4.3 Configuration Management

This section describes the configuration management tools used by ECS operators:

1. ClearCase
2. Microsoft Access EMD Change Manager (ECM) Configuration Change Request (CCR) Tool
3. IBM Rational ClearCase Baseline Manager (BLM)
4. AssetSmart ILM (Inventory, Logistics and Maintenance) Manager
5. FLEXnet Publisher
6. TestTrack Pro

This page intentionally left blank.

4.3.1 ClearCase

This section presents an orientation of ClearCase. ClearCase terminology such as VOB (Versioned Object Base, a public storage area for files) and views (operator private storage), is used throughout this section. Refer to the ClearCase Introduction document for both a more detailed description of ClearCase and an explanation of the terminology used. Refer to ClearCase's Introduction, Administrator, and Reference documentation for detailed explanations of ClearCase functionality.

ClearCase is a COTS software product used in ECS to perform source code management and build functions. It provides the staffs at ECS sites and Riverdale the capability to organize and store software in a software library, to control software changes and versions, and to assemble sets of software for release purposes. Specifically, ClearCase is used at the ECS Development Facility (EDF) to control access to custom code files; to control and log file changes; to perform builds of software and keep a record of the build's content (files, compiler, and other resources used).

The ClearCase view and VOB servers run on Linux-based hosts.

ClearCase is used to perform a variety of operator functions. The most frequently used functions are listed in Table 4.3.1-1.

Table 4.3.1-1. Common ECS Operator Functions Performed with ClearCase (1 of 2)

Operating Function	Command/Script or GUI	Description	When and Why to Use
Establish a View	Setview /GUI (View Menu, Set Option) selection	The command or the GUI selection activates a view and allows user access to controlled files.	(1) Used to activate a reproducible workspace for a developer for working with specific file versions and directories for a task. (2) Used to assemble sets of software for release purposes.
Checkout Software	Checkout/GUI (Checkout) selection	The command or the GUI creates a view private, modifiable copy of a file version.	Used when a developer/maintainer needs to modify an existing version of software.
Checkin Software	Checkin/GUI (Checkin) selection	The command or the GUI selection creates a permanent new version of a file.	Used when a developer/maintainer needs to return a modified file version to the ClearCase software library.

Table 4.3.1-1. Common ECS Operator Functions Performed with ClearCase (2 of 2)

Operating Function	Command/Script or GUI	Description	When and Why to Use
Perform software builds	Clearmake/GUI (Building menu)	(1) ClearCase build utility that automates the process of software builds. (2) Facilitates derived object sharing. (3) Creates a record of the build so that it can be repeated.	Used when it's time to build, integrate and/or test developed/revised software.
Display the mount-point and storage directory of all VOBs on the system	Cleartool lsvob/GUI (Admin menu)	ClearCase utility that determines and displays default/specified information about all of the VOBs that have been established.	(1) Used to list one or more VOBs. (2) Used to determine which VOBs are mounted. (3) Used to determine which VOBs are private or public (refer to *ClearCase Reference Manual* for details).

4.3.1.1 Quick Start Using ClearCase

To invoke the ClearCase graphical user interface GUI from the command line prompt type:

/usr/atria/bin/xclearcase.

4.3.1.1.1 ClearCase Graphical User Interface

ClearCase has a Command Line Interface (CLI) and a GUI. The GUI enables execution of all the common functions and facilitates graphical examination of the version history of objects in VOBs. When ClearCase is invoked, a Transcript screen as shown in Figure 4.3.1-1 appears. The Transcript screen displays status of functions executed and displays warning and error messages. It automatically appears when the status of an activity needs to be displayed.

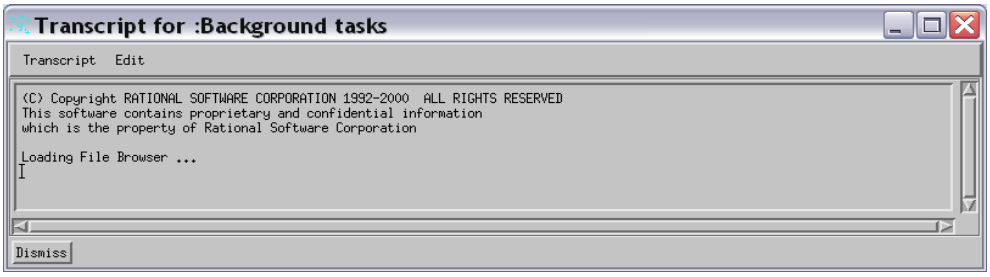


Figure 4.3.1-1. ClearCase Transcript Screen

4.3.1.1.1.1 4.3.1.1.1.1Establish View

Operator access to versions of files in a VOB is facilitated by a view. When ClearCase is initiated, the operator is asked to select a view. Available views are displayed in the View Tag Browser Screen as shown in Figure 4.3.1-2. Select a view by highlighting the desired view and clicking the "Ok" button at the bottom of the screen.

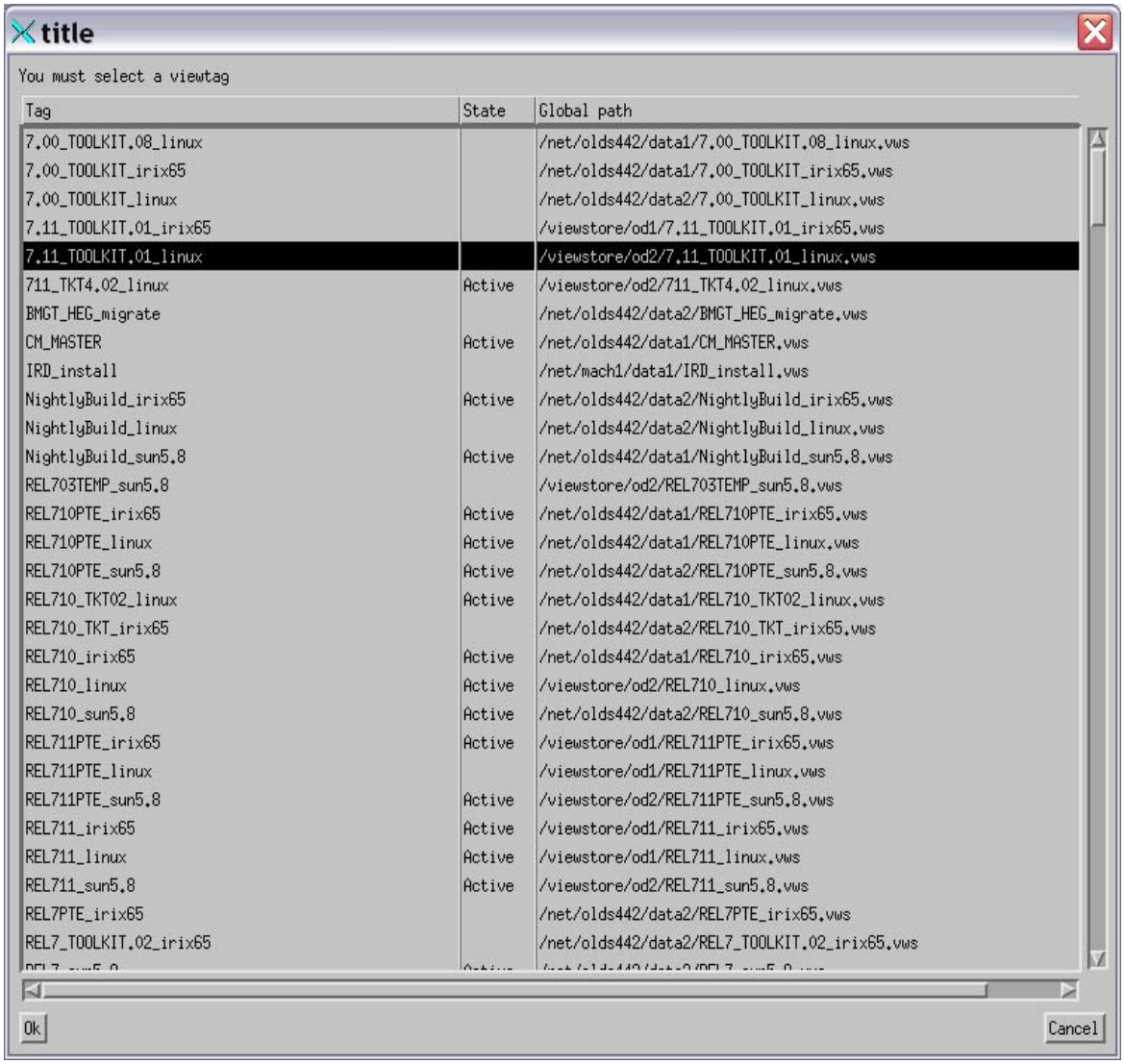


Figure 4.3.1-2. View Tag Browser Screen

After a View is selected the ClearCase File Browser screen, the main GUI screen, appears as shown in Figure 4.3.1-3. The File Browser screen displays the current directory name just below the toolbar and displays the contents of the directory in the space below the directory's name. A variety of GUI-oriented functions can be initiated from this screen. Explanations of the menu bar and the toolbar items are provided in Chapter 3 of the ClearCase User's Manual.

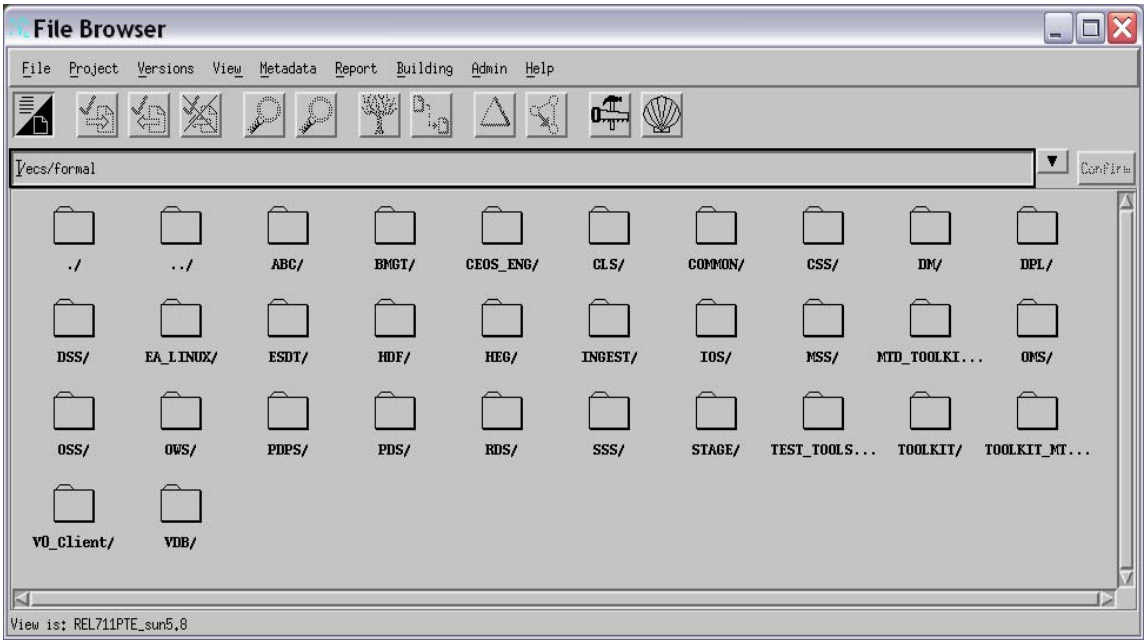


Figure 4.3.1-3. ClearCase File Browser Screen (Main Screen)

4.3.1.1.1.2 4.3.1.1.1.2Checkout Software

Software file versions in a ClearCase VOB are in a read-only state. An operator must check a file version out of the VOB before any editing of the file version can be accomplished. Check out a file version by selecting the file and clicking the checkout icon  on the toolbar. An alternate method is to select the file, click the Versions menu, then the Checkout option, then one of the "Reserved or Unreserved" options shown in Figure 4.3.1-4.

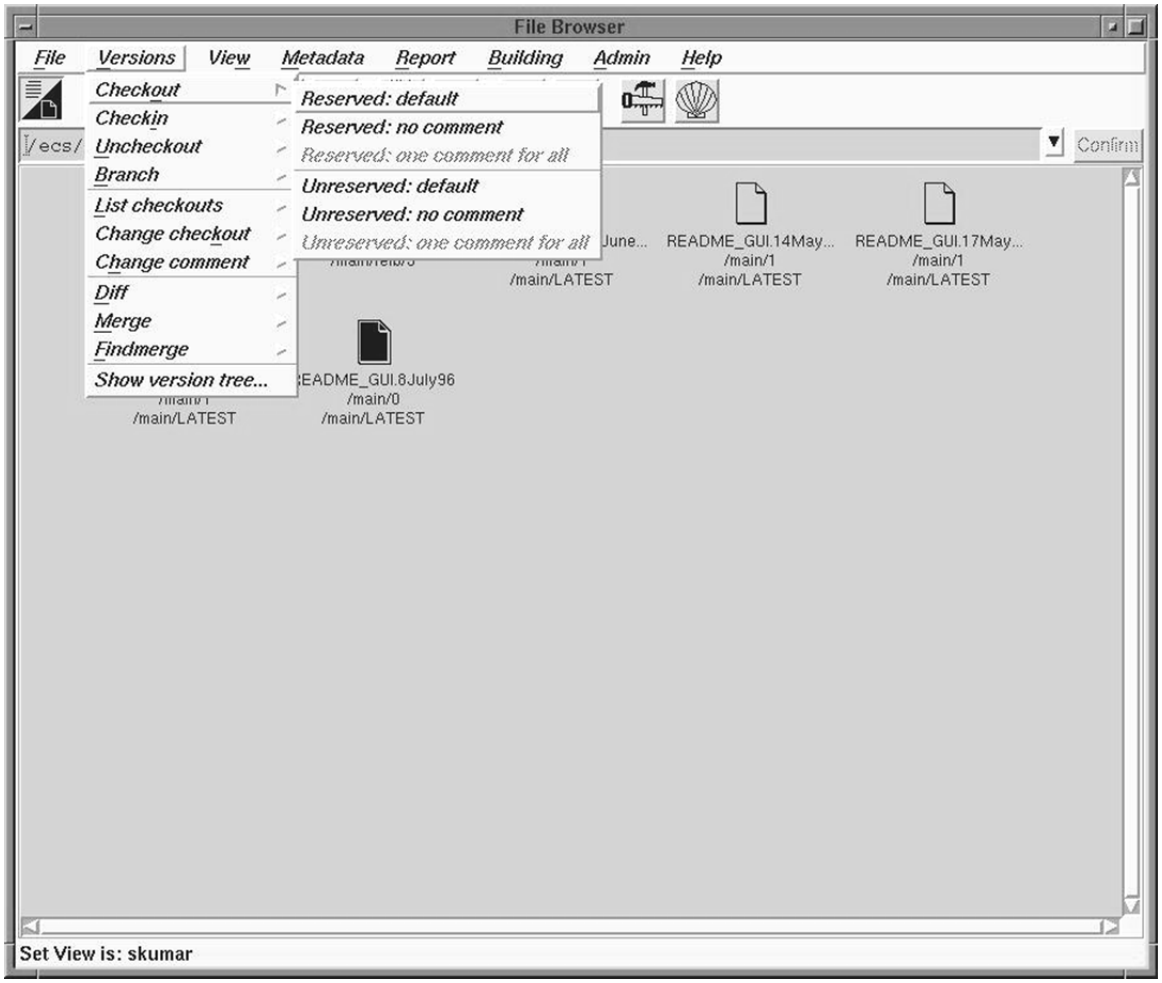


Figure 4.3.1-4. ClearCase File Browser Screen (Checkout Software)

If the operator is authorized and the view is set up to checkout files, then the checkout process continues and the ClearCase Prompt screen appears as shown in Figure 4.3.1-5. This screen gives the operator the opportunity to enter an explanation of why the file version is being checked out.

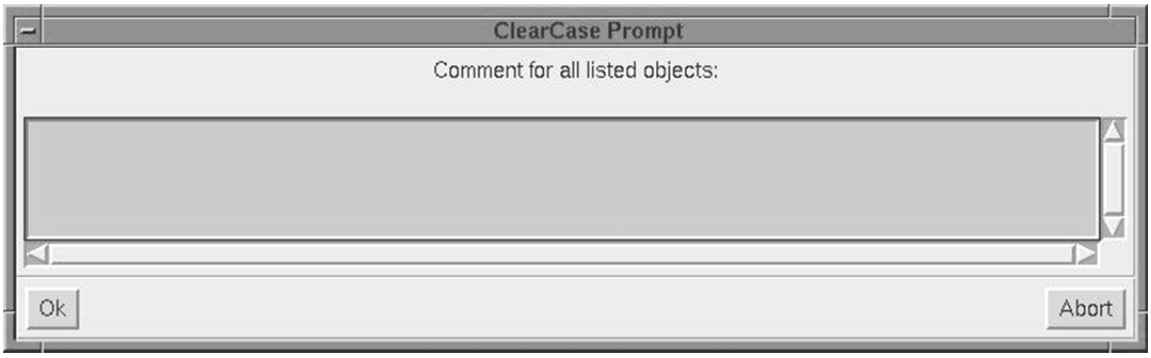


Figure 4.3.1-5. ClearCase Prompt Screen (Checkout Comment)

After appropriate comments are entered, click the "Ok" button and ClearCase adds the comments to the historical record for the file version. The File Browser screen reappears as shown in Figure 4.3.1-6 and it shows that the file version has been checked out. Note the added check mark for the README_GUI.8.July96, file. Addition of the check mark is an indication of a successful checkout.

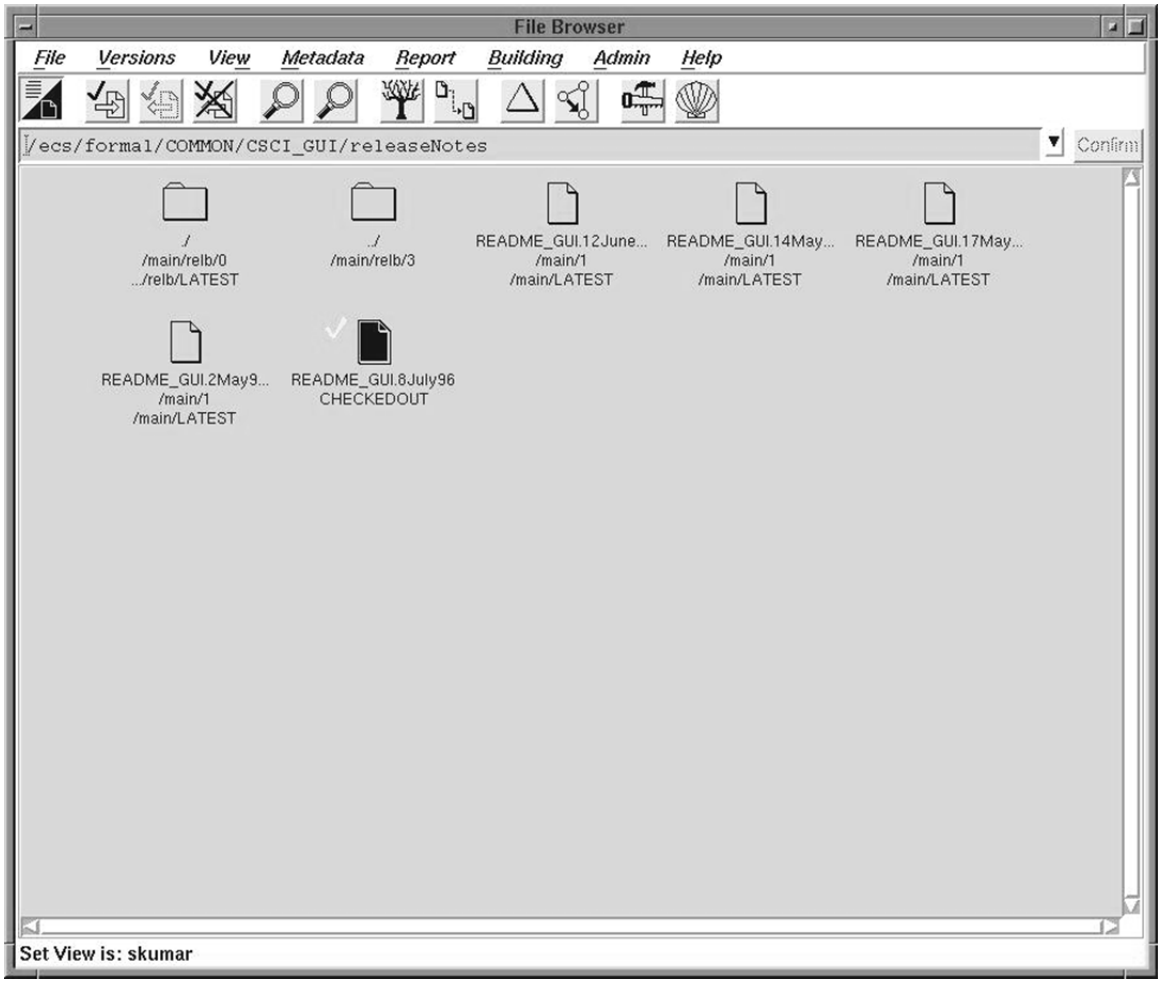


Figure 4.3.1-6. File Browser Screen (File Version Checked-Out)

To verify that the file version has been checked out on a branch, click the Vtree icon  on the File Browser toolbar. This activates the Version Tree Browser and it displays a graphical image of the branching as shown in Figure 4.3.1-7. Note that the checked out file version has been placed on the main branch (/main) in the example below.

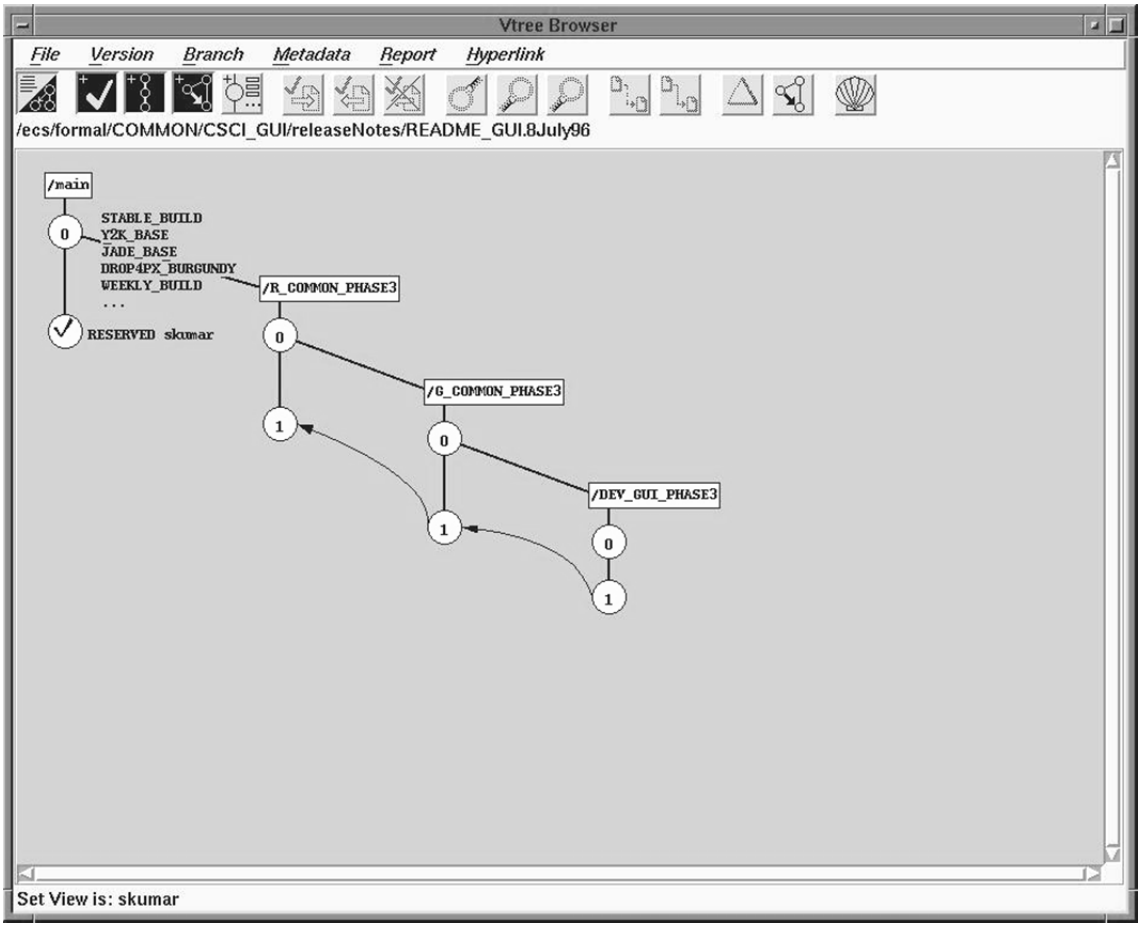


Figure 4.3.1-7. ClearCase Version Tree Screen

4.3.1.1.1.3 4.3.1.1.1.3Checkin Software

A software file version checked out of the ClearCase library for editing must be checked in to the library for it to become a new version of the original file. Click the checkin icon  on the File Browser toolbar to initiate the check-in process. A ClearCase Prompt box appears as shown in Figure 4.3.1-8 to facilitate the adding of comments at check in to the file version's record. Enter a comment and click the "Ok" button to continue or just click the "Ok" button to continue the check-in process.

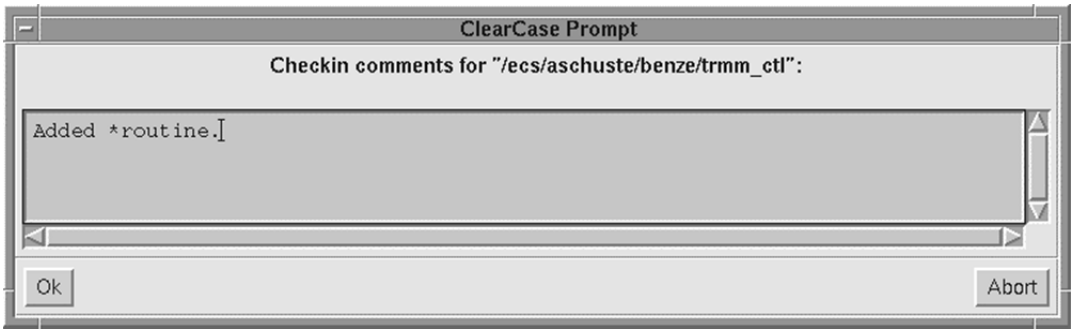


Figure 4.3.1-8. ClearCase Prompt Screen (Checkin Comment)

The File Browser screen reappears as shown in Figure 4.3.1-9 and it shows that the file version has been checked in. Note that the check mark that was next to the README_GUI.8July96 file has been removed. Removal of the check mark is an indication of a successful checkin.

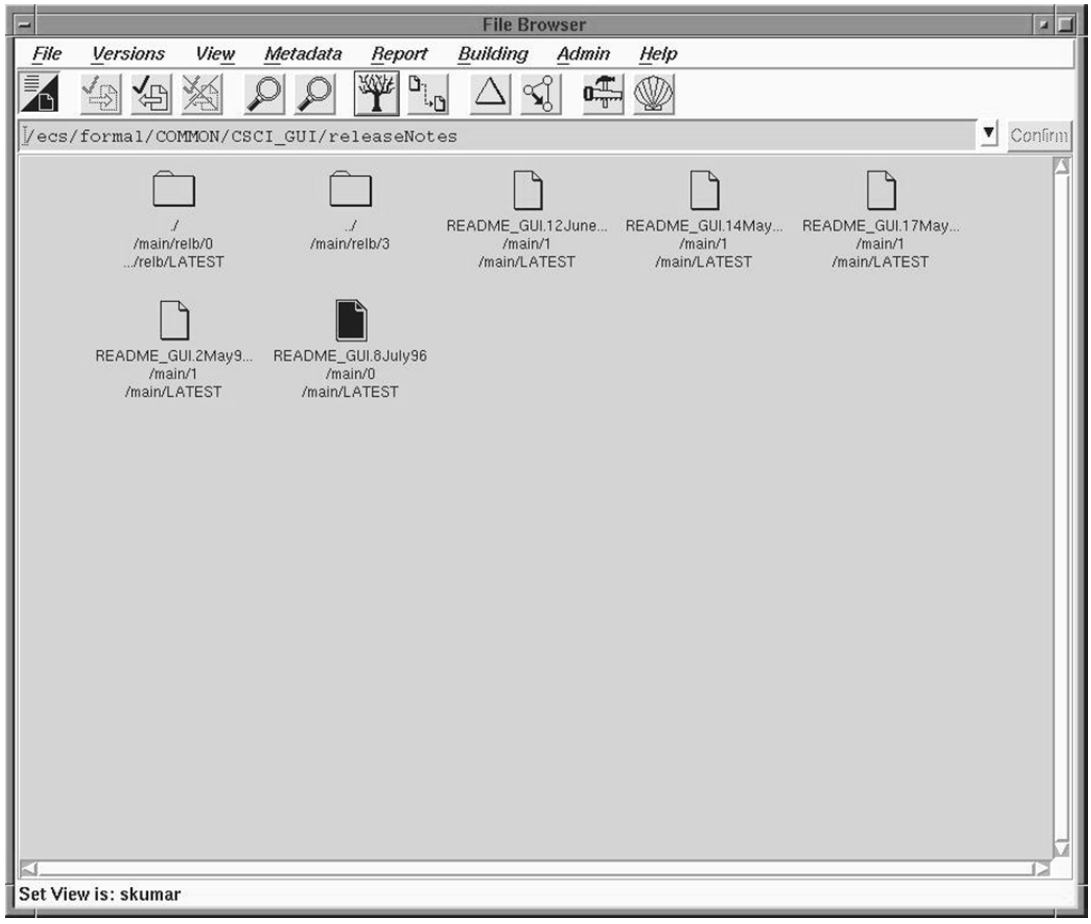


Figure 4.3.1-9. ClearCase File Browser Screen (File Checked-In)

4.3.1.1.1.4 4.3.1.1.1.4Perform Build

The Building menu on the File Browser as shown in Figure 4.3.1-10 is used to produce derived objects. The Building menu is the GUI version of the command line interface build utility called clearmake. Reference the *ClearCase Introduction* and the clearmake section of the *ClearCase Command Reference* documents for information on the use of this capability.

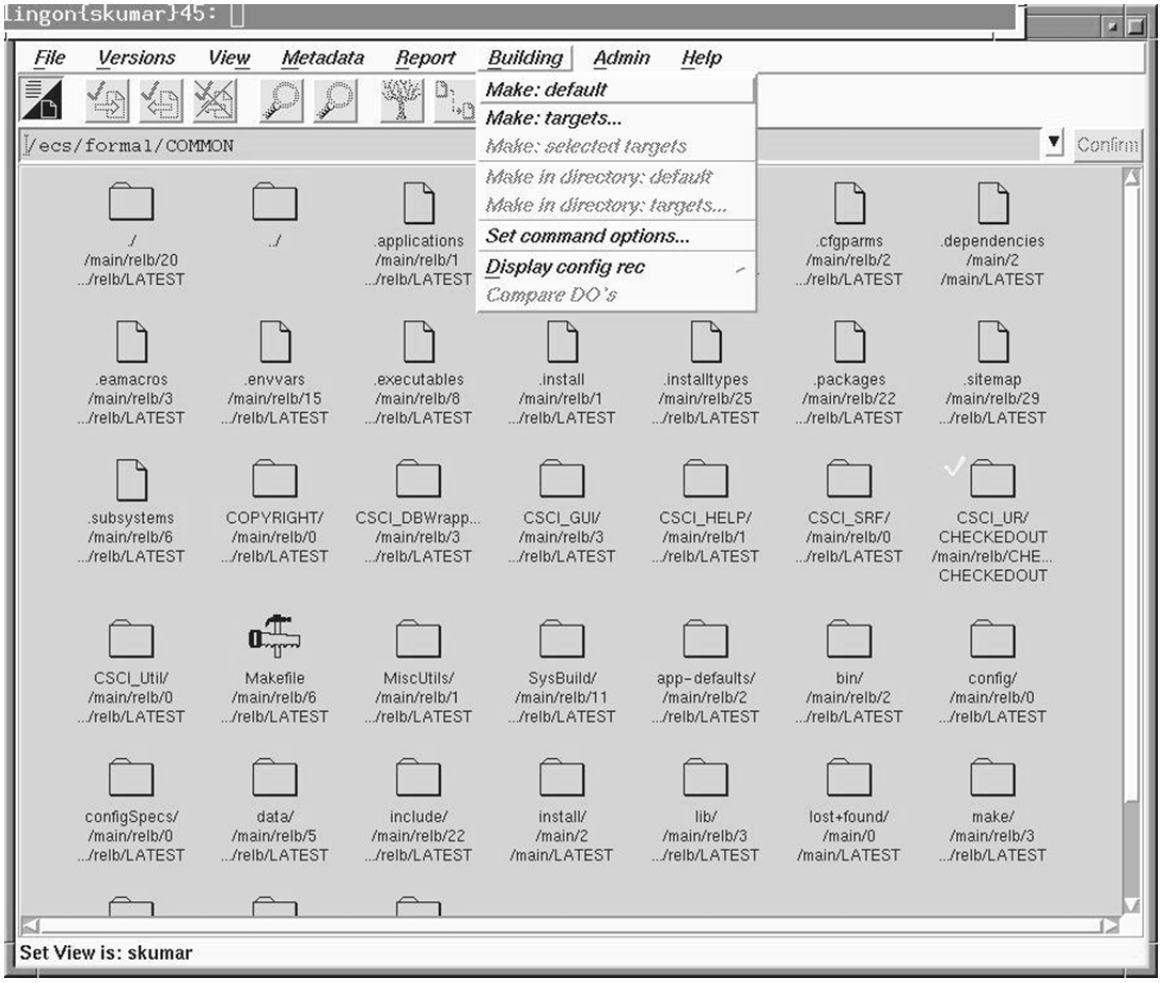


Figure 4.3.1-10. File Browser Screen (Build Menu)

4.3.1.1.2 4.3.1.1.2Required Operating Environment

For all COTS packages, appropriate information on operating system environments, tunable parameters, environment variables, and a list of vendor documentation can be found in the EED Release Notes for each product. Refer to the latest release notes for ClearCase posted on the ECS Baseline Information System web page at your local site. There is a link on the EBIS home page for all of the Release Notes.

4.3.1.1.3 4.3.1.1.3Databases

ClearCase data is stored in VOBs and views. Reference the *ClearCase Administrator's Guide* for a detailed description of the ClearCase databases.

4.3.1.1.4 4.3.1.1.4Special Constraints

None

4.3.1.1.5 4.3.4.4.5Outputs

Reference the *ClearCase Command Reference* document for a description of the ClearCase outputs.

4.3.1.1.6 4.3.1.1.6Event and Error Messages

ClearCase creates an event record for most of the processing activities that modify the VOB and stores it in the VOB database. These records are linked to the derived objects. These records provide a chronological event history for the objects. Reference the *ClearCase Reference Manual* for detailed information about logging of ClearCase events. The reference manual describes the contents of an event record, VOB objects that have event histories, and ClearCase operations that cause event records to be written.

ClearCase error messages indicate that a problem has occurred. Some errors are user correctable and others require correction by the operations staff. In both cases, ClearCase records error and status information in its log files. Reference the *ClearCase Reference Manual* for a description of the error logs, the ClearCase programs that use them, the error logs location, and their format.

4.3.1.1.7 4.3.1.1.7Reports

None

This page intentionally left blank.

4.3.2 Microsoft® Access® EMD Change Manager (ECM) Configuration Change Request (CCR) Tool

There are two CCR tools, one for use in the Riverdale facility and one for use at LP DAAC. The LP DAAC version is used for LP DAAC internal change control, while the Riverdale version is used for the entire ECS program. The LP DAAC version was derived from the Riverdale version and provides a subset of features for LP DAAC use. Unless otherwise stated, the following describes the Riverdale version of the tool. For the LP DAAC version, simply exclude Procurement Type CCRs and the Stakeholders function.

The Access® CCR tool is a custom application specifically designed to serve as an efficient configuration management tool to facilitate change control against the ECS baseline. It generates and maintains records in a Microsoft® Access® application that describe what changes are to be applied to the operational system baseline configurations for the DAACs (LP DAAC, ASDC, NSIDC, ECHO), VATC, PVC, and the EDF2 hosts at the ECS Development Facility (EDF) which are provided through the ECS Baseline Information System (EBIS). The CCR tool has created and approved 3082 CCRs and managed 8167 Engineering Change Orders (ECOs) electronically for ECS since January 1, 2005. Exported CCRs are conveyed by EBIS, and EBIS change tracking pages use embedded hyperlinks to reference them, signifying their importance to change control. Each DAAC has an EBIS file system that is a replication of the Riverdale EBIS file system.

Inputs to the tool are created CCRs which get electronically circulated for Sponsorship, Stakeholder review, and Change Configuration Board (CCB) approval. The LP DAAC version does not include the Stakeholder review step. The tool is integrated with IBM® Lotus® Notes®. A feature of the tool is the recording of electronic signatures. At the time of signing, the date and time of the User's PC is recorded and their name. This is important for the change record.

Outputs from the tool are 4 PDF files, corresponding to the CCR cover sheet, the additional sheet, the Stakeholders sheet, and the Engineering Change Orders (ECO) sheet. Also, an HTML formatted file contains the four sheets in a single file. Any ECOs within approved CCRs then are used to modify the baseline with the use of the ClearCase® BLM tool. Open ECO reports are also an output of the tool to ensure ECOs are managed. Riverdale uses the CCR for Procurements. All Procurement CCRs are suppressed from all of the EBIS file systems.

The following COTS software are prerequisites for the CCR Tool:

- Microsoft® Office® Access® 2003 (SP2 or higher)
- IBM® Lotus® Notes® 6.5 [Release 6.5.2 June 01, 2004] or higher
- Microsoft® Office® Word® 2003 (SP2 or higher)

4.3.2.1 4.3.2.1Introduction

An introduction of the tool functionality is in order before proceeding with the actual User Instructions.

Approved, non-Procurement CCRs are available on EBIS from the following at the URLs:

http://pete.edf.rvl.us.ray.com/baseline/	(for Riverdale use only, primary repository)
http://ebis.gsfc.nasa.gov:10160/baseline/	(ESDIS only)
http://e4iil01u.ecs.nasa.gov:10160/baseline/	(LP DAAC only, previously EDC DAAC)
http://l4iil01.larc.nasa.gov:10160/baseline/	(ASDC only, previously LaRC DAAC)
http://n4iil01u.ecs.nasa.gov:0160/baseline/	(NSIDC only)

Timely coordination of the CCR and getting concurrences/approvals from affected offices is the primary goal of the ECM CCR tool and thereby the tool makes extensive use of the project's integrated email capability. Figure 4.3.2-1 on the next page shows the process from ahigh level. The diagram shows the email flow as a result of electronic signatures being applied as the CCR progresses.

Electronic versions of all approved CCRs are viewable within the EBIS file system. Use the above links to launch EBIS, then use the links at the bottom of the home page to view each year's CCRs.

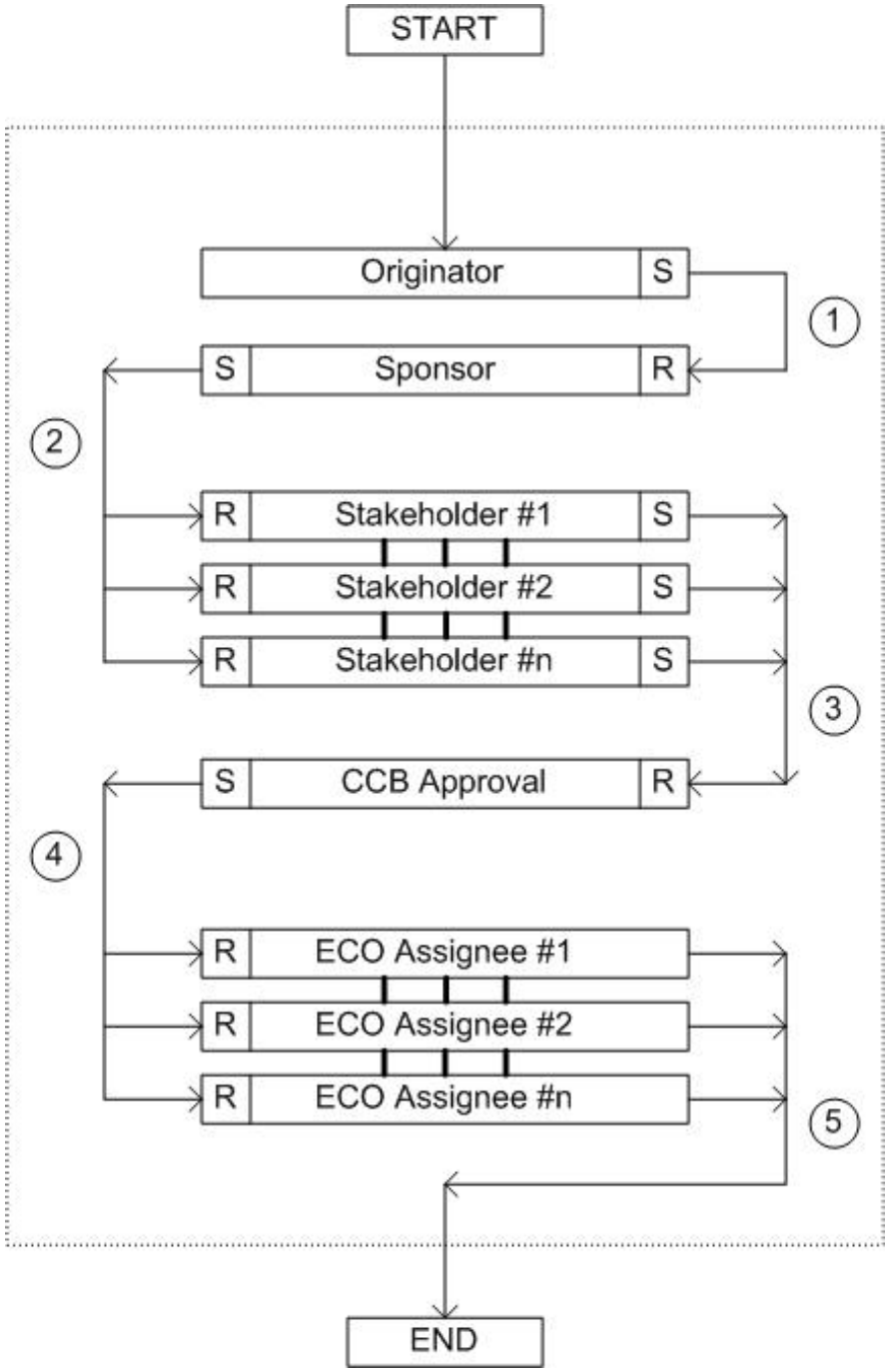


Figure 4.3.2-1. CCR Tool Flowchart

4.3.2.1.1 4.3.2.1.1Pre-Approval Stage

The pre-approval stage occurs with an Originator completing the CCR, including the first sheet, the Supplementary Procurement Information sheet (in Procurement CCR only), the additional

sheet, and the Stakeholder sheet, and the associated ECOs. Just after the Originator electronically signs, an email will be constructed and **S**ent to the perspective Sponsors, indicated by the "Originator" box and the **S** in the box to the right. The **R** just the left of the Sponsors box indicates that the Sponsors **R**eceives the email notice from the Originator, and needs to review the CCR, and needs to apply their electronic signature.

When a Sponsor signs a CCR, the CCR process takes one of two paths:

- For non-Procurement CCRs, the Stakeholders have to review the CCR after the Sponsor signs and the Stakeholders will be sent email concurrently. The Stakeholder email list is generated from the check boxes that were marked by the Originator during the formation of the CCR. The Authorized Signature list provides those folks who may sign for each check.
- For Procurement CCRs, the Procurement POCs have to review the CCR after the Sponsor signs and they are emailed concurrently. The Procurement POCs email list is generated from the information entered on the Supplementary Procurement Information page of the CCR. Once all Procurement POCs have concurred on the CCR, the Stakeholders have to review the CCR next and are emailed concurrently. Note, if a Procurement POC nonconcurs on the CCR, the CCR is sent back to the Originator for revision.

4.3.2.1.2 4.3.2.1.2Approval Stage

After a CCR is sponsored, all Stakeholders are concurrently emailed to notify them of a new CCR that needs to be reviewed. The CCR moves into this approval stage to allow all Stakeholders to review the CCR. Each Stakeholder must interact with the tool in order to agree or disagree. Stakeholders may provide comments should they choose. If at any time a significant change needs to be made to any information contained within the CCR, the CCR should be "modified." Once "modified," the CCR will need to be re-circulated for signatures. Only the Originator can "modify" the CCR.

The approval stage of the CCR consists of the CCB chairperson's signatures. The CCR is approved when the appropriate chairperson(s) signs. Once the CCR is approved, then all of the ECOs assignees are emailed. The Originator generated the ECOs earlier during the creation of the CCR.

4.3.2.1.3 4.3.2.1.3Post-Approval Stage

The post-approval stage of the CCR process consists of the ECOs being worked. The CCR is considered closed when all of the ECOs have been worked. In order to close an ECO, the ECO assignee needs to interact with the tool to get credit for closure. Once the CCR is closed within the tool, all records are frozen. CCR Closure is the **END** of the change control process depicted in Figure 4.3.2-1 above. If after the CCR is approved, and the intent of the CCR needs to be changed because of something learned after the CCR approval, then the CCR should be revised. A revision means to CLONE the original CCR, and provide text within the CCR that clearly indicates the changes. The revised CCR then needs to be re-circulated for signatures, just like the originally processed CCR.

4.3.2.2 4.3.2.2Tool Usage

Upon launch, the tool presents the copyright banner depicted in Figure 4.3.2-2 shown below. This only is shown for 6 seconds and then the Main Menu is shown.

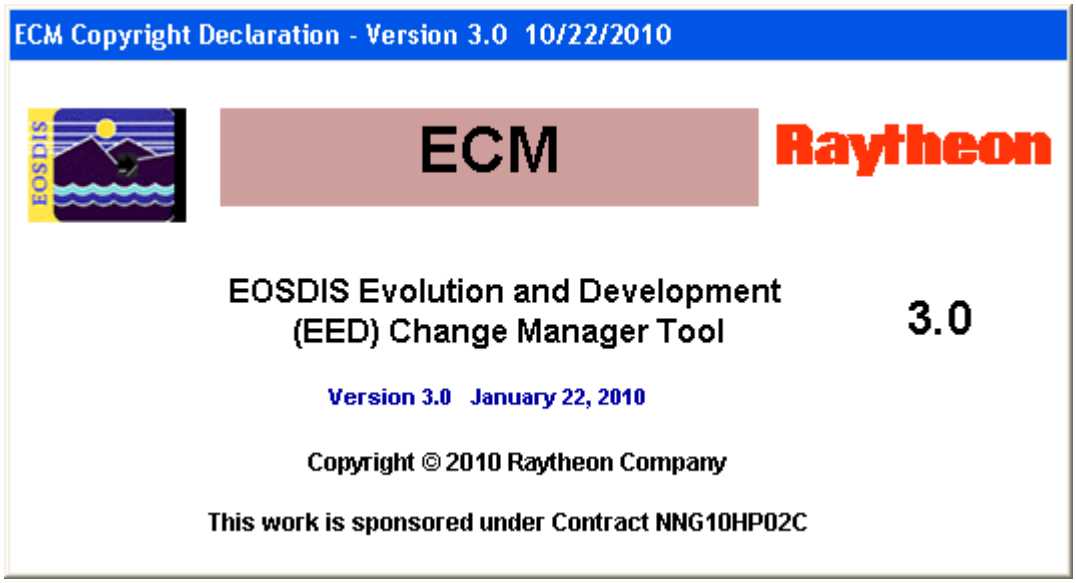


Figure 4.3.2-2. ECM Tool Copyright/Version Banner

The version and date are provided in the header of the Copyright Banner. The User's Guide will be kept current to the state of the tool's software. Currently the code version is "Version 2.0 and the User's Guide revision that goes with the code's 2.0 version is "Revision 2.0."

When the ECM banner page ends, the "EMD CCR Tool - Main Menu" will appear as shown in Figure 4.3.2-3. All functions of the CCR tool are available from this Main Menu.

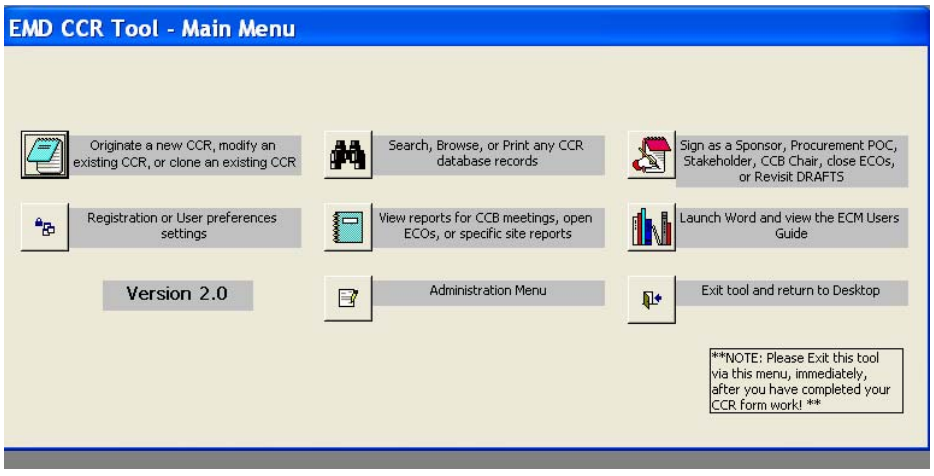


Figure 4.3.2-3. ECM Tool Main Menu

4.3.2.2.1 4.3.2.2.1Password Changes

To change your password, when you know you old password, follow the following steps:

1) From the CCR Tool – Main Menu, go to the Microsoft® Access main menu bar at the top of the window. Select the "User and Group Accounts" icon, which is the right most icon. The icon is a profile of a right facing woman. If you hold you mouse cursor over the icon for a few seconds, a small text box will be displayed indicating "User and Group Accounts".
2) Select the icon.
3) A User and Group Accounts window will appear. You will only be able to change your own password. There are three tabs that appear within the window, with the "Users" tab showing as the default. Refer to Figure 4.3.2-4 below.

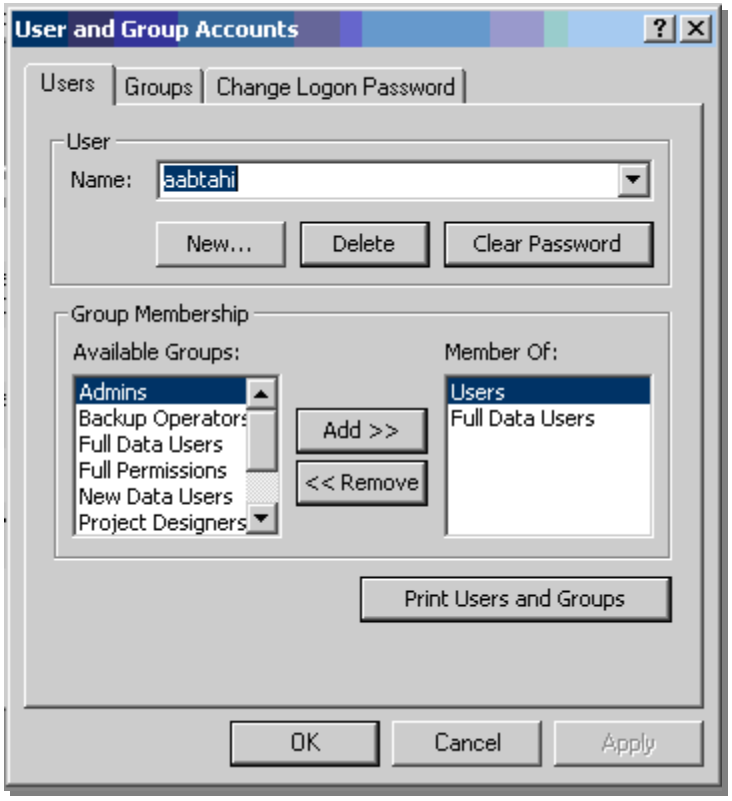


Figure 4.3.2-4. User and Group Accounts Window

4) Double click on the Name: that is shown, probably "aabtahi". Enter your name id, which is your first initial followed by up to 7 letters of your last name.
5) Next, select the "Change Logon Password" tab.
6) The "Change Logon Password" tab, when selected, will present a form by which you can modify your password.

