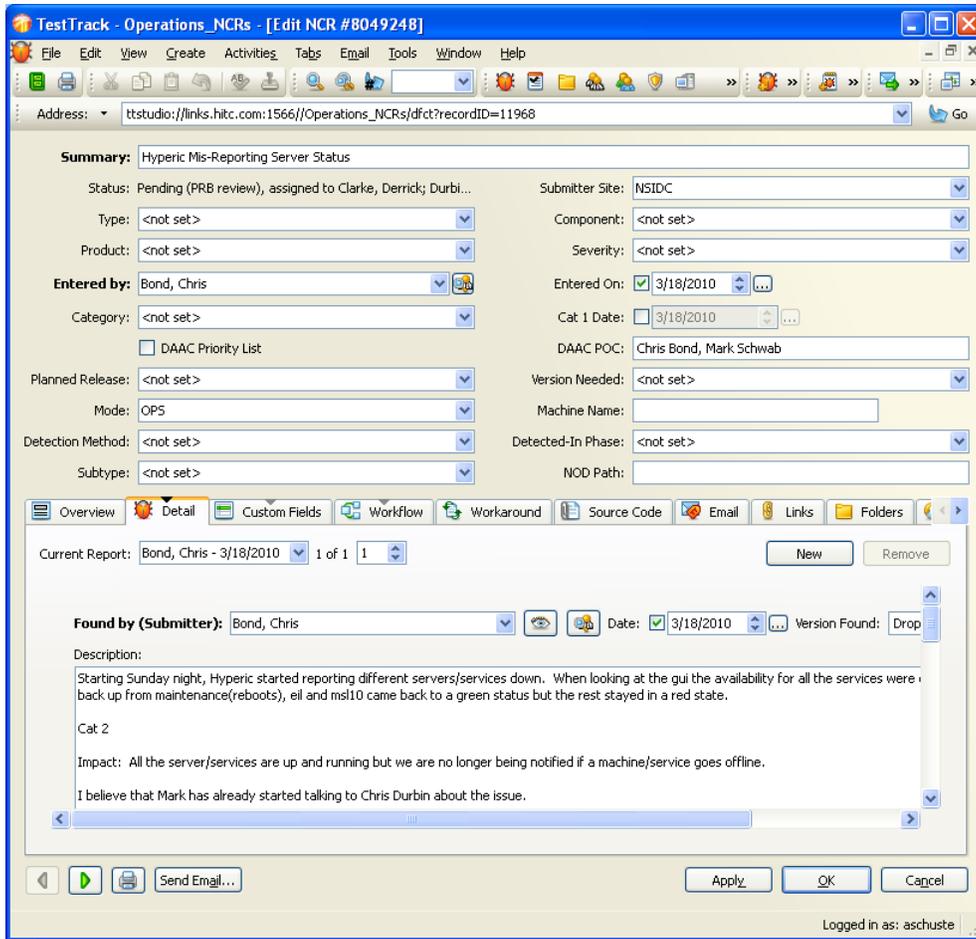


Figure 8.3-29. Edit NCRs GUI

4 On the Open GUI (Figure 8.3-30):

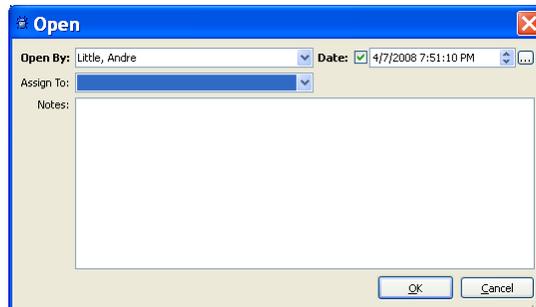


Figure 8.3-30. Open GUI

- 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 members 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:
-

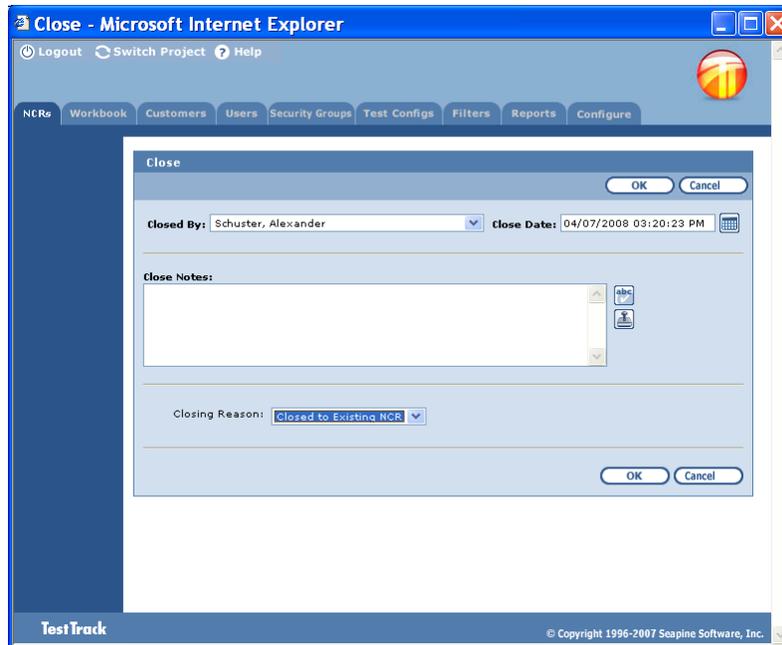


Figure 8.3-31. Close Page

- 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 pick list.
 - 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:

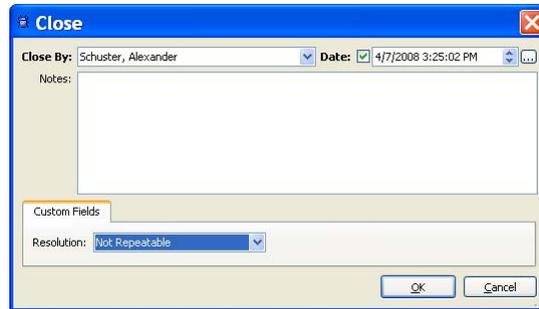


Figure 8.3-32. Close GUI

- 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 pick list.
 - 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/ladmin &
```
 - 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.

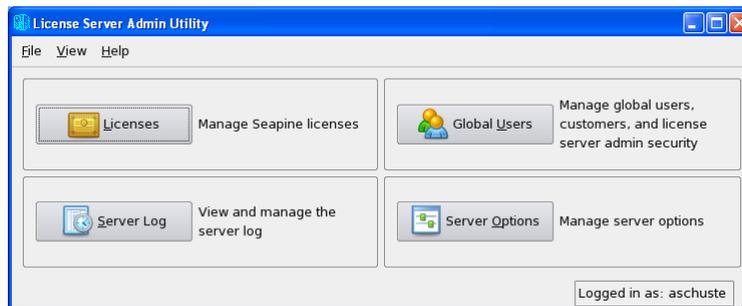


Figure 8.3-33. License Server Admin Utility GUI

- 4 Click **Add** on the **Global Users** GUI (Figure 8.3-34).

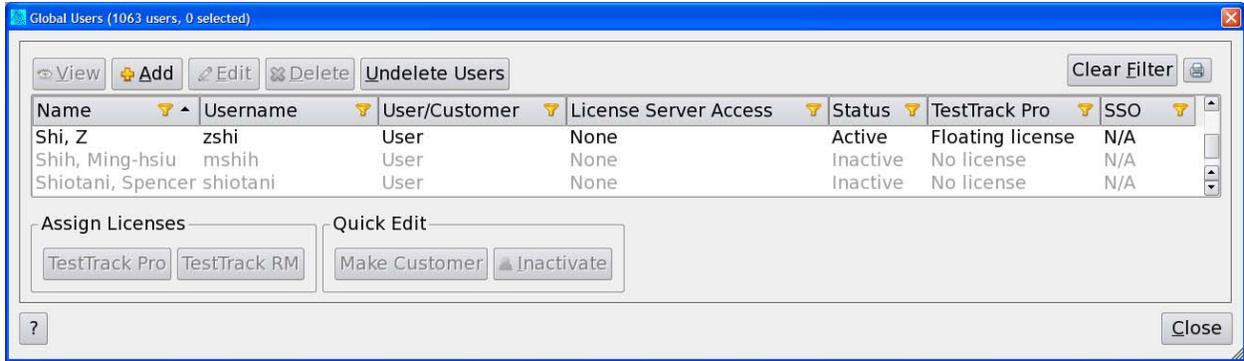


Figure 8.3-34. Global Users GUI

5 On the **Add User** GUI (Figure 8.3-35):

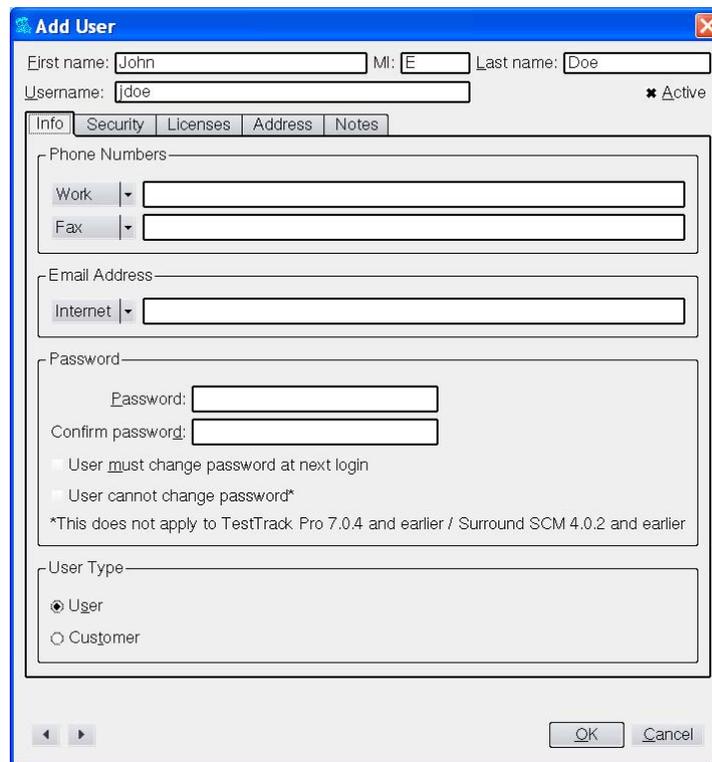


Figure 8.3-35. Add User GUI

- 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 login 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.

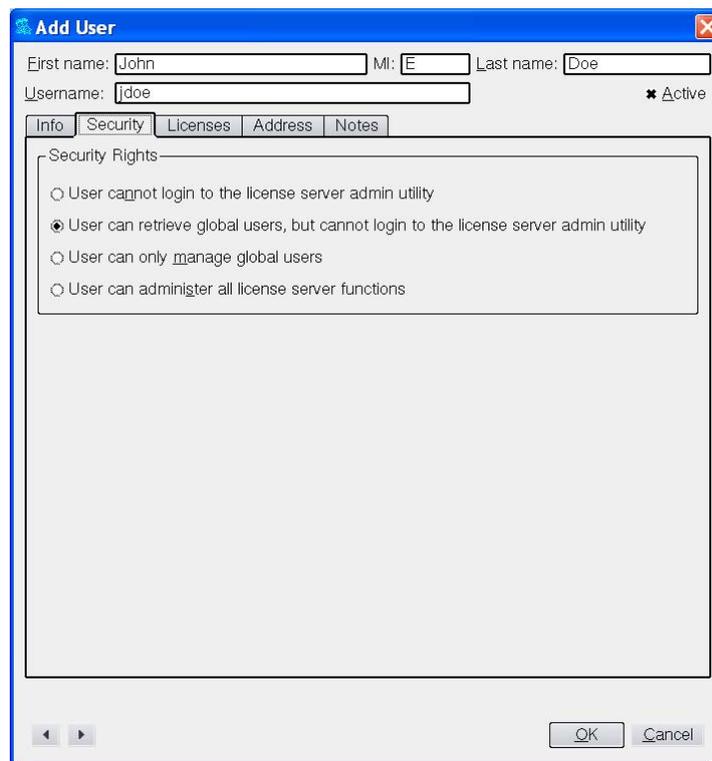


Figure 8.3-36. Add User GUI (Security tab)

8 On the Licenses tab (Figure 8.3-37):

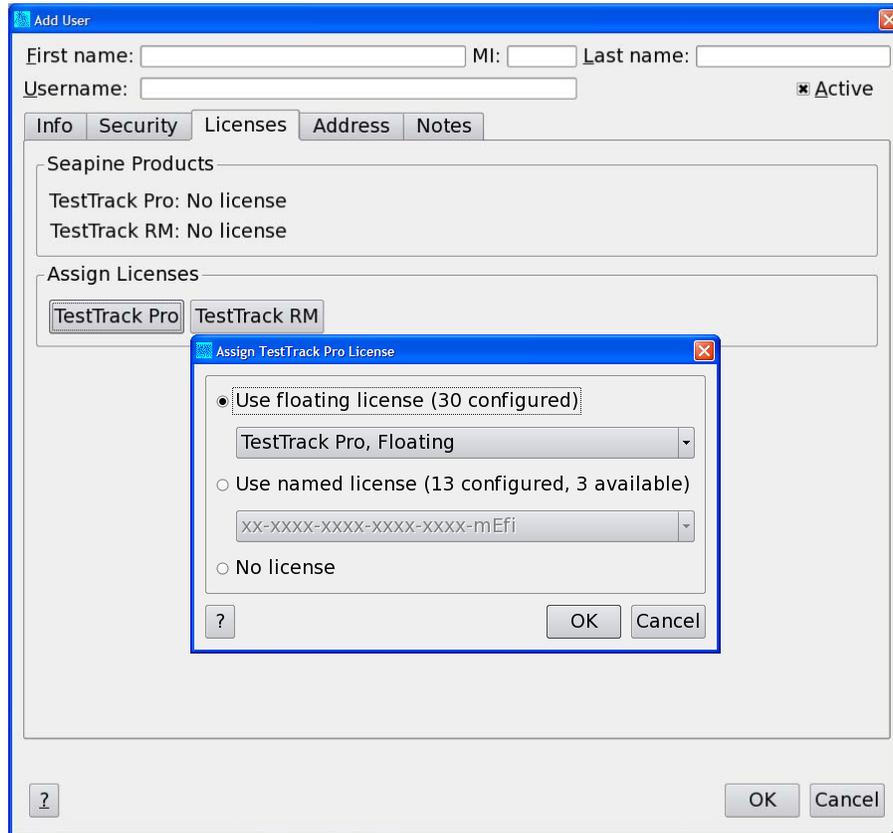


Figure 8.3-37. Add User GUI (Licenses tab)

- 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.

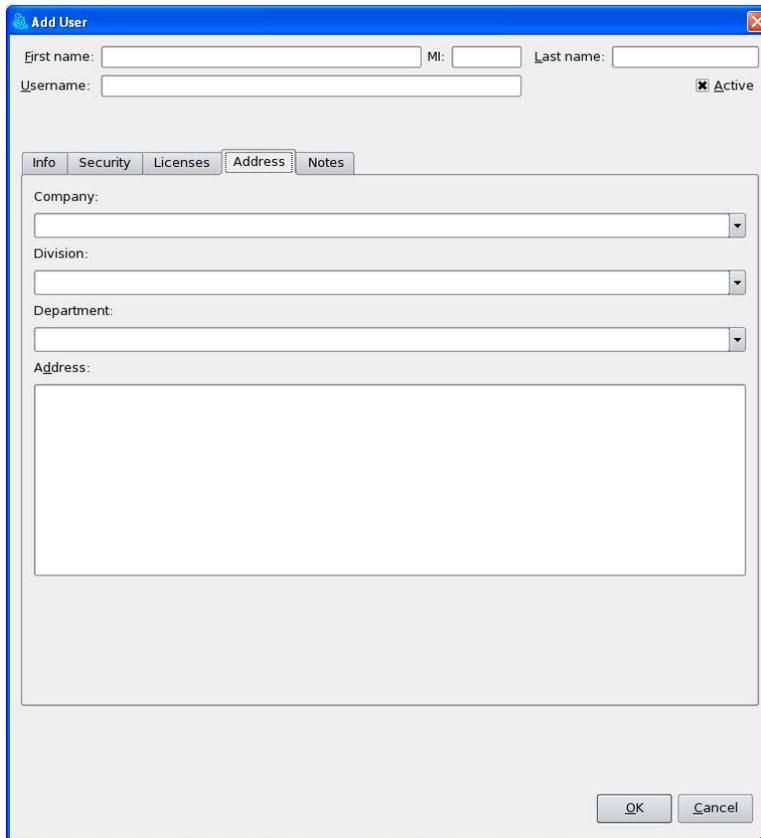


Figure 8.3-38. Add User GUI (Address tab)

- 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!