7) Enter your current password into the "Old Password:" text box, then your new password in the "New Password:" text box and the "Verify:" text box. Refer to Figure 4.3.2-5.

Figure 4.3.2-5. Change Logon Password Tab

8) Then select the "OK" button at the bottom of the form for the change to take place.
9) An administrator can reset your password to "null", should you forget your password. Then you may reset your password from "null" to whatever you like. Note that you do not enter any text at all into the "Old Password:" text box when your password has been reset to "null". "Null" just means that the password does not have any characters.

4.3.2.2.2 4.3.2.2.2Accessing the User's Guide

The ECM CCR Tool Users Guide can be viewed and printed from the Main Menu (Figure4.3.2-3). When selected, the icon showing stacked books will launch Microsoft® Word and display the User's Guide.

4.3.2.2.3 4.3.2.2.3Logging off the CCR Tool

A user should exit the tool and Microsoft® Access by selecting the "**Exit tool and return to Desktop tool**" button on the Main Menu window. It is positioned at the bottom right section of the Main Menu. Note, one should always navigate back to the Main Menu and exit the CCR tool

using the **Exit tool and return to Desktop** button." Please do not exit any other way. Exiting the tool via the aforementioned button will properly close the ECM CCR Tool and Microsoft® Access and leave you at your Desktop. Also, always log in, perform your work, then log out of the tool when finished.

4.3.2.3 4.2.2.3CCR Creation, Draft, Modify, and Clone Functions

Configuration Change Requests (CCR) are used to gain approval for additions, modifications, and deletions of configuration control items in the ECS baseline and configuration control items in the EDF. This section will cover how to create and modify a CCR.

4.3.2.3.1 4.3.2.3.1CCR Creation

After logging into the CCR tool, the CCR tool's Main Menu is eventually displayed as shown in Figure 4.3.2-6 below. All CCR process activity is initiated from the Main Menu.

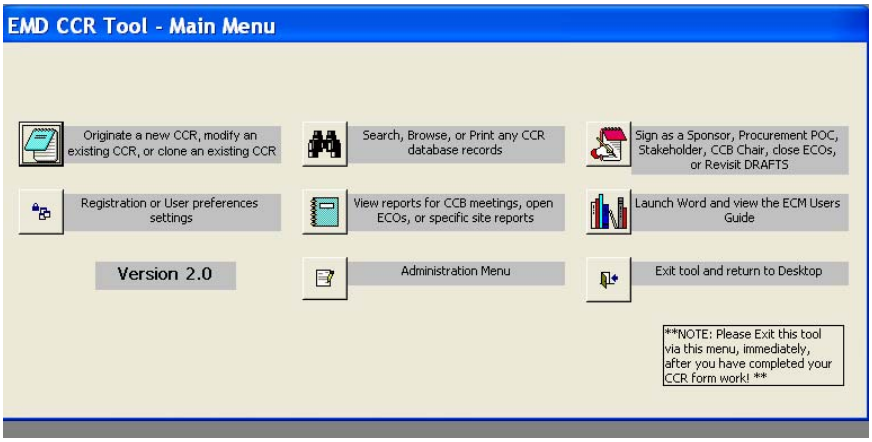


Figure 4.3.2-6. CCR Tool Main Menu

In order to create a CCR, either as a "Draft" or for submission, select the "**Originate a new CCR - - -**" button. It is the first button in the upper left section of the "**EMD CCR Tool – Main Menu**" window. Selecting this button will launch the CCR Creation Menu window shown below in Figure 4.3.2-7. There are four possible actions in this menu:

1) Create a new CCR – use this button to create a new CCR from scratch.
2) Modify an existing CCR – use this button when you need to modify a CCR that has not yet been approved. Note, when you modify a CCR, any electronic signatures present in a CCR at this point will be removed and the process starts over for this CCR. This ensures that any and all changes are reviewed by those that signed the CCR before the change was made.
3) Clone an existing CCR – use this button when you need to revise an approved CCR or when you want to create a CCR with a new CCR number using an existing approved CCR as a basis.

4) Return to main menu – use this button when you want to leave the CCR Creation/Edit Menu and return to the tool's Main Menu.

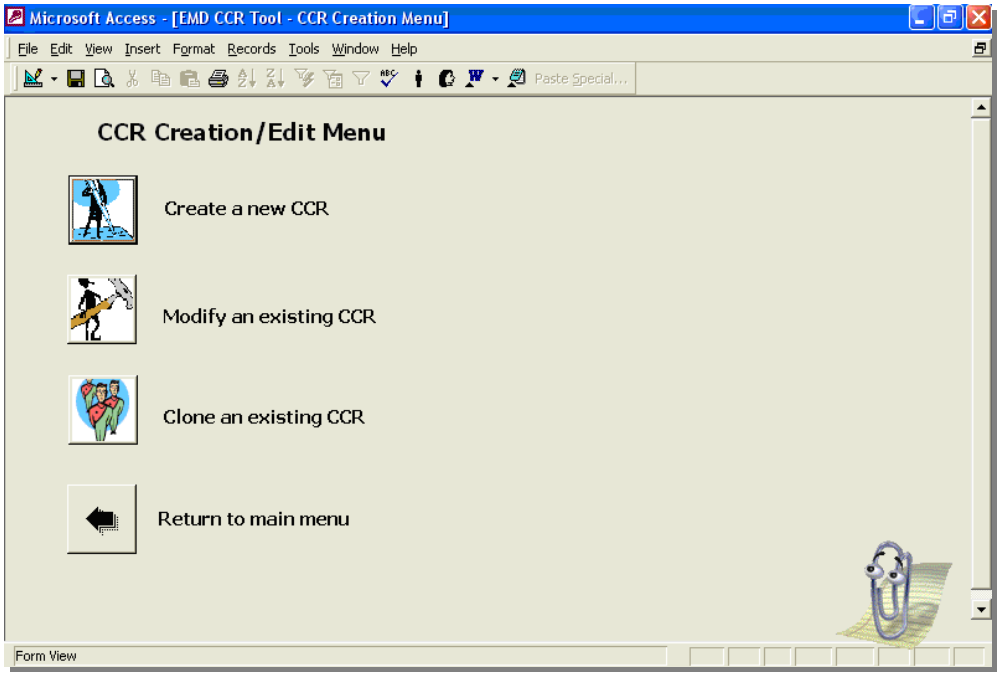


Figure 4.3.2-7. CCR Creation Menu

Clicking the **Create a new CCR** button will initiate the CCR creation process. The CCR tool will automatically display the forms that are required for the CCR based on the user's input. The first form to be displayed will be the Main CCR Form Sheet.

4.3.2.3.2 4.3.2.3.2Main CCR Form Sheet

The first form that is displayed is the CCR Form and it is shown in Figure 4.3.2-8 below. The first seven fields: "**1. Originator:**", "**2. Log Date:**", "**3. CCR #:**", "**4. Rev:**", "**5. Telephone:**", "**6. Rm #**", and "**7. Org:**" are automatically filled by the CCR tool. The remainder of the fields is to be completed by the CCR originator.

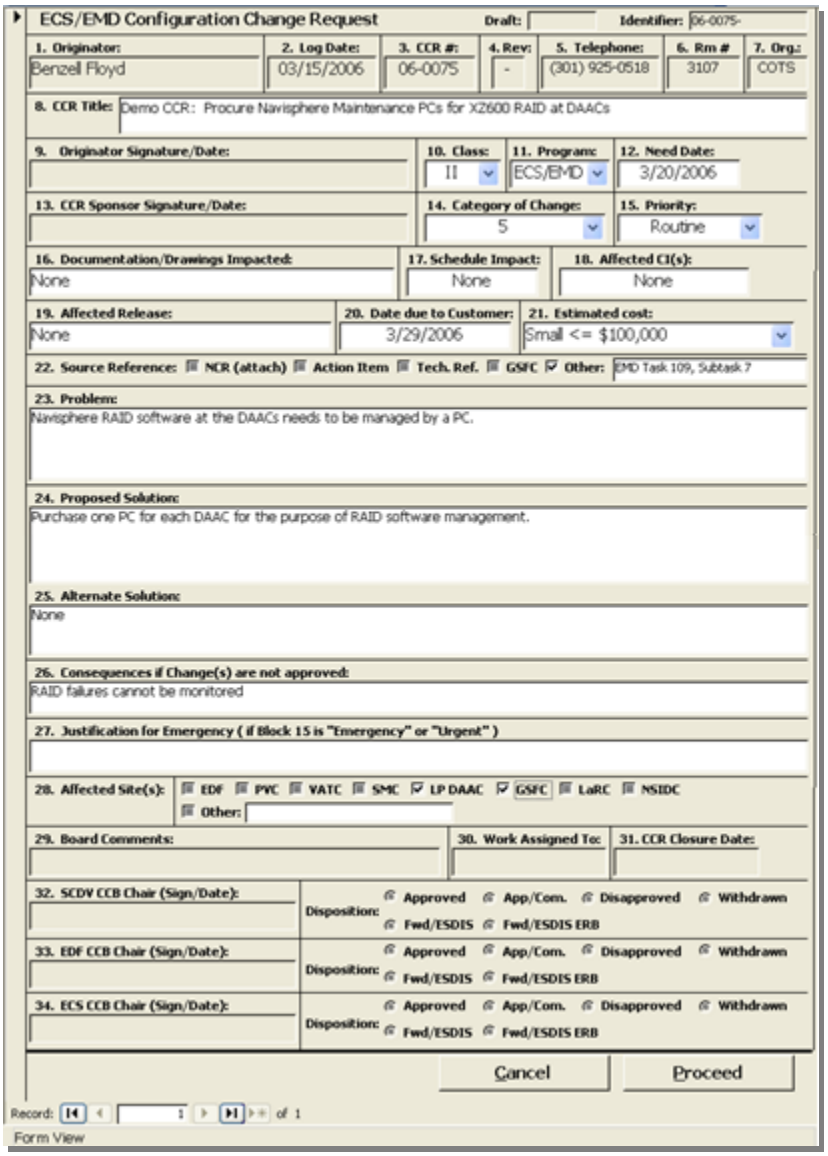


Figure 4.3.2-8. CCR Form

The forms used to create a CCR are determined by the "Category of Change" value that is selected in field # 14. In this example, the "Category of Change" value is "5" (for Procurement).

So a Procurement type CCR is being created. All of the white background fields need to be completed by the user. Cutting and pasting text files can be performed when entering data.

Fields 10, 11, 14, 15, and 21 have drop down menus, which constrain the entry that may be entered. Field 22, *Source Reference*, and field 28, *Affected Sites*, have check boxes. Check the appropriate boxes. Note, if "Other" is checked in field # 22 or field # 28, you must enter the name of the source/Affected Site name respectively in the box beside "Other".

When the fields are completed, select the "**Proceed**" button. Note, if any required fields have not been populated, then a message from the Office Assistant will appear, stating the field that needs some text. Simply go back onto the form and complete the missing field. If everything is in order, clicking the Proceed button will take you to the next form. The next form to be displayed is determined by the value in field #14, the "Category of Change field." If the value is a number other than "5," then the Additional Sheet form (Section 4.3.2.3.2.2) is displayed next. If the value is "5," then the Supplementary Procurement Information form (Section 4.3.2.3.2.1) is displayed, next.

4.3.2.3.2.1 4.3.2.3.2.1Supplementary Procurement Information

The Supplementary Procurement Information sheet is the next sheet to be displayed if the CCR is a procurement type CCR. The Supplementary Procurement Information sheet holds the specific procurement information and the name of the Bill of Material (BOM) file that is associated with the CCR. The Supplementary Procurement Information sheet is displayed below in Figure 4.3.2-9.

Some fields are automatically populated by the CCR tool, but the information in the white boxes on the form needs to be entered by the user. Fields' value criteria are as follow: Field # 5, "Not to Exceed" must be greater than zero. Field # 6, "On Dock Need Date" must have a date entered. Field number 8, Sub Task Lead, must have a name selected from the pull-down menu or the word, "NoOne," entered in the Sub Task Lead's box.

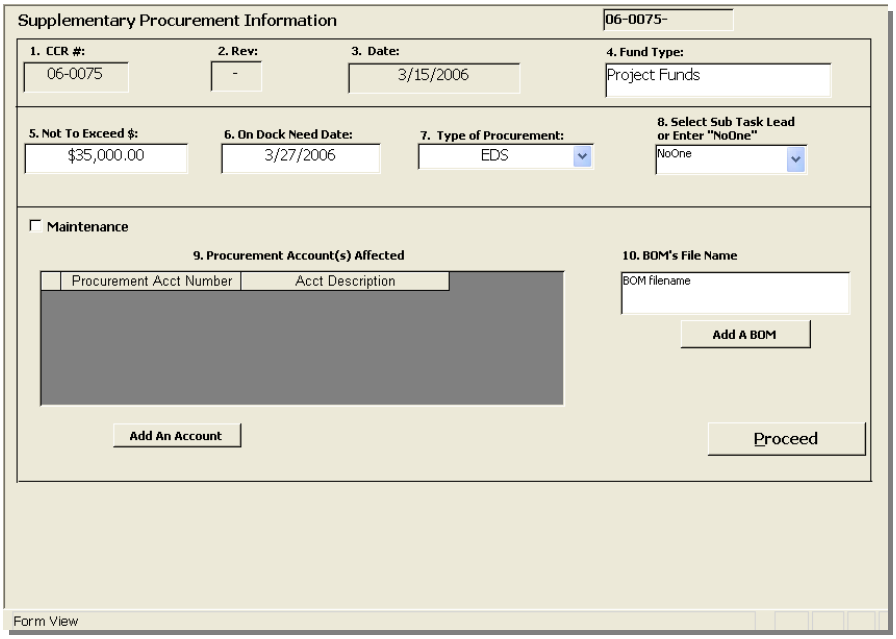


Figure 4.3.2-9. Supplementary Procurement Information form

Every Procurement type CCR must have at least one Procurement Account entered. To enter an account number, click the Add Account button and the Add Procurement Account window is displayed as shown in Figure 4.3.2-10 below.

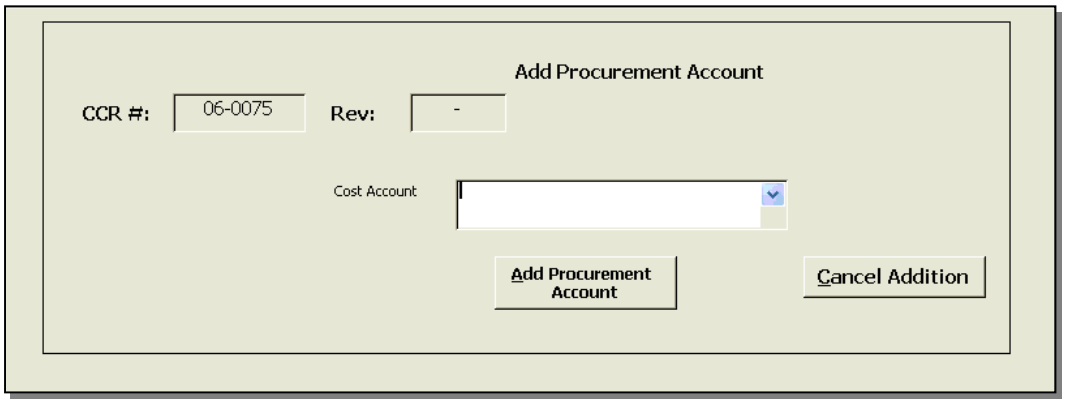


Figure 4.3.2-10. Add Procurement Account Window

On the Add Procurement Account window, click the pull-down on the Cost Account field and a list of valid Cost Accounts are displayed as shown in Figure 4.3.2-11.

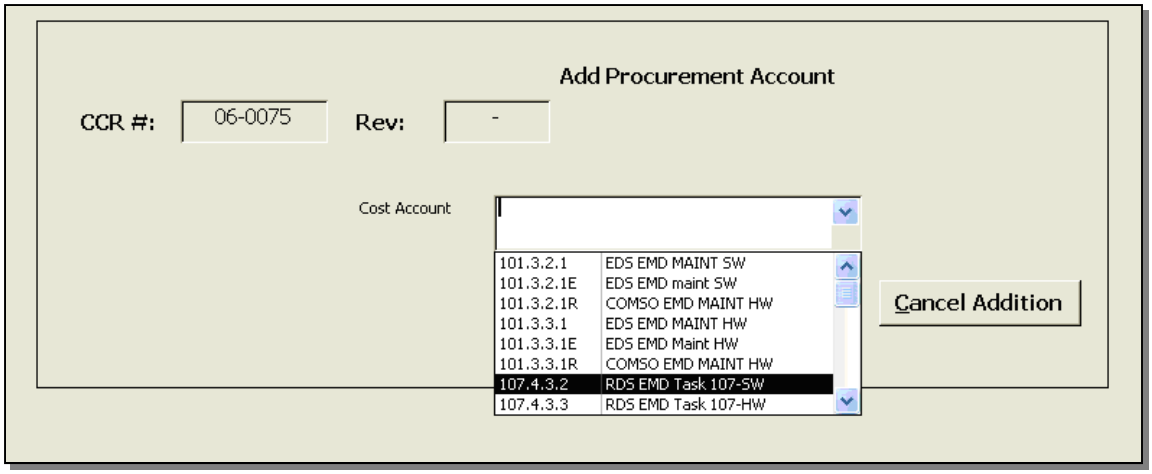


Figure 4.3.2-11. Cost Accounts List

Select the appropriate account from the pull-down menu and the account number will be displayed in the Cost Account field as shown in Figure 4.3.2-12.

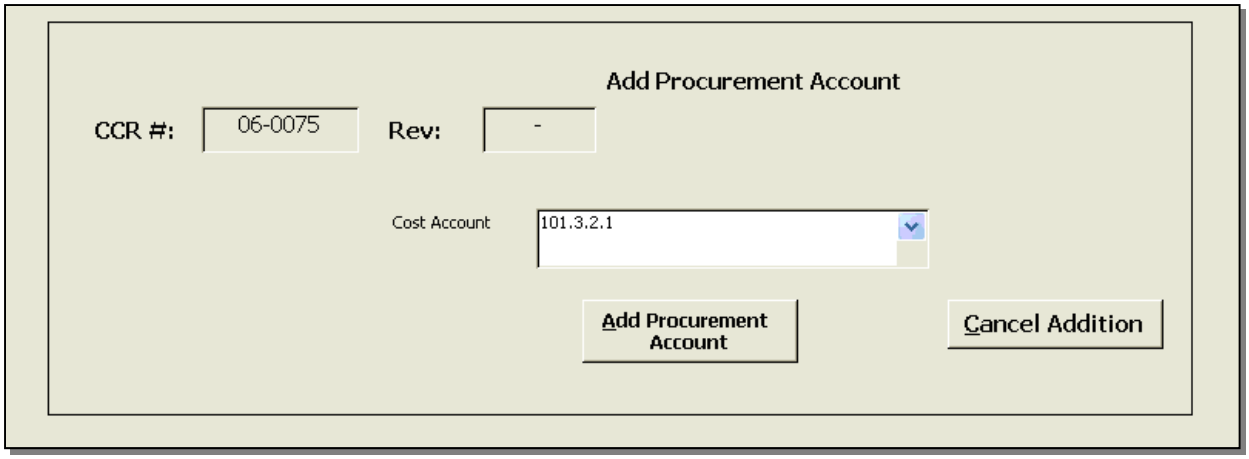


Figure 4.3.2-12. Cost Account Number Selected

Click the "Add Procurement Account button and the account is added to the Supplementary Procurement form as shown in Figure 4.3.2-13.

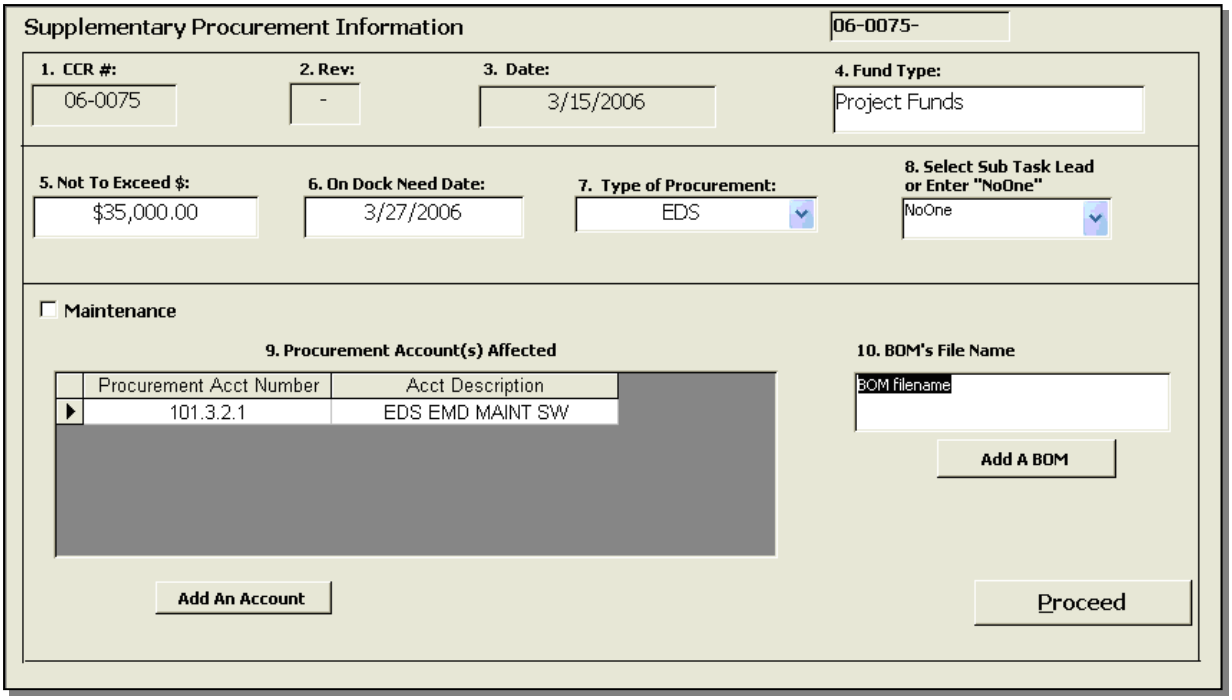


Figure 4.3.2-13. Account Number Added

Each Procurement type CCR has to have a Bill of Material (BOM) attached for review by the Sponsor, Procurement POCs, Stakeholders and CCB Chairpersons. Click the "Add A BOM" button and the Procurement BOM Snapshot window is displayed as shown in Figure 4.3.2-14.

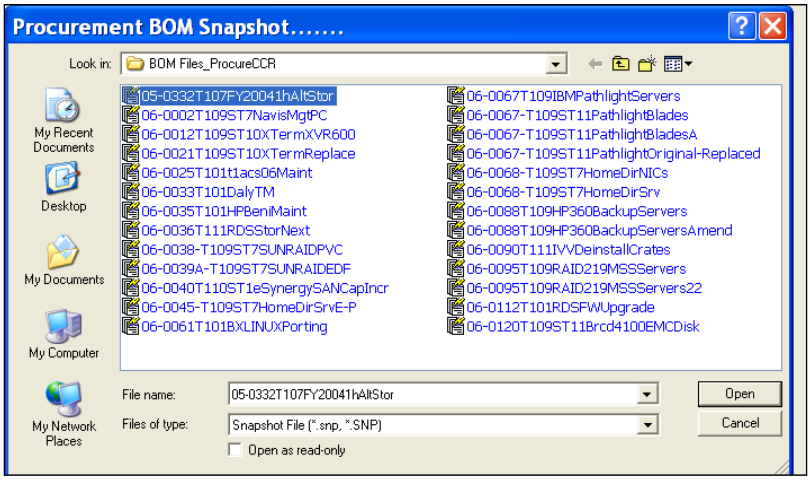


Figure 4.3.2-14. BOM Files

Select the BOM file that is associated with the CCR that you are working on and then click the Open button on the Procurement BOM Snapshot window. The BOM file information should now be displayed in the BOM's Filename box as shown in Figure 4.3.2-15.

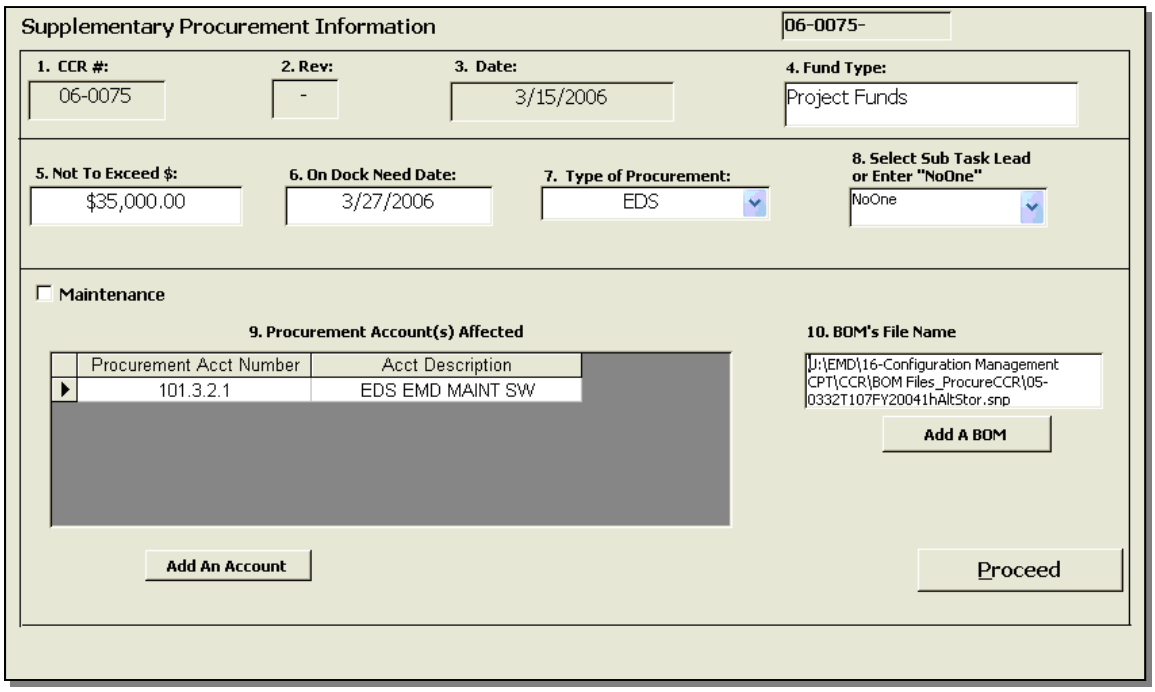


Figure 4.3.2-15. BOM File Added

Once the Supplementary Procurement Information sheet is completed, click the Proceed button. If any of the required fields are not completed, the CCR tool will provide an informative message and remain on the Supplementary Procurement Information form until you complete the entry or entries. If all required fields are completed, the CCR tool will take you to the Additional Sheet form.

4.3.2.3.2.2 4.3.2.3.2.2Additional Sheet

The Additional Sheet is used to hold information that would not fit on the CCR Form page, information that provides further explanation for the information on the CCR Form page, or brief installation instructions. The Additional Sheet form is displayed in Figure 4.3.2-16.

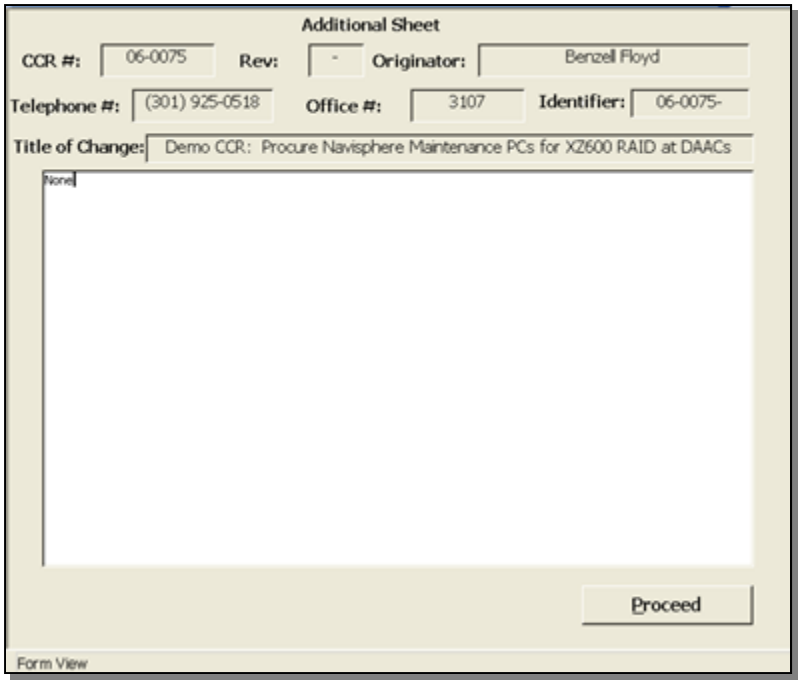


Figure 4.3.2-16. Additional Sheet Form

If there is no additional information to be entered, enter "None" in the white space.

Note: Place lengthy installation instructions in a separate file (attachment) and make reference to that file's name and location (usually L:\CCR_Attachment\<CCR Number>) in the white space on the Additional Sheet page.

Once you are satisfied with the entry, select the "**Proceed**" button to continue. Once the Proceed button is selected, the CCR tool moves to the Stakeholders Concurrences Sheet.

4.3.2.3.2.3 4.3.2.3.2.3Stakeholder's Concurrences Sheet

The Stakeholder's Concurrences Sheet is displayed after the Additional Sheet is removed. The Stakeholder's Concurrences Sheet is used to show the Offices that may be impacted by the solution being proposed on the CCR and to document the Offices' concurrences. The Stakeholder's Concurrences Sheet is shown in Figure 4.3.2-17. The CCR header information is automatically filled in by the CCR tool. Select the boxes for the offices that will be impacted by the CCR. You must select at least one office.

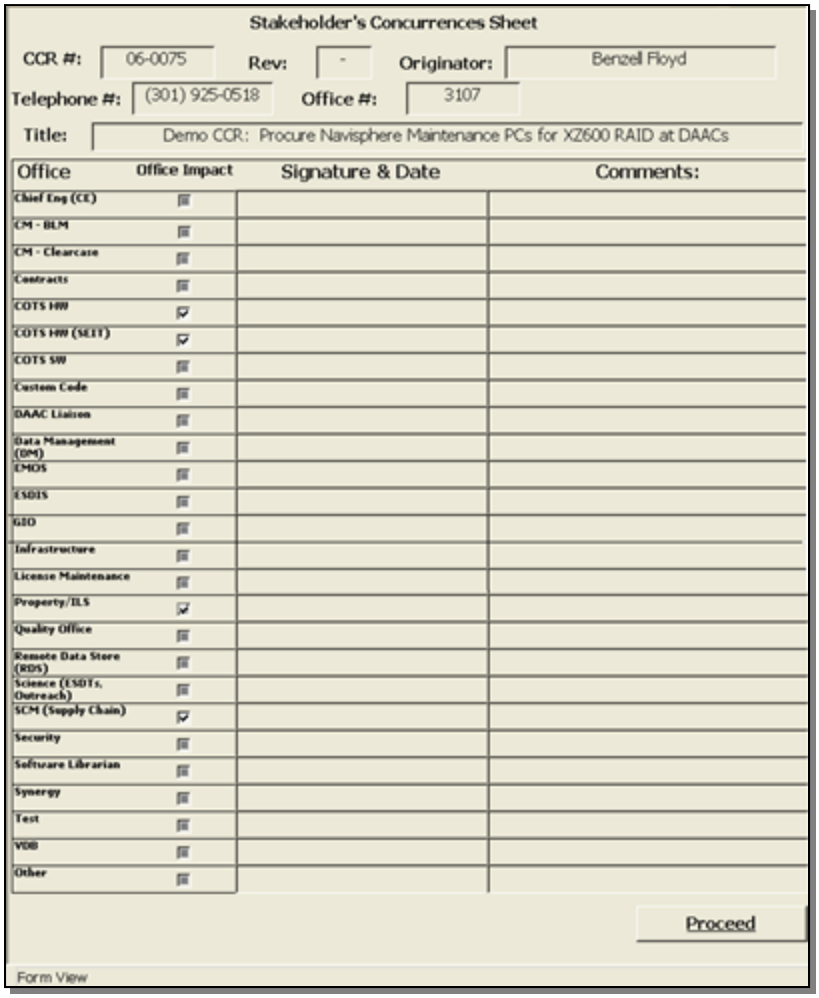


Figure 4.3.2-17. Stakeholders' Concurrences Sheet

After the applicable impact offices have been selected, select the **Proceed** button to move to the last page of the CCR Form, the Engineering Change Order (ECO) Sheet.

4.3.2.3.2.4 4.3.2.3.2.4Engineering Change Orders (ECOs) Sheet

The Engineering Change Order Sheet is used to describe the tasks that have to be completed for implementation of the CCR's solution. There must be at least one ECO on each CCR. Figure 4.3.2-18 shows the starting window for the ECO Sheet.

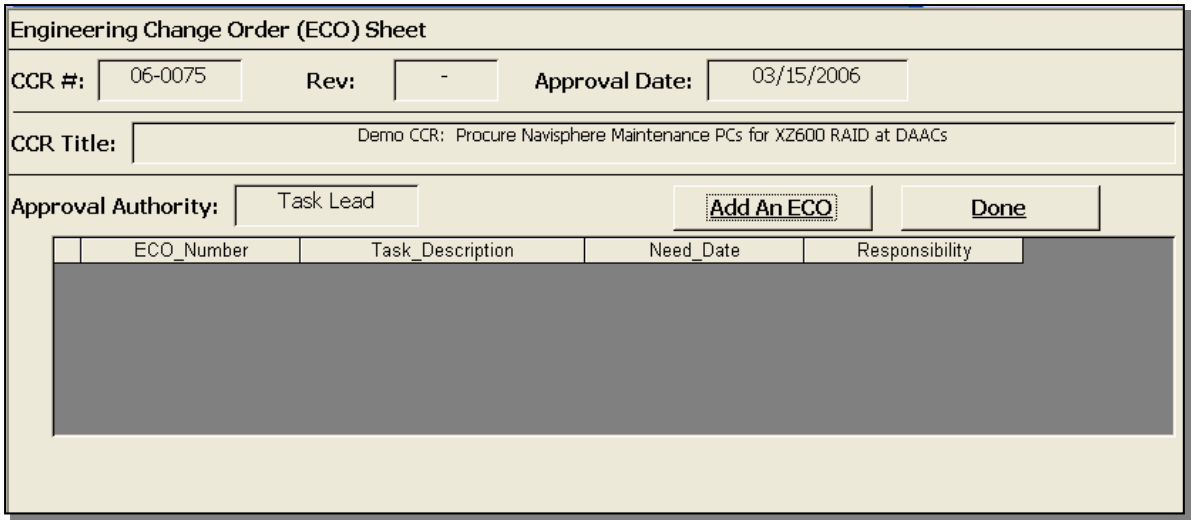


Figure 4.3.2-18. Starting Window for the ECO Sheet

To enter an ECO, click the **Add An ECO** button. The CCR tool will then display the "Add An ECO" as shown in Figure 4.3.2-19. The ECO number field will be filled in by the CCR tool. The CCR originator must filled in the remaining fields: **Task Description** {summarize the action to be completed; use action verbs, for example, install software, remove server, etc.; also include details like location of files, machine name, software to be replaced, etc.}. **Responsibility** {Select the individual or the organization that will be responsible for completing the task). **Need Date** {Enter the date that action is to be completed.} Example entries for these fields are shown in Figure 4.3.2-19.

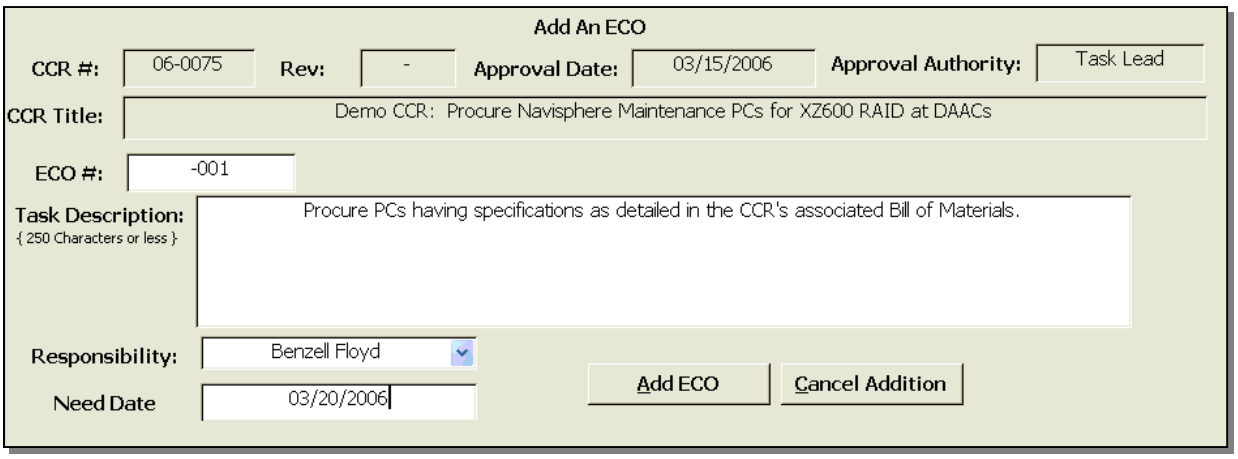


Figure 4.3.2-19. Completed ECO Entries

After all fields are completed, click the **Add ECO** button to store the ECO. After the ECO is stored, the CCR tool moves back to the initial ECO window. The added ECO is now displayed as shown in Figure 4.3.2-20. If there are other ECOS to be added, select the **Add An ECO** button again and repeat the aforementioned ECO process.

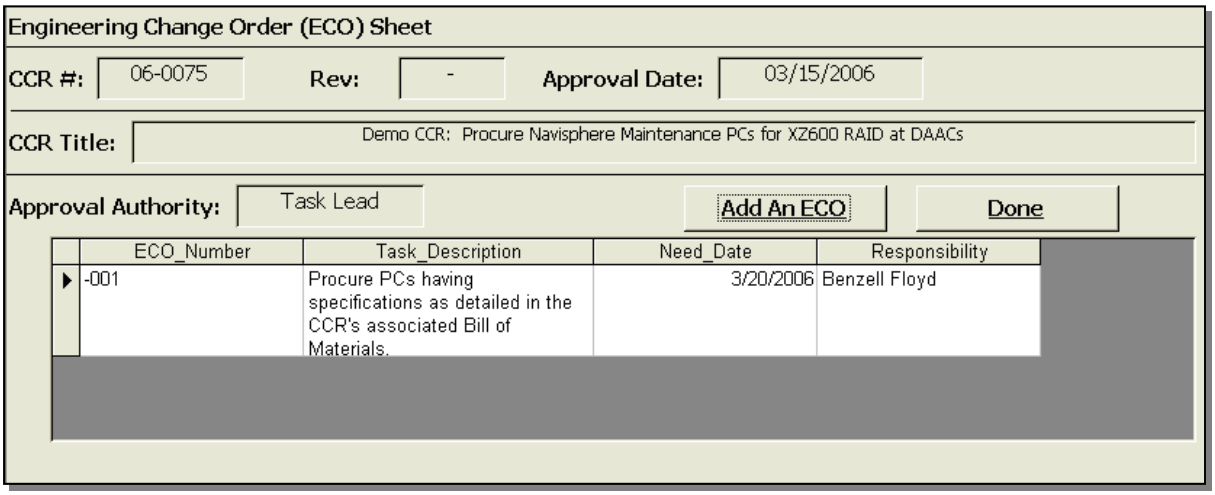


Figure 4.3.2-20. Added ECO Displayed

All of the added ECOs will be displayed will be displayed as shown Figure 4.3.2-21. Once all of the ECOs have been added, select the **Done** button to continue the CCR creation process.

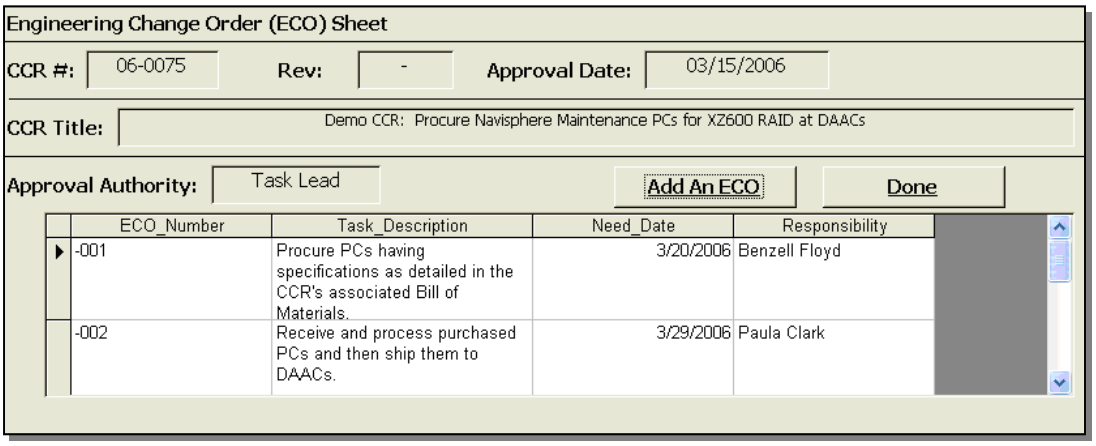


Figure 4.3.2-21. Complete List of ECOs

Once the tool determines it has all the information, the Office Assistant prompt as shown in the bottom right side of Figure 4.3.2-22 below will appear. The purpose of this prompt is to determine what you want to do next.

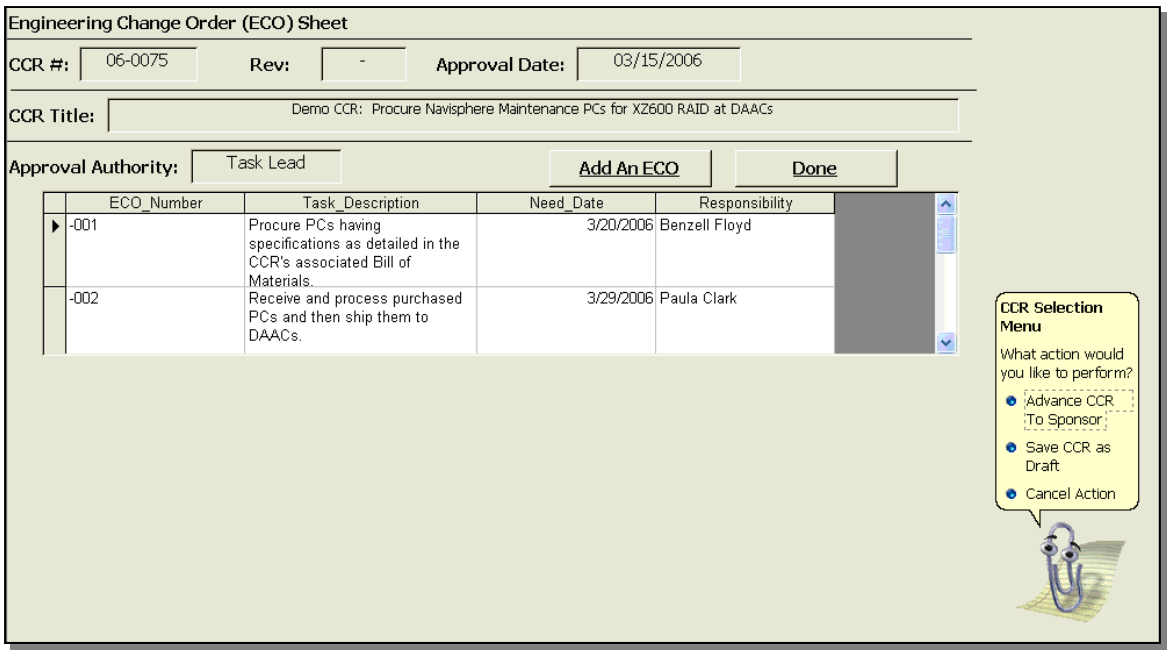


Figure 4.3.2-22. CCR Selection Menu

To proceed, select one of the listed actions:

1) Advance CCR to Sponsor – select this action if you are satisfied with the content of the CCR and you are ready to sign the CCR and send it to the sponsor for signature.
2) Save CCR as Draft – select this action if the CCR is incomplete and you're not ready to sign it.
3) Cancel Action – select this action if you are not ready to leave the ECO form.

Correct responses to actions 1) and 2) are provided in the following Sections 4.3.2.3.3 and 4.3.2.3.4.

4.3.2.3.3 4.3.2.3.3Advance CCR to Sponsor Action

Selecting Advance CCR to Sponsor will cause the Office Assistant prompt to be displayed as shown in Figure 4.3.2-23.

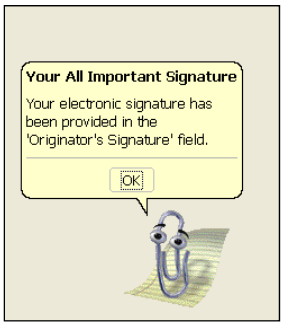


Figure 4.3.2-23. Confirmation of Originator Signature

Click the OK button and the next Office Assistant prompt is displayed as shown in Figure4.3.2-24.

Figure 4.3.2-24. Confirmation of Emailing CCR to Sponsor

Click the OK button on the Next Step prompt and the CCR tool takes you back to the CCR Creation Menu as shown in Figure 4.3.2-25. At this point, the CCR has been created and is stored in the CCR tool database. It can be reviewed by all CCR tool users if it is a non-procurement CCR. It can only be reviewed by procurement authorized personnel if it is a procurement CCR.

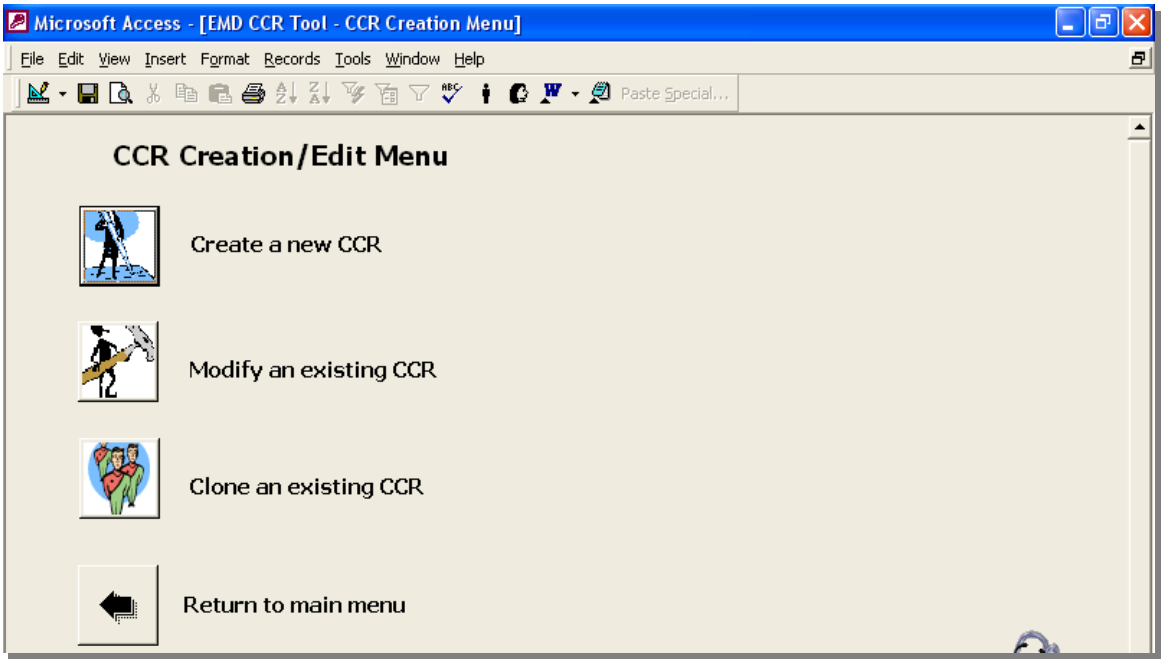


Figure 4.3.2-25. CCR Creation/Edit Menu

From CCR Creation/Edit Menu, click the "Return to main menu" button to get back to the Main Menu.

4.3.2.3.3.1 Save CCR as Draft Action

Selecting the "Save CCR as Draft" action will cause the Office Assistant prompt in Figure 4.3.2-26 to be displayed.

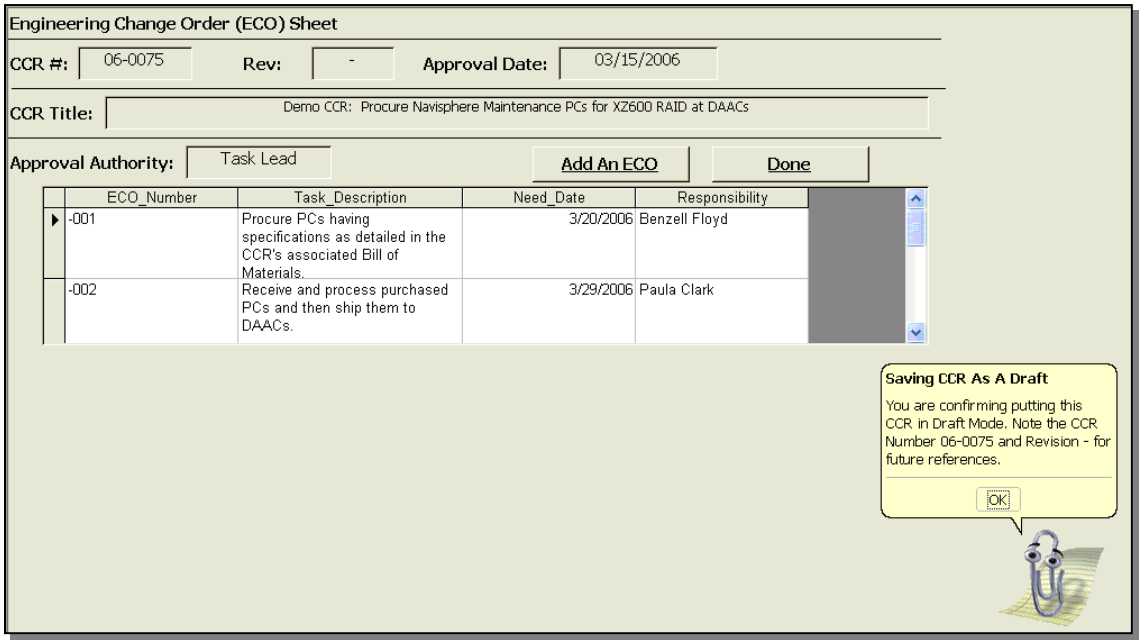


Figure 4.3.2-26. Saving CCR As A Draft

Click the OK button on the Office Assistant "Saving CCR As A Draft" prompt and the CCR tool will take you back to the CCR Creation/Edit Menu shown in Figure 4.3.2-27. At this point, the CCR has been stored as a draft CCR and only the CCR's originator can review it. Click the "Return to main menu" button to get back to the Main Menu.

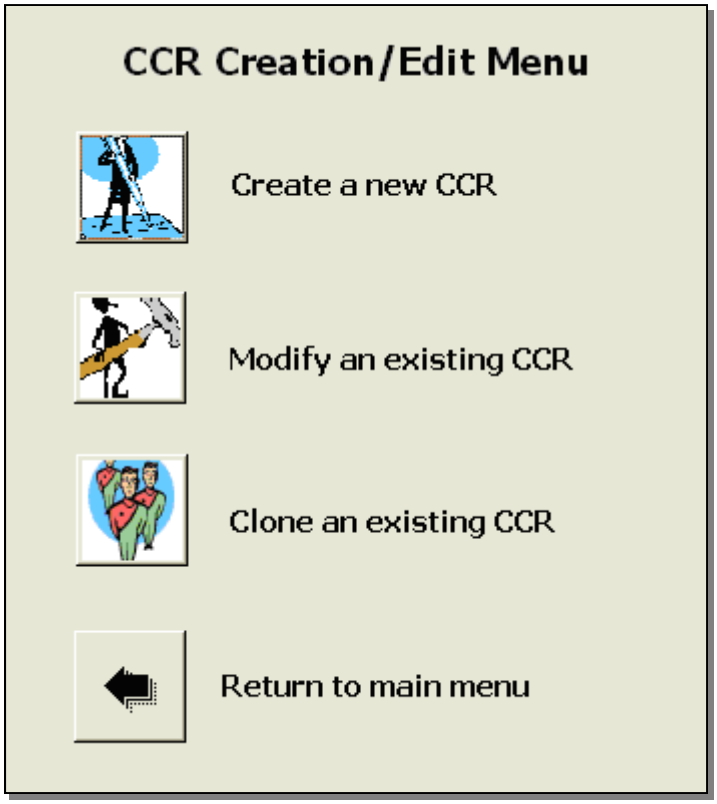


Figure 4.3.2-27. CCR Creation/Edit Menu

4.3.2.4 4.3.2.4CCR Attachments

Some CCRs need to have an attachment, a file that can be viewed by Sponsors, Procurement POCs and Stakeholders. The attachment file should be stored on the "V" drive in the folder: V:\Core\EED\16-Configuration Management (CM) CPT\CCR\CCR_Attachments<CCR #>. For example, an attachment file for CCR # 06-0075 would be placed in "V:\Core\EED\16-Configuration Management (CM) CPT\CCR\CCR_Attachments\06-0075." Be sure to make reference to the attachment in the note section of the Additional Sheet. For example, on the Additional Sheet, enter "The documentation for CCR # 06-0075 has been placed in the following location: V:\Core\EED\16-Configuration Management (CM) CPT\CCR\CCR_Attachments\06-0075."