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.
Ops Supervisor	All permissions except for admin commands and others considered admin commands. Typically assigns problem priority and resolution responsibility.
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.

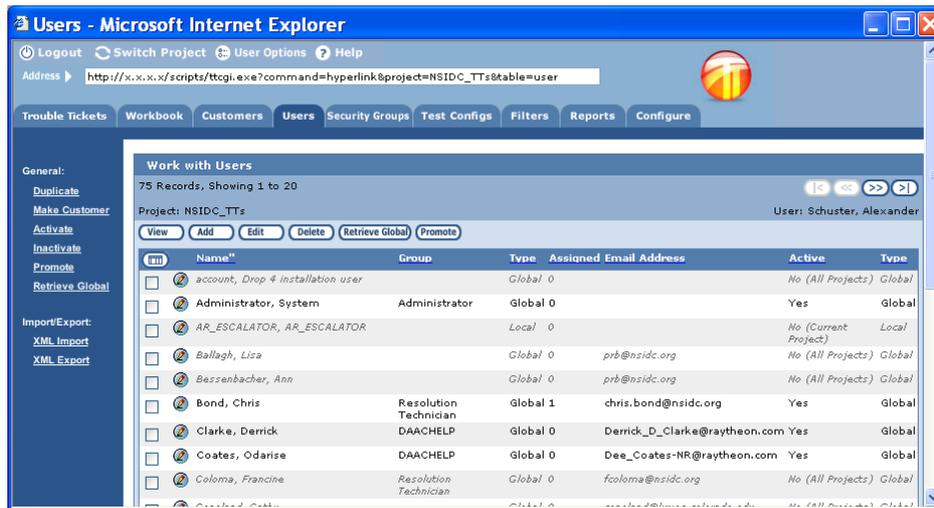


Figure 8.3-39. Users Web Page

- 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.

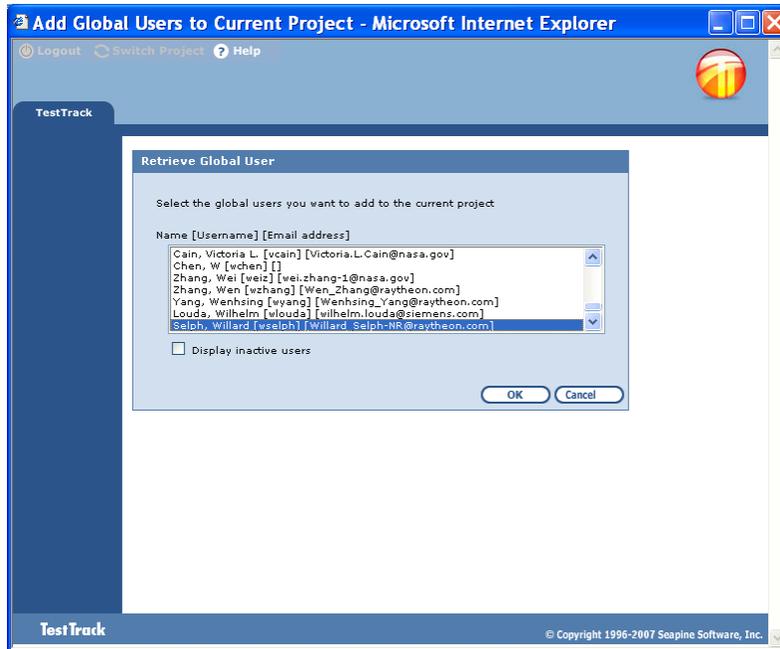


Figure 8.3-40. Retrieve Global User GUI

- 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 pick list for that field.

Note: To change an existing user's privileges, simply re-map the profile to another group.

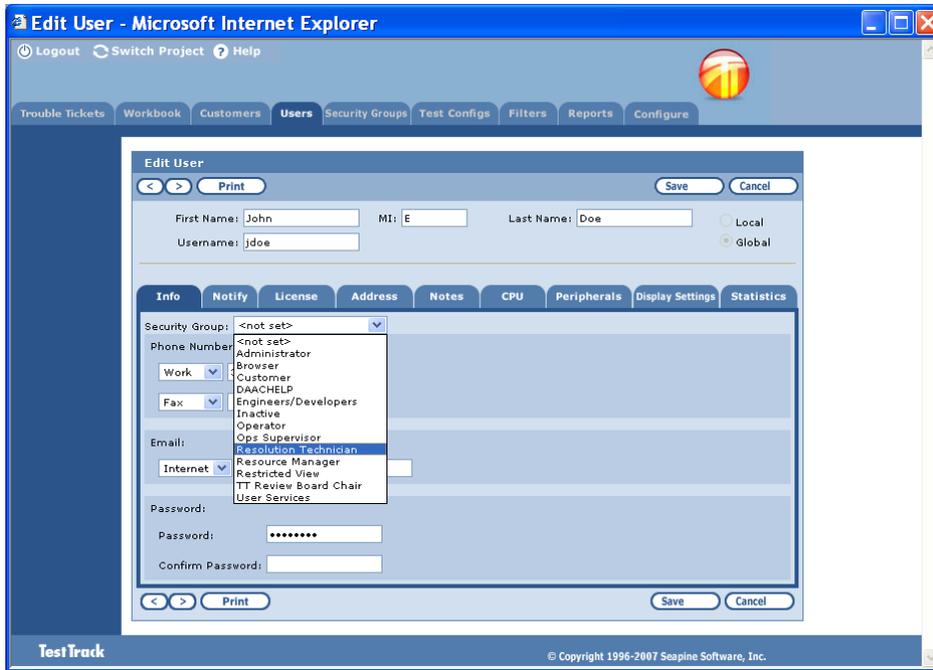


Figure 8.3-41. Edit Users Web Page

- 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.

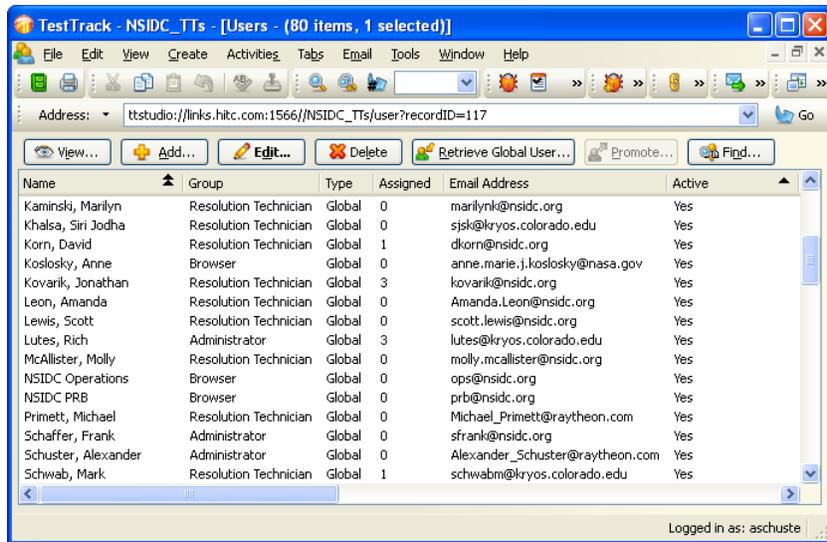


Figure 8.3-42. Users GUI

- 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 pick list for that field (Figure 8.3-44).

Note: To change an existing user’s privileges, simply re-map the profile to another group.

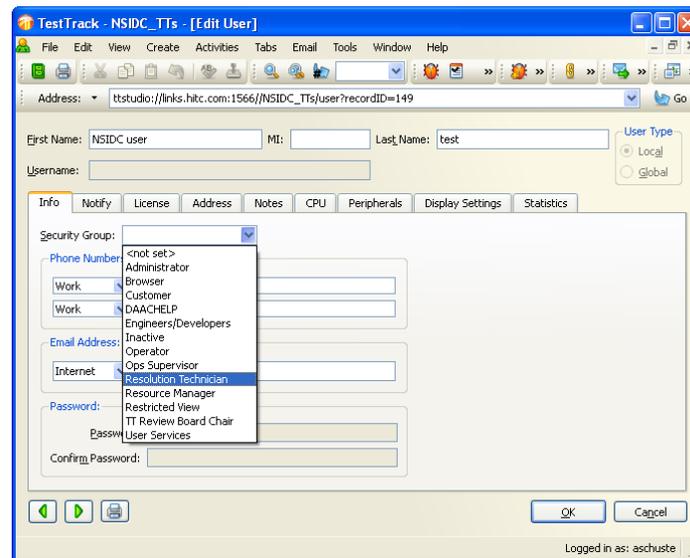


Figure 8.3-44. Edit User GUI

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.

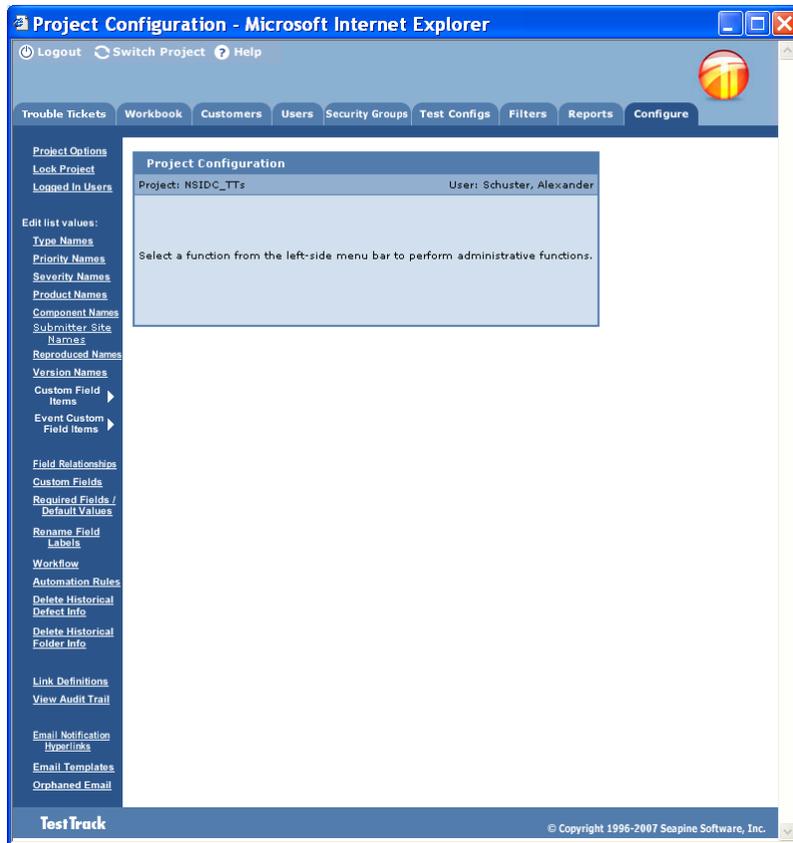


Figure 8.3-45. Project Configuration Web Page

- 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.

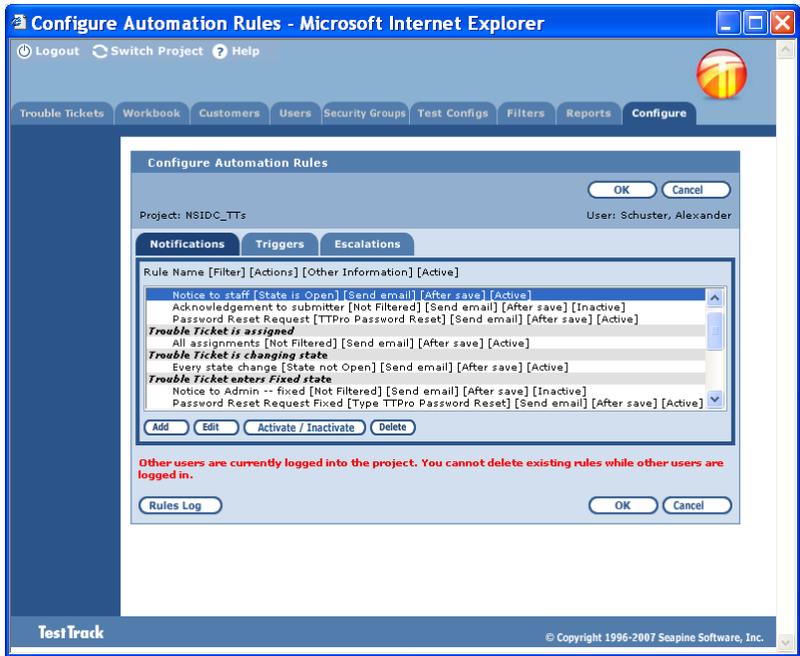


Figure 8.3-46. Configure Automation Rules Web Page

c. On the **Precondition** tab (Figure 8.3-47):

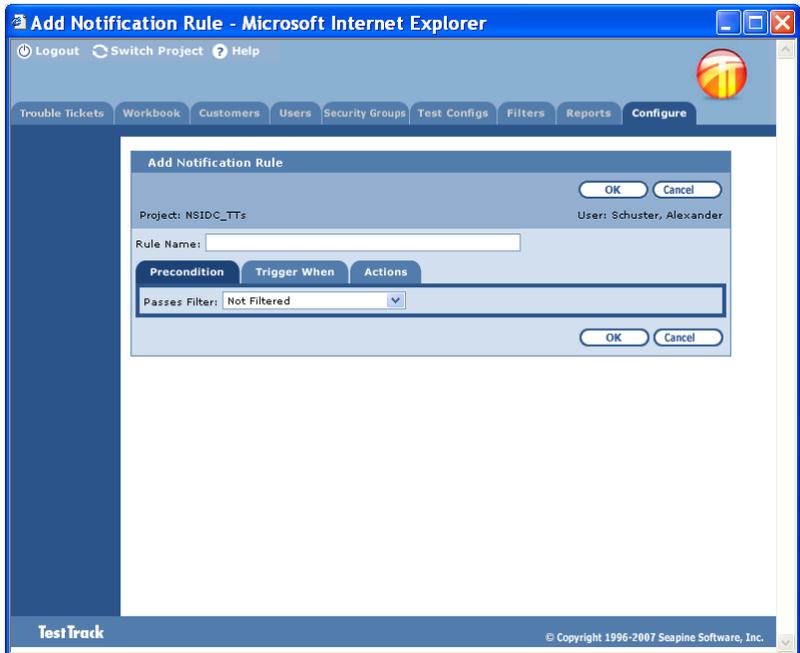


Figure 8.3-47. Add Notification Rule (Precondition tab) Web Page

- 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.