4.3.2.5 4.3.2.5CCR Draft

At the end of the CCR creation process, the CCR originator has the option of signing a CCR and sending it to the Sponsor for signature or the CCR can be saved as a draft. If the CCR is saved as a draft CCR then only the CCR originator can review and make changes to it. The CCR has to be taken out of "draft" mode, so to speak, by its originator, finalized, and then signed by the originator before anyone else can see it. This section tells how to complete a draft CCR.

4.3.2.5.1 4.3.2.5.1Retrieve the Draft CCR

Login into the CCR tool and eventually the Main Menu is displayed as shown in Figure 4.3.2-28.

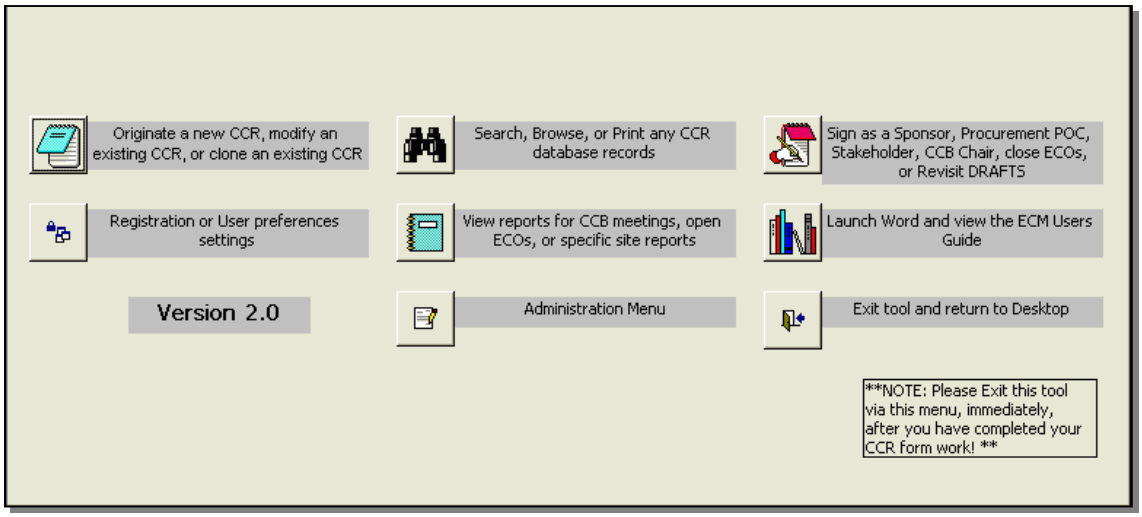


Figure 4.3.2-28. CCR Tool's Main Menu

Click the button in the upper right corner with "Revisit DRAFTS" in its label. The CCR tool will display the My Work Menu as shown in Figure 4.3.2-29. Click the "Draft Mode" CCRs button to get to a list of your draft CCRs.

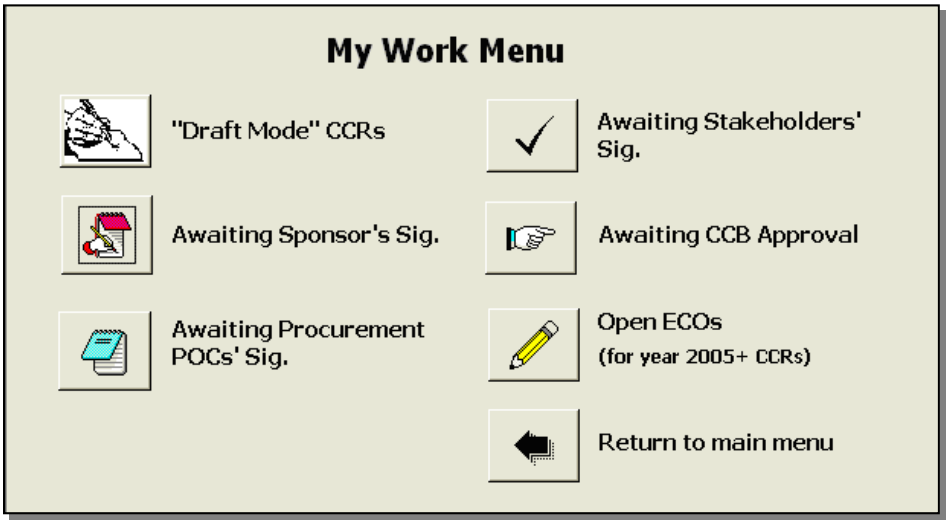
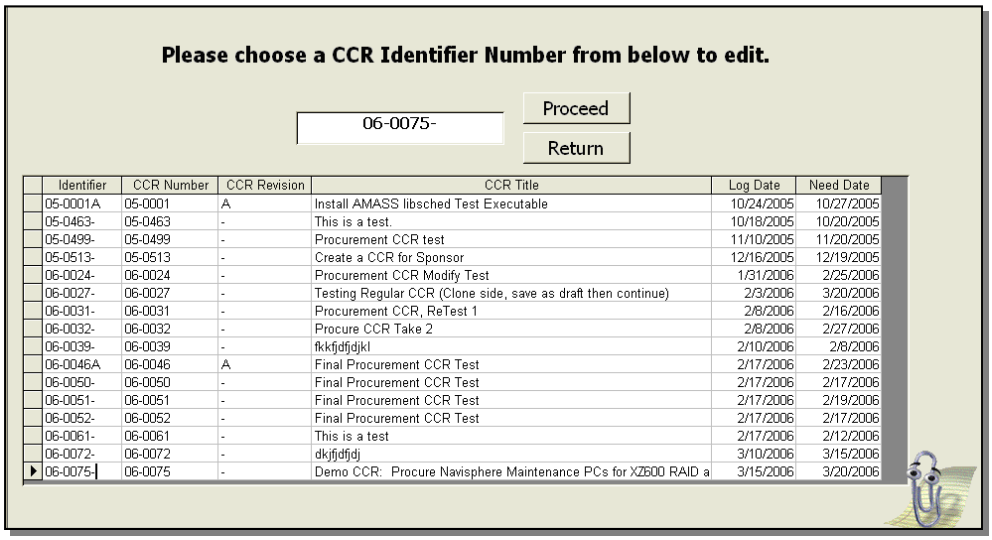


Figure 4.3.2-29. My Work Menu

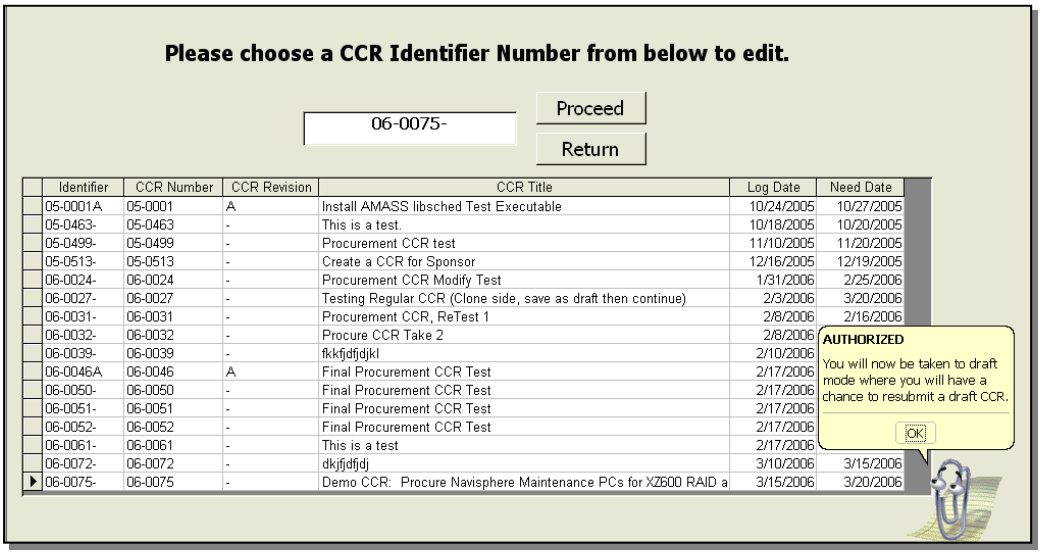
When the "Draft Mode" CCRs button is clicked, the CCR tool will display the "MyWork Menu – Drafts" form as shown in Figure 4.3.2-30. Click the desire CCR numberin the Identifier column and the CCR tool will copy that CCR number to the white space above the list of CCR numbers. At this point, if you click the "Return" button, you will be taken back to the My Work Menu.



Identifier	CCR Number	CCR Revision	CCR Title	Log Date	Need Date
05-0001A	05-0001	A	Install AMASS libsched Test Executable	10/24/2005	10/27/2005
05-0463-	05-0463	-	This is a test.	10/18/2005	10/20/2005
05-0499-	05-0499	-	Procurement CCR test	11/10/2005	11/20/2005
05-0513-	05-0513	-	Create a CCR for Sponsor	12/16/2005	12/19/2005
06-0024-	06-0024	-	Procurement CCR Modify Test	1/31/2006	2/25/2006
06-0027-	06-0027	-	Testing Regular CCR (Clone side, save as draft then continue)	2/3/2006	3/20/2006
06-0031-	06-0031	-	Procurement CCR, ReTest 1	2/8/2006	2/16/2006
06-0032-	06-0032	-	Procure CCR Take 2	2/8/2006	2/27/2006
06-0039-	06-0039	-	fkkfjdfjdjkl	2/10/2006	2/8/2006
06-0046A	06-0046	A	Final Procurement CCR Test	2/17/2006	2/23/2006
06-0050-	06-0050	-	Final Procurement CCR Test	2/17/2006	2/17/2006
06-0051-	06-0051	-	Final Procurement CCR Test	2/17/2006	2/19/2006
06-0052-	06-0052	-	Final Procurement CCR Test	2/17/2006	2/17/2006
06-0061-	06-0061	-	This is a test	2/17/2006	2/12/2006
06-0072-	06-0072	-	dkjfjdfjdj	3/10/2006	3/15/2006
06-0075-	06-0075	-	Demo CCR: Procure Navisphere Maintenance PCs for XZ600 RAID a	3/15/2006	3/20/2006

Figure 4.3.2-30. My Work Menu – Drafts form

If you click proceed, the CCR tool will display the prompt shown in Figure 4.3.2-31. Click OK to proceed.



Identifier	CCR Number	CCR Revision	CCR Title	Log Date	Need Date
05-0001A	05-0001	A	Install AMASS libsched Test Executable	10/24/2005	10/27/2005
05-0463-	05-0463	-	This is a test.	10/18/2005	10/20/2005
05-0499-	05-0499	-	Procurement CCR test	11/10/2005	11/20/2005
05-0513-	05-0513	-	Create a CCR for Sponsor	12/16/2005	12/19/2005
06-0024-	06-0024	-	Procurement CCR Modify Test	1/31/2006	2/25/2006
06-0027-	06-0027	-	Testing Regular CCR (Clone side, save as draft then continue)	2/3/2006	3/20/2006
06-0031-	06-0031	-	Procurement CCR, ReTest 1	2/8/2006	2/16/2006
06-0032-	06-0032	-	Procure CCR Take 2	2/8/2006	
06-0039-	06-0039	-	fkkfjdfjdjkl	2/10/2006	
06-0046A	06-0046	A	Final Procurement CCR Test	2/17/2006	
06-0050-	06-0050	-	Final Procurement CCR Test	2/17/2006	
06-0051-	06-0051	-	Final Procurement CCR Test	2/17/2006	
06-0052-	06-0052	-	Final Procurement CCR Test	2/17/2006	
06-0061-	06-0061	-	This is a test	2/17/2006	
06-0072-	06-0072	-	dkjfjdfjdj	3/10/2006	3/15/2006
06-0075-	06-0075	-	Demo CCR: Procure Navisphere Maintenance PCs for XZ600 RAID a	3/15/2006	3/20/2006

Figure 4.3.2-31. Authorized to Retrieve Draft Prompt

The CCR tool will now display the selected draft CCR.

4.3.2.5.2 4.3.2.5.2Finalize Draft CCR

When a draft CCR is retrieved, the focus is initially on the CCR Form page as shown in Figure 4.3.2-32. Each of the CCR Form's pages (Supplementary Procurement Information, Additional Sheet, Stakeholder's Concurrence, and ECO Sheet) is available for updates. Note, the Supplementary Procurement Information page is only on procurement type CCRs. Non-procurement CCRs will not have a Supplementary Procurement Information page.

There are some minimum changes that one has to make to a draft CCR. Dates that were entered in section "12. Need Date" and section "20. Date Due to Customer" fields during CCR creation were removed when the CCR was saved as a draft. So, even if there are no other changes on the CCR Form page, dates for these fields have to be entered again.

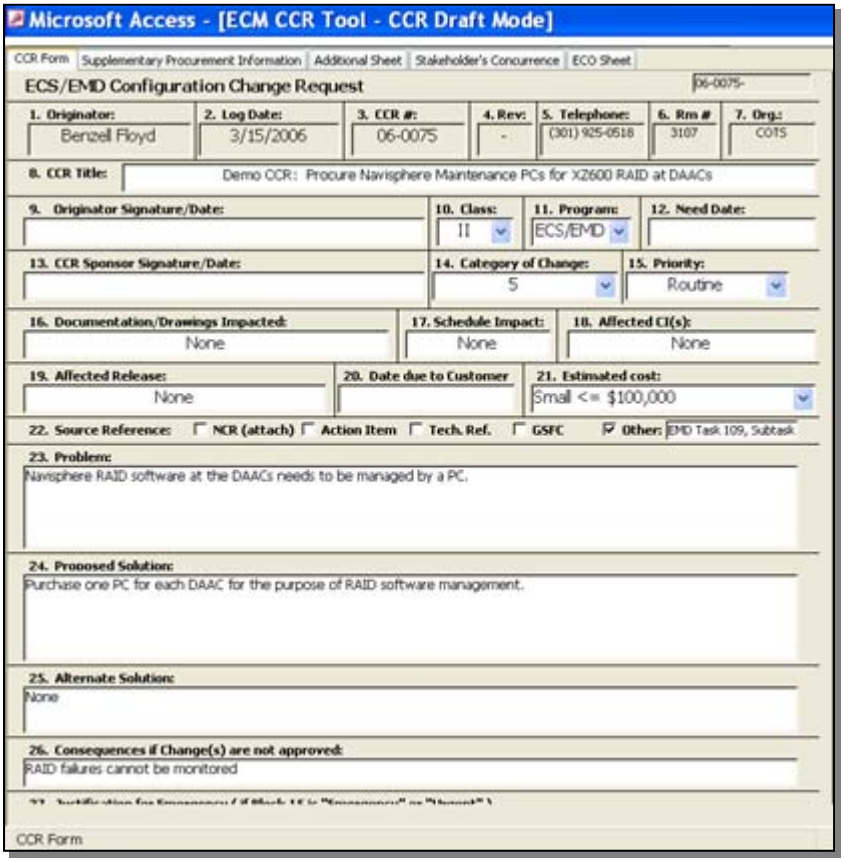


Figure 4.3.2-32. Draft CCR Form

For a procurement type CCR, the Supplementary Procurement Information page shown in Figure4.3.2-33 must be updated as well. The date in section "6. On Dock Need Date" (that was

entered during CCR creation) was removed when the CCR was placed in draft mode. So, a date has to be reentered into that field.

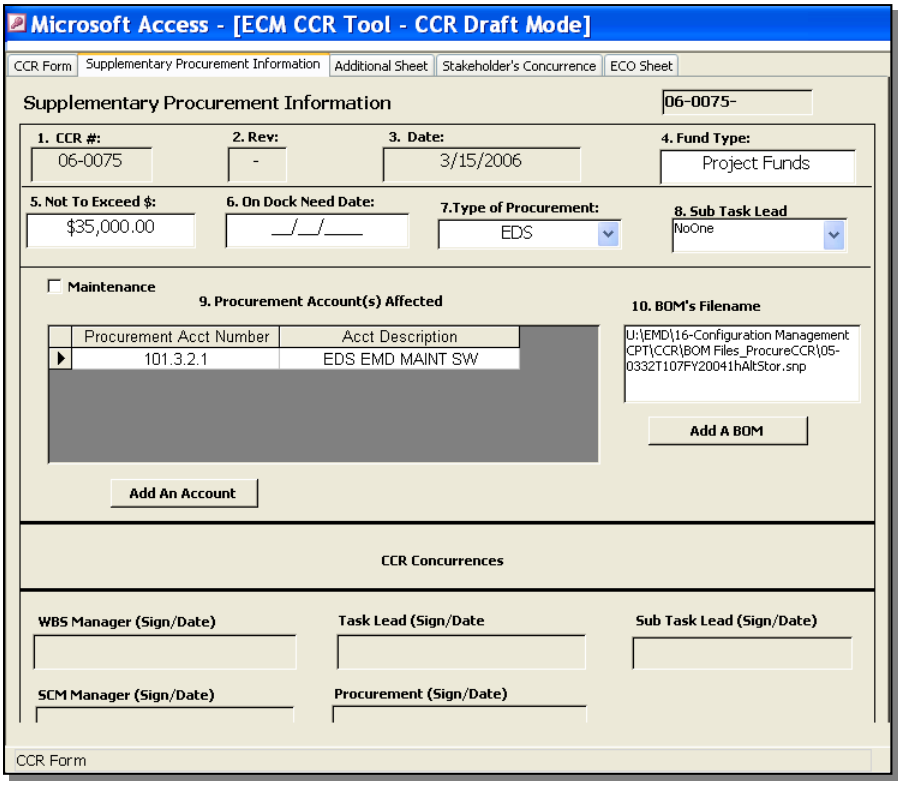


Figure 4.3.2-33. Supplementary Procurement Information Page

When all updates have been made to the draft CCR and you are ready to sign the CCR, go to the ECO Sheet page of the CCR form and click the "Done" button. Upon clicking of the "Done" button, the CCR tool displays the prompt shown in Figure 4.3.2-34.

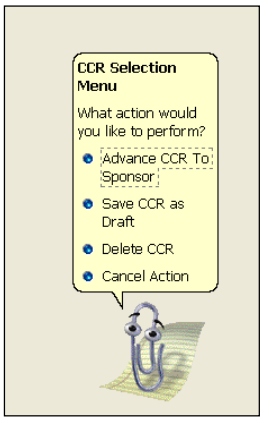


Figure 4.3.2-34. CCR Action Prompt

You have a choice of several actions:

1) Advance CCR to Sponsor – select this action if you are satisfied with the content of the CCR and you are ready to sign the CCR and send it to the sponsor for signature.
2)) Save CCR as Draft – select this action if the CCR is incomplete and you're not ready to sign it.
3) Delete CCR – select this action if you want to delete the draft CCR. A message will be displayed asking if you are sure you want to delete the draft CCR. Select "Yes" to have the draft CCR deleted.
4) Cancel Action – select this action if you are not ready to leave the draft CCR form.

Select the "Advance CCR to Sponsor" action and the prompt shown in Figure 4.3.2-35 is displayed.

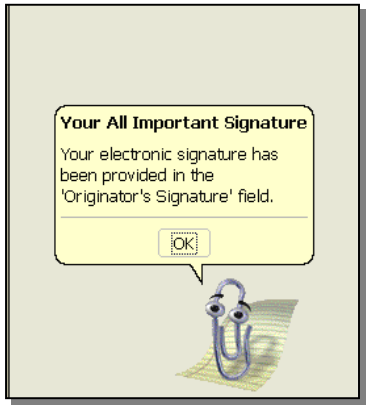


Figure 4.3.2-35. Confirmation of Signature Prompt

Click OK on the "Signature" prompt and the prompt shown in Figure 4.3.2-36 is displayed.

Figure 4.3.2-36. Next Step Prompt

Click OK on the "Next Step" prompt and the CCR tool will take you back to the My Work Menu – Drafts form, Figure 4.3.2-37 below.

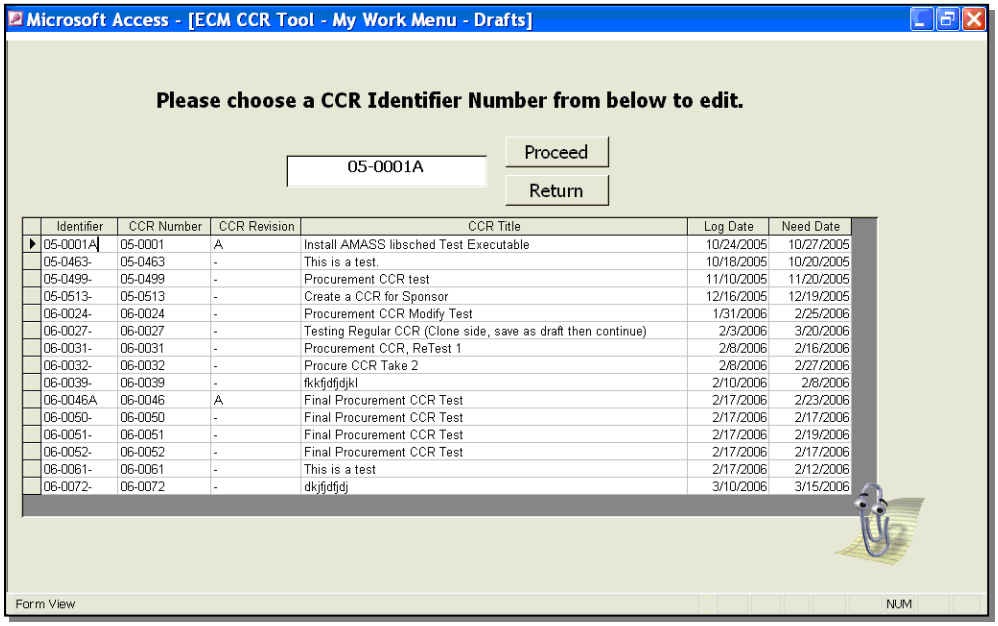


Figure 4.3.2-37. My Work Menu – Drafts Window

Click the Return button to get back to the "My Work Menu" (Figure 4.3.2-38).

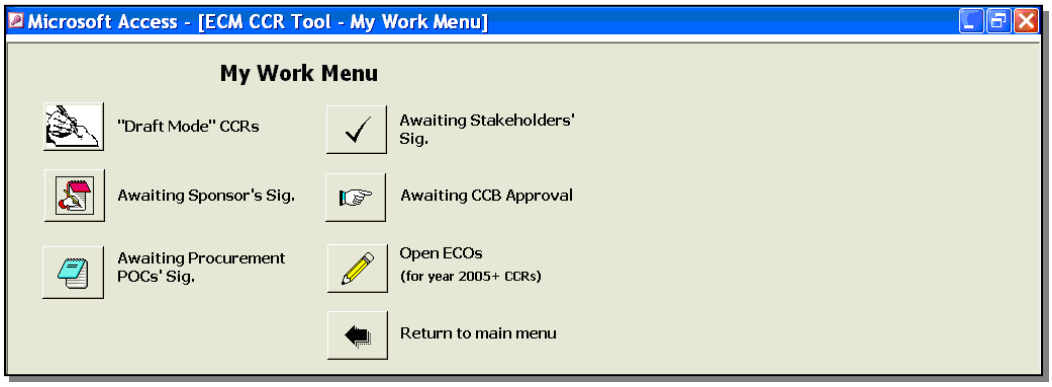


Figure 4.3.2-38. My Work Menu

Click the "Return to main menu" button on the My Work Menu to get back to the Main Menu (Figure 4.3.2-39).

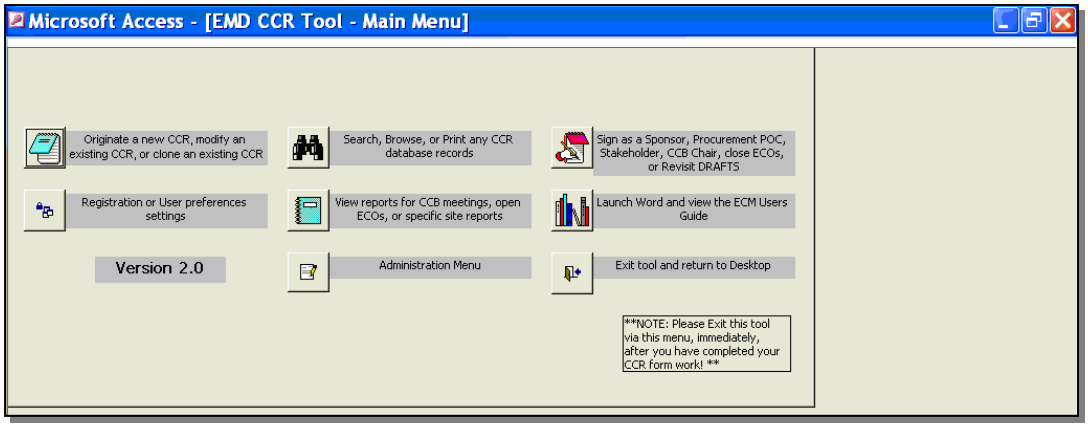


Figure 4.3.2-39. Main Menu

The draft CCR has now been finalized. The CCR tool has sent an email message to the Sponsor to let the Sponsor know that there is a CCR waiting for his/her signature.

4.3.2.5.3 4.3.2.5.3Modify A CCR

Sometimes during the processing of a CCR, changes have to be made after the originator has signed but before the CCR is approved by the CCB Chairperson. In this case, the CCR has to be taken back to draft mode so that the originator can make the necessary changes. This process is the similar to modifying a Draft CCR.

4.3.2.5.4 4.3.2.5.4CCR Clone

Sometimes after a CCR has been approved by CCB Chairperson(s), necessary changes to the CCR are identified. Since the CCR has already been approved, a revision to the CCR or a new CCR must be created to include the identified changes. This saves the user time when a new CCR will have similar content to an existing CCR. The default for the new CCR number is the next one available, but a check box exists that allows the user to set the new CCR to the next revision. For instance if the CCR to be cloned is "09-0123" and the user wants the new CCR to be Rev A, then by selecting the check box that appears, the new CCR will be "09-0123A".

4.3.2.5.5 4.3.2.5.5Printing a CCR

CCRs can be viewed and printed after the originator signs the CCRs. However, any CCR printed before the CCB Chairperson approves it, will not have all of the electronic signatures populated. To print a CCR we start off with the Main Menu as shown in Figure 4.3.2-40.

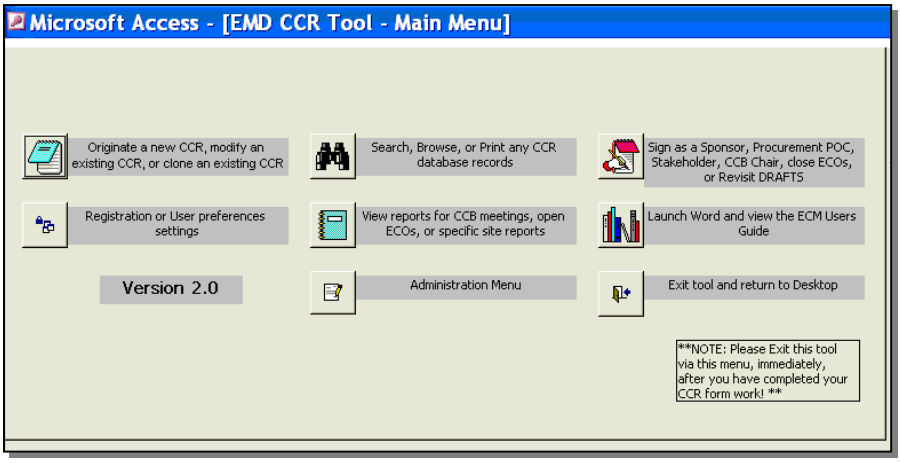


Figure 4.3.2-40. Main Menu (Printing a CCR)

Click the "Search, Browse, or Print any CCR database records" button and the CCR Search/Browse Menu is displayed as shown in Figure 4.3.2-41. There are three buttons on the Search/Browse Menu:

1) Search/Browse all CCRs button– enables one to see all of the CCRs in the database but does not show the Supplementary Procurement Information page of procurement type CCRs. The Supplementary Procurement Information page is for review by procurement officials only.

2) Search all procurement CCRs button–enables personnel that are authorized to view "Procurement" type CCRs to see all pages of the procurement CCRs. For everyone else, the "Search all procurement CCRs" button is gray (inactive).

3) Return to Main Menu button – this button returns you to the Main Menu.

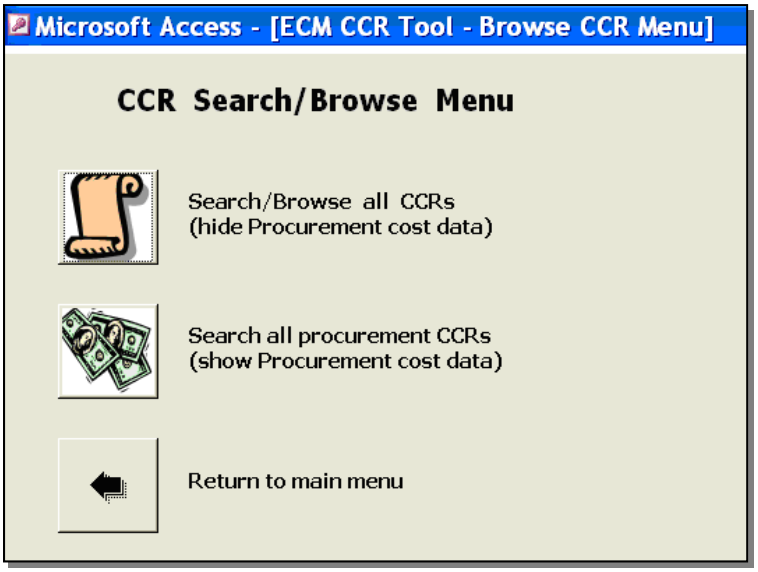


Figure 4.3.2-41. Browse CCR Menu

Since a procurement type CCR was used as the example in this guide, a procurement authorized login was used to log into the CCR tool. So the "Search all procurement CCRs" button is active. Click the "Search all procurement CCRs" button and the CCR Lookup Procurement form (Figure 4.3.2-42) is displayed. If the "Search/Browse all CCRs" button had been clicked a CCR Lookup form would have been displayed.

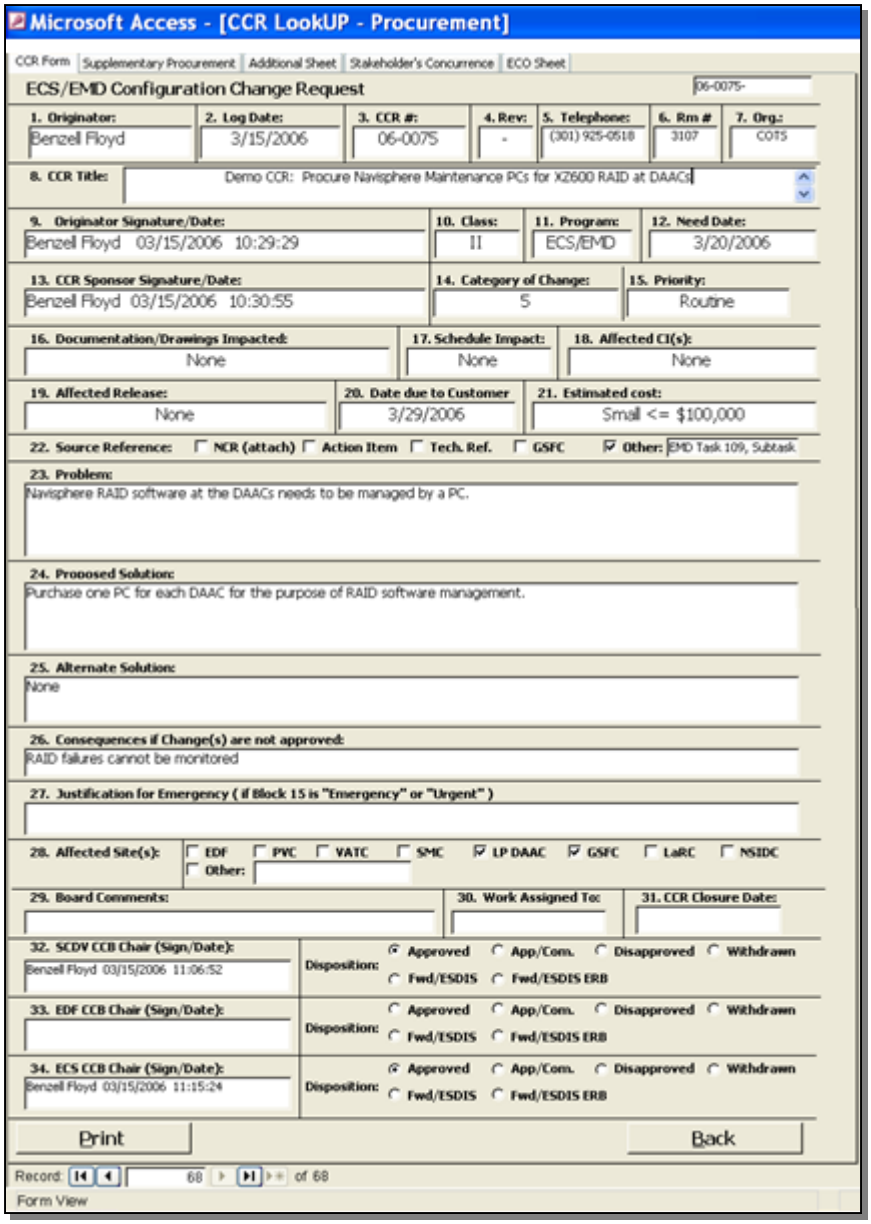


Figure 4.3.2-42. CCR Lookup Procurement Form

When the form is first displayed, the first CCR record in the database is displayed. Click the arrow at the bottom of the form to move to the desired CCR (in this case, it is CCR 06-0075). To print the CCR, click the "Print" button and the Office Assistant prompt shown in Figure 4.3.2-43 is displayed.

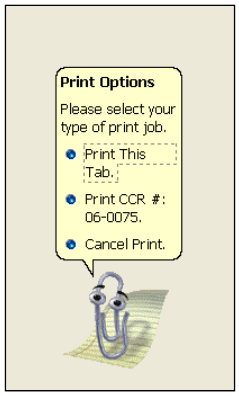


Figure 4.3.2-43. CCR Print Options

The Office displays several print options. The options are defined as follow:

1) Print This Tab – print the tab/page (CCR Form, Supplementary Procurement, Additional Sheet, Stakeholder's Concurrence, or ECO Sheet) that you are currently on. Click this option and a copy of the tab/page is sent to your default printer.

2) Print CCR #: <CCR Number> - print the entire CCR. Click this option and a copy of the entire CCR is sent to your default printer.

3) Cancel Print – Terminate print options. Click this option, the Office Assistant is removed and the focus is placed back on the CCR form.

Click the option that is desired and then click the "Back" button at the bottom of the page to get back to the Main Menu.

4.3.2.6 4.3.2.6CCR Coordination, Approvals

A CCR requires the concurrence/approval of several EMD entities before it can actually be implemented. After a CCR is signed by the CCR originator, it must then be concurred with by the Sponsor, Procurement POCs (for procurement type CCRs only), and Stakeholders. The CCR must be approved by the CCB(s) Chairperson. The CCR tool activity for each of these coordination entities will be discussed in this section.

4.3.2.6.1 4.3.2.6.1CCR Sponsor Signature

The CCR Sponsor performs the first review of the CCR after the originator has completed the CCR and signed it. The CCR tool sends an email message to the perspective CCR Sponsors, in order to notify the Sponsors of a submitted CCR. This section covers the instruction of electronically signing as a Sponsor.

The prospective CCR sponsors will have received an email stating the CCR number that needs to be sponsored. Upon notification, the sponsor logs into the CCR tool and the Main Menu (Figure 4.3.2-44) is displayed.

To sign a CCR as a Sponsor, first click the button in the upper-right corner of the Main Menu.

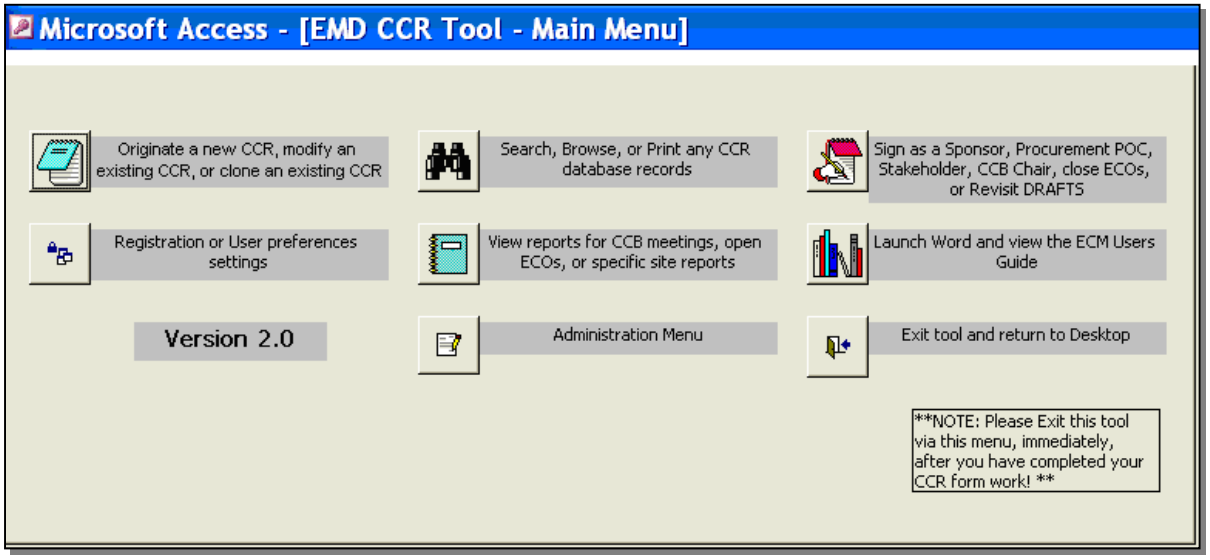


Figure 4.3.2-44. Main Menu

The My Work Menu (Figure 4.3.2-45) will be displayed next. On the My Work Menu, click the "Awaiting Sponsor's Sig."

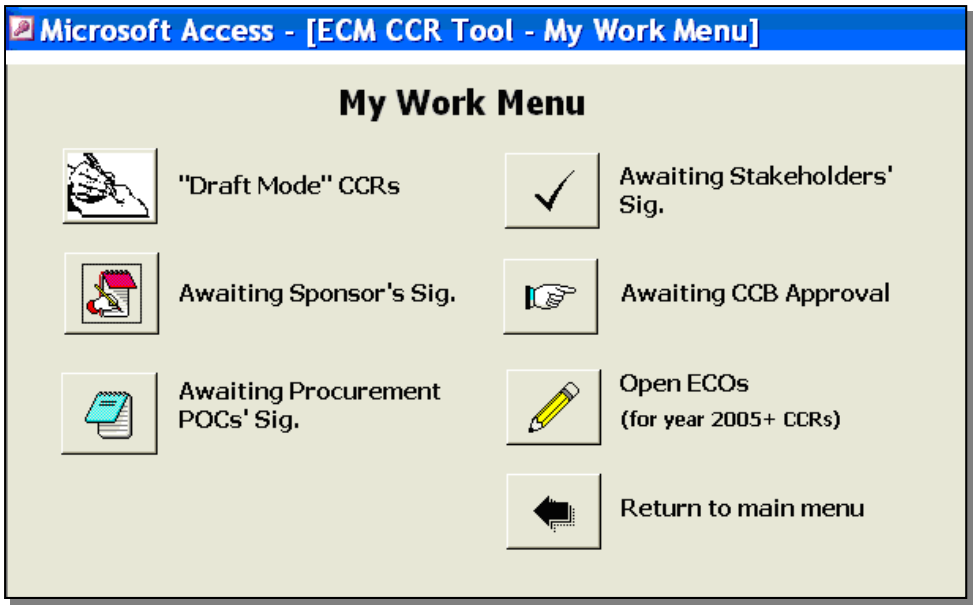


Figure 4.3.2-45. My Work Menu (Sponsor Sig.)

The My Work Menu – CCR Sponsor Signature Page (Figure 4.3.2-46) is displayed next. It will list all of the CCRs that are available for you to sponsor.

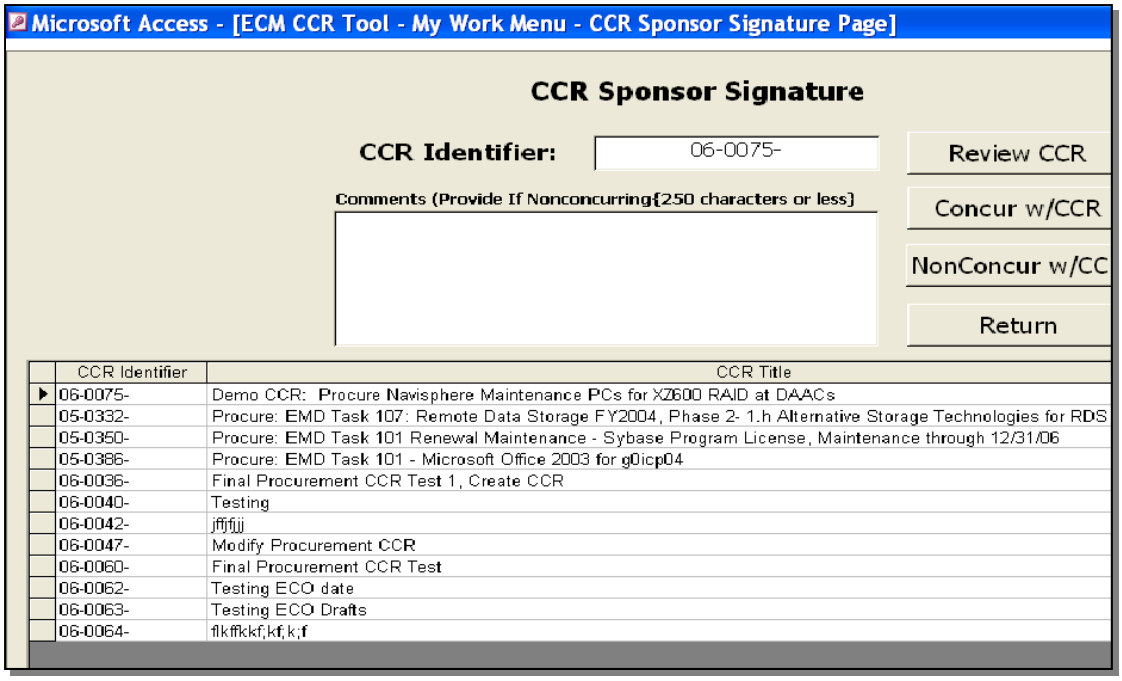


Figure 4.3.2-46. CCR Sponsor Signature Form

Click the desired CCR listed in the CCR Identifier column and the CCR identifier will be copied to the white space above the list of CCRs as shown above in Figure 4.3.2-46.

There are four possible actions that a Sponsor can take:

1) Review CCR – click the "Review CCR" button to review the contents of the CCR. All pages of the CCR will be available for review. If it is a procurement type CCR, then you can also review the BOM on the Supplementary Procurement Information page by clicking the "Display BOM" button on that page. Note, there is no Supplementary Procurement Information page in the non-procurement type CCR. Click the "Back" button on the Review CCR form to return to the Sponsor Signature form.
2) Concur w/CCR – click the "Concur w/CCR" button if you agree with the contents of the CCR. Once sponsor concurrence is obtained, a notification email message is sent to Procurement POCs (if this is a procurement type CCR) or to Stakeholders (if this is a non-procurement type CCR) for their review of the CCR, next. Refer to Section 4.3.2.6.1.1 for prompts and responses for this action.
3) NonConcur w/CCR – click the "NonConcur w/CCR" button if you disagree with the contents of the CCR. If you nonconcur, you have to provide a brief reason for nonconcurring in the "Comments" box. The CCR tool will email the comments back

to the originator and place the CCR in draft mode to enable the originator's revisions. Refer to Section 4.3.2.6.1.1 for prompts and responses for this action.

4) Return – click the "Return" button if you want to return to the previous form, My Work Menu (Figure 4.3.2-45).

4.3.2.6.1.1 4.3.2.6.1.1Concur w/CCR Action

If the "Concur w/CCR" button is clicked, the Office Assistant will respond as shown in Figure4.3.2-47.

Figure 4.3.2-47. Confirmation of Sponsor's Concurrence

Click "Yes" to the Confirmation of Sponsor's Concurrence prompt and the Office Assistant will respond as shown in Figure 4.3.2-48.

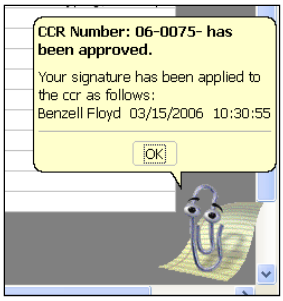


Figure 4.3.2-48. Sponsor Approval Response

Click OK to close the Confirmation Office Assistant and the CCR tool places the focus back on the CCR Sponsor Signature form (Figure 4.3.2-46)

Click "No" to the Confirmation of Sponsor's Concurrence prompt the Office Assistant will respond as shown in Figure 4.3.2-49.

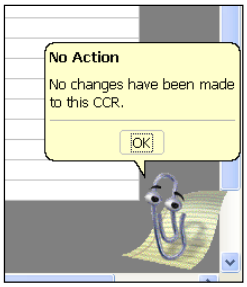


Figure 4.3.2-49. No Action Response

Click OK to close the No Action Office Assistant and the CCR tool places the focus back on the CCR Sponsor Signature form (Figure 4.3.2-46).

4.3.2.6.1.2 4.3.2.6.1.2NonConcur w/CCR Action

For non concurrence actions, a brief comment must be entered into the "Comments" box then click the "Nonconcur w/CCR" button. The Office Assistant will respond as shown in Figure 4.3.2-50.

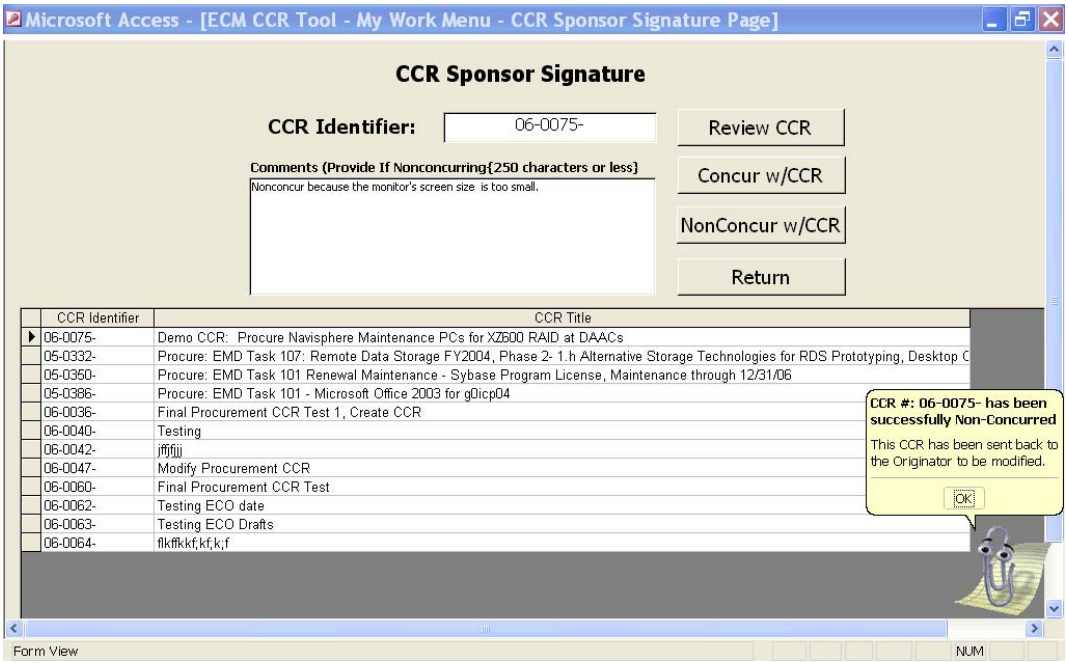


Figure 4.3.2-50. Sponsor NonConcur

Click OK to close the Office Assistant and the CCR tool places the focus back on the CCR Sponsor Signature form (Figure 4.3.2-51). The CCR has now been removed from the list and has been placed back in draft mode to enable originator revision.

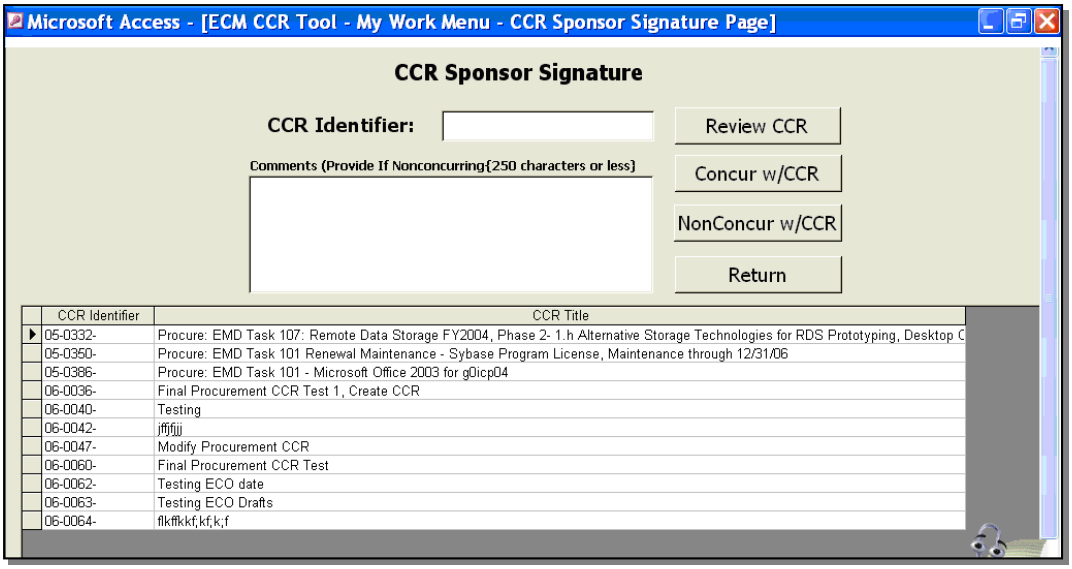


Figure 4.3.2-51. CCR Sponsor Signature Form

4.3.2.6.2 4.3.2.6.2Procurement POCs Signatures

The Procurement POCs (WBS Manager, Task Lead, Sub Task Lead (if assigned), SCM Manager, and Procurement Section) reviews procurement type CCRs after the Sponsor signs the CCR. After the Sponsor signs the CCR, the CCR tool sends an email message to the Procurement POCs (for procurement CCRs only). This section covers the instruction of electronically signing as a Procurement POC.

The perspective Procurement POCs will have concurrently received an email stating the CCR number that needs to be reviewed and concurred. Upon notification, the Procurement POC logs into the CCR tool and the Main Menu (Figure 4.3.2-52) is displayed.

To sign a CCR as a Procurement POC, first click the button in the upper right corner of the Main Menu and labeled "Sign as Sponsor, Procurement POC - - - -"

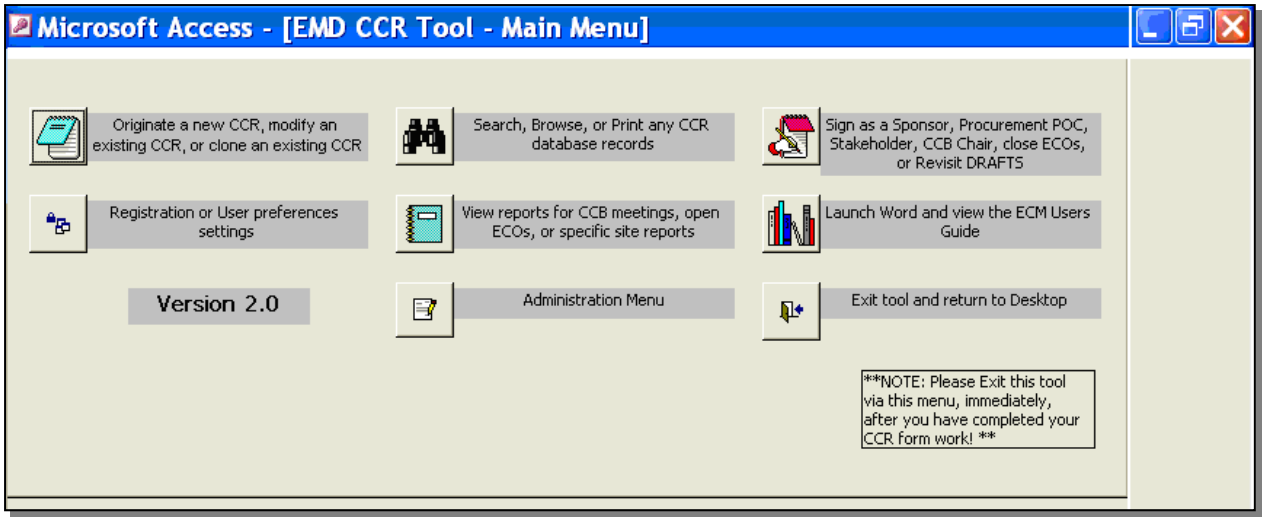


Figure 4.3.2-52. Main Menu

The CCR tool will display the My Work Menu as shown in Figure 4.3.2-53.

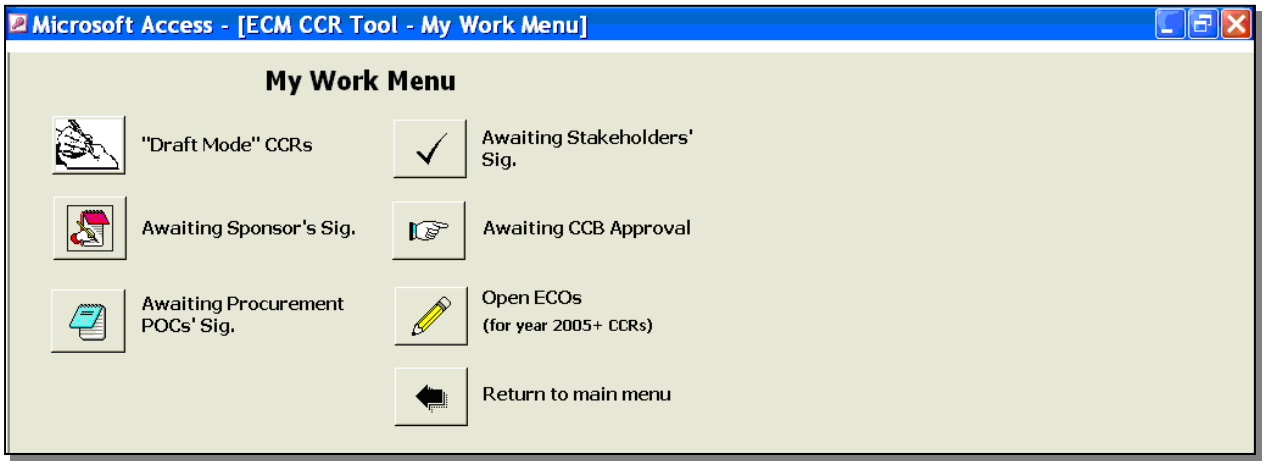


Figure 4.3.2-53. My Work Menu

Click the "Awaiting Procurement POCs' Sig." button and the My Work Procurement Menu is displayed as shown in Figure 4.3.2-54.

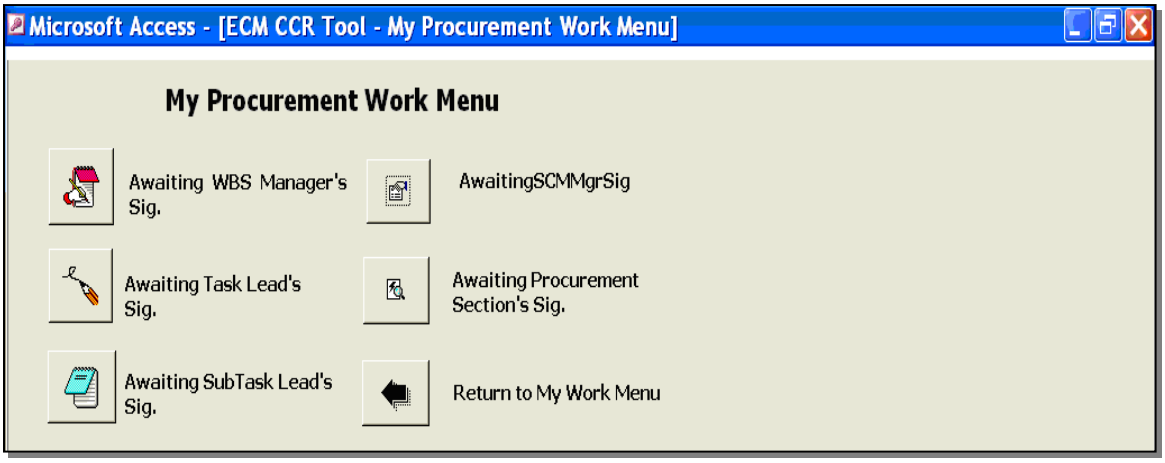


Figure 4.3.2-54. My Procurement Work Menu

On the My Procurement Work Menu click the button for the role that you play in the CCR approval process. In this example, the WBS Manager role is being used for demonstration purposes. The procedure is the same for all Procurement POCs. In this example the "Awaiting WBS Manager's Sig. was clicked and the CCR tool displayed the Procurement CCR – WBS Manager Signature form as shown in Figure 4.3.2-55.

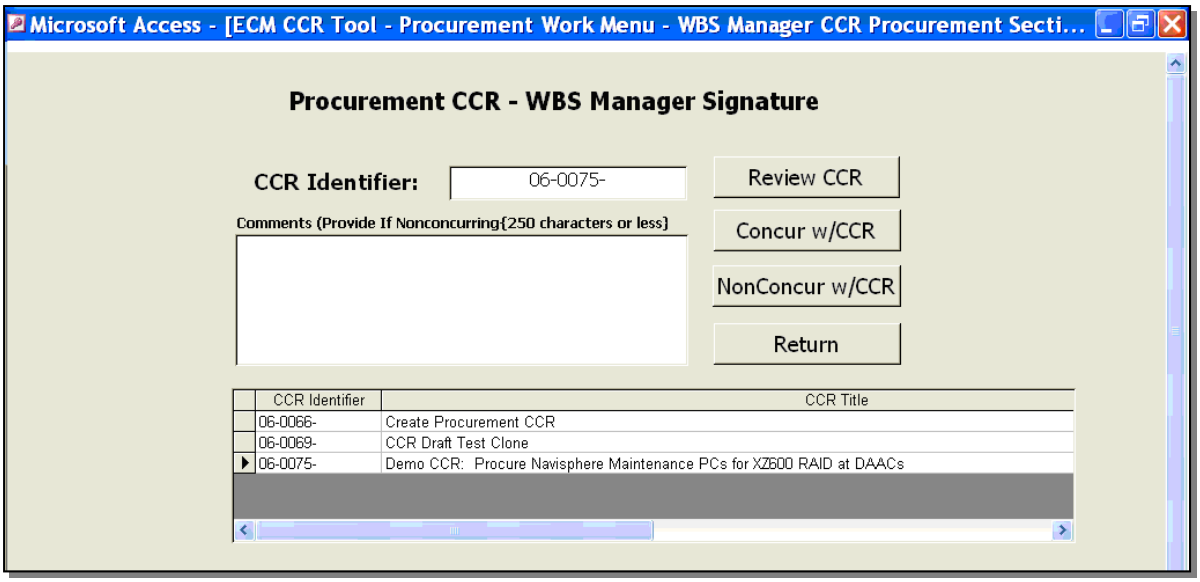


Figure 4.3.2-55. Procurement CCR – WBS Manager Signature form

Click the CCR identifier in the CCR Identifier column and the CCR tool places the CCR identifier in the CCR Identifier's box above the list.

There are four possible actions that a Procurement POC can perform:

1) Review CCR- click the "Review CCR" button to review the contents of the CCR. All pages of the CCR will be available for review. Access to the CCR's BOM is set up on the Supplementary Procurement Information page. Click the "Display BOM" button on that page and the BOM will be displayed. Click the "Back" button on the Review CCR form to return to the Procurement POC's Signature form.
2) Concur w/CCR – click the "Concur w/CCR" button if you agree with the contents of the CCR. Once all Procurement POCs concurrences have been obtained, a notification email message is sent to Stakeholders for their review of the CCR, next. Refer to Section 4.3.2.6.4.1 for prompts and responses for this action.
3) NonConcur w/CCR – click the "NonConcur w/CCR" button if you disagree with the contents of the CCR. If you nonconcur, you have to provide a brief reason for nonconcurring in the "Comments" box. The CCR tool will remove all signatures obtained up to this point, will email the comments to the originator and other signers and place the CCR in draft mode to enable the originator's revisions. Refer to Section 4.3.2.6.2.1 for prompts and responses for this action.
4) Return – click the "Return" button if you want to return to the previous form, My Procurement Work Menu (Figure 4.3.2-54).

4.3.2.6.2.1 4.3.2.6.2.1Concur w/CCR Action

If the "Concur w/CCR" button is clicked, the Office Assistant will respond as shown in Figure 4.3.2-56.

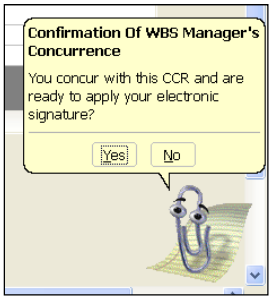


Figure 4.3.2-56. Confirmation of Procurement POC's Concurrence

Click "Yes" to the Confirmation of Procurement POC's Concurrence prompt and the Office Assistant will respond as shown in Figure 4.3.2-57. No action is performed if "No" is clicked.

Figure 4.3.2-57. Procurement POC Approval Response

Click OK to close the Office Assistant and the CCR tool places the focus back on the Procurement CCR Signature form (Figure 4.3.2-58).

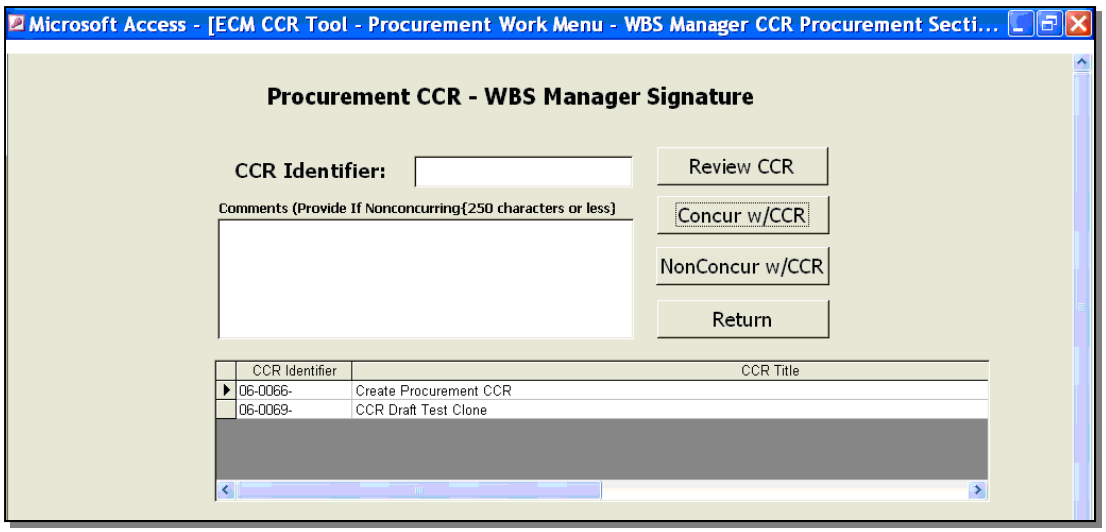


Figure 4.3.2-58. Procurement CCR Signature Form

4.3.2.6.2.2 4.3.2.6.2.2NonConcur w/CCR Action

For Nonconcurrence actions, a brief comment must be entered into the "Comments" box then click the "Nonconcur w/CCR" button. The set of actions follows similarly to Section 4.3.2.6.1.2.

4.3.2.6.3 4.3.2.6.3Stakeholder Signature

The Stakeholders are asked to review the CCR and sign, once a Sponsor has signed and also Procurement POCs have signed (if it's a procurement type CCR). The event of the Sponsor/Procurement POCs signing will cause the tool to email all of the perspective Stakeholders. This email list is comprised of all of the Authorized Signers based on the checked boxes on the Stakeholder sheet. Each Office has at least two and up to five individuals who may

review and sign the CCR as a Stakeholder. This section covers the instruction of electronically signing as a Stakeholder.

The perspective Stakeholder will have received an email stating the CCR number that needs to be reviewed and concurred. Upon notification, the Stakeholder logs into the CCR tool and the Main Menu (Figure 4.3.2-59) is displayed.

To sign a CCR as a Stakeholder, first click the button in the upper right corner of the Main Menu and labeled "Sign as Sponsor, Procurement POC, Stakeholder, - - - - -"

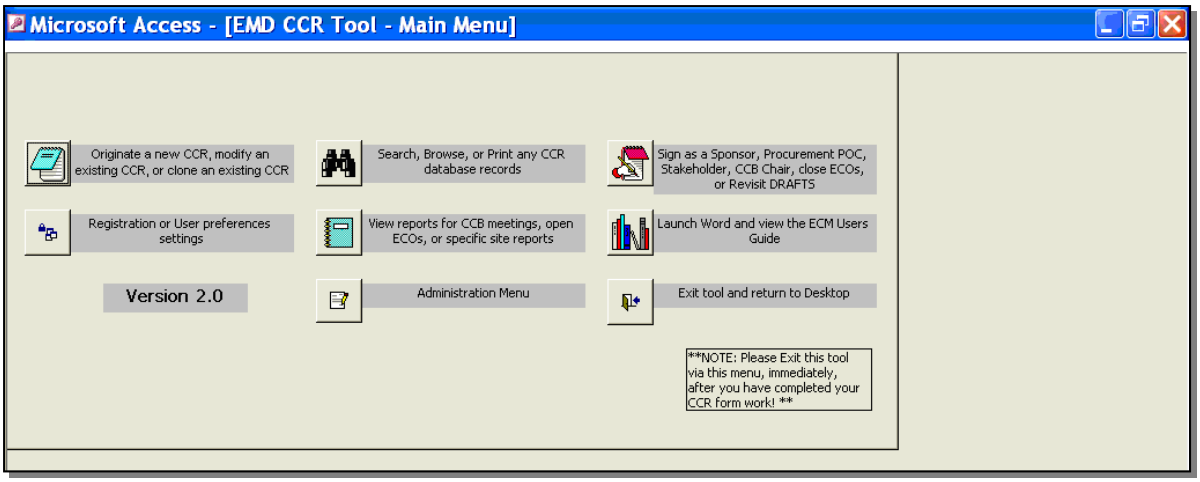


Figure 4.3.2-59. Main Menu

Upon clicking the aforementioned button, the CCR tool displays the My Work Menu as shown in Figure 4.3.2-60.

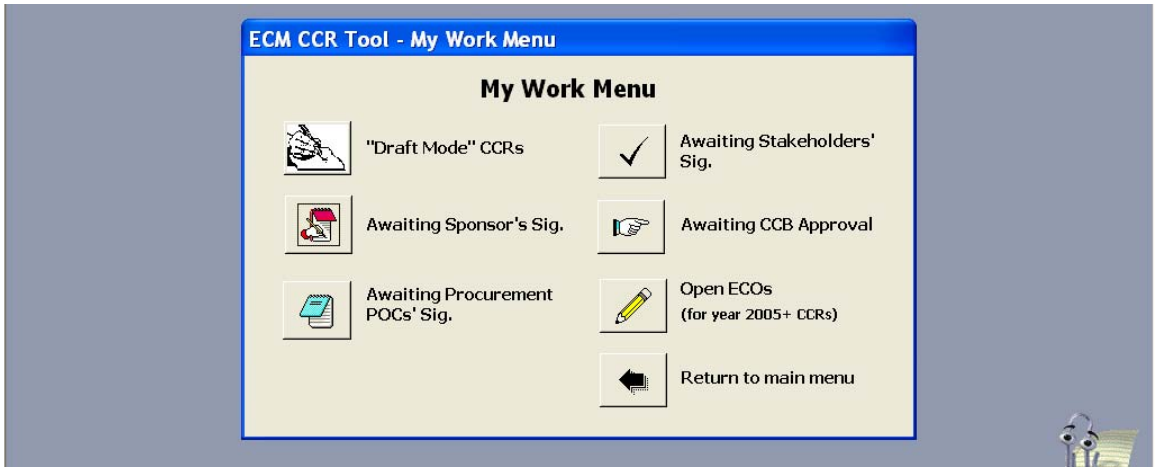


Figure 4.3.2-60. My Work Menu

Click the button, "Awaiting Stakeholders' Sig." and the My Work Menu – Stakeholder's Selection Menu is displayed as shown in Figure 4.3.2-61.

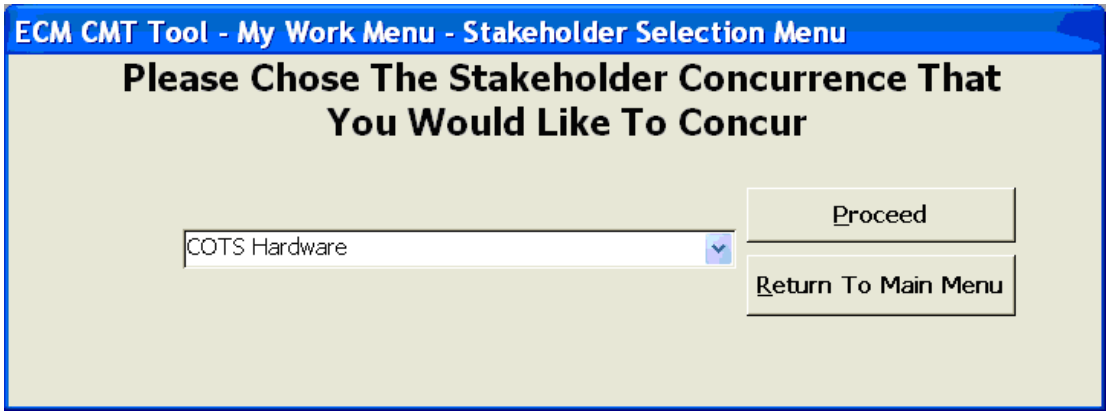


Figure 4.3.2-61. Stakeholder's Selection Menu

Click the pull-down menu on the Stakeholder's Selection Menu form and select the Stakeholder role that you are representing. In this example, the "COTS Hardware" Stakeholder was selected.

Click the Proceed button and the CCR tool displays the appropriate Stakeholder's Concurrence Signature Page as shown in Figure 4.3.2-62. Click the CCR identifier in the CCR Identifier column and the CCR tool copies the identifier into the CCR Identifier box that is above the list.

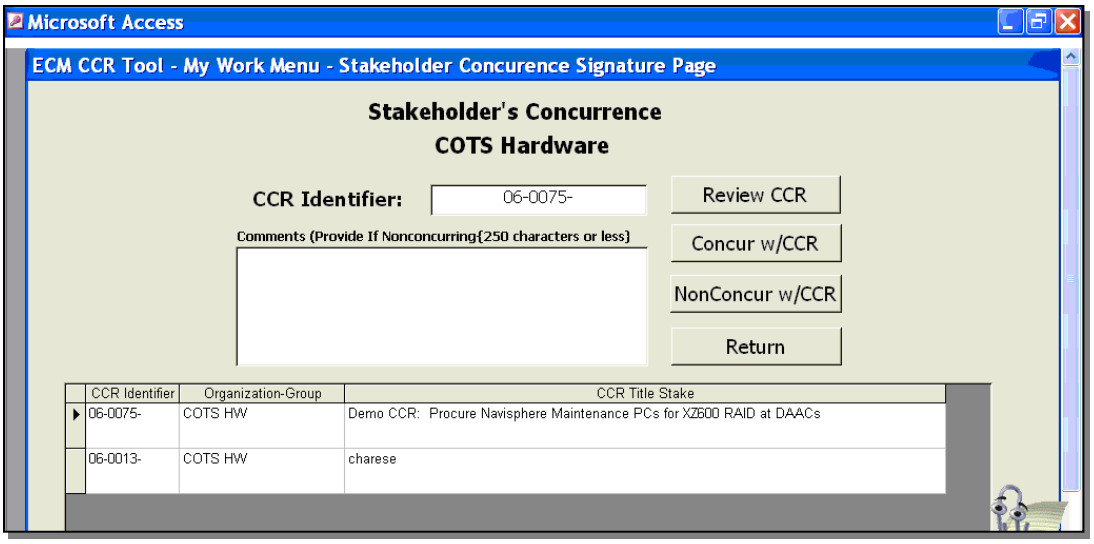


Figure 4.3.2-62. Stakeholder Concurrence Signature Page

There are four possible actions that a Stakeholder can perform:

1) Review CCR- click the "Review CCR" button to review the contents of the CCR. All pages of the CCR will be available for review. For a procurement type CCR only, access to the CCR's BOM is set up on the Supplementary Procurement Information page. Click the "Display BOM" button on that page and the BOM will be displayed. Click the "Back" button on the Review CCR form to return to the Procurement POC's Signature form.
2) Concur w/CCR – click the "Concur w/CCR" button if you agree with the contents of the CCR. Once all Stakeholders concurrences have been obtained, a notification email message is sent to the CCB Chairpersons for their review of the CCR, next. Refer to Section 4.3.2.6.4.1 for prompts and responses for this acion.
3) NonConcur w/CCR – click the "NonConcur w/CCR" button if you disagree with the contents of the CCR. If you nonconcur, you have to provide a brief reason for nonconcurring in the "Comments" box. The CCR tool will remove all signatures obtained up to this point, will email the comments to the originator and other signers and place the CCR in draft mode to enable the originator's revisions. Refer to Section 4.3.2.6.2.2 for prompts and responses for this action.
4) Return – click the "Return" button if you want to return to the previous form, My Stakeholder Selection Menu (Figure 4.3.2-61).

4.3.2.6.3.1 4.3.2.6.3.1Concur w/CCR Action

If the "Concur w/CCR" button is clicked, the Office Assistant will respond as shown in Figure 4.3.2-63. Click "Yes" to the Confirmation of Stakeholder's Concurrence prompt and the Office Assistant will respond as shown in Figure 4.3.2-64. No action is performed if "No" is clicked.

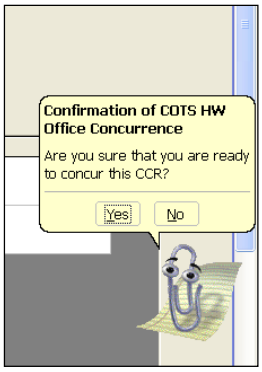


Figure 4.3.2-63. Confirmation of Concurrence Prompt

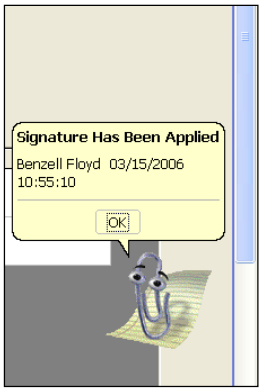


Figure 4.3.2-64. Notification of Signature Applied

Click the OK button on the "Signature Has Been Applied" message. The message prompt is removed, the now concurred CCR is removed from the Stakeholder's Concurrence window as shown in Figure 4.3.2-65.

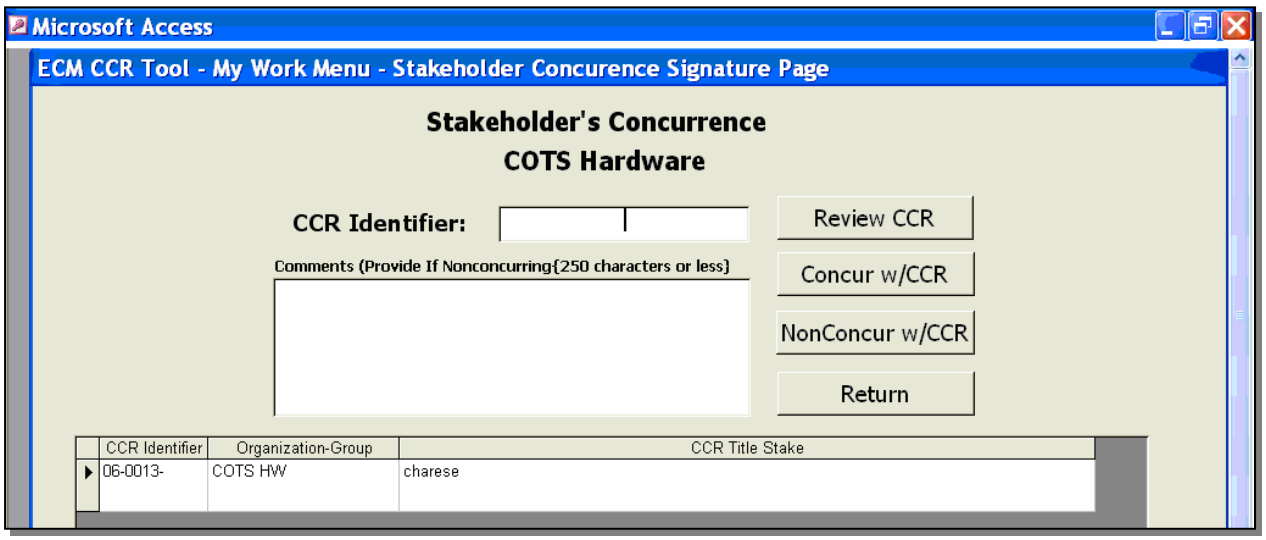


Figure 4.3.2-65. Stakeholder's Concurrence Window

Click the Return button to return to the Stakeholder's Selection window then click the "Return to Main Menu" button on the Selection window to get back to the Main Menu.

4.3.2.6.3.2 4.3.2.6.3.2NonConcur w/CCR Action

For Nonconcurrence actions, a brief comment must be entered into the "Comments" box then click the "Nonconcur w/CCR" button. The subsequent steps and displayed forms will occur as in previous sections for non concurrences.

4.3.2.6.4 4.3.2.6.4CCB Chairperson's Approval

Once the Stakeholders have completed the Stakeholder sheet, an email is sent to the perspective CCB Chairperson(s), in order to notify the Chairpersons of a CCR that is ready for approval. The CCB Chairperson(s) perform the final review of the CCR.

There are three potential CCB Chairs that may need to approve a CCR: EDF CCB Chairperson, SCDV CCR Chairperson, and the ECS CCB Chairperson. CCB approval criteria included within the CCR tool's code and the contents of the CCR enables the tool to determine which CCB Chair should be required to approve a CCR. This section covers the instruction of electronically signing as a CCB Chairperson. To sign as a CCB Chairperson, first click the button in the upper right corner of the Main Menu (Figure 4.3.2-66) and labeled as "Sign as a Sponsor, Procurement POC, Stakeholder, CCB Chair - - -".

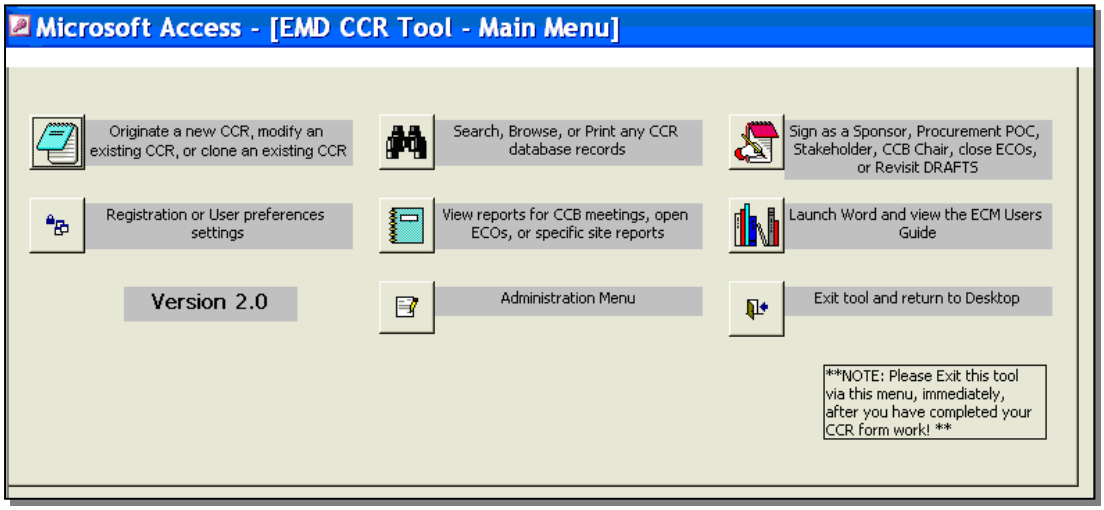


Figure 4.3.2-66. Main Menu

Upon clicking the aforementioned button, the "My Work Menu" (Figure 4.3.2-67) is displayed.

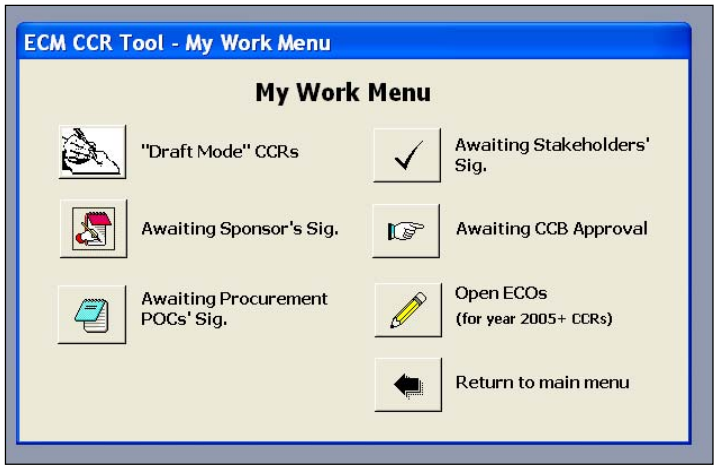


Figure 4.3.2-67. My Work Menu

Click the "Awaiting CCB Approval" button on the My Work Menu and the My CCB Chair Signature Menu (Figure 4.3.2-68) is displayed.

Figure 4.3.2-68. My CCB Chair Signature Menu

Note, that there is a button for each of the CCB Chairs on the My CCB Chair Signature Menu. Click the button for the CCB Chair that you represent. In this example, the "Awaiting SCDV CCB Chair Signature" button was clicked. The CCR tool responds by displaying the SCDV CCB Chair Signature window as shown in Figure 4.3.2-69.

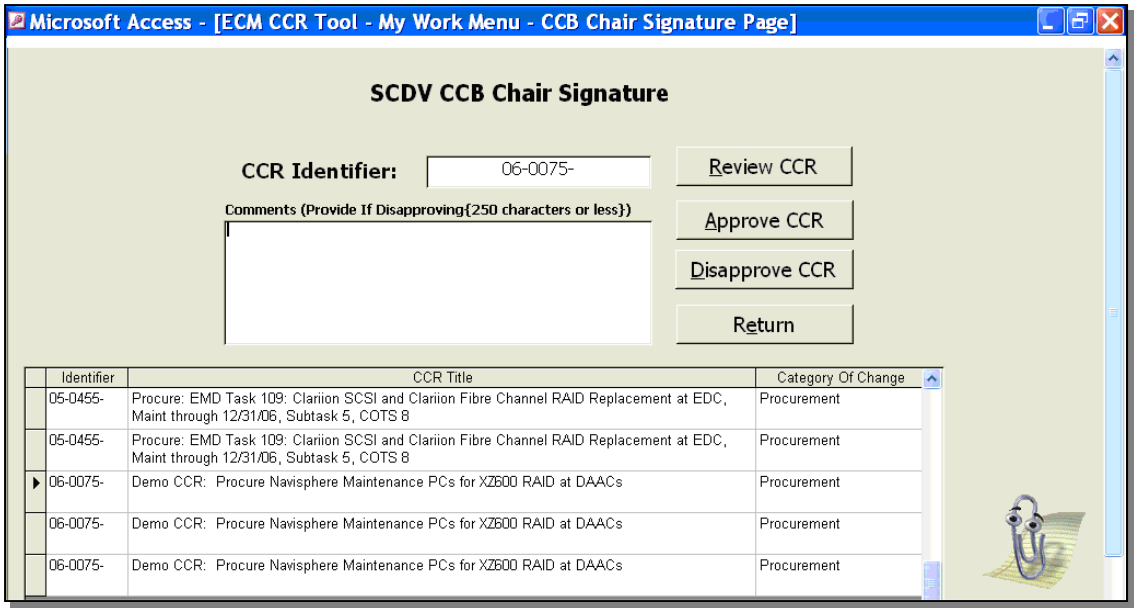


Figure 4.3-2-69. SCDV CCB Chair Signature

On the <CCB Chair> CCB Chair Signature window, click the desired CCR's identifier in the Identifier column and the CCR tool copies the identifier into the CCR Identifier box as shown in Figure 4.3.2-69.

There are four possible actions that a CCB Chairperson can perform:

1) Review CCR- click the "Review CCR" button to review the contents of the CCR. All pages of the CCR will be available for review. Access to the CCR's BOM is set up on the Supplementary Procurement Information page. Click the "Display BOM" button on that page and the BOM will be displayed. Click the "Back" button on the Review CCR form to return to the CCB Chair's Signature form.
2) Approve CCR – click the "Approve CCR" button if you agree with the contents of the CCR. Once all CCB Chairs (if more than one is required) have approved the CCR, Approved box is checked on the CCR Form page of the CCR; a notification email message is sent to all parties to let them know that the CCR has been approved. The ECO assignees are notified of their ECO tasks. Refer to Section 4.3.2.6.4.1 for prompts and responses for this action.
3) Disapprove CCR – click the "Disapprove CCR" button if you disagree with the contents of the CCR. If you disapprove, you have to provide a brief reason for disapproving the CCR in the "Comments" box. The CCR tool check the Disapprove box on the CCR Form page of the CCR; a notification email message is sent to all parties to let them know that the CCR has been disapproved. Refer to Section 4.3.2.6.2 for prompts and responses for this action.
4) Return – click the "Return" button if you want to return to the previous form, My CCB Chair Signature Menu, Figure 4.3.2-68.

4.3.2.6.4.1 4.3.2.6.4.1Approve CCR Action

If the "Approve CCR" button is clicked, the Office Assistant will respond as shown in Figure 4.3.2-70.

Figure 4.3.2-70. Confirmation of CCR Approval

Click "Yes", the CCR is approved and is removed from the list of CCRs; the message prompt is removed. Click "No" and no action is performed.

Click the "Return" button to return to the previous menu, My CCB Chair Signature Menu (Figure 4.3.2-71).

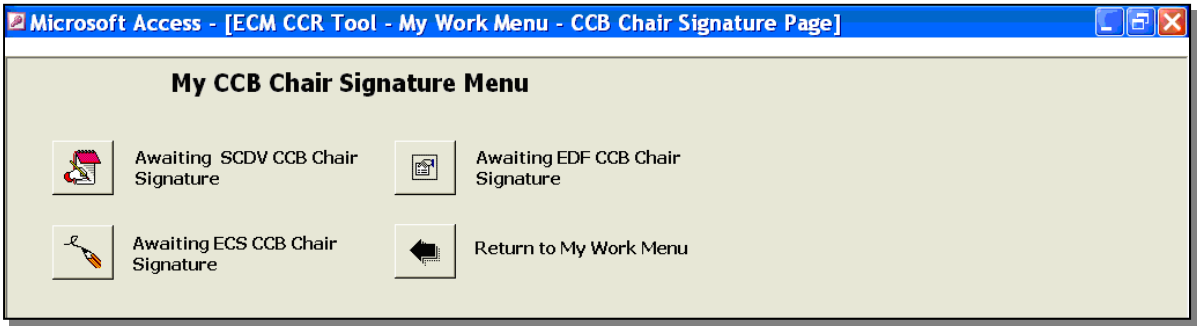


Figure 4.3.2-71. My CCB Chair Signature Menu

Click the "Return to My Work Menu" button on the My CCB Chair Signature Menu to get back to the My Work Menu. Then click the "Return to main menu" button on the My Work Menu to get back to the Main Menu. The front page of a CCB Approved CCR is shown in Figure4.3.2-72.

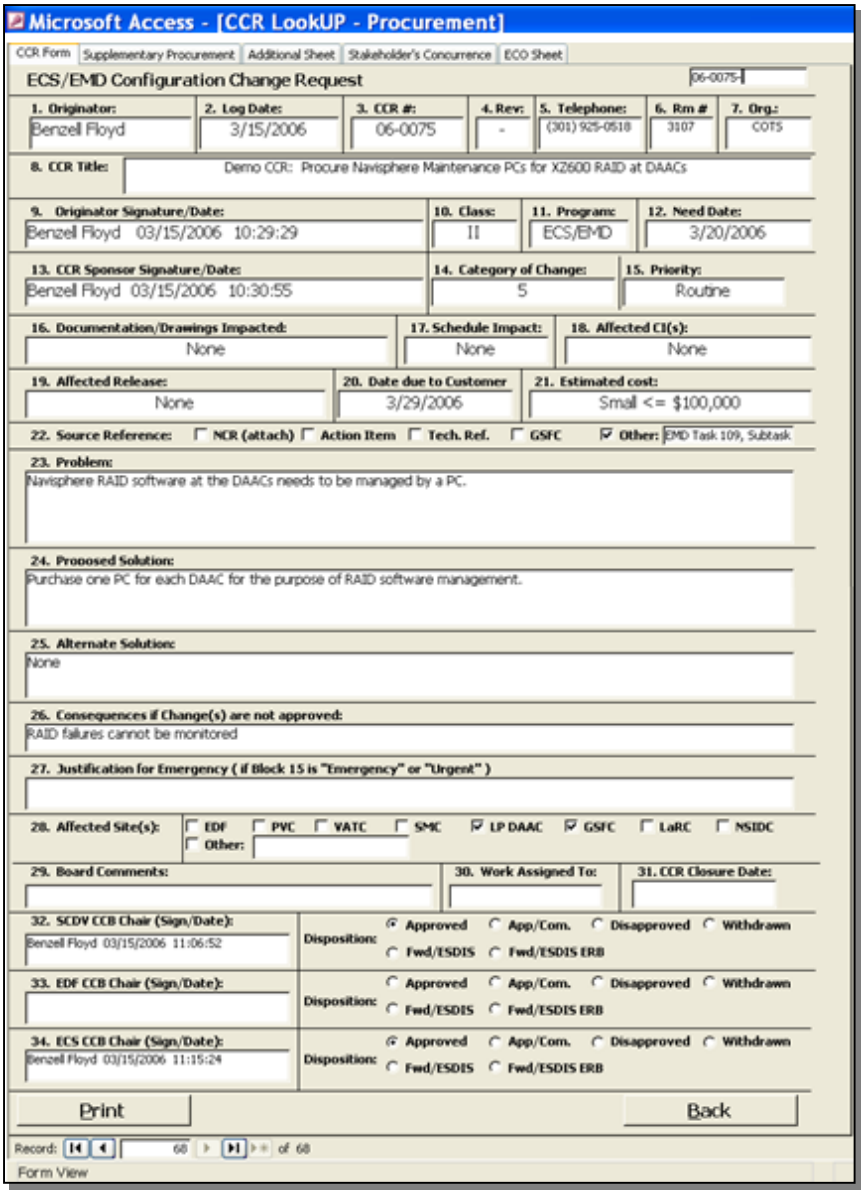


Figure 4.3.2-72. Approved CCR

4.3.2.6.4.2 4.3.2.6.4.2Disapprove CCR Action

For a Disapprove CCR action, a brief comment must be entered into the "Comments" box then click the "Disapprove CCR" button. The Office Assistant will respond as shown in Figure 4.3.2-73.

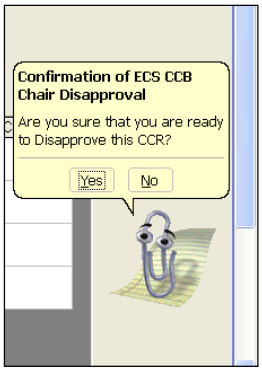


Figure 4.3.2-73. Confirmation of Disapproval Prompt

Click the "Yes" button. The CCR is disapproved and the Office Assistant will respond as shown in Figure 4.3.2-74. Click the "No" button and no action will be taken.

Figure 4.3.2-74. Confirmation of a CCB Chair's Disapproval

Click OK on the disapproval message. The "Disapprove" box on the CCR Form page of the CCR will be checked. No further action will be taken on the disapproved CCR. Click the "Return" button on the <CCB Chair> CCB Chair Signature window and the CCR tool will take you back to the My CCB Chair Signature Menu. Click the "Return to My Work Menu" button on the My CCB Chair Signature Menu and the CCR tool will take you back to the My Work Menu. Click the "Return to main menu" button on the My Work Menu to get back to the Main Menu.

4.3.2.7 4.3.2.7ECO Assignee Close ECO

Once the CCR is approved, the Engineering Change Orders (ECOs) can be worked. The ECOs comprise the work of the CCR. Once a CCB Chairperson has approved a CCR and signed, an email is sent to the ECO Assignees, in order to notify them that the CCR has been approved and that the work of the CCR needs to be performed. When the ECO has been completed, the ECO

Assignee should close the ECO. This section covers the instructions for electronically closing an ECO.

The ECO Assigned logs into the CCR tool and the Main Menu (Figure 4.3.2-75) is displayed.

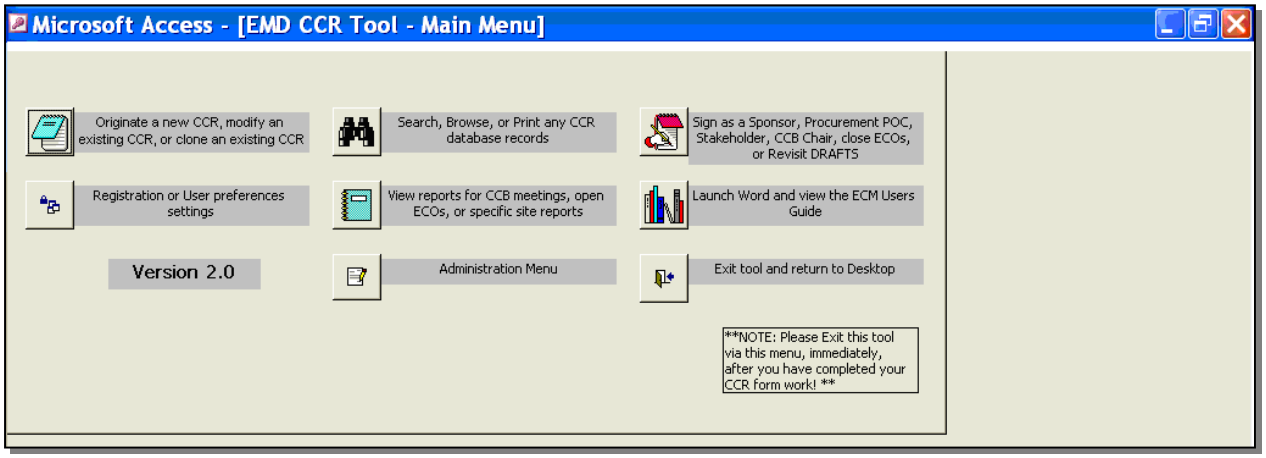


Figure 4.3.2-75. Main Menu

Click the "Sign as a Sponsor, Procurement POC, Stakeholder, CCB Chair, close ECOs - - -" button in the upper right corner. Upon clicking this button, the "My Work Menu" (Figure 4.3.2□76) is displayed.

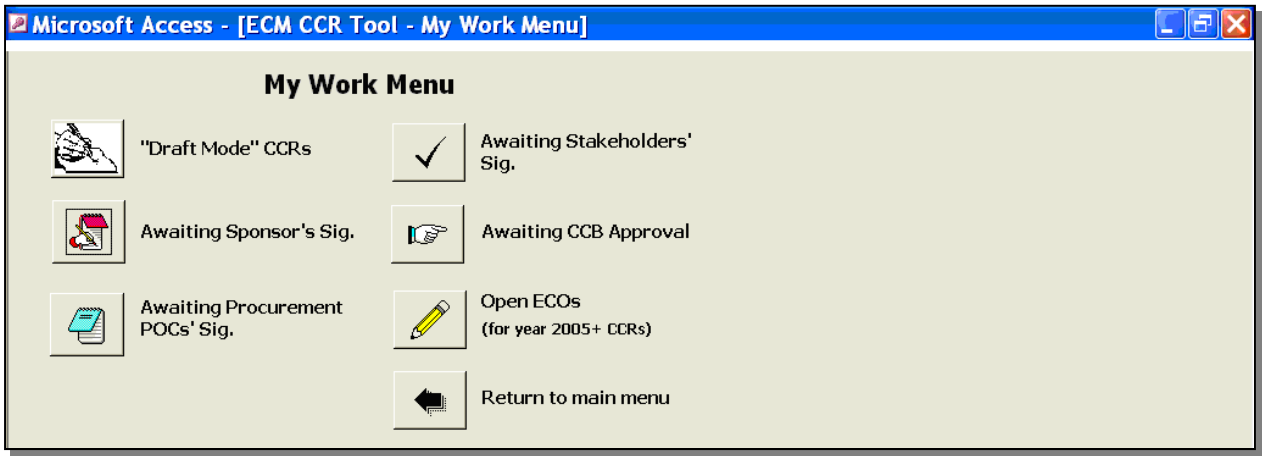


Figure 4.3.2-76. My Work Menu

Click the "Open ECOs" button on the My Work Menu and the frmMyWorkOpenECO form (Figure 4.3.2-77) is displayed. All of the current user's open ECOs are displayed on the form.

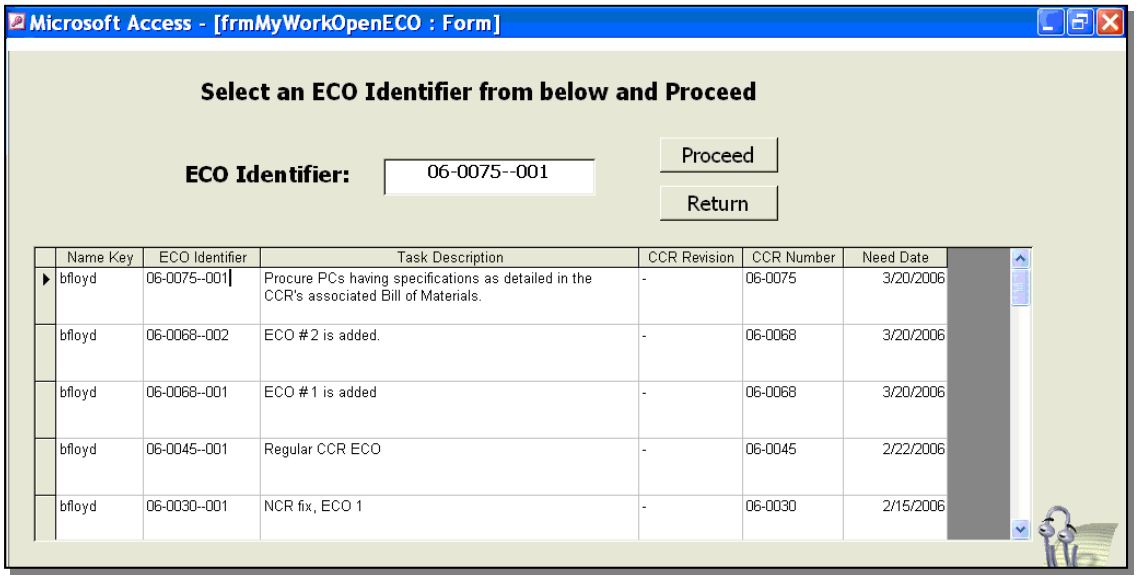


Figure 4.3.2-77. List of Open ECOs

Click the ECO identifier of the ECO (to be closed) in the ECO Identifier column and the CCR tool will copy the identifier into ECO Identifier box above the list. Click the "Proceed" button and the CCR tool displays the Office Assistant message as shown in Figure 4.3.2-78.

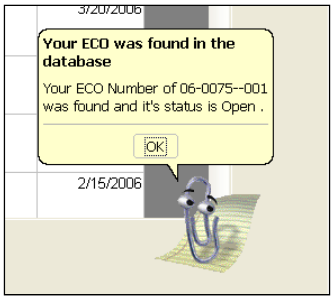


Figure 4.3.2-78. Confirmation For Finding Open ECO

Click the OK button on the Office Assistant and the CCR tool displays the next Office Assistant message as shown in Figure 4.3.2-79.

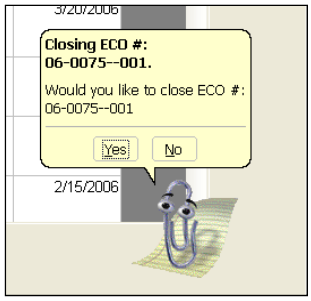


Figure 4.3.2-79. Closing ECO Message Prompt

Note, there are two possible responses, "Yes" and "No." Section 4.3.2.8 (below) covers what happens if "Yes" is selected. Section 4.3.2.9 covers what happens if "No" is selected.

4.3.2.8 4.3.2.8ECO Assignee Close ECO

Click "Yes" and the CCR tool responds with the Office Assistant message shown in Figure4.3.2-80. At this point, the select ECO has been closed and the close date is been entered.

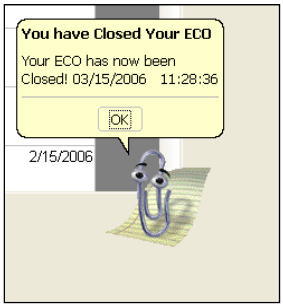


Figure 4.3.2-80. Confirmation of Closed ECO

The ECO is no longer listed in the list of ECOs (see Figure 4.3.2-81).

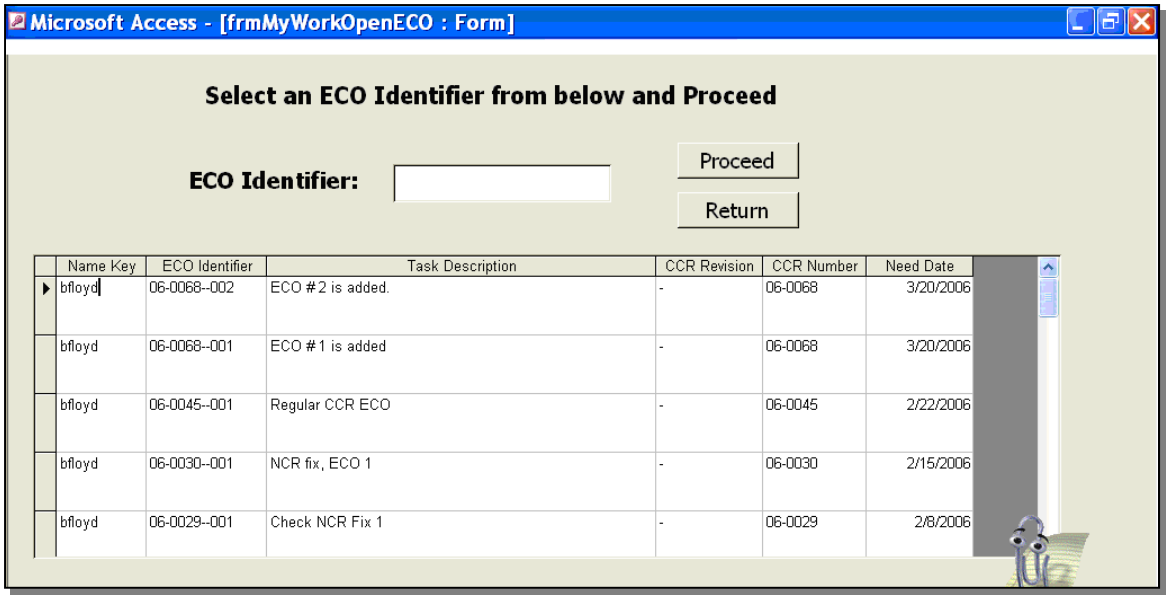


Figure 4.3.2-81. List of Remaining ECOs

Click the "Return" button to return to previous menu and then the "Return" buttons on the following menus to get back to the Main Menu.