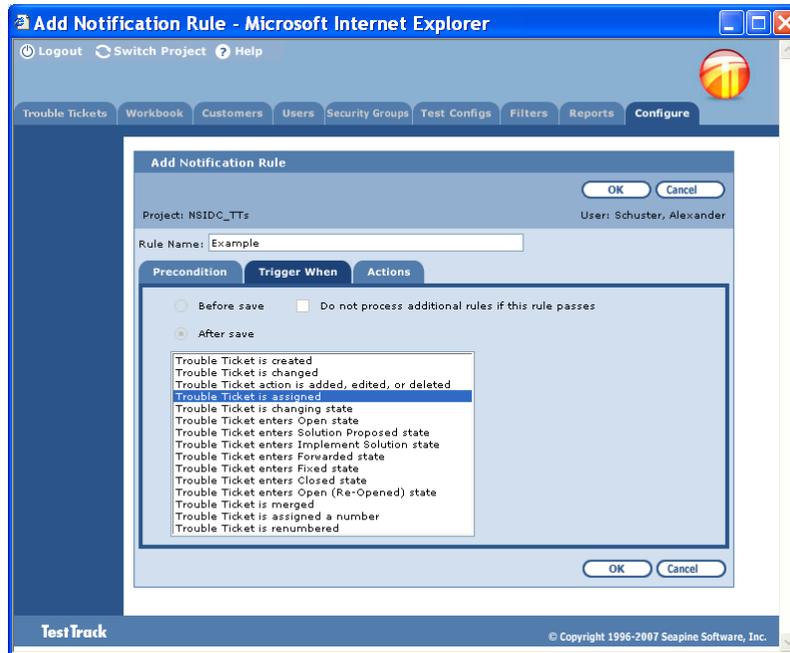


Figure 8.3-48. Add Notification Rule (Trigger When tab) Web Page

- 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):

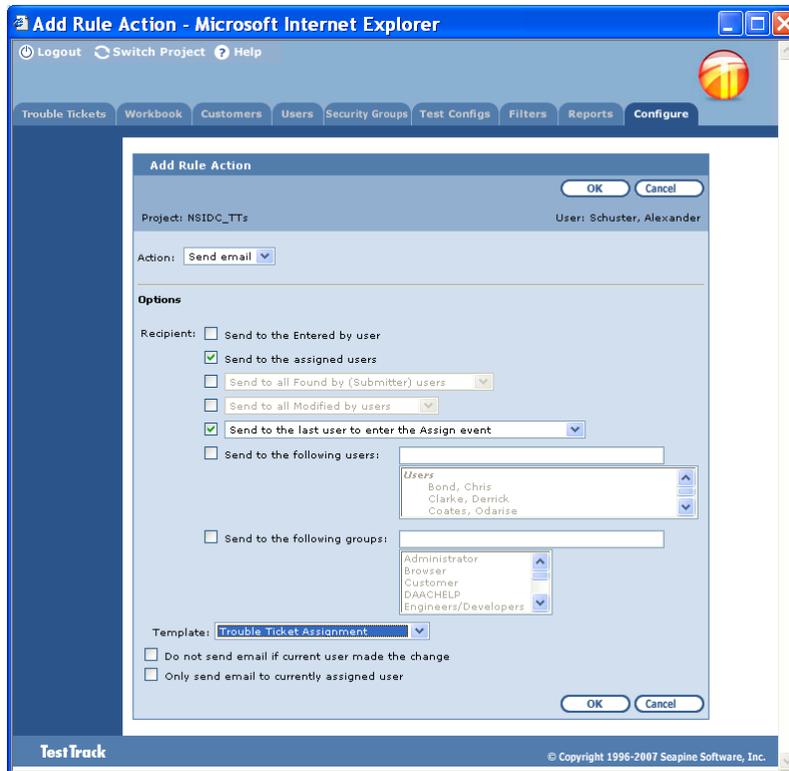


Figure 8.3-50. Add Rule Action Web Page

- i. Use the checkboxes and pick lists 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.

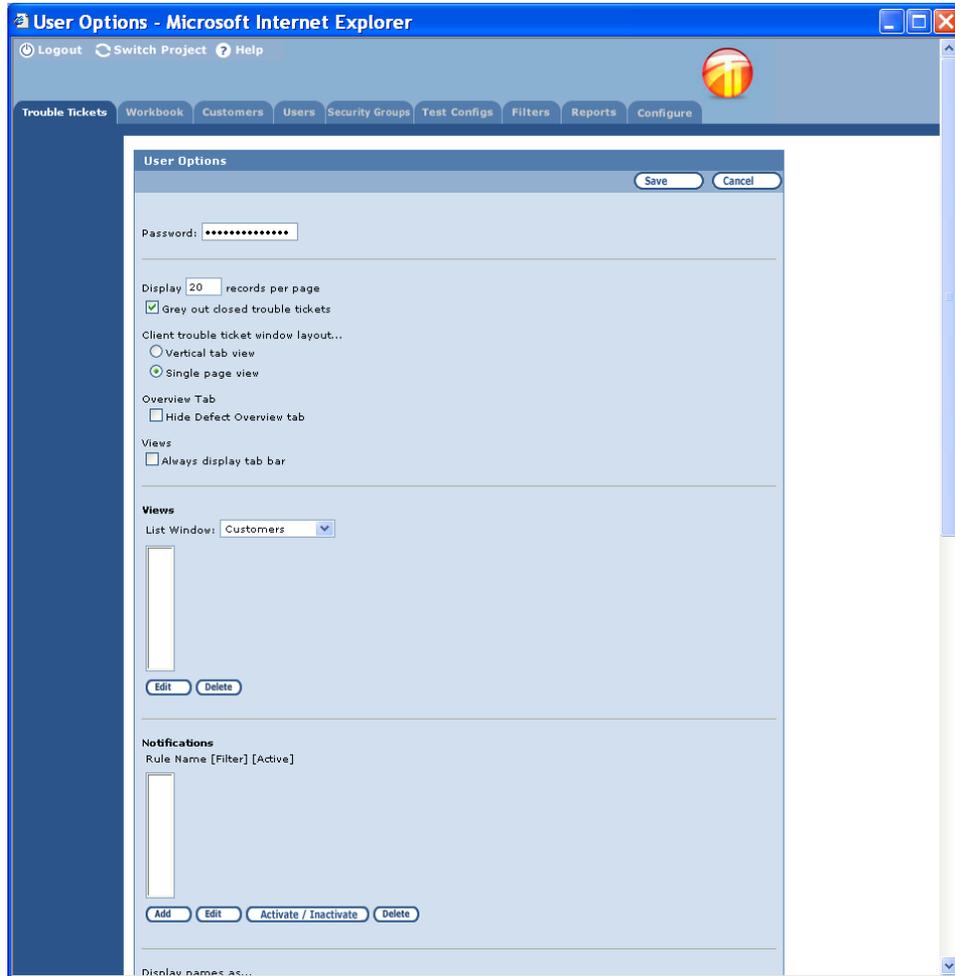


Figure 8.3-51. User Options Web Page

- c. .On the **Precondition** tab (Figure 8.3.52):

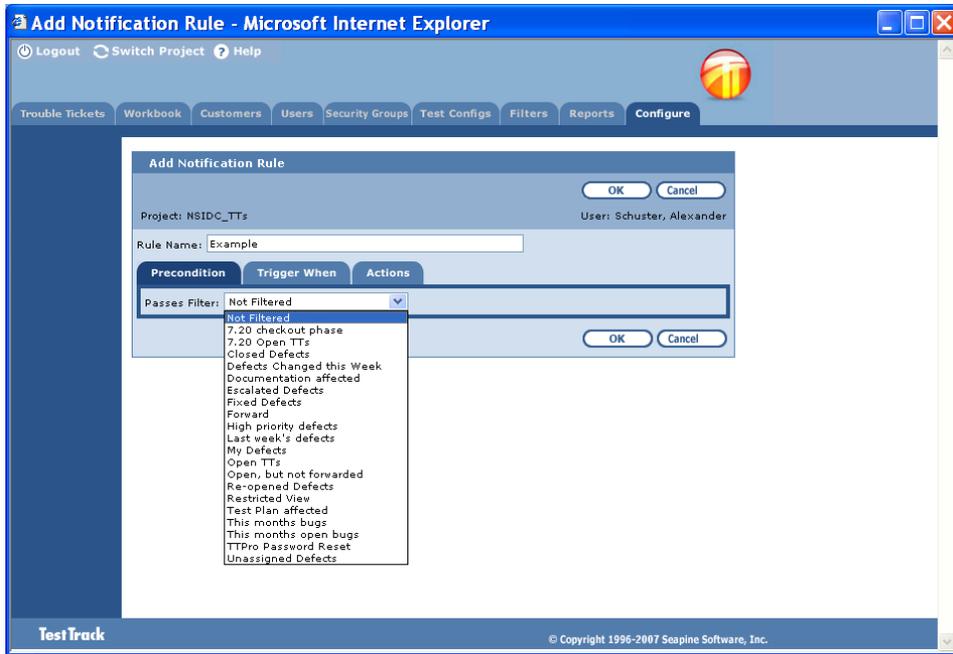


Figure 8.3-52. Add Notification Rule (Precondition Tab) Web Page

- 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.