4.3.2.9 4.3.2.9No Response to Close ECO

If "No" is clicked, the CCR tool responds with the Office Assistant message shown in Figure4.3.2-82. Click "OK" on the message prompt. The Office Assistant message is removed and no action is performed on the ECO. Figure 4.3.2-80 is displayed. At this point, either an ECO identifier can be selected again or the "Return" button can be used to get back to previous forms and eventually to the Main Menu.

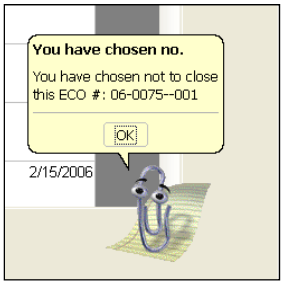


Figure 4.3.2-82. Choose Not To Close ECO Response

4.3.2.10 4.3.2.10Searching the CCR Database

The Microsoft® Access Main Menu provides excellent search capabilities in conjunction with the EED CCR Tool's tables. Select the binoculars icon within the Tool main menu (top right) to search across all CCRs that are in the Access database (the text to the right of the binoculars is **Search across entire CCR database for any information**.). Any CCR field may be searched, within the set of CCR form tabs: *CCR Form*, *Additional Sheet*, *Stakeholder's* Concurrence, or *ECO Sheet*.

It is quite useful to search the database for any information about all CCRs. Microsoft® Access provides the functions for performing searches. It is easiest to show by example.

To obtain a particular CCR that is already in the database, perform the following steps:

1) Select the "Search across entire CCR database for any information." button on the EED CCR Tool main menu. The button has a set of binoculars as an icon.
2) The tool will then launch the CCR form for the cover sheet for CCR 05-0001, which is the first CCR record carried within the tool. Each field can be searched for any character string, and, multiple field searches are also possible. To select CCR 05-0108, set the mouse cursor to the left of the 05-0001 text. The mouse wheel, when moved, will allow incremental movement across the database, but to get right to the CCR of interest, continue with steps below. Note that all of the CCR data can be readily viewed across all four Tabs mentioned above. Refer to Figure 4.3.2-83 on the next page.
3) In the Microsoft® Access menu bar at the very top of the window, note the three filter icons: Filter by Selection, Filter by Form, and Apply Filter. Positioning the mouse cursor on a Filter icon will cause some text from Access to appear to indicate the icon function. Three filter icons, which look like funnels, are present in the Access main menu bar once the binoculars button within the Access application is selected.
4) In the first Search example, the CCR 05-0108 will be obtained. After placing the mouse cursor in the CCR Form field "**3. CCR #:**", select the Filter icon in the Access main menu bar that has the form next to the Filter icon (Filter by Form). Ensure that all of the fields are blank (use the delete key to blank any that are not), then place the mouse cursor in the "**3. CCR #:**" text box.
5) Next, type in the CCR of interest, in this case, 05-0108. Then select the Filter icon in the main menu bar. CCR 05-0108 will then be displayed. To return to the Main Menu, select the "Return to main menu" button on the bottom of the CCR page.
6) Similarly, and text can be searched within any of the CCR fields.
7) Next a search will be performed for all of the AMASS CCRs.
8) Select the binoculars in the Main Menu form.
9) Place the mouse cursor in the "**8. CCR Title:**" field, then select the Filter by Form icon on the Access main menu bar.
10) Delete any fields, then place the mouse cursor in the **8. CCR Title** text box. Enter the text *AMASS*. The wild card asterisks indicate that any text may exists before and after the AMASS string in any CCR Titles.

11) Select the Filter icon. Note that 5 records are returned. This is indicated at the bottom of the form, by the text "Record 1 of 5 (Filtered)". The mouse thumbwheel can then be used to view each of the 5 returned AMASS CCRs.

12) Notice that the text searches are case insensitive. In this case, both strings AMASS and Amass provide hits.

13) All of the CCR tool form fields can be similarly searched.

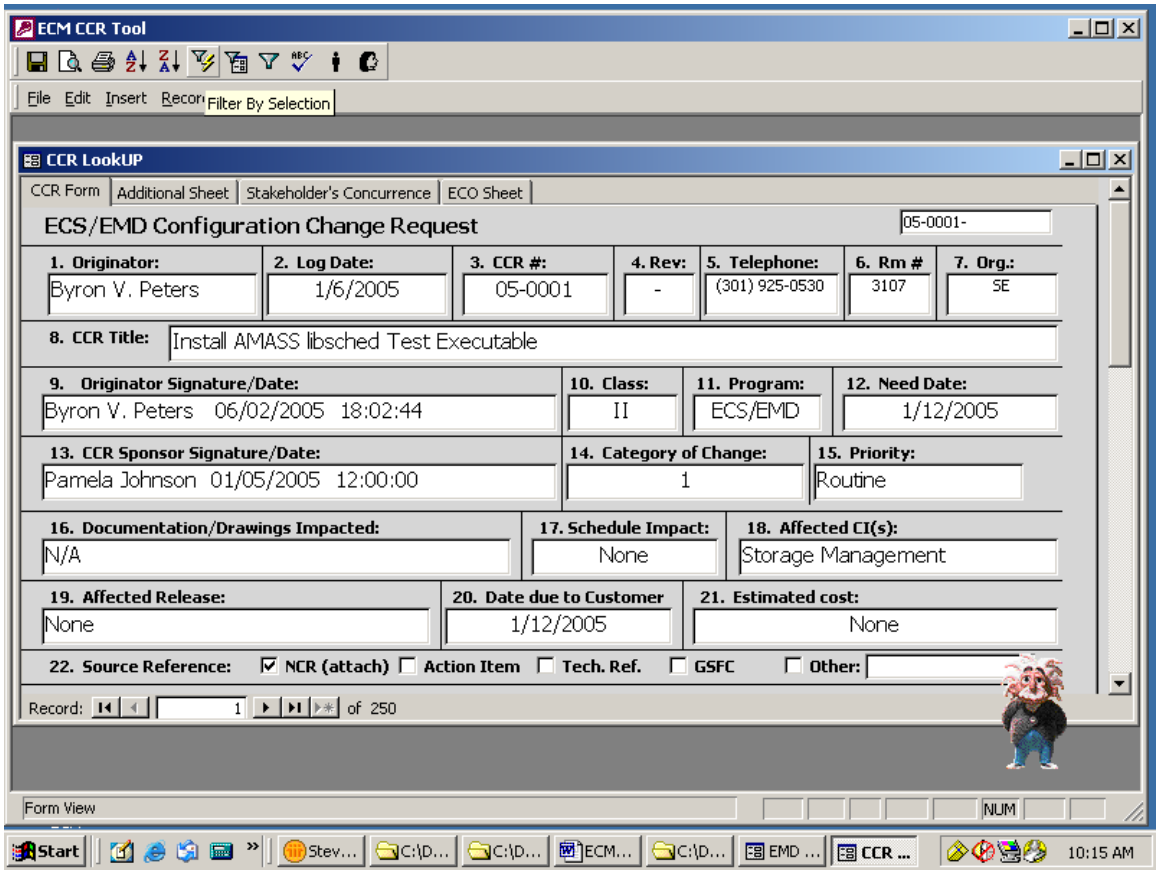


Figure 4.3.2-83. CCR Form Showing Tabs and Filter Controls

4.3.2.11 4.3.2.11CCR Reports

Several CCR Reports can be produced by the CCR tool. To get to the Reporting capability, click the "View reports for CCB meetings, open ECOs, or specific site reports" button on the Main Menu. Below is a brief description of these reports.

4.3.2.11.1 4.3.2.11.1New CCRs

The CCRs are those that are in the CCR database that have not been approved, are not Procurement type CCRs, and are not Draft CCRs. Selecting this button will provide options to Submit, Preview, or Cancel. Typically, Preview is selected just to see the list of new CCRs. A

date field allows an Agenda Date to be selected. Currently, these Agenda Dates fall on Thursdays to support the SCDV CCB.

The Cancel button, when selected, simply returns the User back to the **CCB Agenda CCR Reports** menu.

4.3.2.11.2 4.3.2.11.2Deferred CCRs

These CCRs have been presented to the CCB at least one time, but have been deferred for some reason. Typically, more time is needed to enable the CCR to continue.

4.3.2.11.3 4.3.2.11.3Approved Out of Board CCRs

Most CCRs do not need to be presented at a CCB meeting, and can be approved out of board. An example is a Custom Code type CCR, which is generally approved the same day that it is written. This report function will show these CCRs. The period of time reflected in the report is from the **Begin Date** to the **End Date**, which can be varied according to the User's needs.

4.3.2.11.4 4.3.2.11.4SCDV/DAAC CCB Open ECOs

Engineering Change Orders represent the work of the CCR. Once the CCR is approved, all of its associated ECOs become valid. ECO assignees should try to close the ECOs to the Due Date specified. These reports provide visibility to all approved CCRs' ECOs.

Open ECOs can pertain to the DAACs or Riverdale. This button, when selected, provides the User a choice to select either **Riverdale** or **DAAC**. Also an Agenda date can be entered. This date is used to determine the differences in the ECO due dates with the current date (Agenda date).

4.3.2.12 CCR Tool Problem Reporting

Anyone may create a new Trouble Ticket (TT) to document a problem with the tool. Use Seapine's TestTrack Pro tool to create a new TT. Before writing and submitting a new TT, do the following:

1) Review the ECM CCR Tool User's Guide to determine if you are executing the CCR tool properly. If not, follow the instructions in the guide.
2) Contact the CCR Tool Admin and ask for assistance.
3) Review the existing TTs and determine if your issue has already been reported. This is necessary to avoid duplicating an existing TT.

This page intentionally left blank.

4.3.3 IBM® Rational® ClearCase® Baseline Manager (BLM)

ClearCase BLM is a custom application specifically designed to serve as an efficient configuration management tool to manage the ECS Baseline. It generates and maintains records that describe the compositions of the baseline operational system configurations for the DAACs, ECHO, VATC, PVC, EDF, URS, and Earthdata hosts at Riverdale and the Goddard Space Flight Center. These records identify baseline versions of hardware and software items as well as their relationship. BLM keeps chronological histories of baseline changes and provides traceability to predecessor versions and system releases.

BLM produces 34 html format Technical Documents comprising over 300,000 lines of information.

In addition the tool provides visibility as a function of approved CCRs as well as references to associated Release Notes documents.

These 34 reports are accessible at URLs:

http://pete.edn.ecs.nasa.gov/baseline/	(for Riverdale use only, primary repository)
http://ebis.gsfc.nasa.gov:10160/baseline/	(ESDIS access only)
http://e5iil01v.cr.usgs.gov:10160/baseline/	(LP DAAC access only)
http://l5iil01v.larc.nasa.gov:10160/baseline/	(ASDC access only)
http://n5iil01u.ecs.nsidc.org:10160/baseline/	(NSIDC access only)

The design of the distributed EBIS web servers and reports ensures that the ECS Information System (EBIS) information is secure.

BLM maintainss a set of ClearCase version controlled elements along with scripts and internal information about how they relate. Control item identifier (CID) records represent resources such as COTS software and host names that together form operational systems. BLM's catalog of control item identifiers resides in the /ecs/cm/CIDs directory. The ClearCase BLM tool is an enhanced ClearCase GUI (OSF/Motif) that uses the capability of ClearCase to manage the GUI scripts, records, and posting and replication scripts. Baseline records can only be modified with approved CCRs.

BLM is installed only at the EDF in Riverdale, MD. It is used by CM personnel to manage baseline data about resources deployed to all external ECS sites, including the DAACs, ECHO, as well as the three internal ECS sites, the PVC, VATC, and the EDF. Recent additions include the URS and Earthdata sites.

4.3.3.1 Internal ClearCase BLM Data Constructs

The ECS baseline data for COTS software, COTS software patches, operating systems, operating system patches, data files, databases, ECS hosts and host functions, resides in ClearCase as "text_file" elements. A default configuration specification is used to manage the information using the CM_MASTER view tag name.

A variety of files and methods hold this information and is explained in detail below. Note that the architecture of the data design portion of BLM minimizes the number of steps to update the baseline by implementing newly approved CCRs.

There are 10 data constructs described below. One or more constructs is referenced by scripts in order to generate the specific baseline reports.

4.3.3.1.1 Control Item Identifiers

This describes the Control Item Identifiers (CIDs) for the ECS COTS software. The ClearCase directory that holds all of the CIDs is /ecs/cm/CIDs/. Within this directory are ClearCase text_file elements. Text_file elements are used because they can be directly edited, and they require the least amount space for storage.

Each CID is a Comma-Separated Variable (CSV) formatted file, which means that each of the fields uses a comma (,) as a delimiter. This format was chosen since the files can be readily exported/imported with Microsoft Windows products, such as Excel. The record format for each CID is contained on one line, and consists of 16 items, described below:

1) ECS NAME - This is the name of the ECS COTS S/W, using a familiar nomenclature. The ECS NAME may contain 30 characters or less, with no embedded commas. Other restricted characters are: !, @, #, $, %, ^, &, *, ~, `, ?. These characters have special meaning in the UNIX Operating System.
2) COMMODITY CODE – A character used to convey the procurement nature of the COTS product. This field is 1 character, and can be a "P" to mean Purchased, and "F" to mean Freeware, an "S" to mean Shareware, or a "-" to mean "unknown". These four characters are the only characters known to the algorithms that reference this field.
3) RESP ORG – This is the Responsible Organization, or the group which has the most knowledge regarding the use and placement of the product. A maximum of 6 characters may be used to represent the RESP ORG item within each CID record. A "-" indicates that the RESP ORG is unknown.
4) VARIANT – This item may use at most 10 characters, and is the host operating system that would have this COTS software installed. Current variants are "Linux", "Windows", MacOS, CentOS, VMware ESXi, Solaris, and "JunOS".
5) MFR/DEV NAME – This is the manufacturer or developer of the COTS software. A maximum of 30 characters can be used to represent the name of the manufacturer or developer. A "-" indicates that the MFR/DEV NAME is unknown.
6) VERSION – This is the version of the COTS software. Specifically, the version nomenclature used by BLM is the manufacturer nomenclature. The manufacturer nomenclature may contain "minor" version information that must be represented in the baseline data for accurate tracking and identification. A maximum of 21 characters can be used to represent the VERSION.
7) PRINCIPAL DIRECTORY – A maximum of 50 characters conveys the installation location. Nearly all COTS software resides in multiple sub directories. To keep the installation location reasonable, the highest sub directory is represented. All of the COTS software must reside at the PRINCIPAL DIRECTORY level or lower.
8) CONTROL ITEM ID – A Control Item Identifier (CID) is a 9 character string which uniquely identifies a record with the /ecs/cm/CIDs BLM directory. The first character is always a "b", and is always followed by an 8 character integer. The

storage of this value in the record, which is also the file name within the /ecs/cm/CIDs directory, provided redundancy. CID values range from b00084000 through b00087000.

9) COMMENT – In order to provide further information, a maximum of 60 characters may be used. Commas may not be used, as well as the character set described in the ECS NAME field in 1).
10) CRITICAL ITY – Each COTS software is either Critical or Not Critical. A Critical COTS S/W product is required in order that the custom software may operate on the installed host. The CRITICALITY is either "YES", "NO", or "-" for unknown. This field must be equal to or less than 3 characters in length.
11) ITEM SUBCLASS – A maximum of 7 characters may represent the item subclass. Typical subclasses are "program" or "OS", and describe a major category in which the COTS software belongs. Nearly all CIDs are either "program" or "OS" (Operating System). A "-" indicates that the ITEM SUBCLASS is unknown.
12) REF CODE – A REF CODE may be at most 1 character, and is a Reference Code. A "-" indicates that the Reference Code is unknown.
13) CSCI – Computer Software Component Identification – A CIDs CSCI may be at most 5 characters. A "-" indicates that the CSCI is unknown.
14) RELEASE NOTES – Usually, but not always, a COTS software product uses a Software Release Notes document to provide installation instruction, installation hosts, and a variety of other pieces of information. The format of this record may use a maximum of 16 characters. A typical Release Notes field looks like "914-TDA-349". A "914-TDA-none" is used if the Release Notes is not applicable.
15) CCR – Configuration Change Request. As any baseline change requires a CCR, it is useful to contain this number in the CID record. A CCR may contain up to 7 characters, but usually 6 characters are sufficient. A CCR looks like "14-0123". Revision A to CCR "14-0123" would be "14-0123A".
16) EFFECTIVITY DATE – The BLM tool uses the CCR approval date as the effectivity date The EFFECTIVITY DATE contains 8 characters, and is of the format mm/dd/yy, e.g., "03/20/14".

4.3.3.1.2 Current Hosts List

The Current Hosts list contains all of the ECS baseline hosts. The ClearCase path is "/ecs/cm/host_data/current_hosts". The UNIX file date for this file is the timestamp to indicate when the file was last changed.

There are as many lines to the file as there are current hosts. There are four fields within each record. Column 1 is the ECS host name. Column 2 is the ECS sub system to which the ECS host belongs. Column 3 is the CSCI for the ECS host, and column 4 is the ECS host major function.

1) ECS Host Name – This is the string returned from "uname –n" while logged onto the ECS host. Host name formats are 7 letters, generally. The first letter designates the ECS site, "e" for EDC, or LP DAAC, "c" for ECHO, "l" for LaRC, or ASDC, "n" for NSIDC, "p" for PVC, "t" or VATC, "f" for EDF, and "D" for Earthdata. Also, the letters "c", "d", "f", and "i" designate the Riverdale Linux Evolution hosts. (e.g.,

"c5cbl01v"). ECHO host names do not follow ECS naming conventions but are alphabetic strings from between 3 and 10 characters. URS host names begin with the string "urs". Earthdata host names are functional in nature.

2) ECS Host Subsystem – This is the ECS functional component. The sub system name is three letters followed by the word "Subsystem". The second column is always exactly 13 characters long, e.g "AST Subsystem".
3) CSCI – A specific set of up to 5 characters which identify the Computer Software Component Identification.
4) ECS Host Major Function – Each ECS host exists for a purpose. The purpose is stated in column 4 of this construct, and may contain a maximum of 30 characters.

4.3.3.1.3 Data List

There are two entities that are present in the reports, "data" and "databases". The Data List construct exists to provide the "data". This construct path is /ecs/cm/BLM/host_data/data, and is a ClearCase text_file element that is directly editable. It is a CSV formatted file.

Each record (line) within this file is comprised of 7 fields:

1) ECS Host Name – This is the name of the hosts, e.g., "e5eil01". The name can be a maximum of 10 characters.
2) Data Name – This is the data that is conveyed by the Construct. A typical data name is "Production data", or "Ingest files". The Data Name can have a maximum of 50 characters.
3) Data Version – This is the version of the Data Name. This can be at most 7 characters, and represents the major version of the data, such as "REL 8.3".
4) Data Construct Type – For this construct, the fourth field must always say "data".
5) Data CID – Data Control Item Identifier. This field has a CID format entry, and has to be exactly 9 characters in length.
6) Data CSCI – Computer Software Component Identification – A CSCI may be at most 5 characters.
7) Data Responsible Organization – The ECS organization who isthe owner of the data. This field may be a maximum of 6 characters.

4.3.3.1.4 Databases List

There are two entities that are present in the reports, "data" and "databases". The Databases List construct exists to provide the "databases." This construct path is /ecs/cm/BLM/host_data/databases, and is a ClearCase text_file element that is directly editable. It is a CSV formatted file.

Each record (line) within this file is comprised of 8 fields:

1) ECS Host Name – This is the name of the hosts, e.g., "e5eil01". The ECS Host Name can be a maximum of 10 characters.
2) Database Name – This is the data that is conveyed by the Construct. A Database Name example is "AIM DB". The Database Name can have a maximum of 50 characters.
3) Database Version – This is the version of the Database Name. This can be at most 7 characters, and represents the major version of the database, such as "8.3".

4) Database Construct Type – For this construct, the fourth field must always say "database".
5) Database CID – Database Control Item Identifier. This field has a CID format entry, and has to be exactly 9 characters in length.
6) Database Code – A single character, either blank, or the letter "I".
7) Data CSCI – Computer Software Component Identification – A CSCI may be at most 5 characters.
8) Data Responsible Organization – The ECS organization who is the owner of the database. This field may be a maximum of 6 characters.

4.3.3.1.5 Hosts' Functions List

In the ClearCase BLM 920-TDx-002 Hardware/Software Map reports, there may be a few lines, just after the host name, that describe more host attributes, or functions, such as " FLEXnet License Server", or "NIS Master Server". This construct path is /ecs/cm/BLM/host_data/host_functions, and is a ClearCase text_file element that is directly editable. Each record consists of two column groupings.

Each record (line) within this file is comprised of the following:

1) ECS Host Name – This is the name of the host, e.g., "e5eil01". The ECS host name has a maximum of 10 characters. The ECS host name must begin in column 1.
2) Host Function – This is a text string with a maximum of 50 characters. This descriptive text provides information regarding host functionality. The Host Function text must begin in column 14, in order for the data to align correctly in the reports. Embedded commas are permitted in this construct.

Note that the spacing of the host name and the text appears in the record lines exactly as in the output 920-TDx-002 reports. No reformatting of the data is performed in the generation of the reports.

4.3.3.1.6 4.3.3.1.6 Control Item Identifier Type List

Another piece of information is required for the 920-TDS-004 report. This is the CID category. Examples of these are: Compilers, Editing & Viewing, Operating Systems, and the like.

Each record of this file consists of two column groupings:

1) Functional Group Name – The first character of the string must be placed in column 1. The string length may be up to 38 characters.
2) CID – Control Item Identifier number. This number must exist with the /ecs/cm/CIDs directory, described above as Data Construct 1. The 9 character CID must begin in column 39.

4.3.3.1.7 Operating System Patch Sets

These are sets of information residing in the directory /ecs/cm/BLM/patch_sets/. There are about 20 patch sets that are named according to their function. A patch set name may be up to 30 characters in length. An example Patch Nomenclature name is "RedHat_6.5_core". Each line within a patch set (record) is comprised of 6 column groupings, and are described below:

1) Patch Nomenclature – This is a name of the patch set. The string must start in column 4, and may use up to column 27, for a total maximum character length of 24 characters.
2) Patch Description – A comment-like character string that adds information value and detail to the Patch Nomenclature. This data must start in column 29 and be complete by column 83 (or a maximum string length of 55 characters).
3) Patch reference – With each patch release, there is a related Release Notes Technical Document, e.g., 914-TDA-430, or a related Patch Technical Document, such as 911-TDA-034. This field begins in column 85 and is 16 characters in length (to column 101).
4) CCR – This is the CCR number which authorized the patch set's placement in the ECS baseline. Columns 107 through 114 contain the CCR number.
5) Release Notes tech doc - With each patch release, there is a related Release Notes Technical Document, e.g., 914-TDA-430. This field begins in column 118 and is 16 characters in length (to column 133).
6) ECS Subsystem – Up to three characters long, this field relates the patch information to the sub system, such as "IDG".

Note that the column positions are critical; the generated 920-TDx-014 Operating System Patch Maps take these records and directly import them into the records with no reformatting.

With the introduction of the Linux Operating System, all Operating System RPMs (Package Manager) are now carried in the baseline. Please reference the new EBIS Technical Document 911-TDA-035, for example, to view the Red Hat Linux Release 6 update 4 method for patching the Operating System.

4.3.3.1.8 Configuration Change Request (CCR) Data

The BLM Tool relates all change requests to the items changed, including an effectivity date. This construct exists as directory /ecs/cm/CM. Under this directory are sub directories, one for each CCR year. For the year 2014 the sub directory name is 2014_CCRs. So any 2014 year CCRs are found in the path: /ecs/cm/CM/2014_CCRs/.

For each CCR, another sub directory exists, which consists of the last four digits of the CCR, or five digits if the CCR has been revised, like "0123A". The first two digits of the CCR represent the year. So for the example of the CCR 14-0123A, a directory /ecs/cm/CM/2014_CCRs/0123A/ exists. This constructprovides the relations of the CIDs to the ECS hosts. For each CCR sub directory, there are the following sub constructs:

1) "CID_map" file – This file, always named "CID_map", provides the relations of the Machine Impacted file(s) (MI) to the CIDs. It always has at least one line, but may contain more than one line, as a single CCR may relate more than one CID to a host set (MI) file. It has two columns. The first column is the name of an "MI" file, up to 20 characters in length.
2) "MI" file(s) – This is an abbreviation for the "Machines Impacted" file. The source of this information is derived from the CCR's Release Notes document (914-TDA-xxx) or Installation Instruction. Within the Release Notes document is a section that describes ***which hosts*** should receive ***what COTS software***. Most CCRs have a CID_map file with only one MI and CID.

4.3.3.1.9 ClearCase BLM Sequencer

File "/ecs/cm/BLM/scripts/Sequencer" controls which CCRs are applied to the baseline and in what order. This editable yet executable file provides the mechanism for relating the application of CCRs, their MI files and CID_maps, to populate what is known as the "dartboard" area. The first record in this file applies the first CCR to a "null," or empty baseline. The last record applies the last CCR to the "dartboard". The format of each record of this file is:

1) Function Call – This is always the same string, "/ecs/cm/BLM/scripts/Implement_CCR". This function applies the first argument of the call, which is the CCR, to the "dartboard".
2) CCR – Configuration Change Request. A number that identifies a change to a baseline. It authorizes the application of a COTS software product to an ECS host or set of ECS hosts.
3) Comment 1 – This comment is the "function", or COTS software name, of the CCR.
4) Comment 2 – The CCR approval date (Effectivity Date)
5) Comment 3 – This is the Release Notes Technical Document number which is referred to in the CCR.

4.3.3.1.10 ClearCase BLM Dartboard

The ClearCase Derived Objects, located within the "/ecs/formal/BLM/dartboard" directory, comprise the Dartboard. This directory contains one file representing the collective assembly of all applicable COTS S/W products as authorized by approved CCRs for each ECS host. COTS software application is performed by using file concatenation. The earliest approved CCRs appear first in these dartboard files. The last approved CCR appears as the last entry in these files.

Each dartboard file name is an ECS host name like "e5eil01".

The format of each line in a host dartboard file is as follows:

1) ECS host name – This is the ECS host name.
2) Authorizing CCR – This is the CCR from the Sequencer file.
3) BLM Tool user – This is an authorized User of the ClearCase BLM tool.
4) Timestamp – This is the time at which the CCR was applied to the file in the dartboard.
5) CID – This is the entire contents of the CID record, as specified by the CCR's CID_map, MI files, and CID reference.

Note that Data Construct 10 is a ClearCase derived object, and is not "checked-in" like the first Data Constructs. The dartboard directory in conjunction with the "/ecs/cm/BLM/host_data/current_hosts" file is used to populate the 920-TDx-002 Hardware Software Map Technical Documents.

4.3.3.2 ClearCase BLM Graphical User Interface (GUI)

The ClearCase BLM tool makes use of an OSF Motif graphical user interface. This provides convenient drop down menus, and provides a convenient method for dynamically formulating the contents of the drop down menus. The ClearCase BLM tool runs on the Red Hat Linux

operating system. It is always launched on Linux host "c5cbl01v." The GUI uses "gedit" for text editing.

4.3.3.2.1 ClearCase BLM Main Menu

Select the "New_CCR" item from the BLM Main Menu. Use this to step through the process of producing the new baseline reports. This document provides instructions for SDPS although the other sites are processed similarly. The other sites are ECHO, URS, and Earthdata.. The design of the tool's GUI has been optimized to minimize the steps and time needed to create the reports. Refer to Figure 4.3.3-1 to view BLM Main Menu.

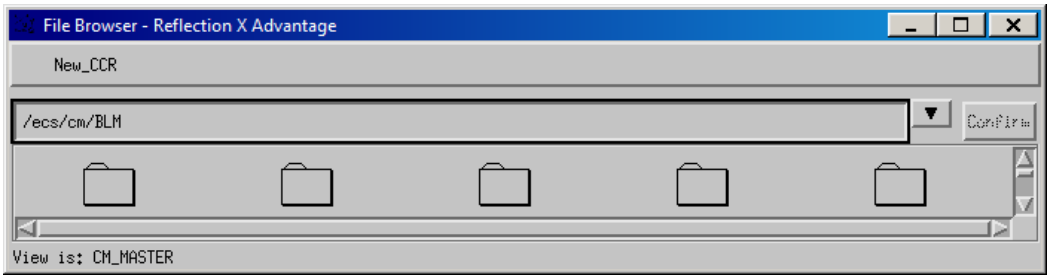


Figure 4.3.3-1. BLM Main Menu

4.3.3.2.2 BLM "Modify SDPS Sequencer"

The Sequencer is shown in Figure 4.3.3-2 below. This figure shows the last entries of the Sequencer. Usually the CCR is added to the end of the Sequencer. The entries are ordered according to approval dates. Sometimes, earlier entries or CCR constructs may need to be removed, so that the previous version of a COTS product will not appear in the 920-TDx-002 reports. The Sequencer is internal to the tool and is not exported.

Other less frequently used data may need to be altered, and again this depends on the nature of the CCR. To remove an ECS host for example, select the "Update Current ECS Hosts" menu line item, and delete the ECS host. If a new CID is added to the database, its function must also be added using the "Update CID Functions" line item.

There are four site baselines that are managed, SDPS, ECHO, URS, and Earthdata. SDPS includes the LP DAAC, ASDC, NSIDC, PVC, EDF, and VATC environments.

Each site has five components, "Modify Sequencer", "Modify CIDs", "Modify Hosts", "Build Baseline", and "Promote Baseline".

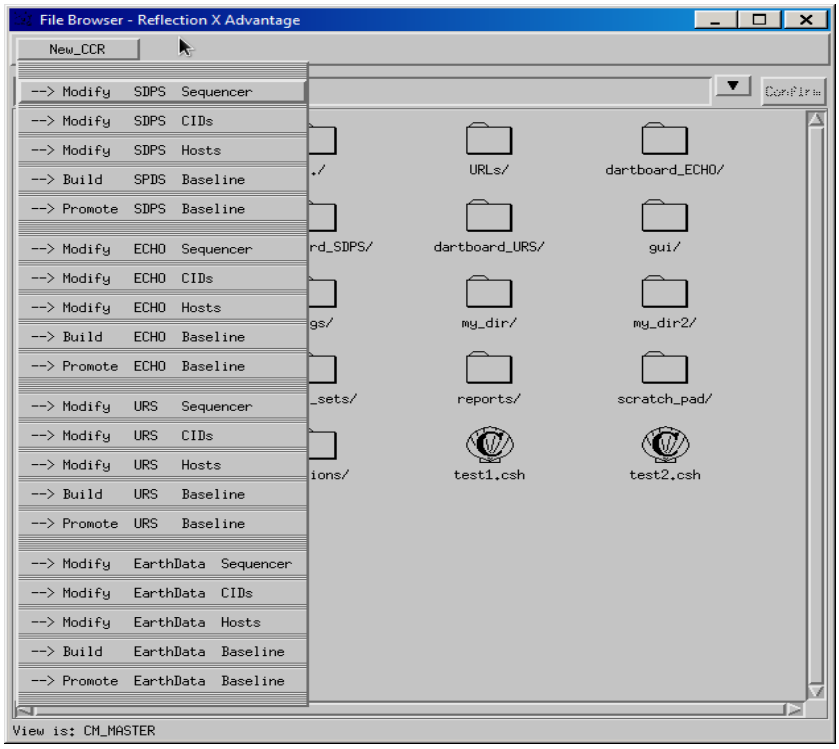


Figure 4.3.3-2. BLM New_CCR Drop Down Menu

4.3.3.2.3 BLM "Modify SDPS Sequencer"

The Sequencer, depicted in Figure 4.3.3-3 is then updated. The new CCR is added to the Sequencer by its approval date shown in column 4. Earlier entries or CCR constructs may need to be modified so that the previous version of a COTS product will not appear in the 920-TDx-002 reports. The Sequencer is internal to the tool and is not exported.

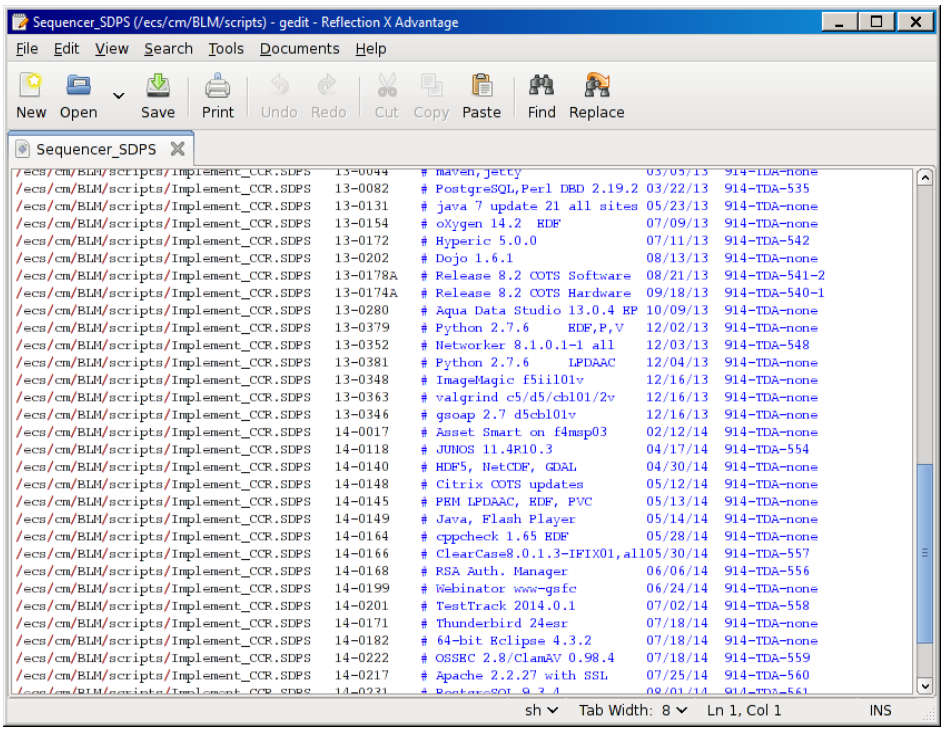


Figure 4.3.3-3. BLM Modify SDPS Sequencer

4.3.3.2.4 BLM "Modify SDPS CIDs"

Selection of the "Modify SDPS CIDs" menu item enables the modification of the SDPS CIDs file. See Figure 4.3.3-4 below for the typical content of the "CID_functions_SDPS" file. There are three columns showing the CID category, CID, and contract. The CID list is alphabetically sorted. This file is used primarily to generate the 920-TDS-030 Where-Used Report for the LP DAAC, ASDC, NSIDC, PVC, VATC, and EDF environments.

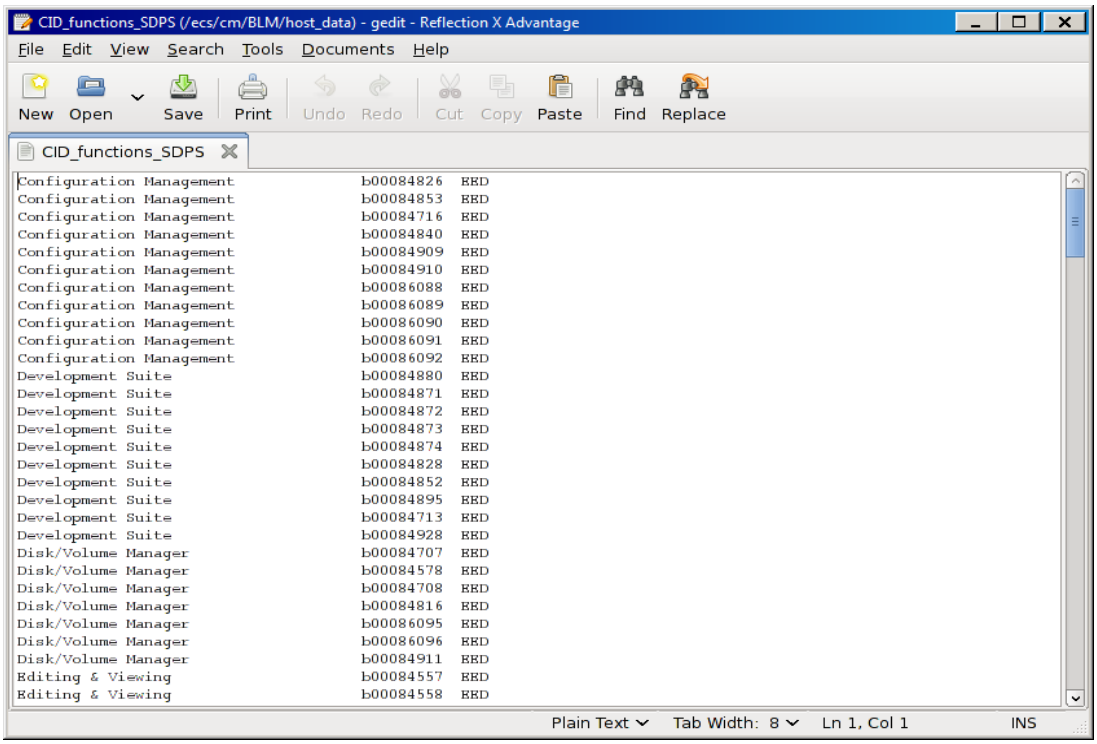


Figure 4.3.3-4. BLM Modify SDPS CIDs

4.3.3.2.5 BLM "Modify SDPS Hosts"

Selection of the "Modify SDPS Hosts" menu item enables the modification of the SDPS host list file. See Figure 4.3.3-5 below for the contents of file "current_hosts_SDPS'. There are four columns showing the host name, host subsystem, HWCI, and the host's functional name. The host list is alphabetically sorted by host name. This file is used primarily to generate the 920-TDS-005 SDPS Hosts report. It is also used to generate the 920-TDx-002 Hardware-Software Reports for the DAACs, PVC, VATC, and EDF environments.

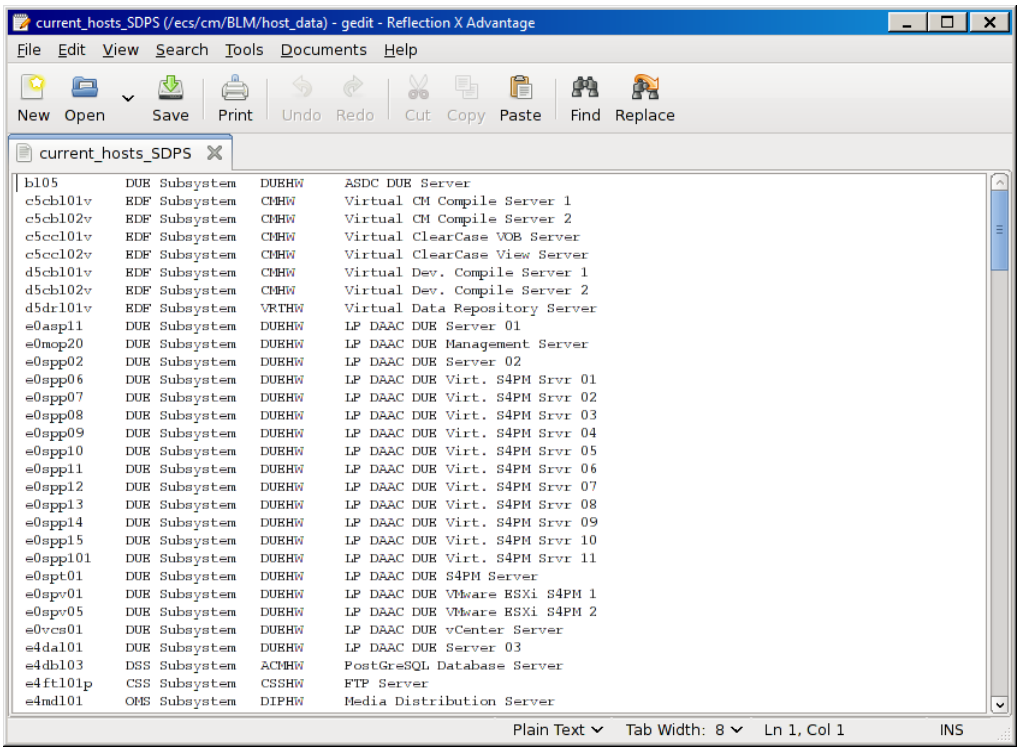


Figure 4.3.3-5. BLM Modify SDPS Hosts

4.3.3.2.6 BLM "Build SDPS Baseline"

Selection of the "Build SDPS Baseline" menu line item will generate all of the new baseline technical documents for SDPS and place them on the primary EBIS server at Riverdale in the /QA_Check/ directories for review. This ensures that there is a step to ensure correctness before the "Promote SDPS Baseline" step. The message below shown in Figure 4.3.3-6 appears and stays until the baseline build is complete.

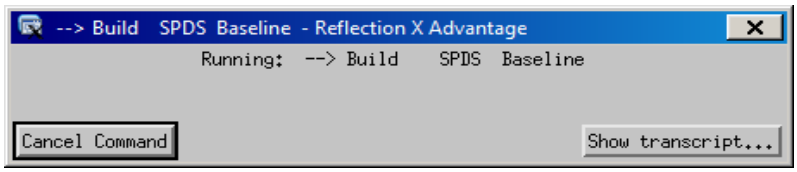


Figure 4.3.3-6. BLM SDPS Baseline

4.3.3.2.7 BLM "Promote SDPS Baseline"

Selection of the "Promote SDPS Baseline" menu item will move (promote) the newly generated versions of the 34 reports from all of the "/QA_Check/" directories in the Riverdale EBIS file system to all of the /Current/ directories. Secure shell scripts are then executed to replicate the new reports to the 4 remote EBIS sites to include LP DAAC, ASDC, NSIDC, and the EBIS server for ESDIS. The previously /Current/ versions are moved to the /Previous/ directories. The reports are discussed in Section 4.3.3.3 below.

All document versions are increased by "1" and the revisions updated on the Technical Documents web pages. A time stamped log file is written to /ecs/cm/BLM/logs.

4.3.3.3 ClearCase BLM Reports

The 34 reports that are automatically produced by the ClearCase BLM tool are listed in Table 4.3.3-1. A total of over 300,000 lines of configuration data are in all of the reports.

Table 4.3.3-1. BLM Produced Reports (1 of 2)

Document Number	Title
920-TDE-002	LP DAAC Hardware-Software Map Report
920-TDL-002	ASDC DAAC Hardware-Software Map Report
920-TDN-002	NSIDC DAAC Hardware-Software Map Report
920-TDV-002	VATC Hardware-Software Map Report
920-TDP-002	PVC Hardware-Software Map Report
920-TDF-002	EDF Hardware-Software Map Report
920-TDC-002	ECHO Hardware-Software Map Report
920-TDU-002	URS Hardware-Software Map Report
920-TDD-002	Earthdata Hardware-Software Map Report
920-TDS-004	SDPS COTS Software Baseline Report
920-TDC-004	ECHO COTS Software Baseline Report
920-TDU-004	URS COTS Software Baseline Report
920-TDD-004	Earthdata COTS Software Baseline Report
920-TDS-005	SDPS Hosts Report
920-TDC-005	ECHO Hosts Report
920-TDU-005	URS Hosts Report
920-TDD-005	Earthdata Hosts Report
920-TDS-007	SDPS Critical COTS Software Report

Table 4.3.3-1. BLM Produced Reports (2 of 2)

Document Number	Title
920-TDC-007	ECHO Critical COTS Software Report
920-TDU-007	URS Critical COTS Software Report
920-TDD-007	Earthdata Critical COTS Software Report
920-TDE-014	LP DAAC Hosts' Operating System Patches Report
920-TDL-014	ASDC Hosts' Operating System Patches Report
920-TDN-014	NSIDC Hosts' Operating System Patches Report
920-TDV-014	VATC Hosts' Operating System Patches Report
920-TDP-014	PVC Hosts' Operating System Patches Report
920-TDF-014	EDF Hosts' Operating System Patches Report
920-TDC-014	ECHO Hosts' Operating System Patches Report
920-TDU-014	URS Hosts' Operating System Patches Report
920-TDD-014	Earthdata Hosts' Operating System Patches Report
920-TDS-030	SDPS Where-Used Reports
920-TDC-030	ECHO Where-Used Reports
920-TUA-030	URS Where-Used Reports
920-TDD-030	Earthdata Where-Used Reports

These reports are viewable at URLs provided below.

http://pete.edn.ecs.nasa.gov/baseline/ (for Riverdale use only, primary repository)

http://ebis.gsfc.nasa.gov:10160/baseline/ (ESDIS only)

http://e5iil01v.cr.usgs.gov:10160/baseline/ (LPDAAC only)

http://l5iil01v.larc.nasa.gov:10160/baseline/ (ASDC only)

http://n5iil01u.ecs.nsidc.org:10160/baseline/ (NSIDC only)

The design of the distributed EBIS web servers and reports ensures that EBIS information is secure. Access to the EBIS URLs at the DAACs is managed by the DAACs. To see those URLs the person must have a UNIX account at the site. The EBIS ESDIS page is sponsored on the c5cbl02v host in the EDF and is managed using firewall rules. Riverdale access is provided to those persons have a UNIX account within the EDF. All pages use Apache as the web server. With the exception of the Riverdale c5cbl02v EBIS server there is an additional level of security by requiring the use of port 10160.

As a convenience a Riverdale Orion network EBIS instance is provided on a shared Windows network drive and is located at V:\Core\EED\EBIS\baseline. Those persons listed at the V:\Core\EED have access to this EBIS file system. This prevents all other Raytheon staff for viewing this EBIS instance. The Orion EBIS is traversable without an Apache web server.

These reports are subsequently used as baseline references for configuration audits. The reports serve as the reference during the audit. Host interrogations provide the as-built configurations. The audit compares the baseline to the as-built reports.

4.3.4 AssetSmart-ILM (Inventory, Logistics and Maintenance (ILM) Manager)

The EDF replaced the previous Remedy system with the AssetSmart COTS package. AssetSmart will be used to implement the Inventory Logistics Management (ILM) capabilities. The basic ILM activities are still regularly performed but now rely on the AssetSmart COTS package instead of the Remedy COTS package.

The ILM Property Custodian and Property Maintenance Engineer are the principal users of ILM system capabilities. The ILM tool will be centralized at the EDF in Riverdale, and will be accessible via the AssetSmart web-interface. Asset Smart improves the current system and processes by providing modules that allow for less data redundancy, appropriate allocation of funds, unified transaction logs, and remote accessibility. This software integrates mission critical real time data with process improvements to provide seamless asset investment planning, asset record management, acquisition, maintenance, EIN Structures, location and asset change tracking, property moves, shipments and installations, utilization status, consumable tracking, disposal and real time asset reporting-empowering the EED property team and equipment end users to make more timely and cost effective decisions, leading to better infrastructure management and customer support.

The EDF maintains the principal data repository and processes all inventory changes. AssetSmart ILM will have the largest positive affect on the other sites, (ASDC, LPDAAC, NSIDC, and ECHO) that has no real-time access to the Remedy- ILM. The AssetSmart ILM tool will provide the other sites via the Internet the ability to view a read only version of the ILM database in order to gain knowledge of system maintenance information before contacting the ILM Property Maintenance Engineer. Through the use of a centralized repository the data will be more searchable, complete, accurate and auditable.

The Asset Smart ILM primary function will be to maintain a system-wide inventory of all hardware and COTS software contained within ECS project. Each inventory item is identified by a unique equipment inventory number (EIN). The most significant relationship maintained among inventory items is EIN structure. EIN structure is the pairing of a parent EIN with its components to define the configuration for an assembly. Each EIN structure has active and inactive dates that establish the time frame during which the pairing is in effect. For tracking and auditing purposes, inventory items (especially hardware), get allocated to ECS parent machines, and some of the items are shipped to sites and installed. After a period, some items may be transferred to other locations or relocated for use with other parent machines. Items are archived when no longer needed or serviceable. Management of consumables is similar to managing spares. Consumables are located centrally at the EDF and at the DAACs. The Property Custodian will control the use of consumables and may request additional consumables.

With the Asset Smart tool, EED will be able to manage and organize all CAP, GFE and IAGP property assets and financial information in a single unified repository that maintains full interactive updates, field validation, and online history of all property transactions. With Asset Smarts Customizable security-protected menus, customizable navigation links and shortcuts, and direct screen to screen navigation, Asset Smart will fit the needs of all end users from Property Administrators to System Hardware and Software engineers.

This document will discuss Asset Smarts primary operational uses and highlight key functionalities. For more information regarding the more advanced modules and functions please refer to the Asset Smart PEMS help manual.

4.3.4.1 Asset Smart Modules

Two modules of AssetSmart were purchased for the use of the problem. SMART|PEMS and SMART|AMIIX which are both outline below.

4.3.4.1.1 SMART|PEMS

The Asset Smart Property and Equipment Management System deliver substantial cost savings and process improvement benefits to EED. The application offers comprehensive tracking and management of company and government property, reducing asset downtime, maintenance and management costs and increasing asset utilization and redeployment. Asset Smart will optimize lifetime value of assets by integrating asset planning/acquisition/tracking/ disposal/investment recovery phases into a cohesive continuum.

PEMS Features include:

- Asset Smart's open user architecture enables EED to maintain all mission critical asset data in a single integrated repository which standardized business processes across the entire project and significantly increasing efficiency.
- Asset Smart has a web interface which enable interactive accessibility worldwide to the EED users. Property Managers and end-users can access real-time asset data from any web browser worldwide.
- Asset Smart has powerful online search tools which allow users to search by any tracked attribute to find required information.
- All interfaces, menus, attributes, business rules, status tracking and data fields can be customized to meet requirements, without requiring significant consulting or configuration by Asset Smart engineers.
- Asset Smart is FAR compliant and has added features that integrate with multiple federal reporting systems such as PCARRS, NASA1018, CHATS, DD250, and the 20-4.

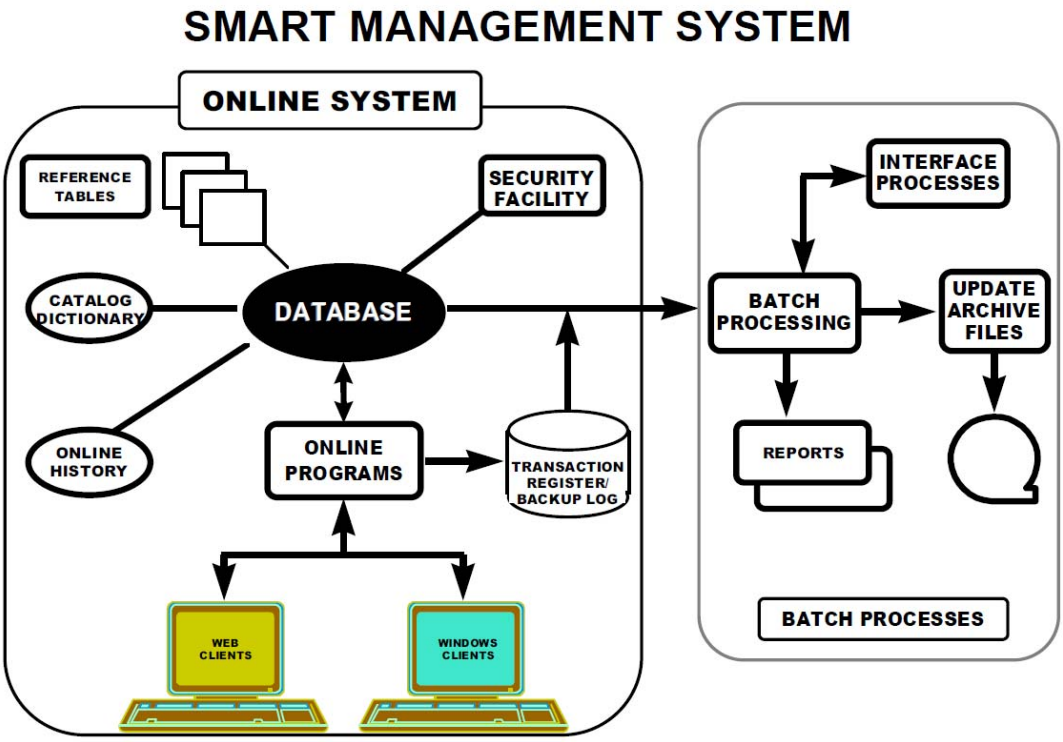


Figure 4.3.4-1. Smart Management System

4.3.4.1.2 SMART|AMIIX

Mobile Work Management Module is a server-based management module that allows for real-time status tracking of unlimited working inventory sets. AMIIX is compatible with Oracle and SQL Server, and runs completely hardware independent, as a disconnected (or connected) operation model. When inventory is completed, AMIIX seamlessly uploads data back to the server, allowing for full online review and approval. AMIIX allows EED to simplify life cycle of asset management and maximize utilization of idle resources.