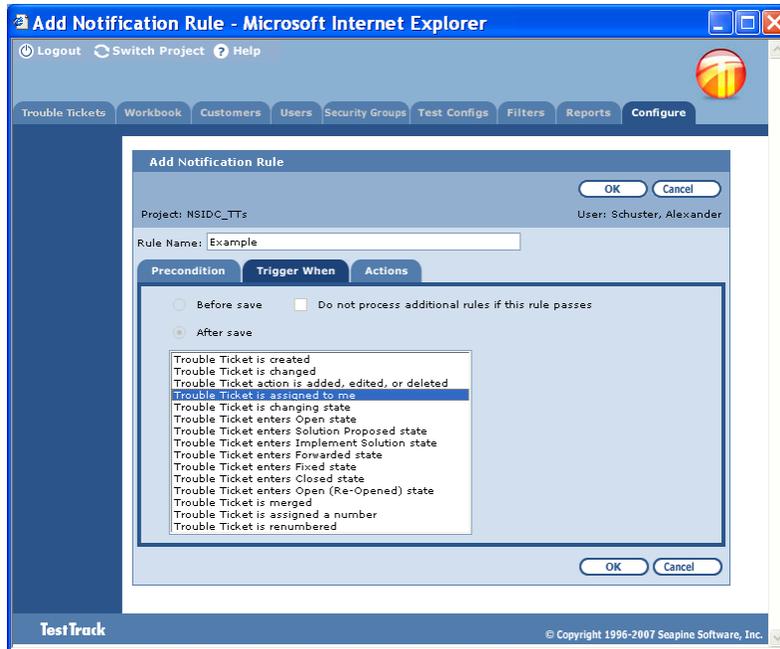


Figure 8.3-53. Add Notification Rule (Trigger When Tab) Web Page

- e. Click the **Actions** tab (Figure 8.3-54).

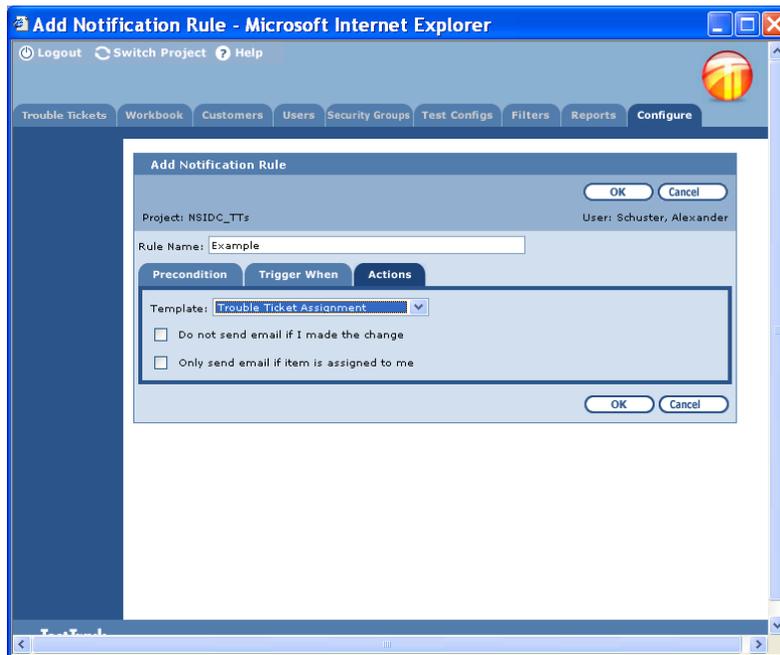


Figure 8.3-54. Add Notification Rule (Actions Tab) Web Page

- 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.

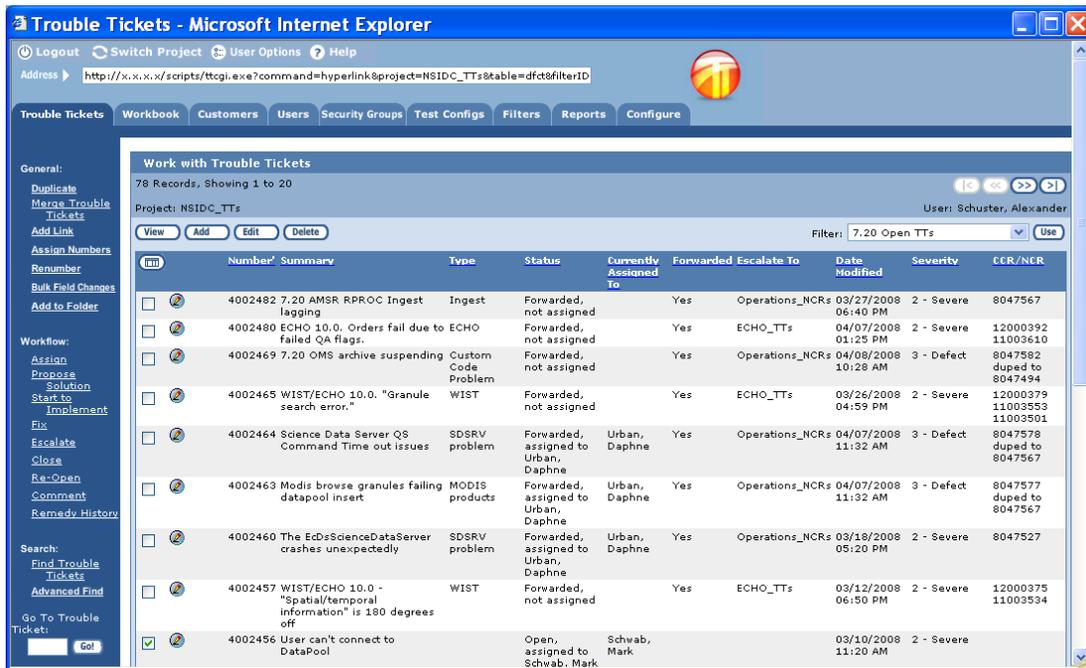


Figure 8.3-55. Work with Trouble Tickets Web Page

- b. Click the **Email** tab on the **Edit Trouble Tickets** page (Figure 8.3-56).

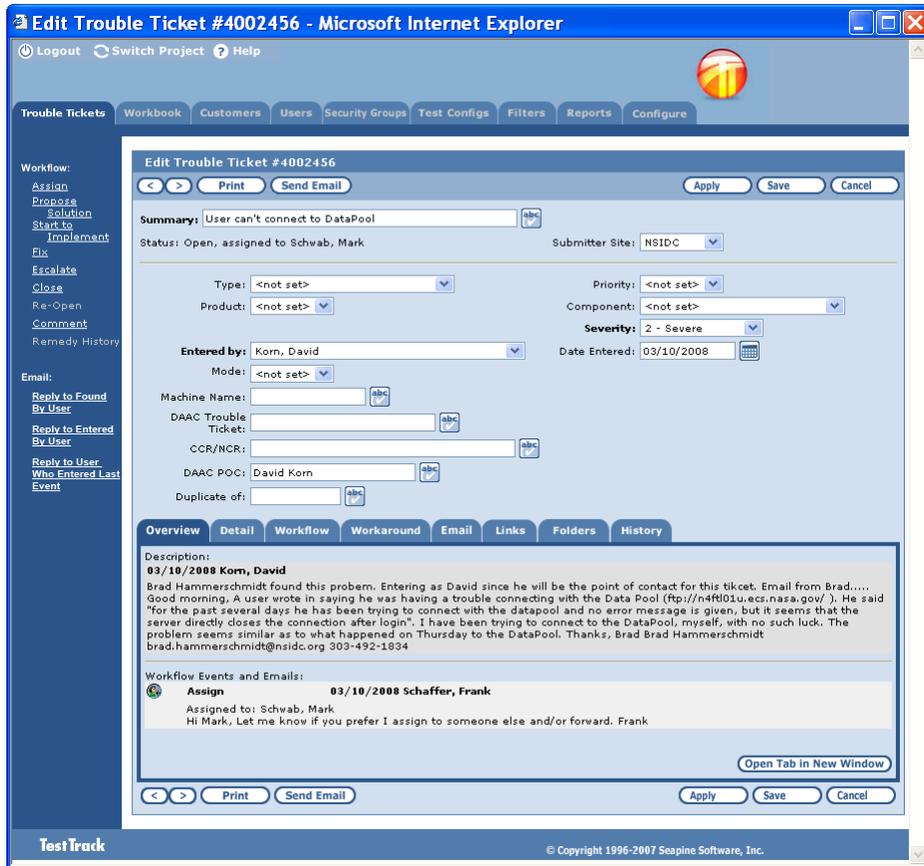


Figure 8.3-56. Work with Trouble Tickets (Detail Tab) Web Page

c. On the **Email** tab (Figure 8.3.57):

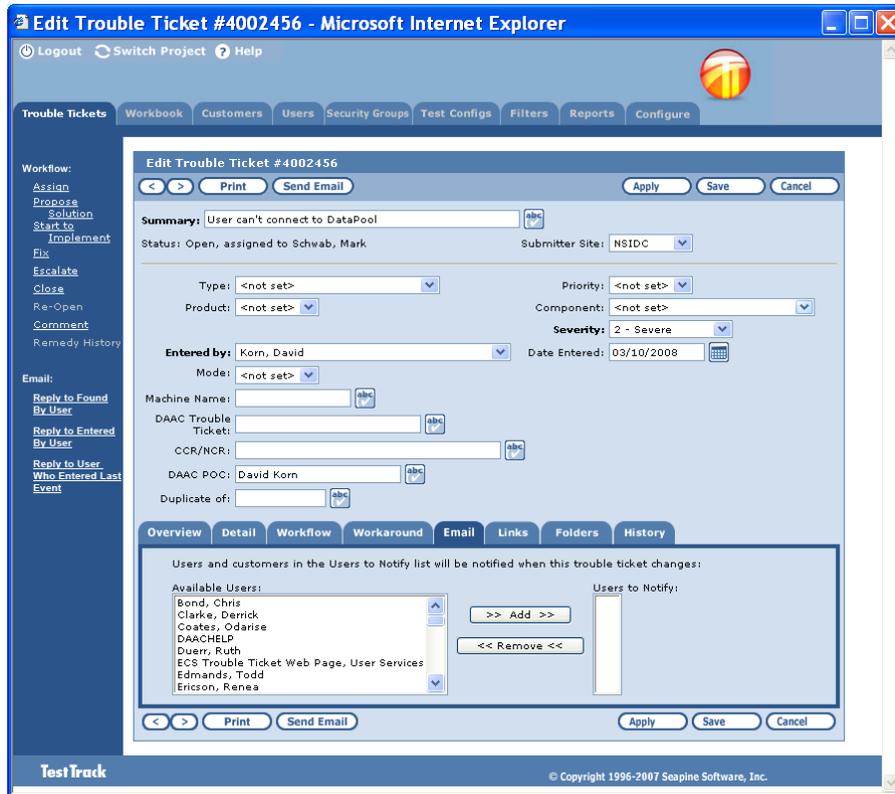


Figure 8.3-57. Edit Trouble Ticket (Email Tab) Web Page

- 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.