AMIIX features include:

- Improved data integrity across the life cycle asset management system, eliminating errors and duplicates and ensuring accurate reporting maximized asset utilization across the enterprise.
- Improved speed and access to real-time, accurate inventory information.
- An integrated, one-stop solution for managers and end-users to review and approve inventory data.
- An external interface that can hook into any outside application or data source via API and backend staging tables.

- Compatible with Microsoft SQL Server, Oracle and any other SQL compliant data source.
- Mobile Technology:
    - Developed on the Microsoft .NET Compact Framework
- Microsoft SQL Server Compact Database backend:
    - Hardware Independent
- Compatible with any device running Windows Mobile 5.x or higher.
- Supports both a disconnected and connected operation model.
- Supports Secure Socket Layer (SSL) Security.
- Requires NO middleware software, device communicates directly with the Web Service.

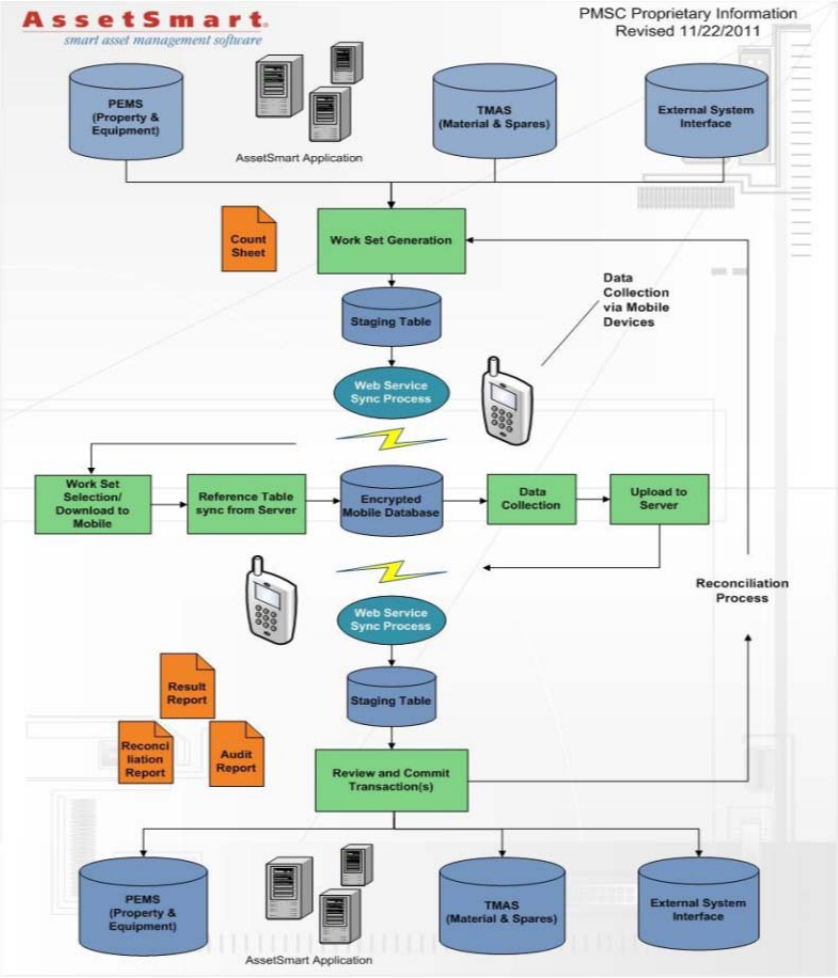


Figure 4.3.4-2. Process Flow

4.3.4.2 Accessing the Asset Smart Application via Web

Asset Smart is located at the following URL

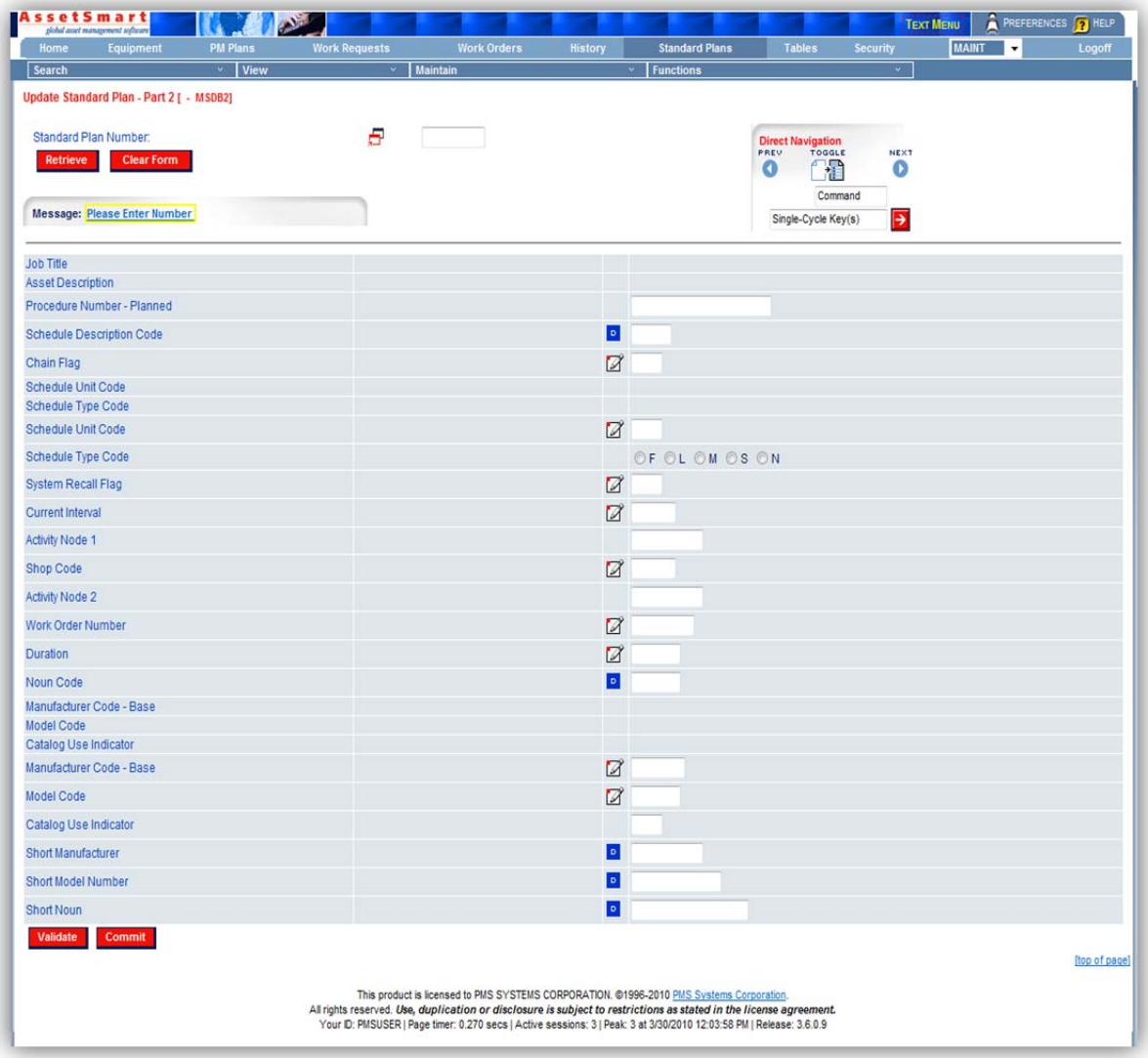
http://155.157.31.126/smart36/

To Log on, you must enter your User ID and Password on the Logon page to access the Main Page.

Main page appears after log-on

The main Navigation feature is the top menu bar, used for accessing screens with drop-down menus.

Two major regions are featured in a transaction screen: Header and Body



4.3.4.3 Asset Smart User interactive Roles

There are ideally four main user types that will interact with the Asset Smart System on a consistent basis. More information regarding the Asset Smart users' processes are outlined and explained in detail in the EED Property Management Plan as well as the EED Process Property Document.

Table 4.3.4-1. Common Users and Operations Performed with Asset Smart

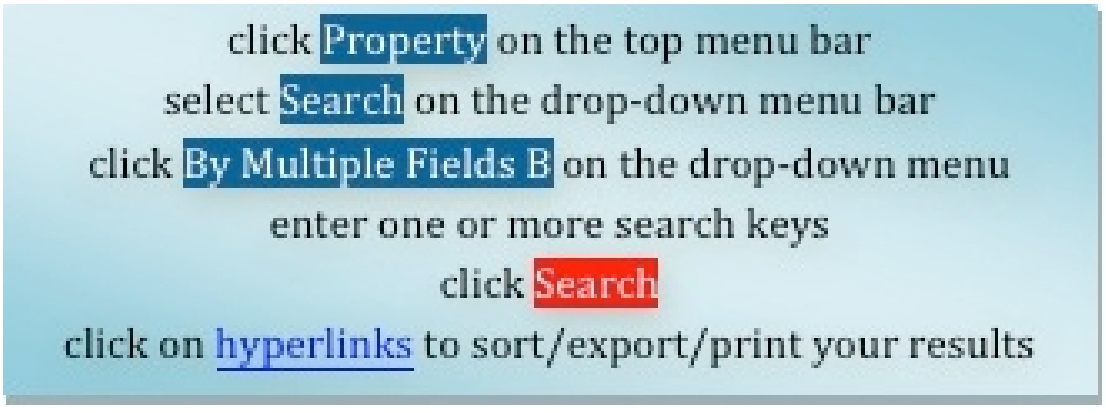
Operating Function	Description	When and Why to Use
General	Search for property items using a specified query performed by a hardware engineer or management	To search for information regarding a item or data set in regards to its location, maintenance information, vendor, etc
Property Management	Maintain information about accountable property items, their product structures, and inter-relationships.	To maintain information that specifies the identity, source, location, transfer, relocation, and installation of procured inventory items.
Property Maintenance	Manage information for required maintenance repairs.	To predefine and monitor scheduled maintenance activities.
System Administrator/Power User	Manage System updates and install patches and implement security roles.	To revise, add, or delete Asset Smart users, security levels, and access permissions.

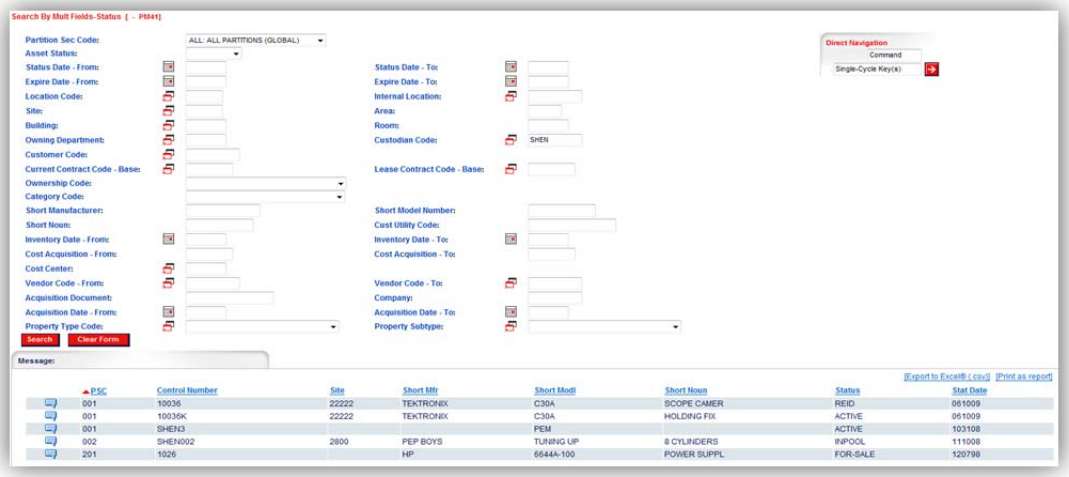
4.3.4.3.1 General Functions

All general functionalities are performed by every functional role and will be accessible to all users.

4.3.4.3.1.1 Search by Multiple Fields

PM41 lets you search Master Property Records by means of a selection of entry keys. Use the drop-down lists and pop-ups provided, when available, to enter your search values. Any combination of searches is supported as long as you enter at least one search key. Your records will be displayed sequentially by number. You have the option to sort and/or print and/or export as .csv (data repository) files these one-line summaries, by clicking on the related links.



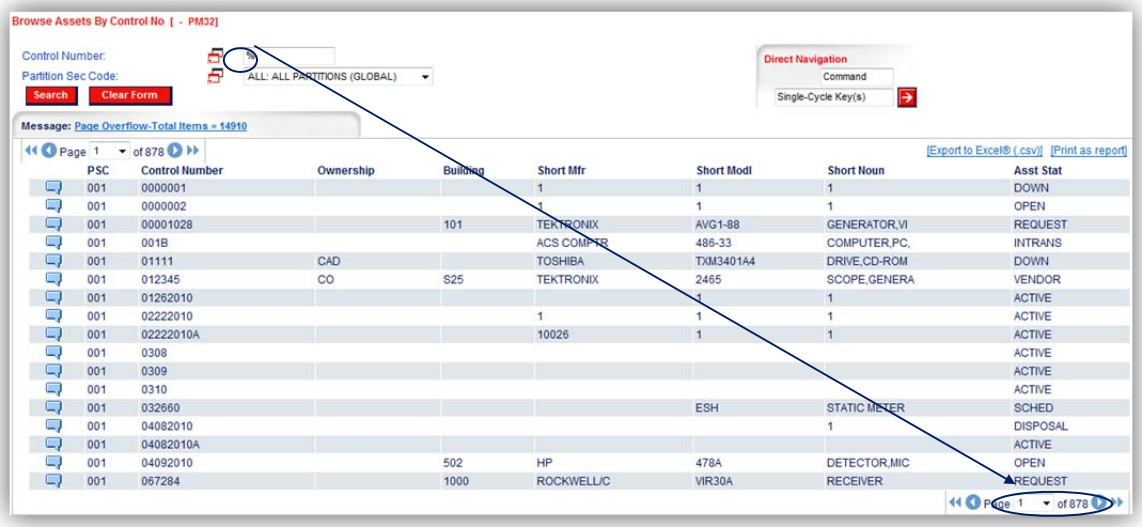


PM2, PM5, PMD4, PSD4, PMDR1, PLD4,

4.3.4.3.1.2 Partial String Search

Partial string searches are available on all transaction screens where they may be of use

They are an easier and speedier way to make inquiries because they allow you to only enter part of a search key (number or code). A variety of options is available: the simplest is to enter a *percentage sign* [%] or a *forward slash* [/] in the search key field and retrieve all records. In the example below, 878 pages of items are returned.

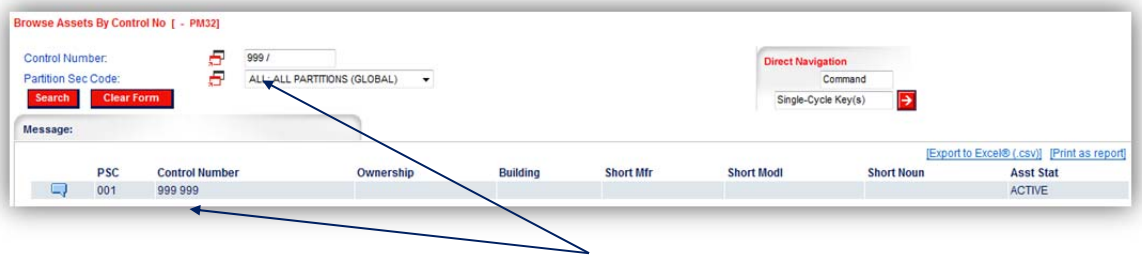


4.3.4.3.1.3 Enter a leading string to narrow your search

A partial string can originate from the beginning, anywhere in the middle, or the end of the search key.

To narrow down your search, the easiest option is to simply enter the first few characters of the search key, i.e., a leading string.

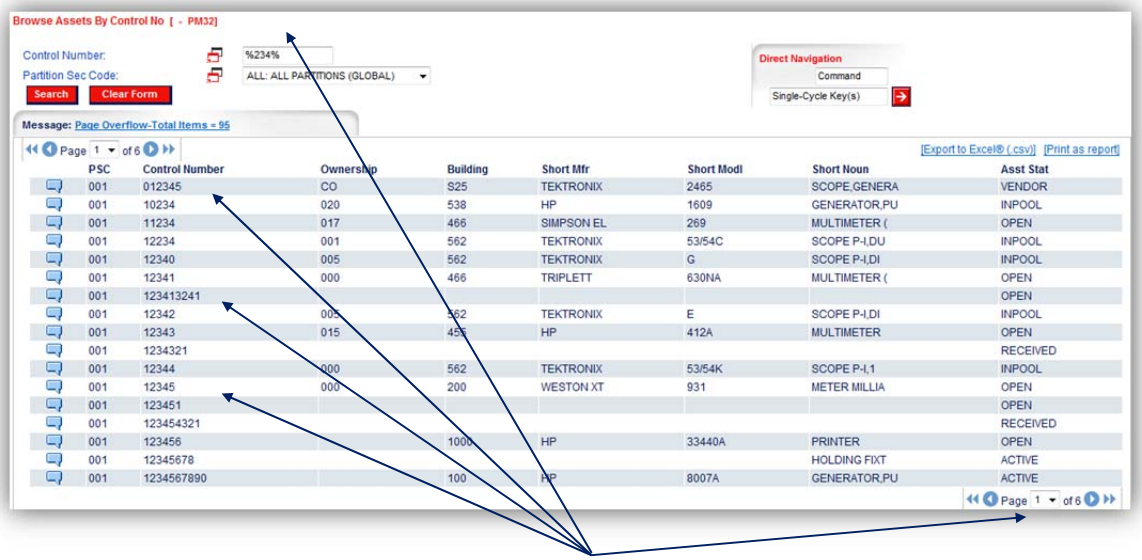
Follow a leading string that has trailing spaces with a [%] or [/]



Enter '999 /' or '999 %' to display all control numbers starting with '999' followed by a space

4.3.4.3.1.4 Place a [%] before and after a string

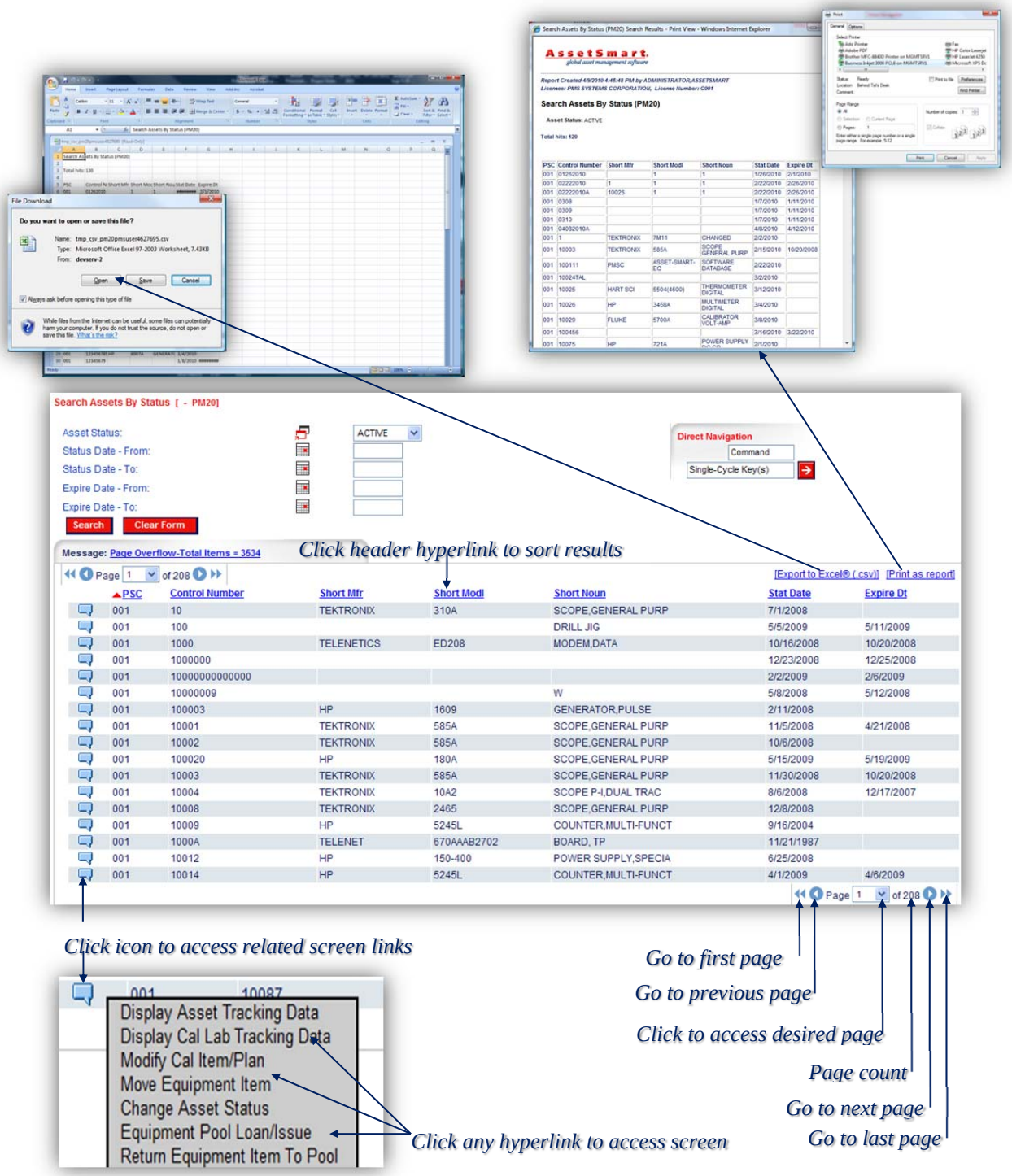
In order to search via a string originating from anywhere (including the beginning and the end) within the search key, the string must be led by a percentage sign or surrounded with percentage signs.



Enter '%234%' or ' %234' to display all control numbers containing that string

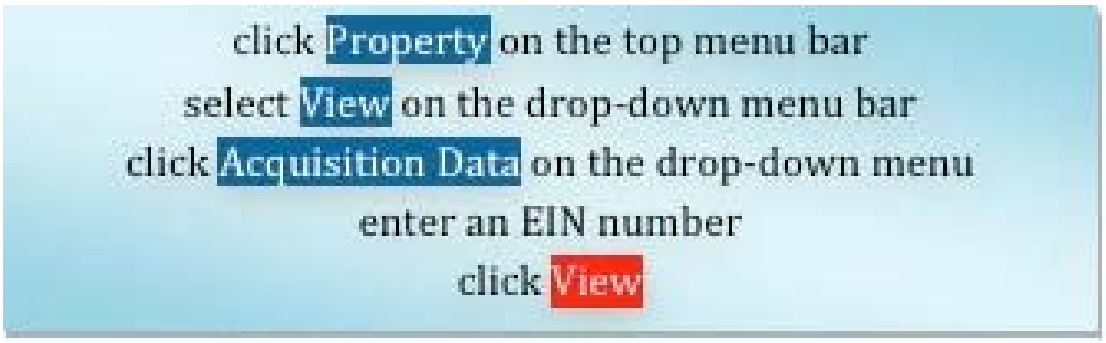
Search screen types display one-line summaries of the resulted records

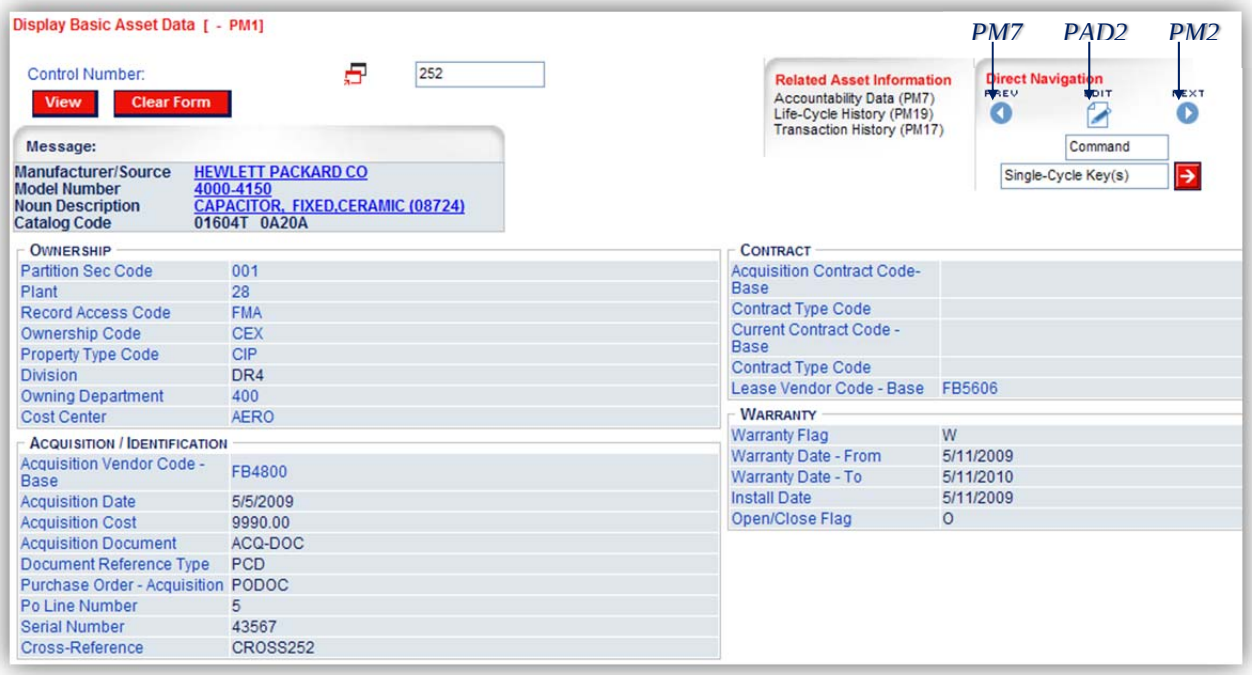
You may avail yourself of capabilities such as scrolling through pages, sorting your results, exporting them to an Excel file and printing them. Each resulted record may also be accessed with related screens.



4.3.4.3.1.5 View Transaction

PM1 lets you view data from a Master Property Record by means of its EIN Number. The fields displayed by PM1 have previously been entered/updated with PAD1/2, PBD2, PCDA2 and PCDB2.





4.3.4.3.2 Property Management

Property Administrators can submit new records, modify existing ones, and perform transactions that capture installation, relocation, movement, and shipment and archive activities. These transactions are logged for historical purposes.

4.3.4.3.2.1 Add and modify records in your database

The body of basic update (add/modify) type screens features data entry fields and flag field radio buttons where values may be entered or set interactively. These values are often edited, validated, and/or defaulted according to individual conditions specified in the transaction descriptions of each module. The field status buttons to the left of entry fields specify what type of operation is required or will occur and can often be clicked to access nested search screens. Many mandatory and defaulted fields are subject to validation and/or editing as well. To ensure valid values are entered, combo boxes and calendar pop-ups are extensively employed.

A value must be entered or set, field is mandatory

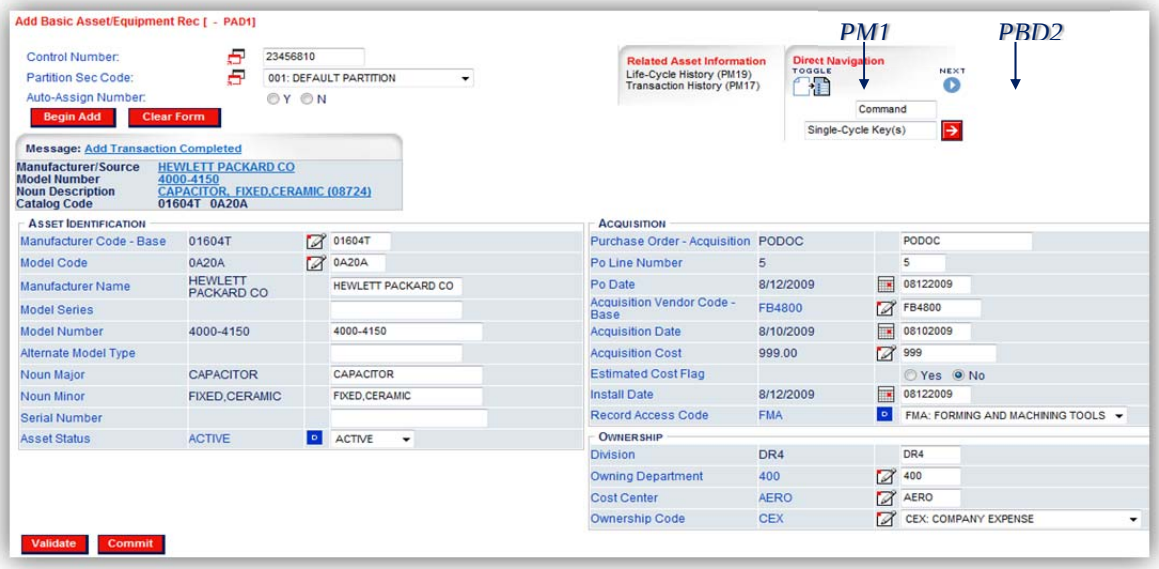
A value will default if specified conditions are met, but a different value may be entered manually

Entered value will be validated and/or edited

4.3.4.3.2.1.1 Adding a Record

PAD1 sets up a Master Property Record by means of a new EIN number which you can either enter yourself or have assigned automatically. You can only use this function once per record; if you need to modify the data entered after you have committed PAD1, use PAD2 (select Modify instead of Add on the drop-down menu). On PAD2, you'll need to enter EIN number of the record you want to update. You can view the fields updated by PAD1 and similar functions with PM1, PM2, and PM3.

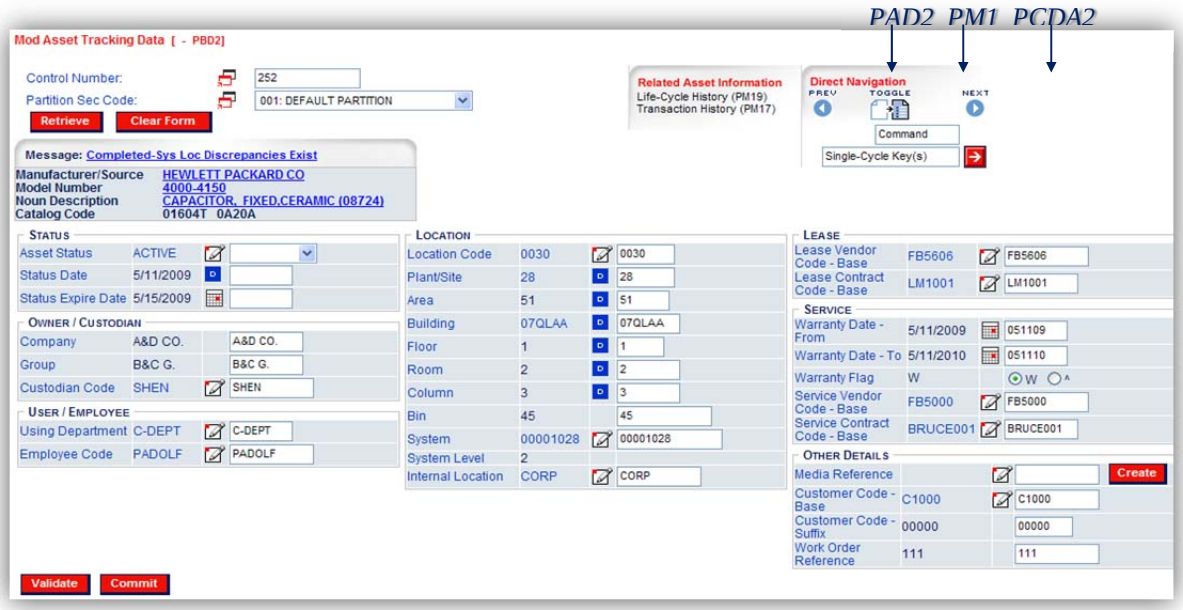
click Property on the top menu bar
select Maintain on the drop-down menu bar
select Add on the drop-down menu
click Master Acq./Data on the sub-menu
enter a EIN number or select **Auto-Assign Number**
click Begin Add
enter your data
click Validate and Commit



4.3.4.3.2.1.2 Modifying a Record

PBD2 adds tracking data to a pre-existing Master Property Record by means of its EIN number. The Partition Security Code will default according to the Control Number. You can use this function as many times as you need to. You can make this record part of a System by entering an EIN number in the System field. Enter the same EIN number of the record you're updating to make it the top component (level '0') of its System; enter a different Control Number to make it a child record (System Level is assigned automatically). Provided that this record has no lower components or children, you can remove it from a System -- by entering the 'not' code (^) in the System field -- or change the System number. You can view the whole hierarchy with PM21 and build a System with PBSD4 Click the Create button to access RMMD1 and add a multimedia object such as a PDF file or other resource, view it with. View references to multimedia with PM59 and on PM2. View other fields updated by PBD2 on PM1 and PM2.

click Property on the top menu bar
select Maintain on the drop-down menu bar
select Add or Modify on the drop-down menu
click Tracking Data on the sub-menu
enter a EIN number
click Retrieve
enter your data
click Validate and Commit



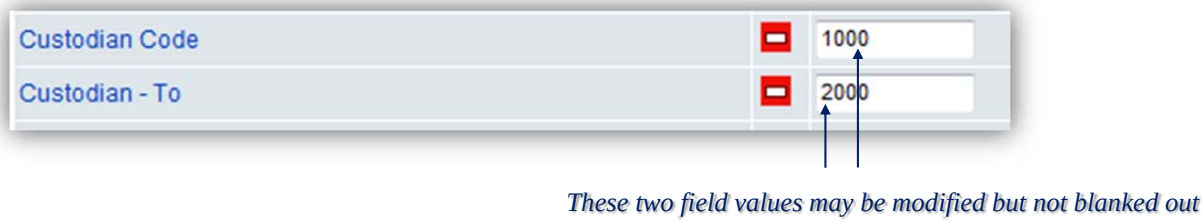
4.3.4.3.2.1.3 Basic Validation

Error messages and field status buttons

As part of the validation process, the interactive message area will display instructions when an error occurs. In the example below, a mandatory entry field has been left empty. Notice how a validation error button appears next to the entry field being validated.

Blank out values with the not-code

The option exists to blank out a value from a data entry field using the not-code [^] by entering SHIFT+6 and clicking the Validate button. Due to data entry logic, some fields will feature a button signaling that a field cannot be blanked out.



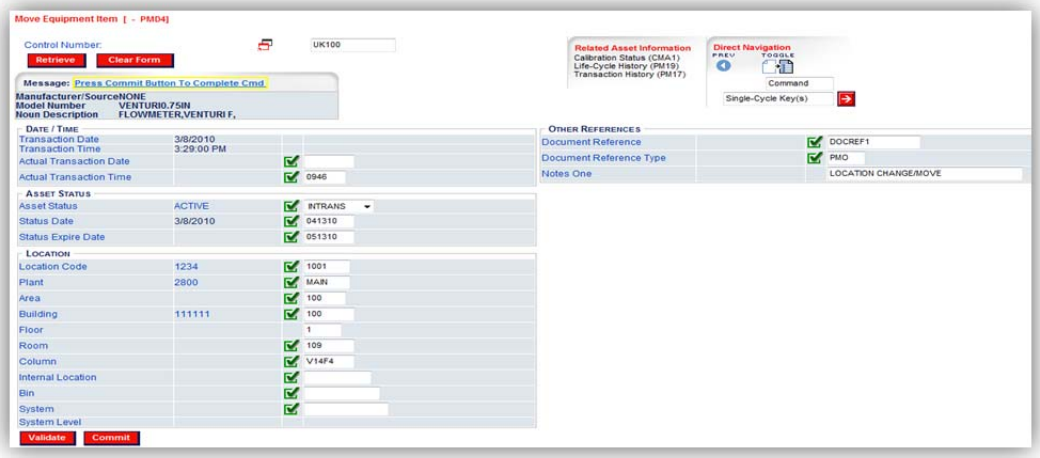
When this button appears, a valid value must be entered

Enter these two keys together in a data entry field and press ENTER to blank out its value

When this button appears, an entered value may not be blanked out

All entered values must be valid before committing your transaction to the database

Click the Validate button at any time to ensure your values have been accepted. When green checkbox buttons appear signaling it's safe to update your database, click the Commit button and you're done.

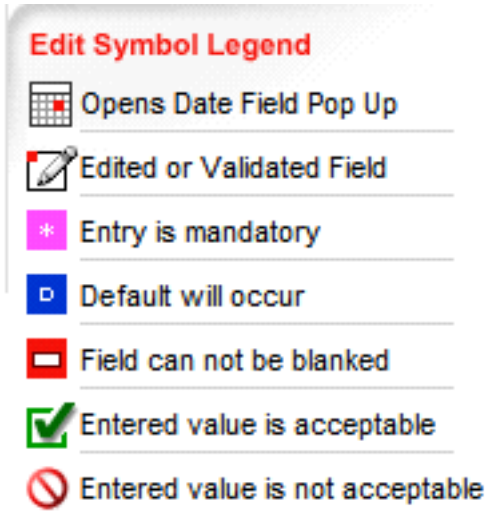


Click this button or enter Alt+V to have the system validate your entries

When these buttons appear, it is safe to click the commit button and update the database

Click this button or enter Alt+S to update a record in the database

Asset SmartSymbol Legend



4.3.4.3.3 Property Maintenance

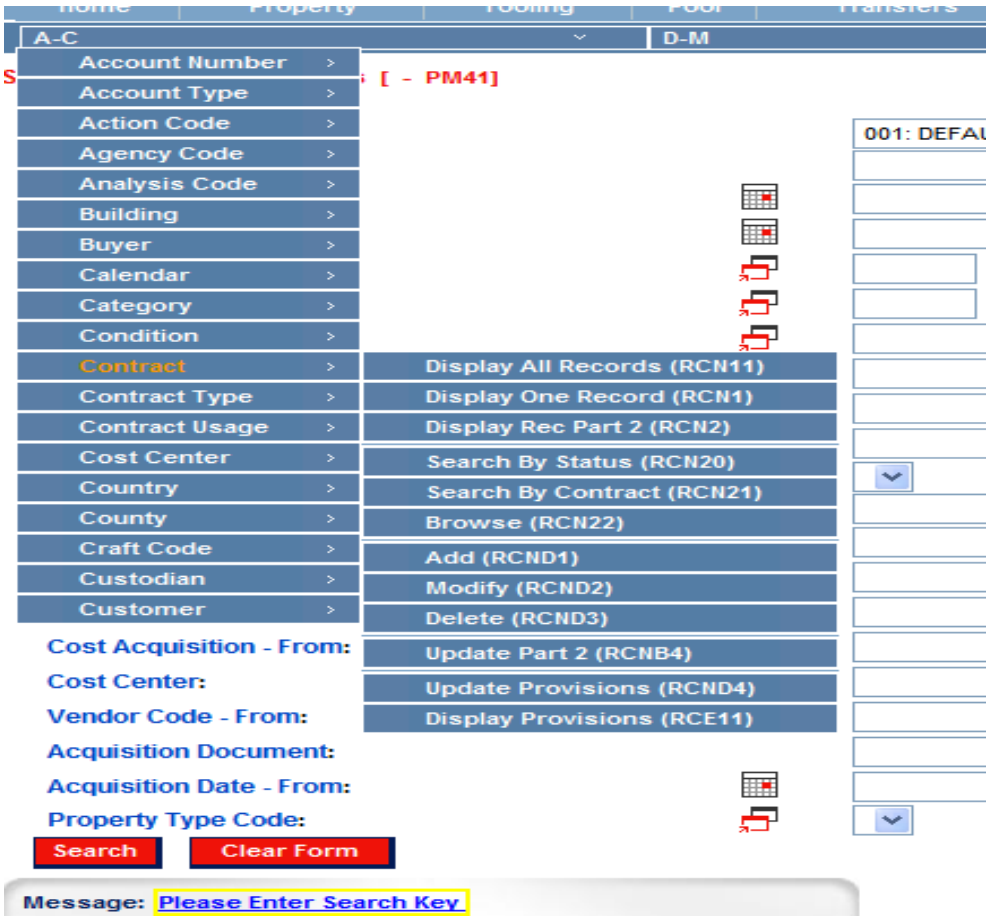
The Contract reference table is the source for all maintenance contract entries and updates. The Contract table defines accountable maintenance contract number, Vendor name, vendor address, and contact information, contract date, and open/closed status.

To Display the Contract table:

click Tables on the top menu bar
select A-C on the drop-down menu bar
select Contract on the drop-down menu
click Display All Records on the sub-menu

You can also choose to display the contract by number or status if the information is available.

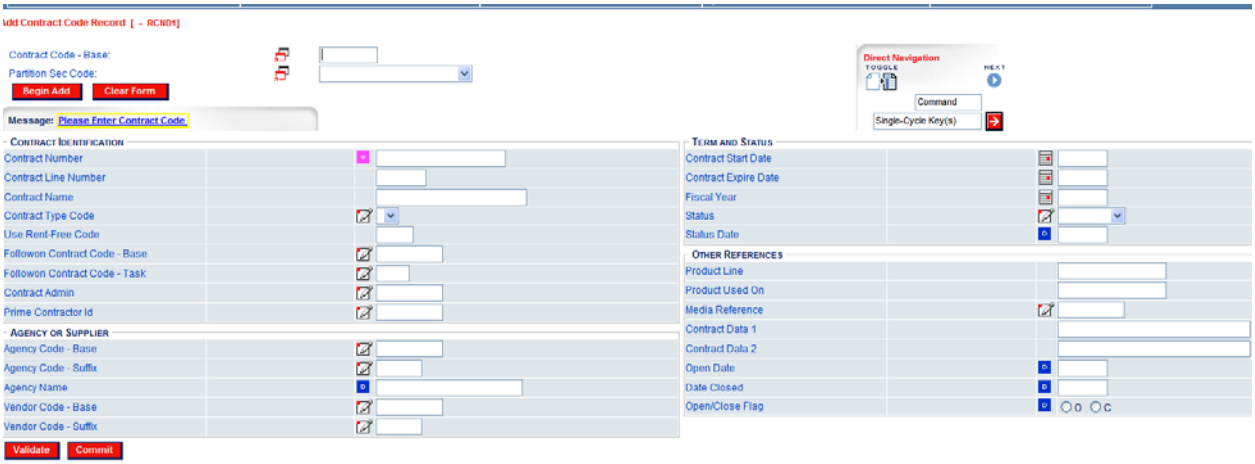
Adding a record



Adding a New Maintenance Contract

Adding a maintenance contract is similar to that of adding a new record. However, the maintenance contract is being added directly to the reference table so that the contract can be accessible by multiple asset records. To create an contract:

click Tables on the top menu bar
select A-C on the drop-down menu bar
select Contract on the drop-down menu
click ADD (RCND1) on the sub-menu
enter The new Contract information
Click Validate and Commit to add to Database



Modifying a record

Modifying an already existing Maintenance contract is similar to modifying an asset record. To modify an existing record:

click Tables on the top menu bar
select A-C on the drop-down menu bar
select Contract on the drop-down menu
click ADD (RCND1) on the sub-menu
enter The new Contract information
Click Validate and Commit to add to Database

4.3.4.3.4 System Administrator/Power User

4.3.4.3.4.1 AMIX (Mobile Inventory)

Please refer to the Asset Smart AMIIX mobile device manual for AMIIX inventory instruction.

4.3.4.3.4.2 Security and New User Adds

The system controls security for application transactions by assigning each to a security class defined by the system security administrator. Each system user's access to any application transaction in turn is controlled by the specific classes to which he is assigned. Use of the system involves access to two tables:

- Command Table
- User Table

When any user initially enters any application running under the security system, a master menu screen will be displayed from which the user must enter an identification code and a password. The system will verify these codes against the user security table. If the data is incorrect or missing, the user will be prompted for a valid identification and/or password. Once the initial

'logon' has been established, the user may then execute any of the commands in the applications for which he is authorized.

Validation of any transaction command in the system is accomplished by verifying the security class for the transaction and then validating this against the set of authorized security classes for the user.

The security class code is comprised of three alpha-numeric characters, thus allowing an almost limitless number of combinations available to the security administrator. For example, Transactions SM1 and SAD1 might be assigned security classes of S01 and SI3 respectively. User A, who is authorized to access both S01 and SI3, can therefore execute both transactions. User B, on the other hand who can access only S01 can execute SM1, but not SAD1. If the security class is not specified for a particular transaction command in the command table, then no security is enforced for that transaction and all users may have access.

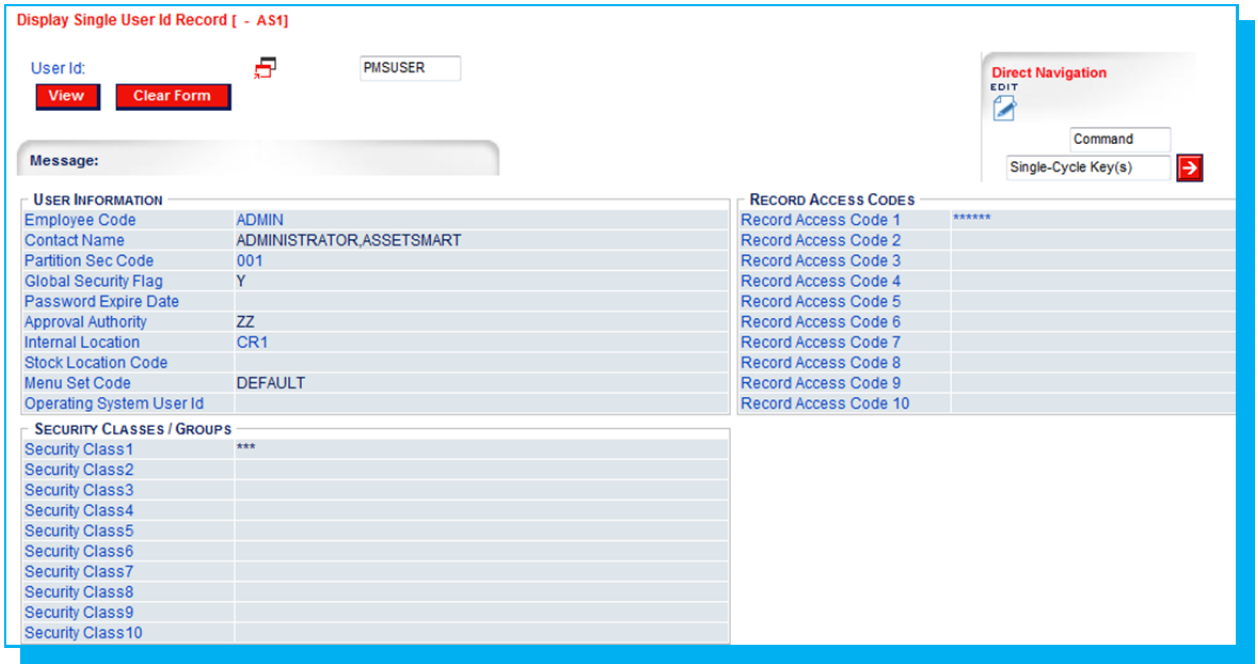
The security facility includes a "wild card" feature wherein an asterisk '*' may be included in the user security class to indicate broader access. For example, a user table with the security code of 'S0*' allows access to all commands in security classes starting with 'S0'.

A user with a code of 'S**' can access all commands in classes starting with 'S'.

A user with '***" can access all transactions in the system except those that control access to his own security record.

To Display one security record

Enter AS1 into the Direct Navigation Command field
Enter the User name
select View



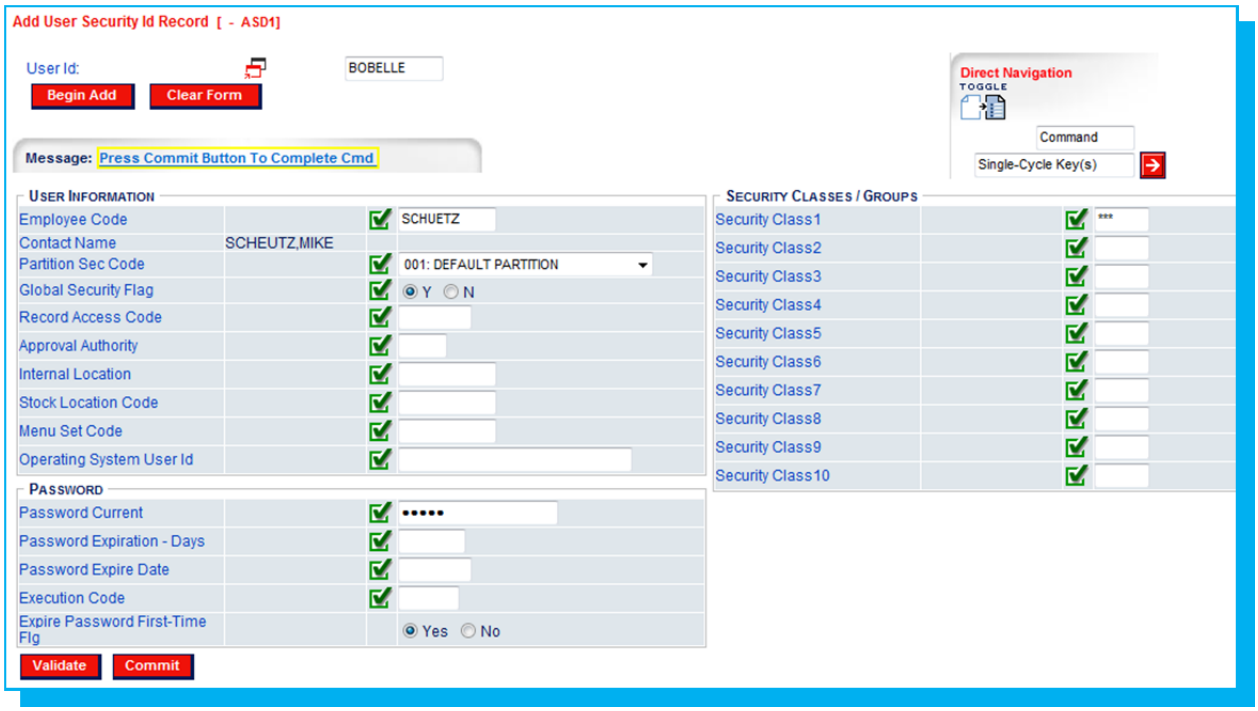
Enter ASD1 into the Direct Navigation Command field

Enter the User name

select Begin Add

enter The new employee username and security information

Click Validate and Commit to add to Database



4.3.4.4 System Reporting

All system reporting will be integrated with the Crystal reports application. The system will use the previous report designs and layout built for the Remedy application to ensure report consistency between the two systems by making a seamless transition.

This page intentionally left blank.

4.3.5 FLEXnet

FLEXnet (formerly FLEXlm) is a commercially available network license management product from Acresso Software that helps ECS sites administer licenses and enforce licensing provisions for FLEXnet-enabled COTS software. It enforces licensing provisions based on information from vendor-provided license keys and lets license administrators allow, deny, or reserve check out of licenses based on user, host, or display. FLEXnet handles floating (concurrent use) licenses, node locked licenses, and combinations of the two.

FLEXnet processing elements include license manager daemons, vendor daemons, license files, and FLEXnet-enabled applications. One or more license manager daemons control vendor daemon operations and enables client applications to contact them. Vendor daemons grant or deny concurrent use licenses requested by applications, tracking how many are checked out and by which users. License files are text files that contain the provisions for one or more licenses from one or more vendors, including the name of the vendor daemon needed to serve the license and the host(s) to use as license server(s). The applications communicate with the license and vendor daemons using embedded FLEXnet client software to request licenses in order to run.

FLEXnet permits use of single, multiple, or redundant server hosts, and can operate more than one license manager daemon on a given node. A license manager daemon serves all the licenses in the license file it uses, and different license files use separate license manager daemons (distinguished by the port number they use to communicate). In a redundant license server configuration, license manager daemons for a license file are executed on three server nodes such that all licenses in the file are available if any two out of the three server nodes is running. In a multiple license server configuration, licenses are allocated among multiple license files and a separate license manager daemon is run for each file.

Table 4.3.5-1 summarizes the operating functions that FLEXnet supports.

Table 4.3.5-1. Common ECS Operator Functions Performed with FLEXnet (1 of 2)

Operating Function	Function Name	Description	When and Why to Use
Start license manager	lmgrd	Starts FLEXnet's main daemon program, which reads the license file and manages vendor daemons and the connections between them and their client applications.	Used to initiate license management server processes.
Stop license manager	lmdown	Shuts down all license daemons (both lmgrd and all vendor daemons) on all nodes.	Used anytime to stop network license activities, such as when the license manager host is to be rebooted.

Table 4.3.5-1. Common ECS Operator Functions Performed with FLEXnet (2 of 2)

Operating Function	Function Name	Description	When and Why to Use
Install decimal format licenses	lminstall	Converts licenses between decimal and readable formats and between different versions of FLEXnet license formats.	Used anytime primarily to install decimal format licenses in readable format.
Read new licenses	lmreread	Causes the license servers to reread the license file they are using and start any new vendor daemons.	Used anytime to put the provisions of an updated license file into effect.
Monitor the status of network licensing activities	lmstat	Generates lists containing such information as active licenses, users of licensed product features, users of individual license management daemons, and status of server nodes.	Used anytime to check on the health and functioning of license server daemons, identify licenses installed, determine licenses in use, or review logged licensing events.
Rotate report log	lmnewlog	Causes a vendor daemon to move its existing report log information to a new file.	Used anytime to prevent report logs from growing too large.
Switch to new debug log	lmswitch	Causes a vendor daemon to use a new or different file as its debug log.	Used anytime to record one vendor's debug information in a file separate from the others'.
Switch to new report log	lmswitchr	Causes the license servers to use a new or different file as the report log.	Used anytime to move daemon logging to a different location.
Troubleshoot problems serving licenses	lmdiag	Performs problem diagnosis.	Used anytime to help determine why a license cannot be checked out.
Obtain license key from vendor	lmhostid	Reports the hostid of a system.	Used anytime to determine the host code that must be provided to vendors when obtaining a software license.
Recover inaccessible licenses	lmremove	Removes a single user's license for a specified feature.	Used when a client node crashes in order to recover a checked out license not automatically freed.
Determine version compatibility between the license server and an application	lmver	Reports the FLEXnet version of a library of binary files.	Used anytime to determine what version of FLEXnet a FLEXnet-enabled product uses.

4.3.5.1 Quick Start Using FLEXnet

Operators interact with FLEXnet via the license manager daemons and license files. FLEXnet's user interface is a set of UNIX-like commands for starting, stopping, and requesting services

from a license manager daemon. Command arguments specify input parameters, most notably the name of the license file whose contents determine the servers, daemons, and license provisions affected by the command. Operators install and maintain license files using any preferred editor.

4.3.5.1.1 Command Line Interface

To start FLEXnet license server daemons in a consistent, predictable manner, start the flexnet service:

```
> service flexnet start
```

Before it invokes FLEXnet's "lmgrd" program, the script adds the extension "_old" to the current FLEXnet log file (if any) so the new daemon will create its own. It then runs "lmgrd" as user "flexlm" to avoid running as "root", and it specifies the license and log file paths the daemons are to use (i.e., "/var/flexnet/license.dat" and "/tmp/license_log", respectively).

If license manager daemons are needed to serve licenses in additional license files, they can be started by running the "lmgrd" program as follow:

```
> su flexlm  -c "umask 022; /var/flexnet/lmgrd -c license_file -l logfile -p &"
```

To stop the FLEXnet license daemons that are running on all machines in the network, execute the FLEXnet command:

```
> /var/flexnet/lmdown –c license_file_list -all
```

However, to shut down the license manager daemons on a single machine only, log on to the machine and type the following command instead:

```
> service flexnet stop
```

Table 4.3.5-2 summarizes commands available with FLEXnet. See the *FLEXnet Licensing End Users Guide* for the complete description of each command and its arguments.

Table 4.3.5-2. Command Line Interfaces (1 of 3)

Command Line Interface	Description and Format	When and Why Used
lmborrow	lmborrow {*vendor* | all} enddate [*time*]	To use a license temporarily on a computer intermittently connected to the license server.
lmdiag	lmdiag [-c *license_file_list*] \ [-n] [*feature*[:*keyword*=*value*]]	To diagnose problems when a license cannot be checked out.
lmdown	lmdown [-c *license_file_list*] [-q] [-all] [-force	To shutdown selected license daemons (both lmgrd and selected vendor daemons) on all nodes.

Table 4.3.5-2. Command Line Interfaces (2 of 3)

Command Line Interface	Description and Format	When and Why Used
lmgrd	lmgrd [-c *license_file_list*] \ [-l [+]*debug_log_path*] [-2 -p] [-local] \ [-x lmdown] [-x lmremove] [-z] [-v] \ [-help]	To run the main daemon program for FLEXnet.
lmhostid	lmhostid [-n] [-type] [-utf8]	To determine the hostid of a system.
lminstall	lminstall [-i in_lic_file] [-maxlen n] [-e err_file] [-o out_lic_file] [-overfmt {2 | 3 | 4 | 5 | 5.1 | 6 | 7 | 7.1 | 8}] [-odecimal]	To convert licenses between decimal and readable formats and between different versions of FLEXnet formats.
lmnewlog	lmnewlog [-c *license_file_list*] \ *feature renamed_report_log* or: lmnewlog [-c *license_file_list*] \ *vendor renamed_report_log*	To move an existing report log to a new file and start a new log at the original filename.
lmpath	lmpath {-add | -override} {*vendor* | all} *license_file_list*	To add to, override, or get the current license path settings
lmremove	lmremove [-c *license_file_list*] *feature user user_host display* or lmremove [-c *license_file_list*] \ -h *feature server_host port handle*	To remove a single user's license for a specified feature. (This is only needed when a client node crashes, since that's the only condition where a license is not automatically freed. If the application is active, it checks out the license again after it is freed by lmremove.)
lmreread	lmreread [-c *license_file_list*] \ [-vendor *vendor*] [-all]	To cause the license daemon to reread the license file and start any new vendor daemons that have been added. In addition, one or all pre-existing daemons are signaled to reread the license file for changes in feature licensing information.
lmswitch	lmswitch [-c *license_file_list*] \ *vendor new_debug_log*	To start a new debug log for a vendor daemon, using a new filename.

Table 4.3.5-2. Command Line Interfaces (3 of 3)

Command Line Interface	Description and Format	When and Why Used
lmswitchr	lmswitchr [-c *license file*] *feature* \ *new-file* or lmswitchr [-c license file] *vendor* \ *new-file* *(v5.0+ onl)*	To start recording license events in a new or different log file.
lmstat	lmstat [-a] [-c *license_file_list*] \ [-f [*feature*]] \ [-i [*feature*] [-s[*server*][-S [*vendor*]] \ [-t *timeout_value*]	To report the status of all network licensing activities.
lmver	lmver *filename*	To identify the FLEXnet version of a library or binary file.

4.3.5.2 FLEXnet Main Screen

FLEXnet does not provide for operator interaction via a GUI. All interactions are through the UNIX command line or a UNIX script.

4.3.5.3 Required Operating Environment

For all COTS packages, appropriate information on operating environments, tunable parameters, environment variables, and a list of vendor documentation can be found in a CM-controlled document for each product. To find the installation and release notes for FLEXnet Publisher, refer to the Release Notes posted on the EMD Baseline Information System web page at your local site.

4.3.5.4 Databases

FLEXnet uses license and options files in lieu of a database. License files are independent text files, each of which contains all the site-specific information FLEXnet needs to serve the licenses specified in the file. Every license manager daemon requires a license file, and different license files require separate license manager daemons. To simplify operations, operators may combine license files obtained from multiple vendors if they are compatible. Refer to the *FLEXnet Licensing End User Guide* for information about the format of a license file, and when and how to combine them.

Options files are text files associated with specific vendor daemons named in license files. These files allow the operator to specify criteria for granting licenses to users, wait time before reclaiming inactive licenses, and how much license usage information is to be logged. FLEXnet does not require an options file. When specified however, there can only be one options file per vendor daemon, and each vendor needs a separate options file. See the *FLEXnet Licensing End User Guide* for details.

4.3.5.5 Special Constraints

FLEXnet cannot be run without one or more license files, and most FLEXnet commands require the name of a license file in order to execute. License files identify the host and port number a client is to use to communicate with the license server. If the license file parameter is missing from the command, FLEXnet tries using the file(s) named in the environment variable LM_LICENSE_FILE. If LM_LICENSE_FILE is not set, the default license file name */var/flexnet/license.dat* is assumed.

The *FLEXnet Licensing End User Guide* recommends the following operating constraints:

- Keep a copy or link of the license file in the vendor's "default" location; some vendors expect to find their license files at pre-determined locations. Refer to the *FLEXnet Licensing End Users Guide*.
- Run lmgrd as a non-privileged user (not *root)* to avoid security risks. Refer to the *FLEXnet Licensing End Users Guide.*

4.3.5.6 Outputs

FLEXnet's principal outputs are inter-process communications with COTS applications attempting to check out and check in FLEXnet licenses, but these are generally transparent to the operator. Outputs visible to the operator include an ASCII log of network licensing events and errors, and messages constituting responses to operator-entered commands.

4.3.5.7 Event and Error Messages

FLEXnet writes both status and error messages to standard output. Typically, operators redirect all output from the startup command "lmgrd" to a file, known as the debug file, to create a FLEXnet log at the site.

See the appendices of the *FLEXnet Licensing End User Guide* lists what causes the more common messages an operator may encounter, but primarily those written by the FLEXnet programs. Event and error messages logged by FLEXnet-enabled COTS applications are sometimes found in the application's manuals. Messages are typically self-explanatory and identify the date/time of the event, the license server host, the product or feature involved, and the name of the user.

4.3.5.8 Reports

FLEXnet's *lmstat* utility can generate the status reports listed in Table 4.3.5-3. Each is written to standard output and may be redirected to a named file or a printer using standard UNIX conventions. Reports are generated on demand as required to meet operational needs.

Table 4.3.5-3. Reports

Report Type	Report Description	Example
lmstat -s	Lists status of clients running on a named host.	Figure 4.3.5-1
lmstat -i	Lists license information about all or a named feature.	Figure 4.3.5-2
lmstat -a	Lists all information about current network licensing activities.	Figure 4.3.5-3
lmstat -A	Lists all currently active licenses.	Figure 4.3.5-4
lmstat -f	Lists users of all or a named feature.	Figure 4.3.5-5
lmstat -S	Lists users of all or a named vendor's features.	Figure 4.3.5-6

4.3.5.8.1 Sample Reports

The figures (Figure 4.3.5-1 through 4.3.5-6) that follow contain sample FLEXnet status reports. One sample is provided for each report listed in Table 4.3.5-3.

```
lmstat - Copyright (c) 1989-2006 Macrovision Europe Ltd. and/or Macrovision Corporation. All
Rights Reserved.
Flexible License Manager status on Mon 6/23/2008 13:18

License server status: 1726@p4nsl01
    License file(s) on p4nsl01: /var/flexnet/license.dat:

   p4nsl01: license server UP (MASTER) v10.8

Vendor daemon status (on p4nsl01):

  rational: UP v10.8
```

Figure 4.3.5-1. All Clients (lmstat -s) Report

```
lmstat - Copyright (c) 1989-2006 Macrovision Europe Ltd. and/or Macrovision Corporation. All
Rights Reserved.
Flexible License Manager status on Mon 6/23/2008 13:16

NOTE: lmstat -i does not give information from the server,
      but only reads the license file.  For this reason,
      lmstat -a is recommended instead.

Feature                 Version   # licenses    Expires         Vendor
_______                 _______   __________    _______         ______
PurifyPlusUNIX          5.00000       1         1-jan-0 rational
```

Figure 4.3.5-2. License Information (lmstat -i) Report

```
lmstat - Copyright (c) 1989-2006 Macrovision Europe Ltd. and/or Macrovision Corporation. All
Rights Reserved.
Flexible License Manager status on Mon 6/23/2008 13:19

License server status: 1726@p4nsl01
    License file(s) on p4nsl01: /var/flexnet/license.dat:

   p4nsl01: license server UP (MASTER) v10.8

Vendor daemon status (on p4nsl01):

  rational: UP v10.8

Feature usage info:

Users of PurifyPlusUNIX:  (Total of 1 license issued;  Total of 0 licenses in use)
```

Figure 4.3.5-3. All Licensing Activities (lmstat -a) Report

```
lmstat - Copyright (c) 1989-2006 Macrovision Europe Ltd. and/or Macrovision Corporation. All
Rights Reserved.
Flexible License Manager status on Mon 6/23/2008 13:20

License server status: 1726@p4nsl01
    License file(s) on p4nsl01: /var/flexnet/license.dat:

   p4nsl01: license server UP (MASTER) v10.8

Vendor daemon status (on p4nsl01):

  rational: UP v10.8

Feature usage info:
```

Figure 4.3.5-4. All Active Licenses (lmstat-A) Report

```
lmstat - Copyright (c) 1989-2006 Macrovision Europe Ltd. and/or Macrovision Corporation. All
Rights Reserved.
Flexible License Manager status on Mon 6/23/2008 13:21

License server status: 1726@p4nsl01
    License file(s) on p4nsl01: /var/flexnet/license.dat:

   p4nsl01: license server UP (MASTER) v10.8

Vendor daemon status (on p4nsl01):

  rational: UP v10.8

Feature usage info:

Users of PurifyPlusUNIX:  (Total of 1 license issued;  Total of 0 licenses in use)
```

Figure 4.3.5-5. Users of All or Named Features (lmstat-f) Report

```
lmstat - Copyright (c) 1989-2006 Macrovision Europe Ltd. and/or Macrovision Corporation. All
Rights Reserved.
Flexible License Manager status on Mon 6/23/2008 13:24


Feature usage info:


Users of PurifyPlusUNIX:  (Total of 1 license issued;  Total of 0 licenses in use)
```

Figure 4.3.5-6. Users of All or Named Vendor's Features (lmstat-S) Report

This page intentionally left blank.

4.3.6 TestTrack

TestTrack Issue Management (or TestTrack for short) provides a Trouble Ticketing service that furnishes both ECS users and operations personnel at the DAACs a common environment for classifying, tracking, and reporting the occurrence and resolution of system-related problems. The Trouble Ticketing Service:

- Provides a GUI for operations personnel to access all Trouble Ticket functions.
- Provides a common Trouble Ticket entry format.
- Stores Trouble Tickets.
- Retrieves Trouble Tickets via ad-hoc queries.
- Allows operations personnel to escalate problems to the EDF for review and resolution.
- Generates reports and statistics.
- Interfaces with user's and operator's e-mail to provide automatic notification.
- Offers an application programming interface, Simple Object Access Protocol (SOAP) Software Development Kit (SDK), through which applications can submit and manage Trouble Tickets.
- Generates a variety of reports about Trouble Tickets, including trend reports.
- Defines a consistent "life-cycle" for Trouble Tickets.
- Can be extended readily due to its highly customizable fields, workflow rules, system notifications, and user permissions.

TestTrack gives ECS operators, technicians, and managers the means to manage a system defect through its lifecycle, whether as a Trouble Ticket at a DAAC or a non-conformance report at the EDF. Within TestTrack a separate project (also known as a "database") exists for each ECS site's Trouble Tickets.

TestTrack has a client/server architecture. The server is hosted on a Linux machine at the EDF, while client access is available locally or remotely via Windows-, Linux-, Mac OS, and Web-based clients.

User Services and other operations and support personnel use TestTrack to perform the functions listed in Table 4.3.6-1. The sections that follow describe the GUIs that perform these functions, many of which include customizations made for ECS. Standard product features are mentioned but not discussed in detail. For more information about them, use the context sensitive help the tool provides, or refer to the following TestTrack vendor documents:

- *TestTrack Installation Guide, Version 2014*
- *TestTrack User Guide, Version 2014*
- *TestTrack Web User Guide, Version 2014*
- *Seapine License Server Admin Guide, Version 2014*

Table 4.3.6-1. Common ECS Operator Functions Performed using TestTrack (1 of 3)

Operating Function	GUI (Section)	Description	When and Why to Use
Access defect tracking services	Login screens (4.3.6.2)	• Operators start their client of choice and use the Login screens to access a TestTrack project. The Login screen is the gateway to TestTrack's features. By default, users land on the Trouble Ticket list screen from where all other functions can be performed.	When there is a need to submit, query, or revise a Trouble Ticket.
Submit a Trouble Ticket	Add Trouble Ticket screen (4.3.6.2.2)	• Operators add a new Trouble Ticket to the system. • Trouble Ticket form is used to enter information about the problem.	When a problem is either found by or reported to User Services.
Browse Trouble Tickets	Edit Trouble Ticket screen (4.3.6.2.3)	• Operators review existing Trouble Tickets. • Allows entry of new information about the problem and recording of events that advance the defect report through its lifecycle states.	When information needs to be added to a Trouble Ticket or when a Trouble Ticket needs to be viewed.
Escalate a Trouble Ticket to the EDF	Escalate screen (4.3.6.2.4.5)	• Operators raise an Escalate event that forwards a specified Trouble Ticket to the EDF. • A script uses TestTrack's SOAP API to create a defect report in the Operations_NCRs project automatically using information from the Trouble Ticket. • Notifications are sent to the EDF and the ticket owner that a ticket has been escalated.	When assistance in resolving the Trouble Ticket is needed from the EDF or the problem requires a hardware or software change.

Table 4.3.6-1. Common ECS Operator Functions Performed using TestTrack (2 of 3)

Operating Function	GUI (Section)	Description	When and Why to Use
Generate reports	Reports screen (4.3.6.2.5)	• Operators run or create new reports. The screen is accessed from the Trouble Ticket list screen. Reports can be viewed, created, edited, deleted, printed, or previewed by selecting the appropriate button on the Reports screen.	When information is needed about one or more Trouble Tickets.
Add, delete, or modify user accounts	License Server Admin tool's Global Users screen (4.3.6.2.13) TestTrack Client Edit Users screen (4.3.6.2.8)	• TestTrack administrators add, delete, and modify user profiles, including user IDs and passwords. • TestTrack administrators assign operators and users to a security groups on a project-by-project basis. Each project's security groups enforce what the operator or user can do in that project.	When there is a need to update: 1) the list of operators and users authorized to access each project; 2) what features and records an operator or user can access; 3) contact information and/or passwords; and. 4) reset individual passwords.
Customize pulldown menus	Setup <field> Names screens (4.3.6.2.9-4.3.6.2.11)	• TestTrack administrators add, edit, reorder, and delete values used in TestTrack's field pulldown menus. This ensures that data is entered uniformly in fields used for categorizing defects.	When current menus require updating.

Table 4.3.6-1. Common ECS Operator Functions Performed using TestTrack (3 of 3)

Operating Function	GUI (Section)	Description	When and Why to Use
Issue Notifications	Configure Automation Rules screen Edit Trouble Ticket screens User Options screen (4.3.6.2.10 & 4.3.6.2.11)	• TestTrack administrators configure rules used by TestTrack for issuing system notifications to individual operators and users. System notifications are used primarily to alert defect report assignees, submitters, etc. when their defect report or its status has changed. • Operators and users designate particular individuals to receive an e-mail whenever a Trouble Ticket or NCR has changed. • Operators and users define personal rules the system uses to e-mail them about changes to defect reports they are authorized to see.	To inform someone via e-mail when a Trouble Ticket or NCR changes in one or more of a variety of ways.

4.3.6.1 Quick Start Using TestTrack

This section describes how to invoke TestTrack. For more information, use the context sensitive help the tool provides, or refer to the following vendor documents:

- *TestTrack User Guide, Version 2014*
- *TestTrack Web User Guide, Version 2014*

4.3.6.1.1 Invoking TestTrack

The various TestTrack clients are started differently.

To start the Windows client on Windows XP:

> Click **`Start → All Programs → Seapine Software → TestTrack → TestTrack Client`** on your desktop.

To start the Linux client, enter:

```
/usr/ecs/OPS/COTS/ttpro/bin/ttclient &
```

To start the Mac client, double-click the TestTrack Client icon in the Applications/TestTrack folder.

To start the Web client, open a browser and enter the following URL:

```
https://links.gsfc.nasa.gov:<port>
```

Under Windows, Linux, and Mac OS, a Login dialog box similar to that in Figure 4.3.6-1 will appear. (See Section 4.3.6.2.14 for a discussion of the Web login screen.)

Select the TestTrack Server you want to access, and enter your TestTrack Username (i.e., login ID) and password. Since the URL for the Web client already specifies the server to use, its Login GUI requests only the Username and Password.

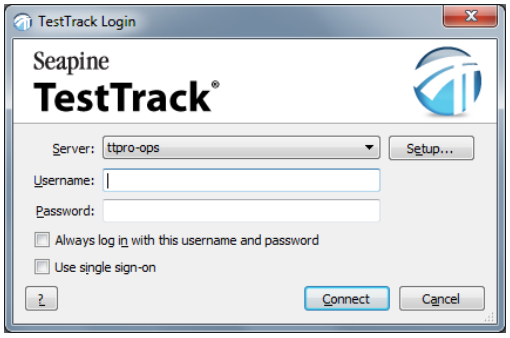


Figure 4.3.6-1. TestTrack Login GUI

Table 4.3.6-2 provides a description of the Login screen's field.

Table 4.3.6-2. TestTrack Studio Login Field Descriptions

Field Name	Data Type	Size	Entry	Description
Server	Selection	*	Required	Your name for this TestTrack server connection.
Username	Selection	*	Required	User's TestTrack login id.
Password	Selection	*	Required	User's TestTrack password.
Always log in with this username and password	Checkbox		Optional	Requests credentials be stored for re-use
Use single sign-on (not available on Linux)	Checkbox		Optional	Requests you be logged in using your network cre

***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.

The Login screen has the following buttons:

- **Setup…** Opens the Edit TestTrack Server GUI for defining server connections
- **Connect** Submits user's credentials to determine which projects the user can access
- **Cancel** Closes the screen and ends the login sequence.

If using TestTrack for the first time, the Add TestTrack Server GUI will appear so you can define a TestTrack server connection (see Figure 4.3.6-2). Your TestTrack administrator can help you set up the connection.

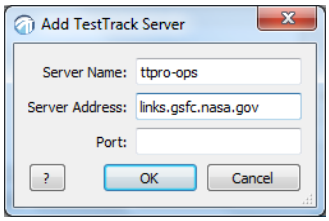


Figure 4.3.6-2. Add TestTrack Server GUI

Table 4.3.6-3 provides a description of the Add TestTrack Server screen's fields.

Table 4.3.6-3. Add TestTrack Server Field Descriptions

Field Name	Data Type	Size	Entry	Description
Server Name	Character	> 200	Required	Name of TestTrack server connection.
Server Address	Character	> 200	Required	Fully qualified domain name of the TestTrack server.
Port	Integer	5	Required	Port on which TestTrack clients communicate with the TestTrack server.

The TestTrack Project Selection screen has the following buttons:

- **OK** Adds the new server definition to the user's configuration
- **Cancel** Closes the screen without accepting entered data.

Upon username and password verification, the TestTrack Project Selection GUI appears (see Figure 4.3.6-3). Use this screen to specify which project to log in to. The Project picklist displays only the projects to which the user has access. If the picklist is empty or indicates that projects are loading, click **Refresh** after a few moments to retrieve a new list. You can set the **Always login to this project** checkbox to use this project as your default in the future.

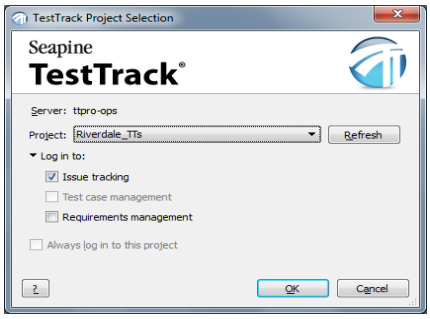


Figure 4.3.6-3. TestTrack Project Selection GUI

Table 4.3.6-4 provides a description of the TestTrack Project Selection screen's fields.

Table 4.3.6-4. TestTrack Project Selection Field Descriptions

Field Name	Data Type	Size	Entry	Description
Project	Selection	*	Required	Name of the project to logon to. Lists only the projects the user is authorized to access.
Login in to	Check box	n/a	Selection	Requests access to Trouble Tickets using TestTrack Issue Management, Test Case Management, and/or Requirements Management license(s).
Always login to this project	Check box	n/a	Optional	Records the specified project as the default for subsequent login requests.

***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.

To conserve licenses, be sure to deselect requests for Licenses your session will not need.

The TestTrack Project Selection screen has the following buttons:

- **Refresh** Retrieves the latest list of available TestTrack projects the user is authorized to access.
- **OK** Logs the user into the selected project.
- **Cancel** Cancels the logon request.

The sections that follow describe the screens displayed by the Windows, Linux, and Mac clients. The Web Client provides the same functionality and fields, but the displays and user interactions are necessarily somewhat different.

4.3.6.2 Main Screen

TestTrack's main screen is shown in Figure 4.3.6-4. From here Trouble Tickets can be submitted, queried, modified, and escalated. The GUI can manage multiple windows concurrently, and it offers a menu bar and a complement of movable toolbars for easily navigating system screens.

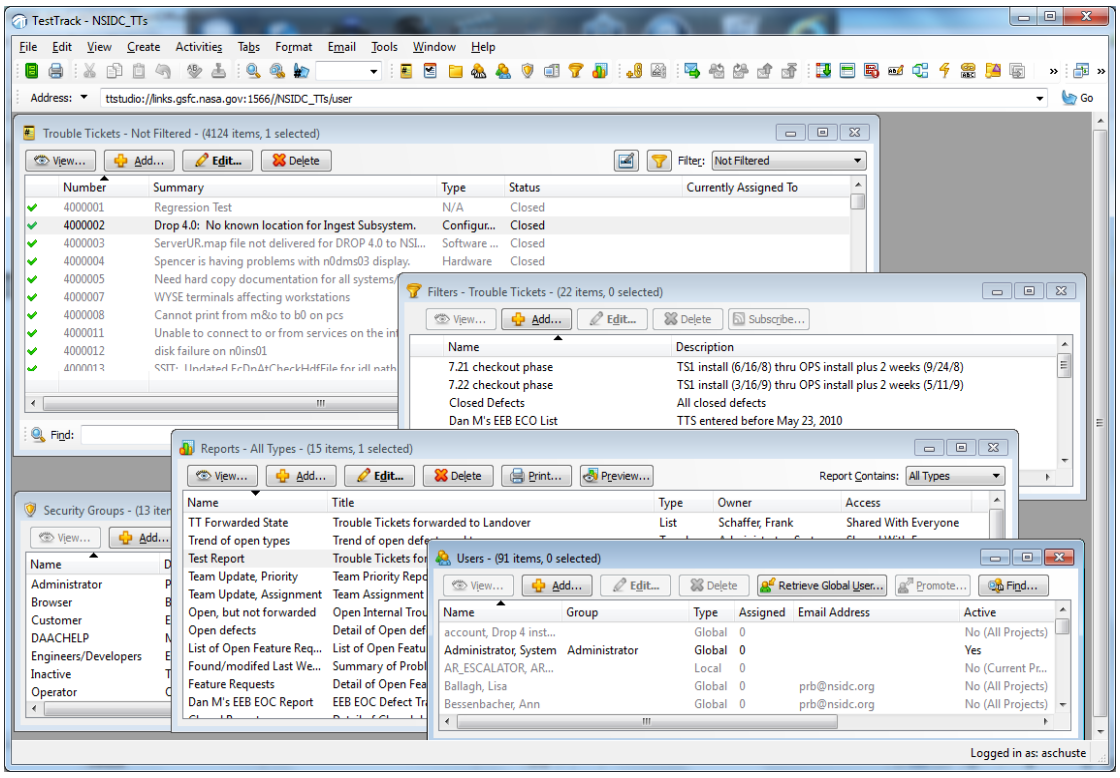


Figure 4.3.6-4. Main GUI

4.3.6.2.1 Trouble Ticket List Screen

Operators and users use the Trouble Ticket List screen (see Figure 4.3.6-5) to browse, select, and open one or more Trouble Tickets. Use the Filter pull down menu to retrieve the records you want. Initiate action on a Trouble Ticket by clicking on a row then on one of the action buttons. Initiate action on multiple records by dragging your mouse over several rows before pressing the action button.

The screen can be configured to display data as you prefer. Insert or remove columns of data by right-clicking on the column heading. Adjust the width of a column by dragging the bar in the column heading that separates it from its neighbor, or double-click on the bar to size it automatically. Sort the data by clicking on a column heading; add a secondary sort by holding the Shift key and clicking on a second column heading.

Important: Exit the screen by selecting **File → Logout and Disconnect** from the TestTrack menu bar. On the Web client, use the **Logout** hyperlink. Otherwise, the system may not release the license immediately.

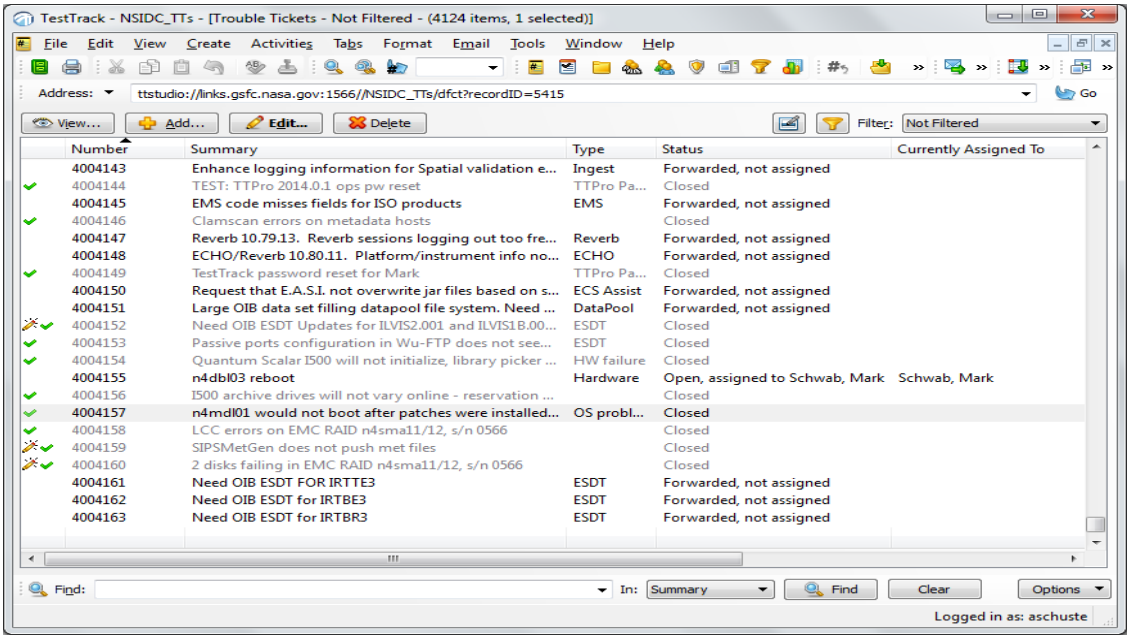


Figure 4.3.6-5. Trouble Tickets List GUI

Table 4.3.6-5 provides a description of the Trouble Ticket List screen's field.

Table 4.3.6-5. Trouble Tickets List Field Descriptions

Field Name	Data Type	Size	Entry	Description
Address	String	n/a	Optional	TestTrack address for the current list window or open item. Can display ttstudio or http addresses.
Filter	Selection	*	Optional	Name for the set of criteria to be used by the system to determine which Trouble Tickets to display.
Find	String		Optional	Value to search for.
In	Selection	*	Optional	Field in which to search for the value.

***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.

The Trouble Tickets List screen has the following buttons:

- **View…** Opens a Trouble Ticket for viewing only.
- **Add…** Opens the Add Trouble Ticket screen for submitting a new Trouble Ticket.
- **Edit…** Opens a Trouble Ticket for modification.
- **Delete** Removes a Trouble Ticket from the database
- **Find** Initiates a search for records that meet the criteria specified by values in the Find and In fields

- **Clear** Clears the find results
- **Options** Opens a menu of advanced conditions for tailoring a record search

4.3.6.2.2 Add Trouble Ticket Screen

The Add Trouble Ticket screen (Figures 4.3.6-6 thru 4.3.6-8) is used for reporting an operational issue or problem in ECS. Depending on how a user's options are configured, the screen will display in either vertical tab (see Figure 4.3.6-6) or single page (see Figures 4.3.6-7 thru 4.3.6-8) format. Clicking **Add** on this screen creates the Trouble Ticket and commits the data to the database.

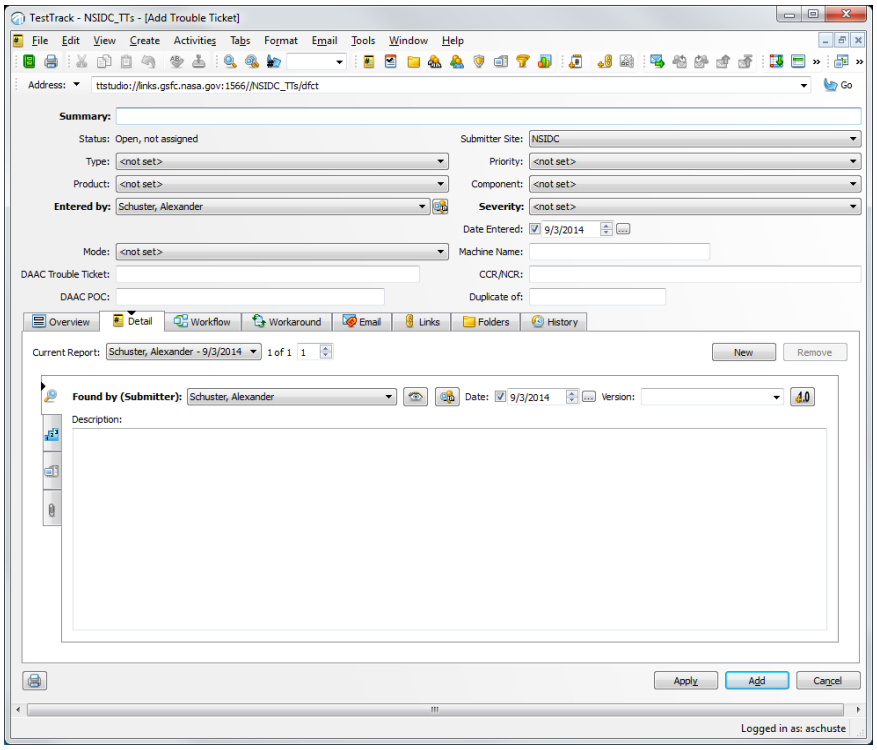


Figure 4.3.6-6. Add Trouble Ticket GUI – Vertical Tab View

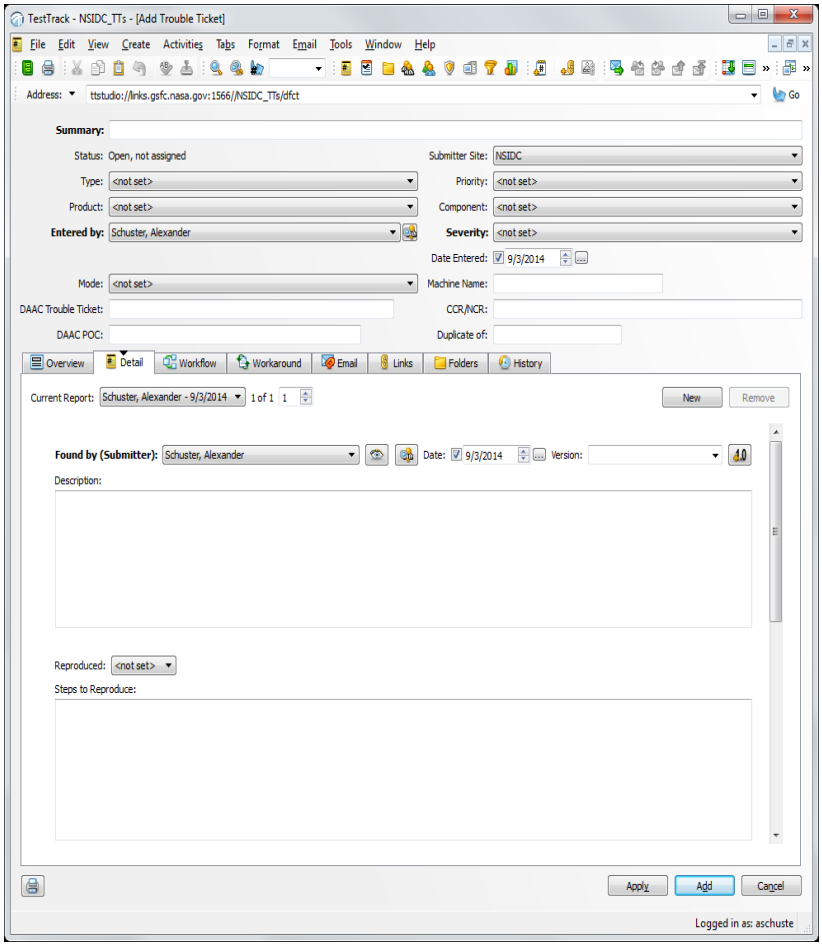


Figure 4.3.6-7. Add Trouble Ticket GUI – Single Page View - Top of Page

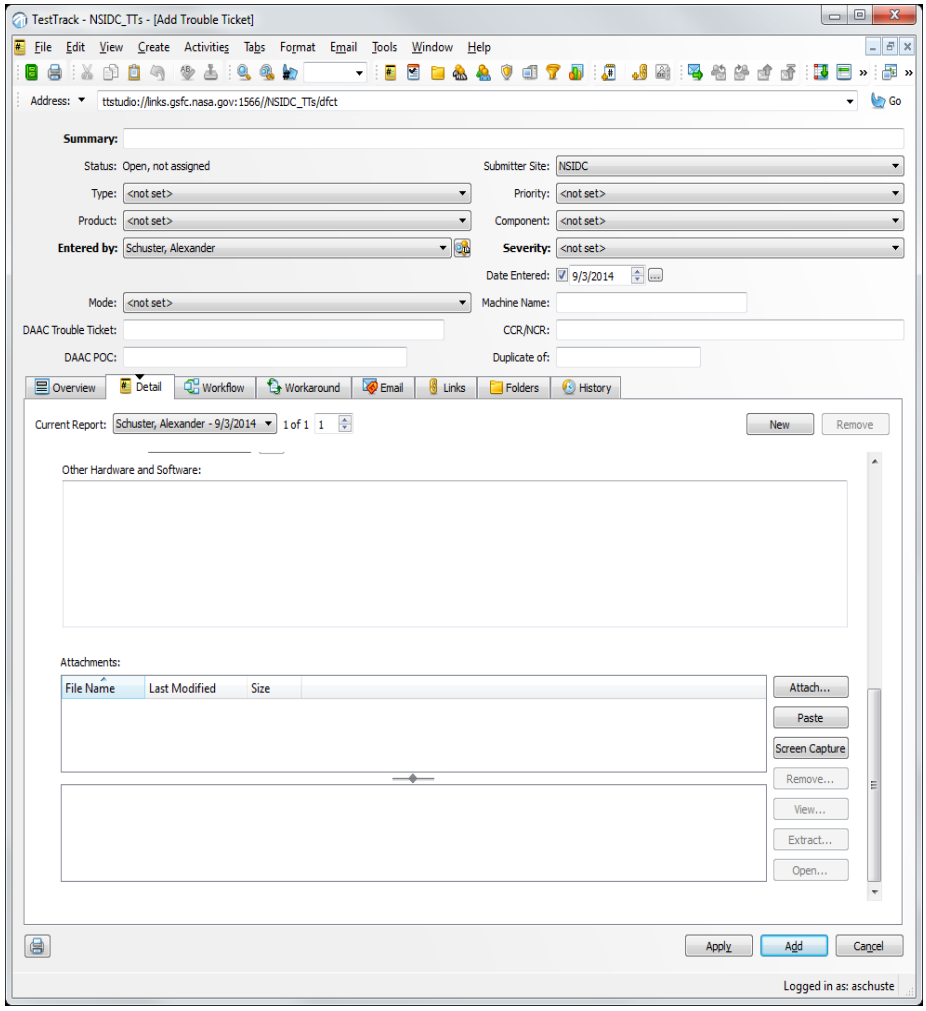


Figure 4.3.6-8. Add Trouble Ticket GUI – Single Page View - Bottom of Page

Table 4.3.6-6 provides a description of the Add Trouble Ticket screen's fields in Figure 4.3.6-6.

Table 4.3.6-6. Add Trouble Ticket Field Descriptions (1 of 2)

Field Name	Data Type	Size	Entry	Description
Summary	Character	154	Required	Short Description of the problem.
Status	Character	n/a	System generated	Status of the Trouble Ticket (a combination of state and assignment status).
Submitter Site	Selection	*	Optional	Trouble ticket's originating site.

Table 4.3.6-6. Add Trouble Ticket Field Descriptions (2 of 2)

Field Name	Data Type	Size	Entry	Description
Type	Selection	*	Optional	Type of problem or issue (e.g., Configuration Error, Hardware Problem, Software Problem).
Priority	Selection	*	Optional	Priority of Trouble Ticket assigned at the site.
Product	Selection	*	Optional	Product exhibiting the problem or issue.
Component	Selection	*	Optional	Product's component exhibiting the problem or issue. In legacy (Remedy) tickets, it is the name of the configuration item with which the problem is associated.
Entered by	Selection	*	Required	Name of the person who created the Trouble Ticket.
Severity	Selection	*	Required	Impact of the problem to the submitter.
Date Entered	Date	n/a	Optional	Date Trouble Ticket was created.
Mode	Selection	*	Optional	Run mode in which problem was detected.
Machine Name	Character	n/a	Optional	Name of machine on which problem was detected.
DAAC Trouble Ticket	Character	n/a	Optional	Legacy identifier of Trouble Ticket (from Remedy ARS).
CCR/NCR	Character	n/a	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 the ECS PRB for advice or resolution.
Duplicate of	Character	n/a	Optional	Identifier of an earlier Trouble Ticket addressing the same issue.
Current Report	Selection	*	Optional	Submitter and date of an occurrence of the problem or issue. Helps browse through multiple reports of the same issue.
1 of n	Selection	*	System Generated	Identifier that distinguishes among multiple instances or reports of the same problem or issue.
Found by (Submitter)	Selection	*	Required	Full Name of the Submitter.
Date	Date	n/a	Optional	Date issue or problem occurred.
Version	Selection	*	Optional	Product version exhibiting the issue.
Description	Character	4060	Optional	Detailed description of the problem.

*** 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.

The Add Trouble Ticket screen has the following buttons:

- **New** Adds another Found By record to the trouble ticket.
- **Remove** Removes the displayed Found By record from the trouble ticket.
- **Edit User** (eye icon) Opens the Found By user's profile record for editing.
- **Find Customer** (customer icon) Opens a menu of advanced conditions for tailoring a record search.
- **Printer** Generates a detail report of the open item.
- **Apply** Opens a Trouble Ticket for viewing only.
- **Add** Saves the trouble ticket and adds it to the project.
- **Cancel** Exits the screen without saving data.

4.3.6.2.3 Edit Trouble Ticket Screen

The Edit Trouble Ticket (see Figure 4.3.6-9) screen is used to update an existing Trouble Ticket and advance it through its lifecycle states. The latter is done by selecting an appropriate item on the Activities menu or clicking the appropriate Activities icon (in this view, the second row of icons on the toolbar), either of which opens an Activity screen (see Section 4.3.6.2.4).

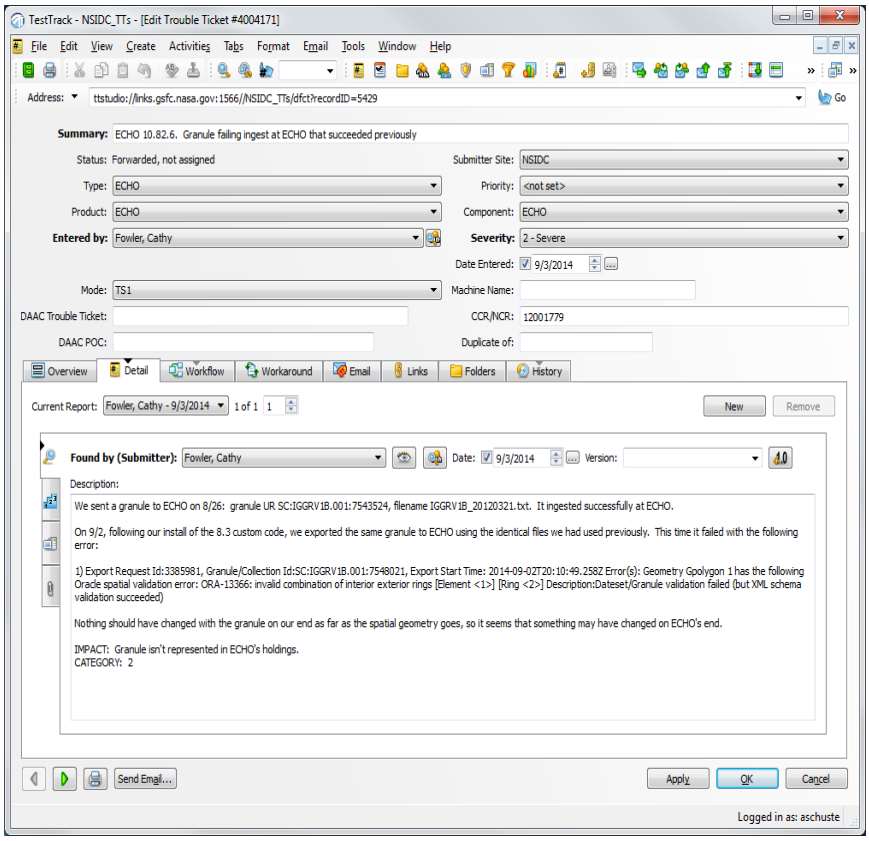


Figure 4.3.6-9. Edit Trouble Ticket GUI

The Edit Trouble Ticket screen's fields are the same as those for the Add Trouble Ticket screen (see Table 4.3.6-6 above).

This screen has four buttons that differ from those on the Add Trouble Ticket screen:

- **Left arrow** Commits changes to the database and displays the previous Trouble Ticket in the Trouble Ticket list**.**
- **Right arrow** Commits changes to the database and displ**ays** the next Trouble Ticket in the Trouble Ticket list.
- **Send Email…** Opens a screen for composing and sending email to one or more TestTrack users. Senders can use an email template to include data about the open trouble ticket.
- **OK** Commits changes to the database.

4.3.6.2.4 Activity Screens

The screens in this section advance Trouble Tickets through their lifecycle states.

Each activity screen has the following buttons:

- **OK** Accepts entered data and **c**loses the screen.
- **Cancel** Closes the screen without accepting entered data.

Important: Clicking **OK** does not update the database. The database is updated only when subsequently closing the calling Add Trouble Ticket or Edit Trouble Ticket screens.

4.3.6.2.4.1 Assign Screen

The Assign screen (see Figure 4.3.6-10) is used for recording that a staff member has been assigned to work on the issue described by the Trouble Ticket.

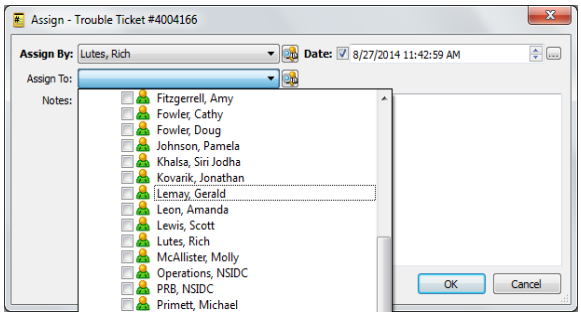


Figure 4.3.6-10. Assign GUI

Table 4.3.6-7 provides a description of the Assign screen's fields.

Table 4.3.6-7. Assign Field Descriptions

Field Name	Data Type	Size	Entry	Description
Assign By	Selection	*	Required	The person who is making the assignment.
Date	Date/Time	n/a	Required	Date assignment is made.
Assign To	Selection	*	Optional	Name of the assignee.
Notes	Text		Optional	Message for the assignee.

***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.

4.3.6.2.4.2 Propose Solution Screen

The Propose Solution screen (see Figure 4.3.6-11) is used for documenting how to resolve the issue described by the Trouble Ticket. Clicking **OK** on this screen advances the Trouble Ticket to the Solution Proposed state.

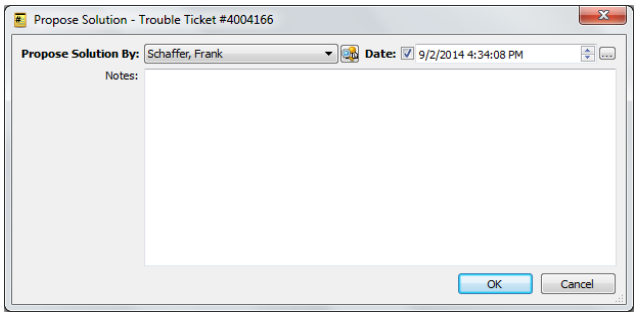


Figure 4.3.6-11. Propose Solution GUI

Table 4.3.6-8 provides a description of the Propose Solution screen's fields.

Table 4.3.6-8. Propose Solution Field Descriptions

Field Name	Data Type	Size	Entry	Description
Propose Solution By	Selection	*	Required	The person who is proposing the solution.
Date	Date/Time	n/a	Required	Date solution is proposed.
Notes	Text	n/a	Optional	The proposed solution.

***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.

4.3.6.2.4.3 Start to Implement Screen

The Start to Implement screen (see Figure 4.3.6-12) is used for documenting work towards implementing the solution to the problem described in the Trouble Ticket. Clicking OK on this screen advances the Trouble Ticket to the Start to Implement state.

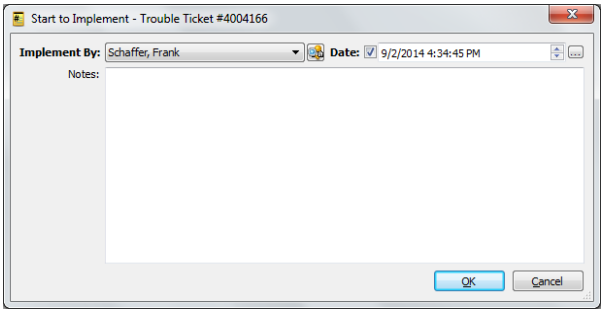


Figure 4.3.6-12. Start to Implement GUI

Table 4.3.6-9 provides a description of the Start to Implement screen's fields.

Table 4.3.6-9. Start to Implement Field Descriptions

Field Name	Data Type	Size	Entry	Description
Implement By	Selection	*	Required	The person who is implementing the solution.
Date	Date/Time	n/a	Required	Date work started towards a solution.
Notes	Text	n/a	Optional	Details on progress towards solution.

***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.

4.3.6.2.4.4 Fix Screen

The Fix screen (see Figure 4.3.6-13) is used for reporting that the issue described in the Trouble Ticket has been solved. Clicking **OK** on this screen advances the Trouble Ticket to the Fixed state.

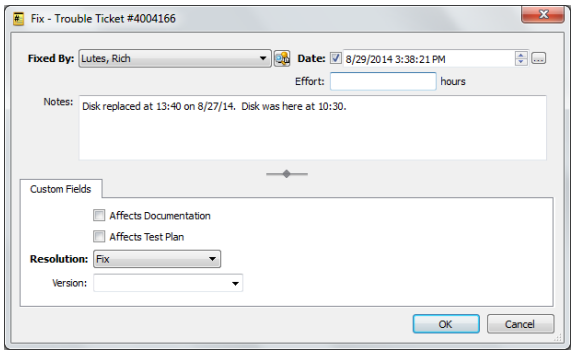


Figure 4.3.6-13. Fix GUI

Table 4.3.6-10 provides a description of the Fix screen's fields.