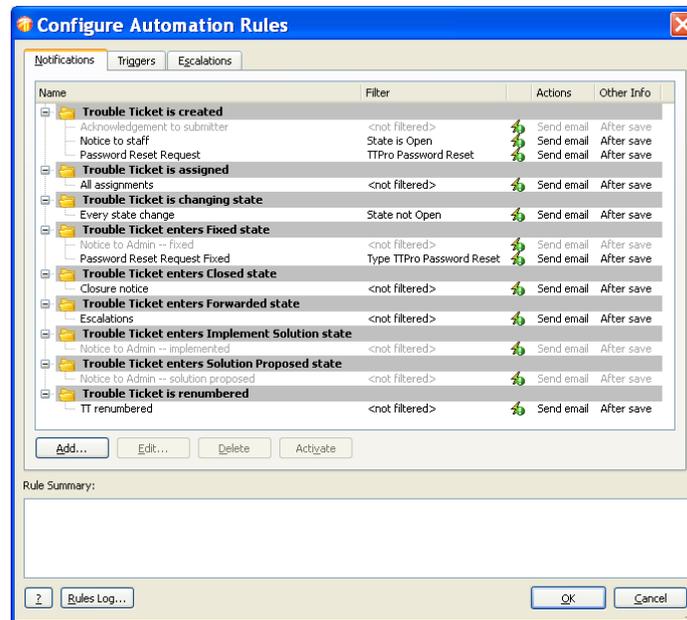


Figure 8.3-58. Configure Automation Rules GUI

- c. On the **Preconditions** tab (Figure 8.3-59):

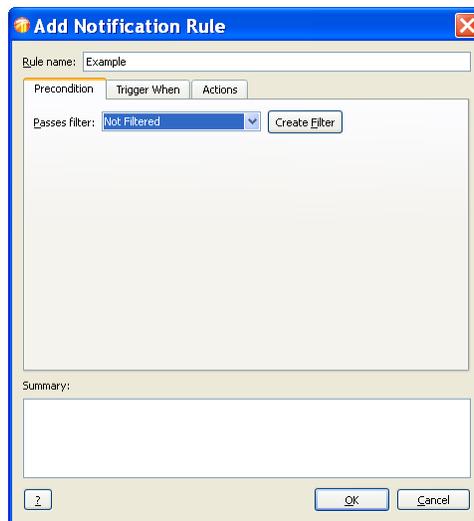


Figure 8.3-59. Add Notification Rule (Precondition Tab) GUI

- 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.

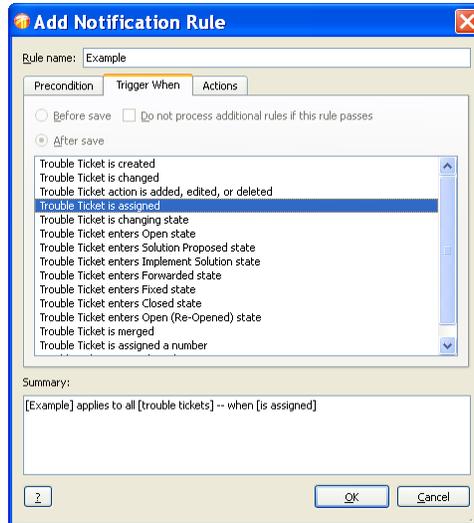


Figure 8.3-60. Add Notification Rule (Trigger When Tab) GUI

- 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.

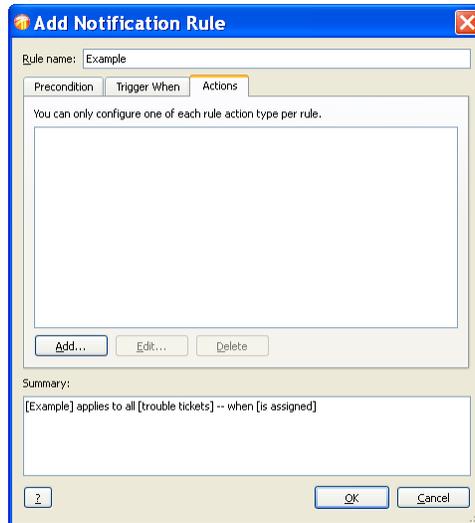


Figure 8.3-61. Add Notification Rule (Actions Tab) GUI

f. On the **Add Rule Action** GUI (Figure 8.3-62):

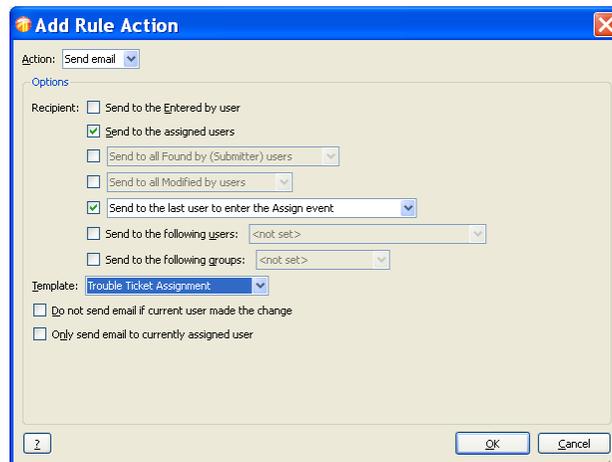


Figure 8.3-62. Add Rule Action GUI

- i. Use the checkboxes and pick lists 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.

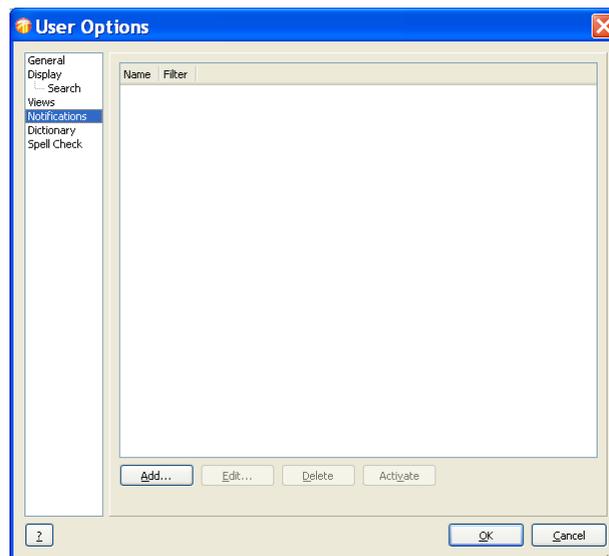


Figure 8.3-63. User Options (Notification Category) GUI

- c. On the **Precondition** tab (Figure 8.3.64):

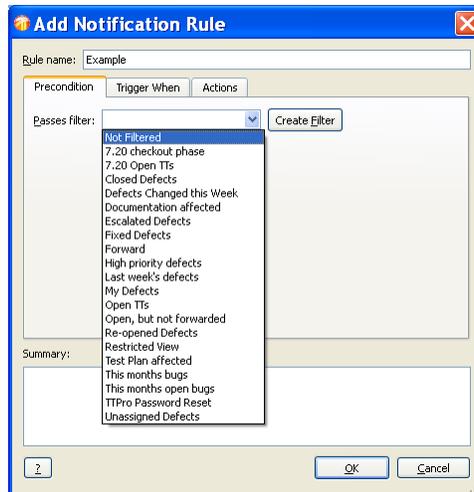


Figure 8.3-64. Add Notification Rule (Precondition Tab) GUI

- 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.

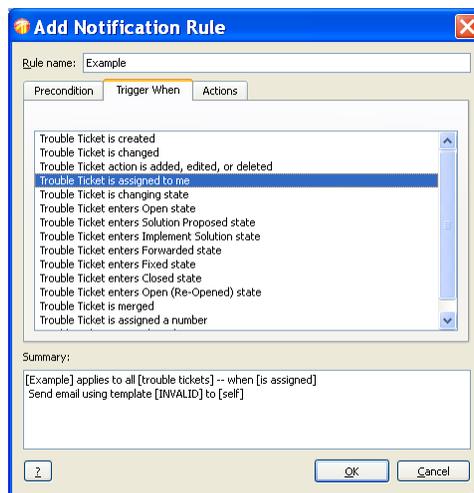


Figure 8.3-65. Add Notification Rule (Trigger When Tab) GUI

- e. Click the **Actions** tab (Figure 8.3-66).

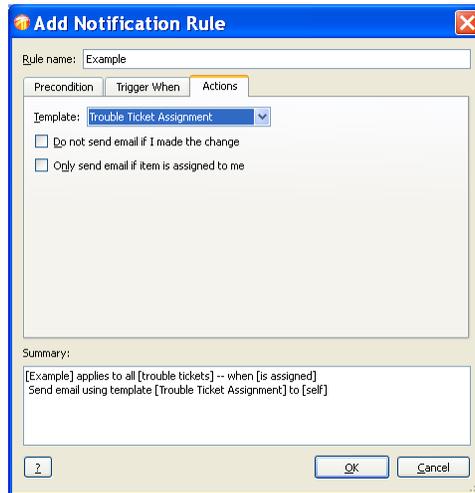


Figure 8.3-66. Add Notification Rule (Actions Tab) GUI

- 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):

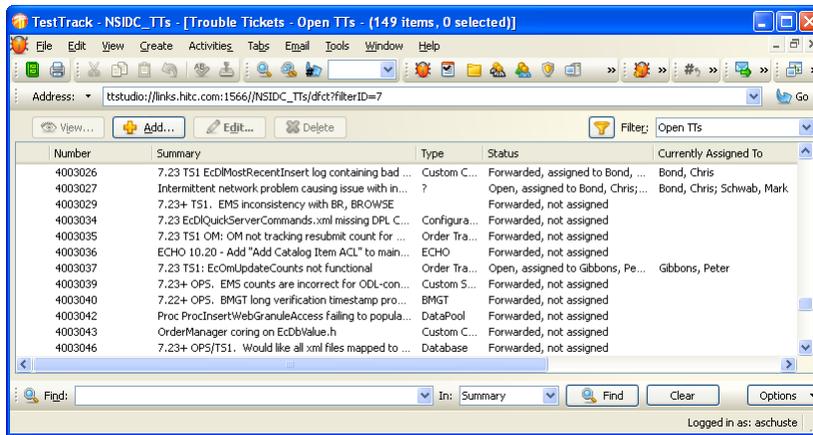


Figure 8.3-67. Trouble Tickets GUI

- 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):

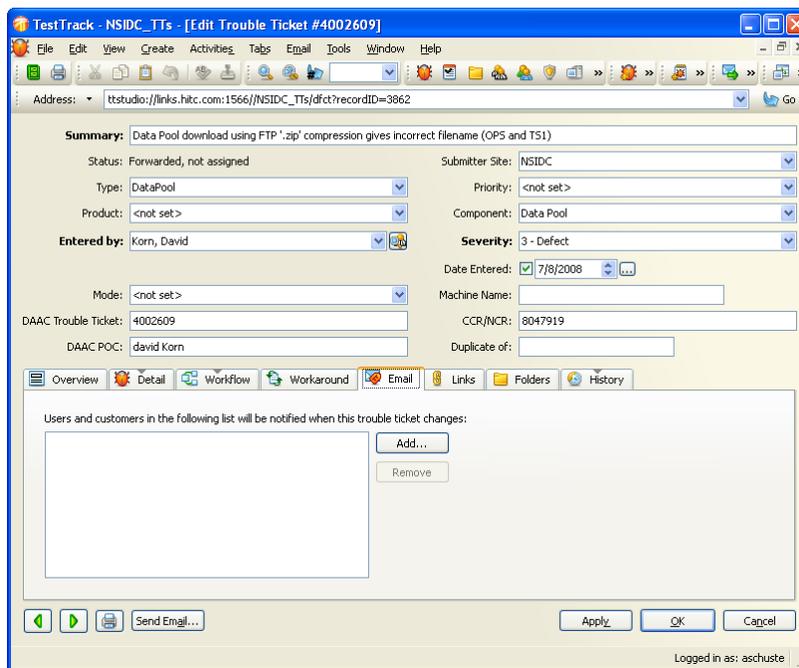


Figure 8.3-68. Edit Trouble Ticket (Email Tab) GUI

- 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 sensitive 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**, and 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).

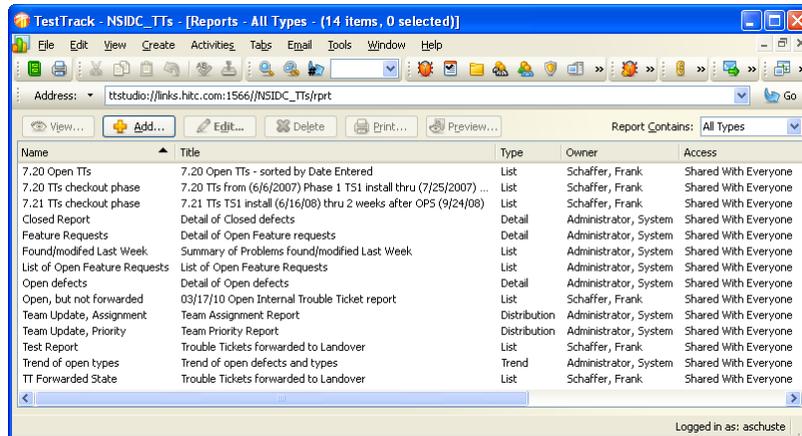


Figure 8.3-69. Reports List GUI

- 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, and 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).

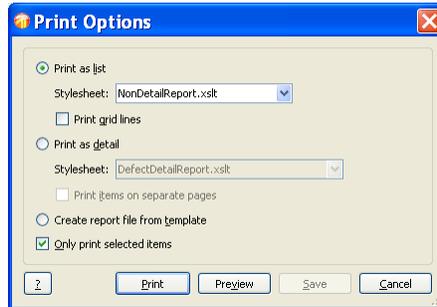


Figure 8.3-70. Print Options GUI

- 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, and 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, and then close your browser window.
-

8.4 Emergency Fixes

Emergency fixes may be needed 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 supervisor (i.e., shift leader) for a decision.

The DAAC cannot afford to have the ATL down until Monday. The Operations Supervisor 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 notifies the Site Property Custodian about the model, version, and serial number of the new board.

The site CM Administrator (CMA) reviews the trouble ticket, and presents it to the local CCB for approval. The CMA then updates their baseline 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 EED Problem Review Board (PRB) for priority review, where it is resolved or translated into an NCR. The PRB reviews all emergency trouble tickets 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 EED PRB.	TT escalated to EED PRB.
PRB reviews emergency NCR, checks for applicability to other sites.	