Table 4.3.6-10. Fix Field Descriptions

Field Name	Data Type	Size	Entry	Description
Fixed By	Selection	*	Required	The person who fixed the problem.
Date	Date/Time	n/a	Required	Date solution was implemented.
Effort	Decimal		Optional	Hours it took to resolve the issue.
Notes	Text		Optional	Details of how the issue was resolved.
Affects Documentation	Check box	n/a	Optional	Is a documentation change req'd?
Affects Test Plan	Check box	n/a	Optional	Is a test plan change req'd?
Resolution	Selection	*	Required	Type of resolution.
Version	Selection	*	Optional	Product version first containing fix.

***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.

4.3.6.2.4.5 Escalate Screen

The Escalate screen (see Figure 4.3.6.14) is used for forwarding an issue to the ECS Problem Review Board (PRB) for advice or resolution. Clicking **OK** on this screen advances the Trouble Ticket to the Forwarded state.

Note: A cron job runs periodically to extract the data from escalated Trouble Tickets in order to create corresponding ECS non-conformance reports (NCRs).

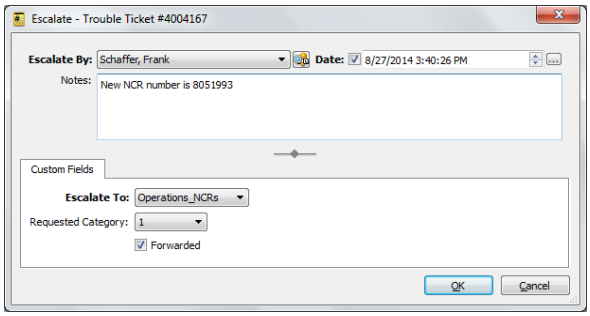


Figure 4.3.6-14. Escalate GUI

Table 4.3.6-11 provides a description of the Escalate screen's fields.

Table 4.3.6-11. Escalate Field Descriptions

Field Name	Data Type	Size	Entry	Description
Escalate By	Selection	*	Required	The person who is escalating the problem.
Date	Date/Time	n/a	Required	Date Trouble Ticket is escalated.
Notes	Text		Optional	Details of how the issue was resolved.
Escalate To	Selection	*	Required	Name of target NCR project.
Requested Category	Selection	*	Optional	A measure of how soon the escalator would like the fix.
Forwarded	Check box	n/a	System	Whether or not the Trouble Ticket has been forwarded to the EDF.

***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.

4.3.6.2.4.6 Close Screen

The Close screen (see Figure 4.3.6-15) is used to document that the issue described in the Trouble Ticket has been rejected or abandoned, or that work has been completed. Clicking **OK** on this screen advances the Trouble Ticket to the Closed state.

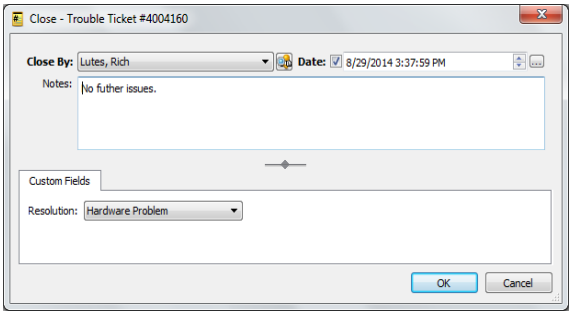


Figure 4.3.6-15. Close GUI

Table 4.3.6-12 provides a description of the Close screen's fields.

Table 4.3.6-12. Close Field Descriptions

Field Name	Data Type	Size	Entry	Description
Close By	Selection	*	Required	The person who closed the Trouble Ticket.
Date	Date/Time	n/a	Required	Date the Trouble Ticket was closed.
Notes	Text		Optional	Supporting information for closing the Trouble Ticket.
Resolution	Selection	*	Required	Why the Trouble Ticket can be closed.

***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.

4.3.6.2.4.7 Comment Screen

The Comment screen (see Figure 4.3.6-16) is used for recording miscellaneous notes related to the Trouble Ticket. It does not change the ticket's life cycle state.

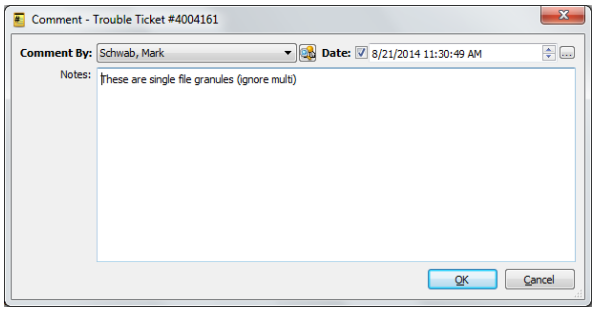


Figure 4.3.6-16. Comment GUI

Table 4.3.6-13 provides a description of the Comment screen's fields.

Table 4.3.6-13. Comment Field Descriptions

Field Name	Data Type	Size	Entry	Description
Comment By	Selection	*	Required	The person who is recording the comment.
Date	Date/Time	n/a	Required	Date the comment is recorded.
Notes	Text		Optional	The comment.

***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.

4.3.6.2.5 Reports Screen

The Reports screen (see Figure 4.3.6-17) is used for generating pre-defined and ad hoc Trouble Ticket reports. Four types of reports are possible: list, detail, trend, and distribution. (See Section 4.3.6.8.1 for an example of each.) TestTrack uses style sheets as templates for generating reports. The screen includes a "Report Contains:" filter that facilitates finding reports by category, such as TTs, Folders, Users, and Security Groups.

The TestTrack User Guide and the TestTrack Web User Guide provide details about the subordinate screens used to define new reports, including how to specify or edit stylesheets, page breaks, sort columns, timeframes, totals, and charts.

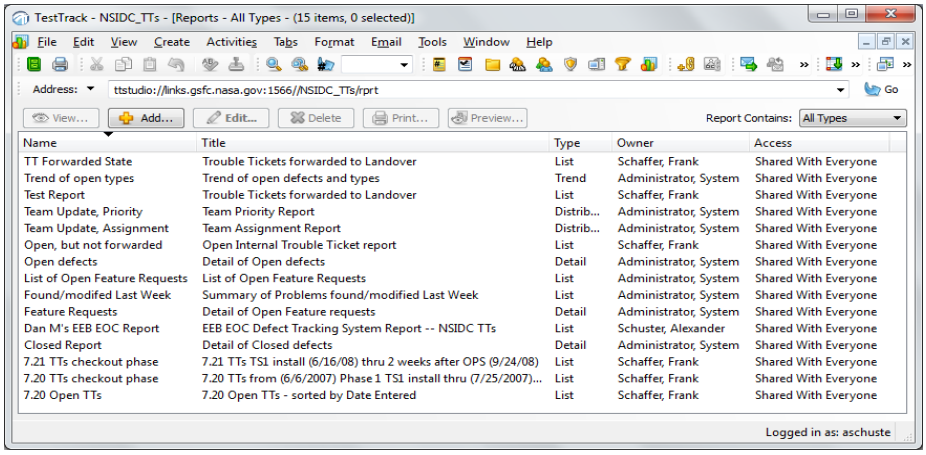


Figure 4.3.6-17. Reports GUI

The Reports screen has the following buttons:

- **View…** Opens a screen for viewing the configuration of the report.
- **Add…** Opens a screen for defining a new report.
- **Edit…** Opens a screen for editing the configuration of a pre-defined report.
- **Delete** Deletes an operator-selected report.
- **Print** Runs the report, directing output to a selected printer (Windows client only)
- **Preview** Runs the report and presents it via the user's default web browser

The Print Options screen (see Figure 4.3.6-18) provides another means of printing adhoc reports containing one or more items from any TestTrack list window, including trouble tickets. This screen is invoked by selecting items to print and then clicking **File → Print…** on TestTrack's menu bar.

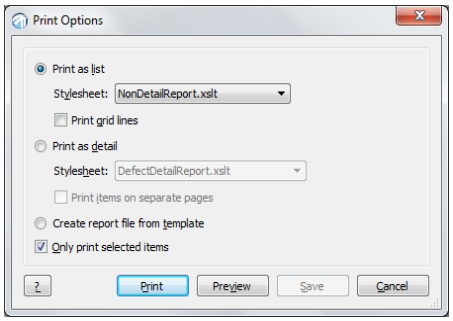


Figure 4.3.6-18. Print Options GUI

Table 4.3.6-14 provides a description of the Print Options screen's fields.

Table 4.3.6-14. Print Options Field Descriptions

Field Name	Data Type	Size	Entry	Description
Print as list	Boolean		Optional	Print columns from list window, one item per line.
Stylesheet	Selection		Required	Definition of the document's appearance.
Print gridlines	Boolean		Optional	Prints lines between cells.
Print as detail	Boolean		Optional	Prints all information about the item.
Print items on separate pages	Boolean		Optional	Inserts a page separator between items.
Create report from template	Boolean		Optional	Prints a report based on a previously created template.
Only print selected items	Boolean	*	Optional	Prints only the items selected on the list window.

The Print Options screen has the following buttons:

- **Print** Generates a report, directing output to a selected printer (Windows client only)
- **Preview** Generates the report and presents it via the user's default web browser
- **Save** Saves the report as a text document
- **Cancel** Cancels the print request.

4.3.6.2.6 Security Groups Screen

The Security Groups screen (see Figure 4.3.6-19) is used to manage profiles that define TestTrack user roles and the system privileges granted to each role. Each TestTrack project has its own set of security groups. Users authorized access to a project must be assigned to one (and only one) security group.

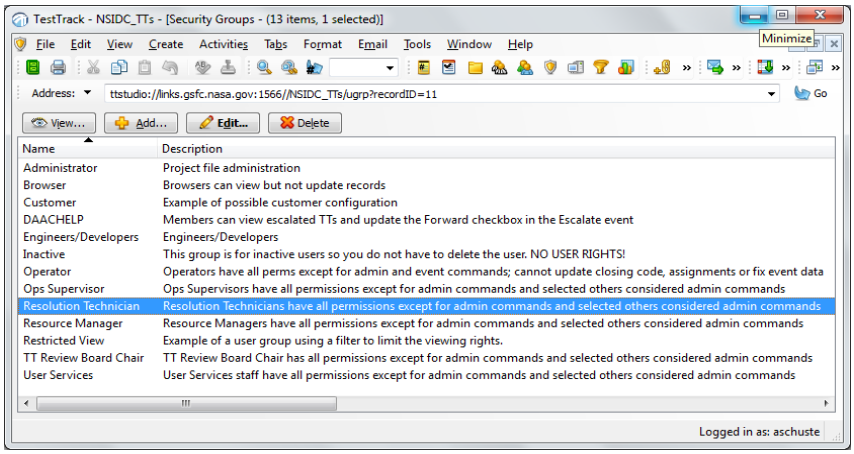


Figure 4.3.6-19. Security Groups GUI

This screen has no data entry fields other than Address described earlier in Table 4.3.6-5.

The Security Groups screen has the following unique buttons:

- **View…** Opens a screen for viewing selected groups' privileges within the project.
- **Add…** Opens a screen for adding a new group and its privileges to the project.
- **Edit…** Opens a screen for updating selected groups' privileges within the project.
- **Delete** Deletes selected security groups. Users who were members of the deleted group(s) are no longer assigned to any project. They cannot access the project nor can they receive project-issued e-mail notifications.

See the TestTrack manuals for descriptions of the Add Security Group, Edit Security Group, and View Security Group screens.

4.3.6.2.7 Users Screen

The Users screen (see Figure 4.3.6-20) is used to manage profiles that define who can access the project's Trouble Tickets. Double-clicking on one or more users in the list opens either the View User or Edit User screens, depending on the client's user options settings.

Profiles can be global or local. Global user profiles can be shared among all TestTrack projects on the network. Local user profiles are known only within the project in which they are defined, but they can be promoted to a global user profile if the user's name is unique among all projects.

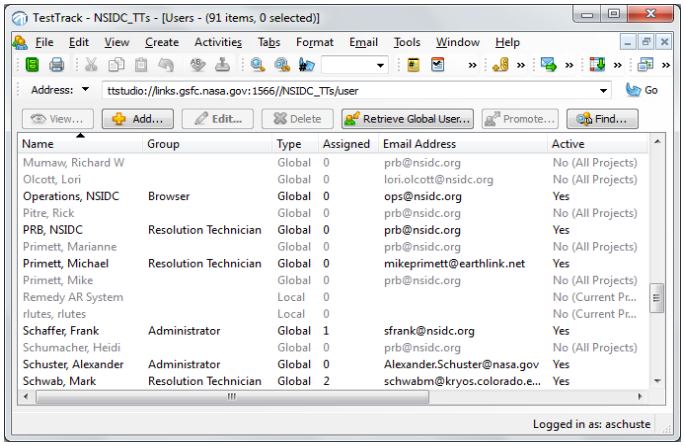


Figure 4.3.6-20. Users GUI

This screen has no data entry fields other than Address described earlier in Table 4.3.6-5.

The Users screen has the following unique buttons:

- **View…** Opens a screen for viewing selected users' profiles within the project.
- **Add…** Opens a screen for adding a new user profile to the project.
- **Edit…** Opens a screen for updating selected user profiles within the project.

- **Delete** Deletes selected user profiles. Deleting a user removes all references to that user from the project's Trouble Tickets.
- **Retrieve Global User…** Adds a user to the project by retrieving the user's profile from the TestTrack license server's global user records.
- **Promote…** Adds selected, local user profiles to the TestTrack license server's global user database.
- **Find…** Opens a screen for specifying advanced criteria for locating matching user records.

See the TestTrack manuals for descriptions of the Add User and View User screens. The Edit User screen is described in the next section.

4.3.6.2.8 Edit User Screen

Use the Edit User screen (see Figure 4.3.6-21) to update user profiles for the project. Its fields are identical to those of the Add User and View User screens.

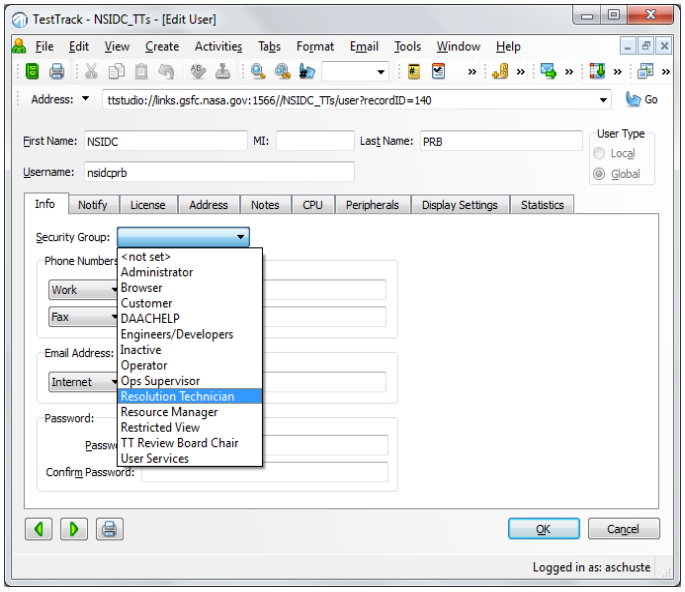


Figure 4.3.6-21. Edit User GUI

Table 4.3.6-15 provides a description of the Edit User screen's fields (Info tab only).

Table 4.3.6-15. Edit User Field Descriptions (Info Tab only)

Field Name	Data Type	Size	Entry	Description
First Name	Character	32	Optional	User's first name. (Optional only if a last name is specified.)
MI	Character	8	Optional	
Last Name	Character	32	Optional	User's surname. (Optional only if a first name is specified.)
Username	Character	32	Optional	User's logon ID
Security Group	Selection	*	Required	User's assigned security group
Phone Number (Type)	Selection	*	Optional	User's phone type (work, home, fax, pager, mobile)
Phone Number (Type)	Selection	*	Optional	User's phone type (work, home, fax, pager, mobile)
Phone Number	Character	32	Optional	User's phone number
Email Address (Type)	Character	32	Optional	User's email type (Internet, MAPI, other).
Email Address	Character	32	Optional	User's e-mail address to use for notifications
Password	Character	n/a	Optional	User's Password
Confirm Password	Character	n/a	Optional	User's Password

***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.

In addition to the fields described in the above table, the Edit User screen contains the following buttons:

- **User Type** Designates whether the user is to be registered with the TestTrack license server's global user database shared by all projects it services.
- **Left arrow** Commits changes to the database and displays the previous Trouble Ticket in the Trouble Ticket list.
- **Right arrow** Commits changes to the database and displ**ays** the n**e**xt Trouble Ticket in in the Trouble Ticket list.

4.3.6.2.10 Setup List Items Screen

The Setup List Items screen (see Figure 4.3.6-22) is used to pre-define values that can be entered via pull down menus attached to specific TestTrack fields. On TestTrack's Trouble Ticket screens, clicking the down arrow icon next to any of these fields displays the choices from which a user can select. This screen is reached by clicking **Tools → Configure List Values → <*field-name*> Values…** on the TestTrack menu bar.

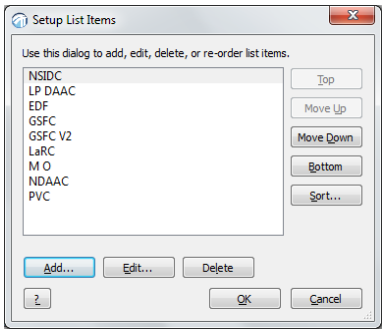


Figure 4.3.6-22. Setup List Items GUI

This screen has no data entry fields.

The Setup List Items screen contains the following unique buttons:

- **Add…** Opens a screen for adding a new value to the pull down menu list.
- **Edit…** Opens a screen for editing the selected value in the pull down menu list.
- **Delete** Deletes the selected value from the pull down menu.
- **Top** Moves the value to the top of the pull down menu's list.
- **Move Up** Move the value one position higher in the pull down menu's list.
- **Move Down** Moves the value one position lower in the pull down menu's list.
- **Bottom** Moves the value to the bottom of the pull down menu's list.
- **Sort…** Sorts the pull down menu's list of values alphabetically, either ascending or descending as specified on a supporting data entry screen.

4.3.6.2.11 Configure Automation Rules Screen

The Configure Automation Rules screen (see Figure 4.3.6-23) is used for defining the conditions for TestTrack to perform certain actions automatically. A separate tab controls each of three types of rules: notification, trigger, and escalation.

Notification rules email users about Trouble Ticket changes. Notifications can be issued for all or any subset of records, using a pre-defined or a custom e-mail template, to anyone authorized access to the project.

Trigger rules prevent users from performing an activity, create a workflow event, modify data, or run a server-side executable whenever a user attempts to save a record.

Escalation rules enter a workflow event, modify record fields, send email, or run a server-side executable based on a schedule.

This screen is invoked by clicking **Tools → Administration → Automation Rules** on TestTrack's menu bar.

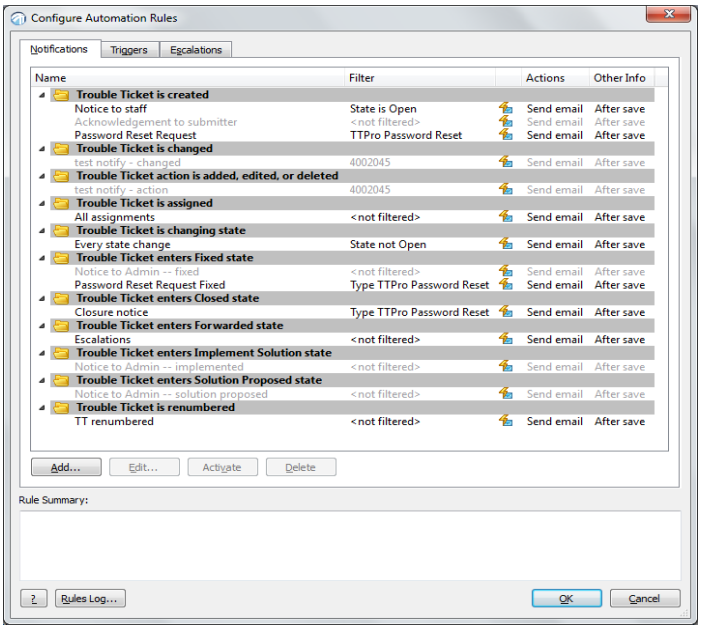


Figure 4.3.6-23. Configure Automation Rules GUI

This screen has no data entry fields.

The Configure Automation Rules screen contains the following unique buttons:

- **Add** Opens a screen for adding rules for the selected Trouble Ticket events. See the TestTrack manuals for a description of this screen and how to use it.
- **Add Default** (Triggers tab only) Opens a screen for adding rules to perform actions on records that are not acted on by other triggers. See the TestTrack manuals for a description of this screen and how to use it.
- **Edit…** Opens a screen for adding rules for the selected Trouble Ticket events. See the TestTrack manuals for a description of this screen and how to use it.
- **Delete** Removes the selected rule.
- **Activate** Enables the selected rule.
- **Rules Log…** Exports the log for the selected rule to a text file for analysis or for use with other tools.

4.3.6.2.10 User Options screen

The User Options screen (see Figure 4.3.6-24) lets users specify personal preferences about how TestTrack behaves. These cover displays, notifications, a personal dictionary, spell checking, and a few, other, more general features. This screen is invoked by clicking **Tools → User Options** on TestTrack's menu bar.

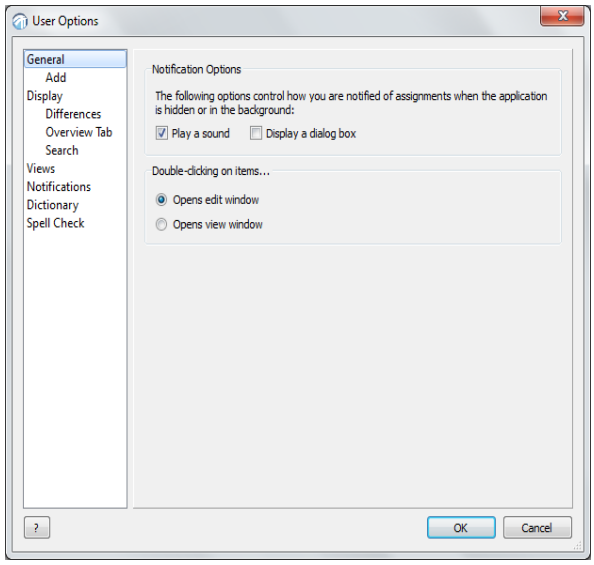


Figure 4.3.6-24. Configure User Options GUI

Most panes on the screen present a series of radio buttons or check boxes. The Dictionary pane, though, provides a dialog for specifying the main dictionary to be used when spell checking and for adding custom words to the dictionary.

See the TestTrack manuals for more details about using this screen.

4.3.6.2.12 License Server Admin Utility

The License Server Admin Utility screen (see Figure 4.3.6-25) is the gateway to the collection of screens for managing TestTrack license server operations. The GUI can be started only from the command line on the TestTrack server machine, and access is generally limited to central TestTrack system administrators.

Start the utility by typing, "**`/usr/ecs/OPS/COTS/ttpro/splicsvr/bin/lsadmin &`**", and then log in.

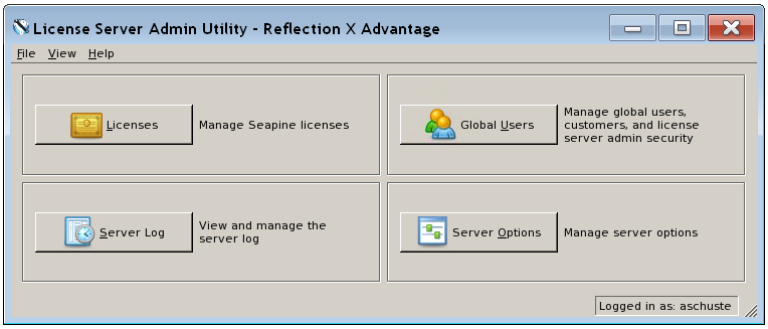


Figure 4.3.6-25. License Server Admin Utility GUI

This screen has no data entry fields.

The License Server Admin Utility screen contains the following unique buttons:

- **Licenses** Opens a screen for adding, editing, and deleting TestTrack licenses, and for associating users with single-user, "named" licenses when applicable. From this screen, administrators can navigate to the Floating Licenses Used screen to view who is currently using TestTrack floating licenses network-wide.
- **Global Users** Opens a screen for adding, editing, and deleting user profiles. See Section 4.3.6.2.13, Global Users Screen, below.
- **Server Log** Opens a screen for viewing, filtering, deleting and exporting license server log entries.
- **Server Options** Opens a screen for configuring log, license server, server database, LDAP, and password options. Password options cover requirements, restrictions and history.

See the Seapine License Server Admin Guide, Version 2014, for a thorough description of the screen mentioned above.

4.3.6.2.13 Global Users Screen

The Global Users screen (see Figure 4.3.6-26) lets TestTrack administrators conveniently manage the user profiles of individuals who need to access TestTrack. Double-clicking on any row in the list opens the profile for the selected user. This screen is invoked by clicking on the Global Users button on the License Server Admin Utility GUI (see Section 4.3.6.2.11)

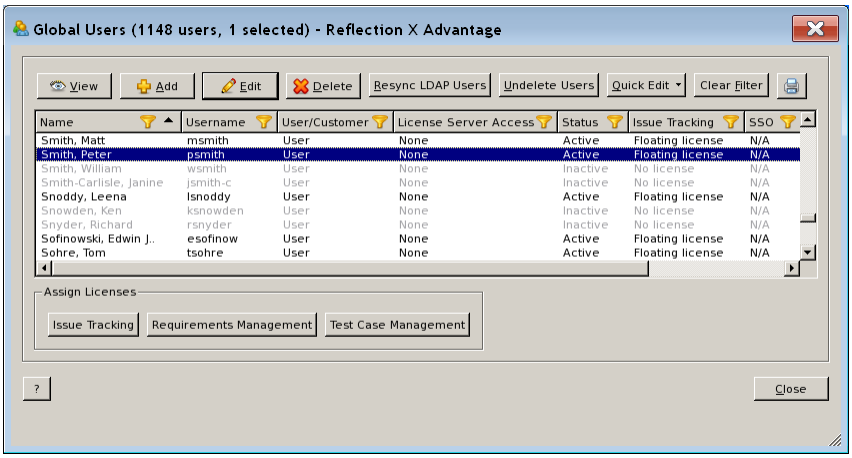


Figure 4.3.6-26. Global Users GUI

This screen has no data entry fields.

The Global Users screen contains the following unique buttons:

- **View** Opens a screen for reading a user's record in the license server database.
- **Add** Opens a screen for adding a new global user to the license server database.
- **Edit** Opens a screen for changing a user's record in the license server database.
- **Delete** Removes the selected user from the license server database.
- **Re-sync LDAP Users** Manually adds users from an LDAP server.
- **Undelete** Opens a screen for restoring a previously deleted user's profile.
- **Quick Edit** Applies Make Customer, Activate, Unlock, and Bulk User Changes operations to select user profiles.
- **Clear Filter** Removes filters that previously applied to user records
- **Issue Tracking** Opens a screen for assigning an Issue Management license to selected users.
- **Requirements Management** Opens a screen for assigning an RM license to selected users.
- **Test Case Management** Opens a screen for assigning a TCM license to selected users.

See the Seapine License Server Admin Guide, Version 2014, for a thorough description of the screen mentioned above.

4.3.6.2.14 TestTrack Web Client's Trouble Ticket Screen

TestTrack has a Web client that has all the features of the Windows client, including submission, querying, and modification of Trouble Tickets via a browser. Users of TestTrack Web need:

- a computer with a Web browser that supports HTML 3.0 or later
- JavaScript enabled

To reach the Web client, start the browser and enter the appropriate secure URL and port number. For example: **`https://<host>.gsfc.nasa.gov:<port_number>`**. The TestTrack login window is then displayed as shown in Figure 4.3.6-27.

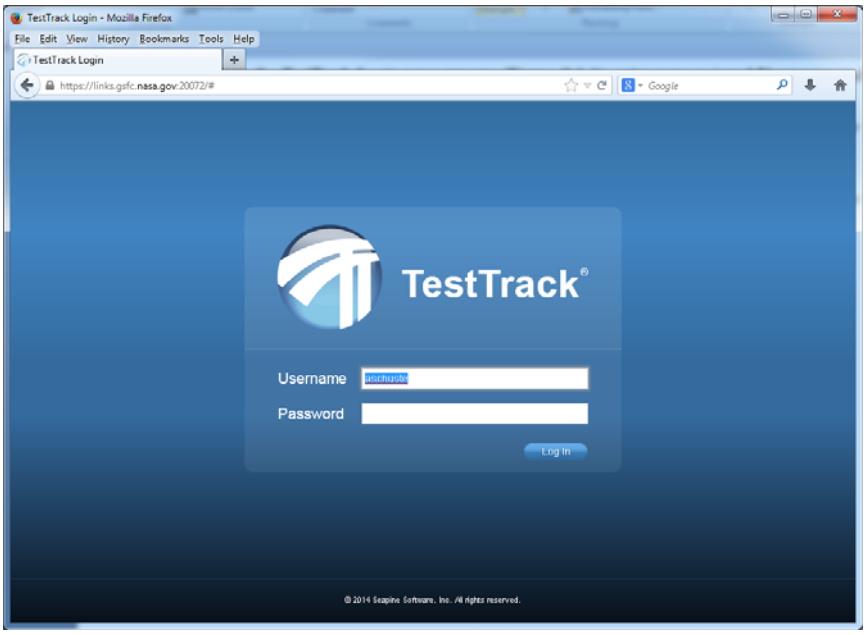


Figure 4.3.6-27. Web Login Window

The Project Selection window is used to choose which TestTrack project.

Upon username and password verification, the TestTrack Project Selection window appears (see Figure 4.3.6-28). Use this screen to specify which project to log in to and which TestTrack components to access. The Project picklist displays only the projects to which the user has access. The Log in to picklist displays only the components to which the user has access.

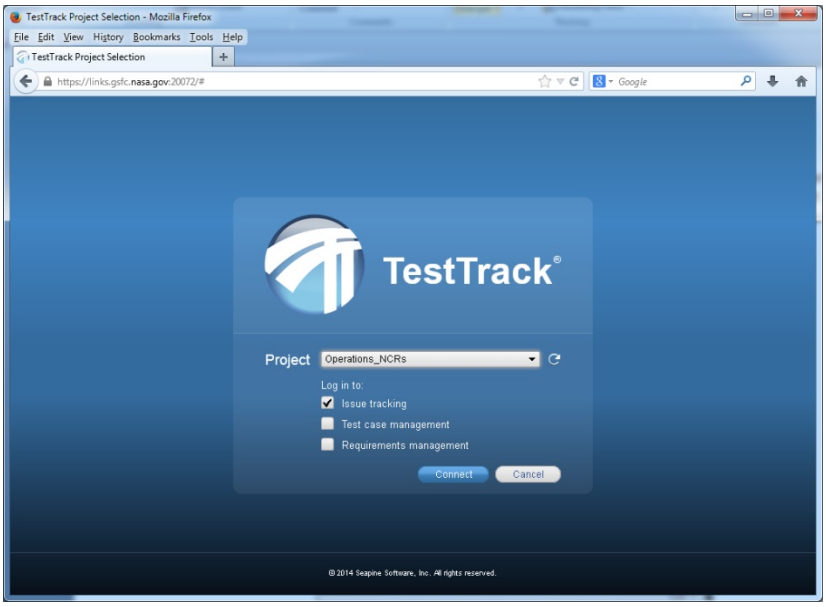


Figure 4.3.6-28. Project Selection Window

Table 4.3.6-16 provides a description of the TestTrack Project Selection window's fields.

Table 4.3.6-16. TestTrack Project Selection Field Descriptions

Field Name	Data Type	Size	Entry	Description
Project	Selection	*	Required	Name of the project to logon to
Login to	Checkbox	*	Required	Names of TestTrack components to use

***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.

The Project Selection screen contains the following unique buttons:

- **Connect** Logs in to the selected project.
- **Cancel** Cancels the login request.

Upon successful login, the Trouble Tickets List page is displayed as shown in Figure 4.3.6-29. As with the Windows client, the Trouble Tickets list page identifies all Trouble Tickets returned by the filter the user selects. Rather than a menu bar, however, the web page uses tabs and a series of action links on the top and the left side of the page to help users navigate and perform actions. To access a Trouble Ticket, users select one or more Trouble Tickets by clicking in corresponding checkboxes on the left, and then selecting View, Edit, or Delete from the Action gear pulldown in the adjacent column. A Logout hotlink at the top right of the display closes the user's connection to the database properly and frees the user's license.

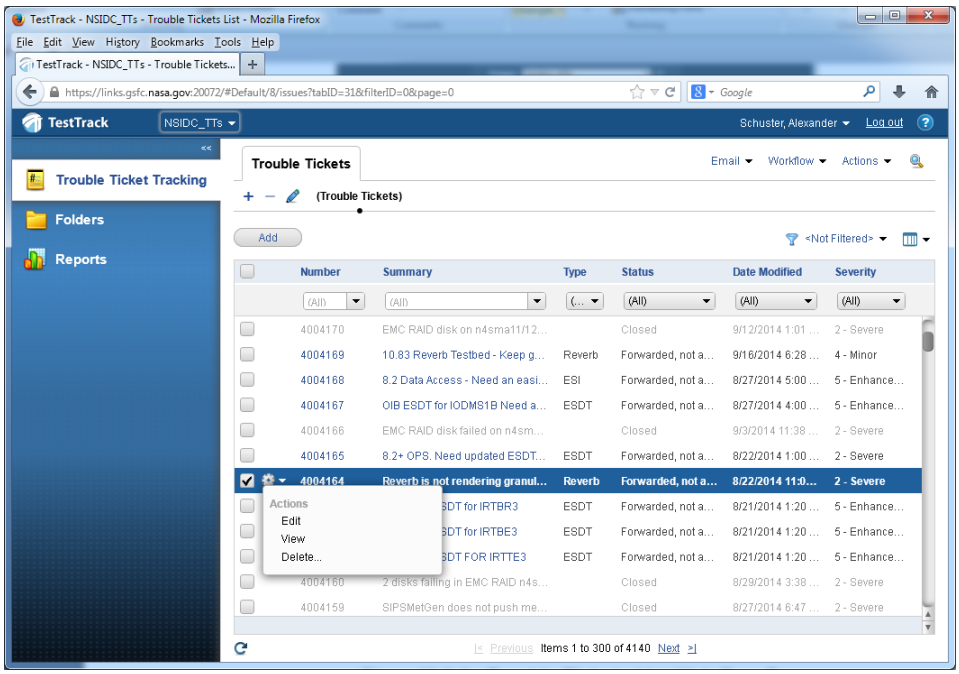


Figure 4.3.6-29. Trouble Ticket List Web Page

4.3.6.3 Required Operating Environment

The TestTrack server runs on a Linux-based machine; Linux-, Windows-, Mac-, and Web-based clients are available for the DAACs. Appropriate information on operating environments, tunable parameters, environment variables, and a list of vendor documentation can be found in the EED Release Notes document 914-TDA-558. To find the documentation for TestTrack, refer to the Release Notes posted on the ECS Baseline Information System web page at your local site. The Release Notes document was distributed to ECS sites with TestTrack. Vendor manuals are available upon request.

4.3.6.3.1 Interfaces and Data Types

Several custom scripts interact with TestTrack to facilitate operations and development. Table 4.3.6-17 identifies these interfaces.

Table 4.3.6-17. External Interface Protocols

Interface (facility)	Type of Primary Interface Protocols	Type of Backup Interface Protocols	Comments
reportMaker	SOAP	Manual	Generates and emails reports to ECS Problem Review Board members
tt_licenseUsage	SOAP	Manual	Logs the number of TestTrack floating licenses in use at, typically, 30 minute intervals
tt_resetpasswd	SOAP	Manual	Automated help for resetting a user's password upon submission of special trouble ticket by a TestTrack administrator
tt2ncr	SOAP	Manual	Escalates Trouble Tickets to the EDF
xfer_ncr	SOAP	Manual	Transfers NCRs between projects

4.3.6.4 Databases

TestTrack uses a native database management system bundled with the product. A distinct Trouble Ticketing database, also known as a project, exists for each ECS site. The Trouble Ticketing databases currentlyy in use are:

- ECHO_TTs
- LaRC_TTs
- LPDAAC_TTs
- LPDAAC_Internal_TTs
- NSIDC_TTs
- Riverdale_TTs

4.3.6.5 Special Constraints

Note that while most TestTrack screens are accessible to all operators, only TestTrack administrators have permissions to modify user permissions, security groups, project workflow, dropdown lists, and system notifications. Privileges are set according to DAAC policy.

4.3.6.6 Outputs

Client output from TestTrack (other than that displayed on GUIs) consists primarily of pre-defined and ad hoc reports in HTML format that are prepared on demand. TestTrack launches the operator's browser of choice to display the reports. Reports can also be printed or saved to a file. See Section 4.3.6.8 for a description of the various reports available.

Server output consists primarily of email notices sent to designated recipients when trouble tickets a created, assigned, updated, and closed.

TestTrack also issues prompts when operator input is required, and writes a variety of error and informational messages to project and license server logs (see Section 4.3.6.7). Using the Server Options screen of the TestTrack Server Admin Utility and the License Server Admin Utility, TestTrack administrators can control the amount of logging performed.

Users may also export selected TestTrack records in either XML or tab- or comma-delimited text format. This is done via GUIs accessible by clicking **File → Export → XML File Export** or **File → Export → Text File Export** on the Trouble Ticket List screen's menu bar.

4.3.6.7 Event and Error Messages

TestTrack does not have an error message guide. Below, however, is a sampling of the information typically logged by TestTrack (see Tables 4.3.6-18 through 4.3.6-20.)

Table 4.3.6-18. TestTrack Startup.log File Messages Example

```
Thu Sep  4 02:33:29 2014 <Info>     Server log startup for TestTrack
2014.0.1 Build 24 (Linux/x64)
Thu Sep  4 02:33:29 2014 <Info>     TestTrack Server initialized.
Accepting connection requests. [2014.0.1 Build 24 (Linux/x64)]
9/4/2014 2:33:46   Operations_NCRs (TestTrack Native)
     DFCT 12252    TSTC 4    TSTR 0    RQMT 0    RDMT 0    TASK 3
                   USER 1043 UGRP 11   RPRT 174  DFLT 714  LINK 31   MAIL 1
                   FOLDPUB 14    FOLDPVT 18    FOLDTYPE 1    TYPE 3
     CUDFDFCT 20   CUDFTSTC 4    CUDFTSTR 4
                   CUDFRQMT 7    CUDFRDMT 3    FLDR 0    TRGRESCL 3
     TRGRPREPRE 1  TRGRPREMOD 0
                   TRGRPREEVT 2  TRGRPRENOTFY 27    TRGRPREEXE 0
     TRGRPOSTEXE 0
Thu Sep  4 06:01:55 2014 <Info>     Starting [Auto-close (sev 5)]
escalation rule.
    DbDir=/usr/ecs/OPS/COTS/ttpro2014/TTServDb/TTDbs/Development_NCRs/
Thu Sep  4 06:01:55 2014 <Info>     Completed [Auto-close (sev 5)]
escalation rule in 0.000000 minutes.
Thu Sep  4 11:15:26 2014 <Activity> Attempting to login as "sfrank" to
the Operations_NCRs project using the native client from
::ffff:128.138.64.120 failed because no floating licenses are available.
    DbDir=Operations_NCRs
    UserName=sfrank
```

Table 4.3.6-19. TestTrack Server Admin Utility Log File Messages Example

```
9/3/2014 2:33:29 AMInformation   0    Server log startup for TestTrack
2014.0.1 Build 24 (Linux/x64)

9/3/2014 10:08:34 AM    Warning  0    Error polling on socket from
client at [] POLLHUP - Hang up.       <not logged in>

9/3/2014 11:48:45 AM    Warning  0    Error polling on socket from
client at [] POLLHUP - Hang up.
     /usr/ecs/OPS/COTS/ttpro2014/TTServDb/TTDbs/LPDAAC_TTs/    Jane
Burckhard [Client]

9/3/2014 12:56:28 PM    Warning  0    Socket error when reading request
from [::ffff:71.179.5.27]: 449505600 ; Unrecognized Buffer Format.
     <not logged in>

9/3/2014 1:58:34 PMWarning   0    Sending email failed while logging
into the SMTP server.  Unable to establish the socket connection to
port 25 on host f5eil01v.edn.ecs.nasa.gov.  Please verify the host IP
```

Table 4.3.6-20. License Server Admin Utility Log File Messages Examples

```
08/13/2014 11:03:11 AM  Unusual Activity   0    No floating license is
available.    dnewman

08/13/2014 12:23:44 PM  Unusual Activity   0    User with ID 1035
attempted to login to project with ID 8 of product Requirements
Management at ::ffff:127.0.0.1 with license type 42 but no floating
license was available.  sfrank

08/13/2014 07:23:19 PM  Unusual Activity   -188268386    A login attempt
from TestTrack at ::ffff:127.0.0.1 failed: no credentials were sent.

08/29/2014 03:35:50 PM  Unusual Activity   0    A login attempt from
TestTrack at ::ffff:127.0.0.1 failed: invalid password.   forward3

09/03/2014 12:33:29 PM  Unusual Activity   0    ThreadMgr attempted to
kill an inactive thread -1848452800 for client at
```

4.3.6.8 Reports

TestTrack can produce detail, list, distribution, and trend reports. Table 4.3.6-21 describes a sample of each.

Table 4.3.6-21. Reports

Report Type	Report Description	When and Why Used
Detail of Open Defects	A full report of every Trouble Ticket not in a Closed state, sorted by Trouble Ticket number (see Figure 4.3.6-25).	When and if someone wants a copy of all open Trouble Tickets.
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 (see Figure 4.3.6-26).	When and if someone wants a list of the Trouble Tickets opened or updated during the past week.
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 (see Figure 4.3.6-27).	When and if someone wants to know how evenly work is distributed among the staff.
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 (see Figure 4.3.6-28).	When and if someone wants to review (or forecast) trends among the types of problems reported.

4.3.6.8.1 Sample Reports

Figure 4.3.6-30 through 4.3.6-33 provides samples of the reports described in Table 4.3.6-21.

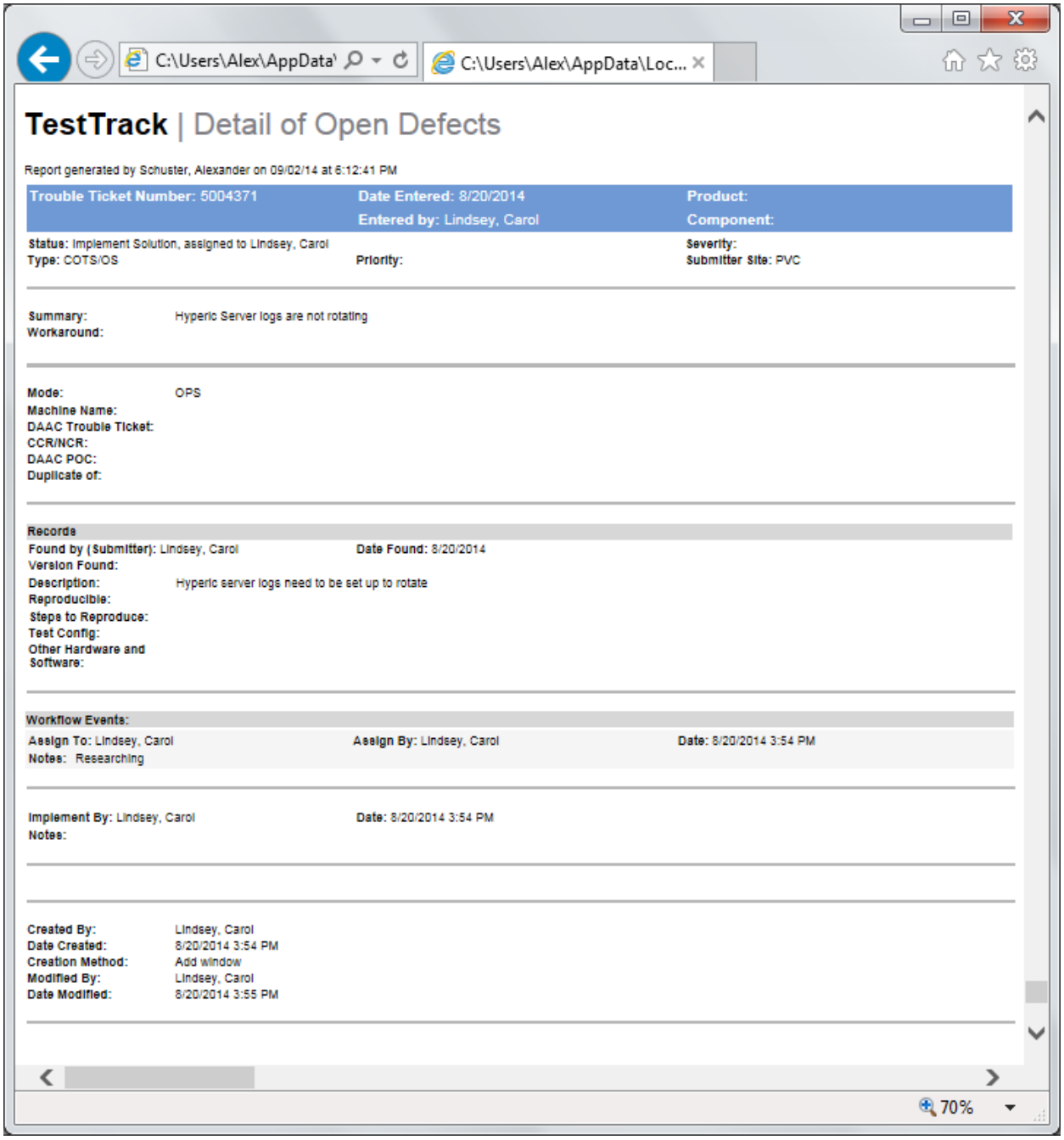


Figure 4.3.6-30. Detail of Open Defects Report

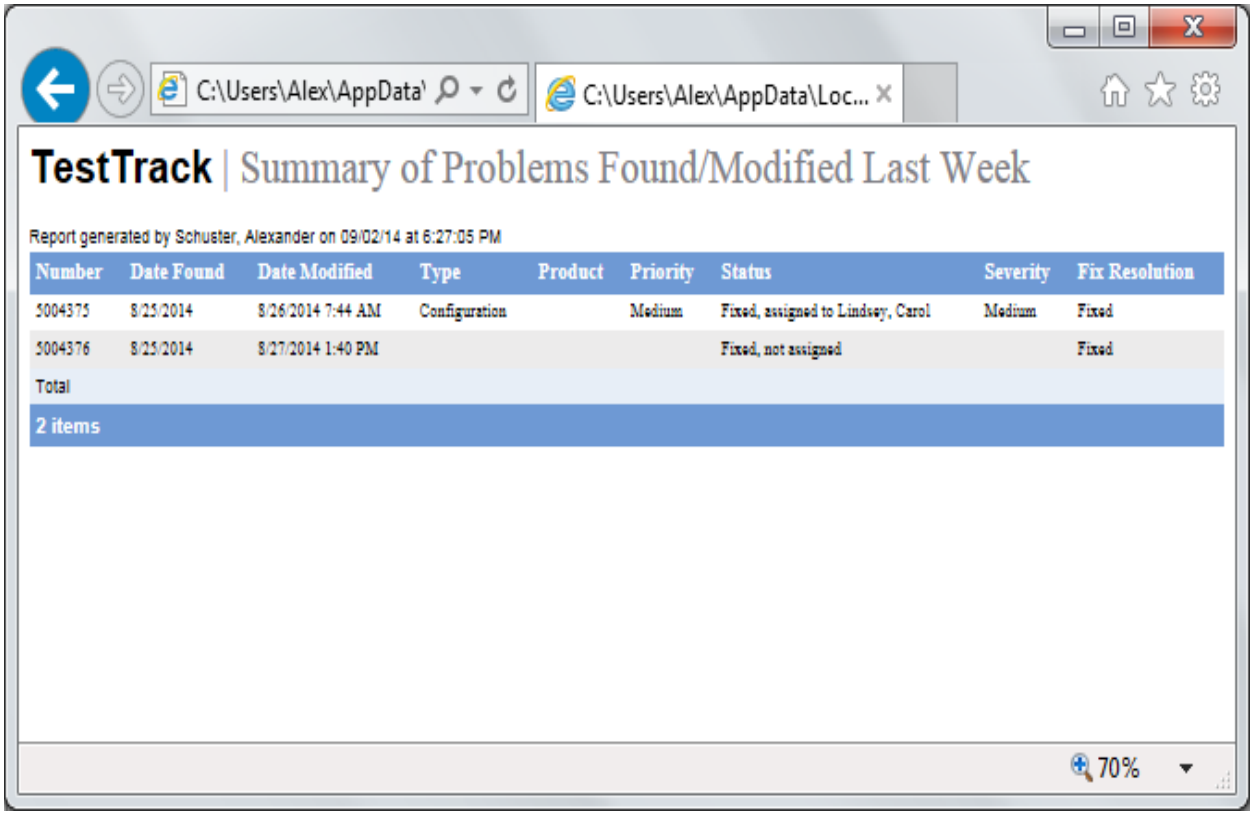
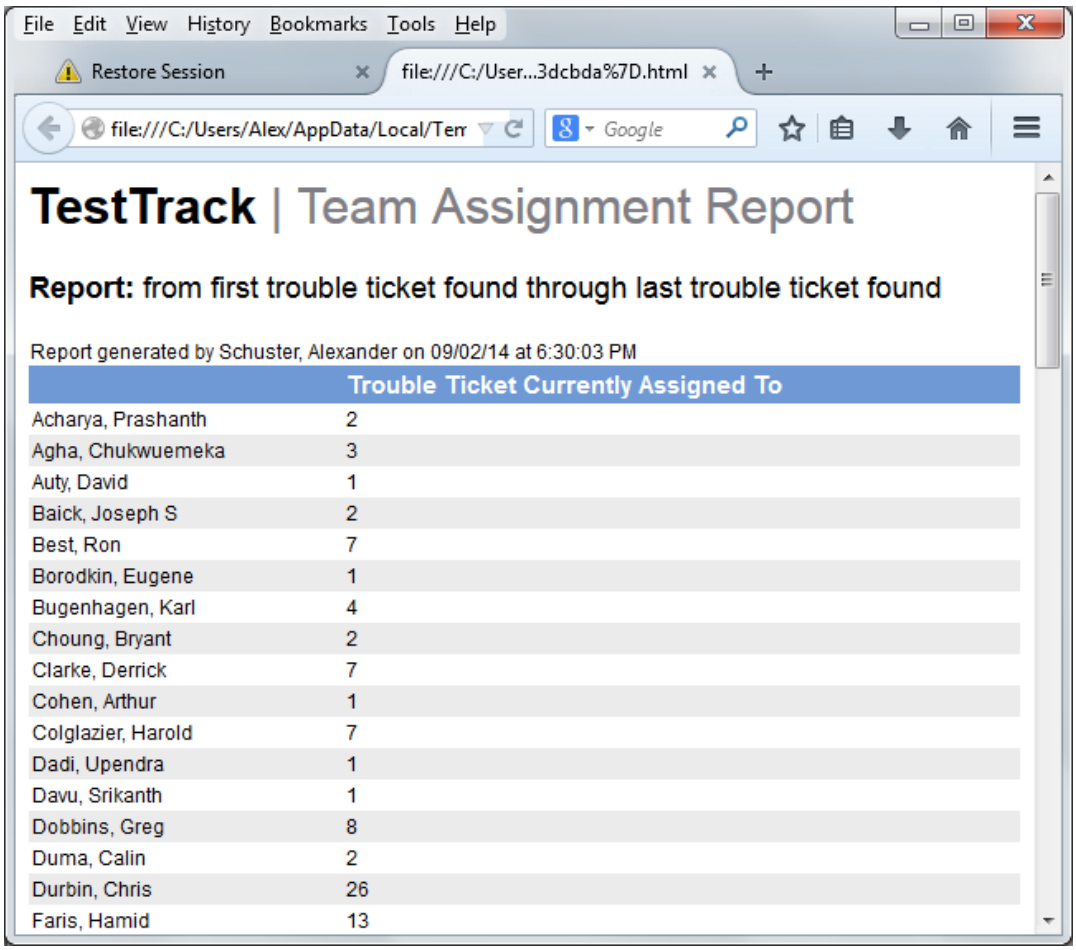
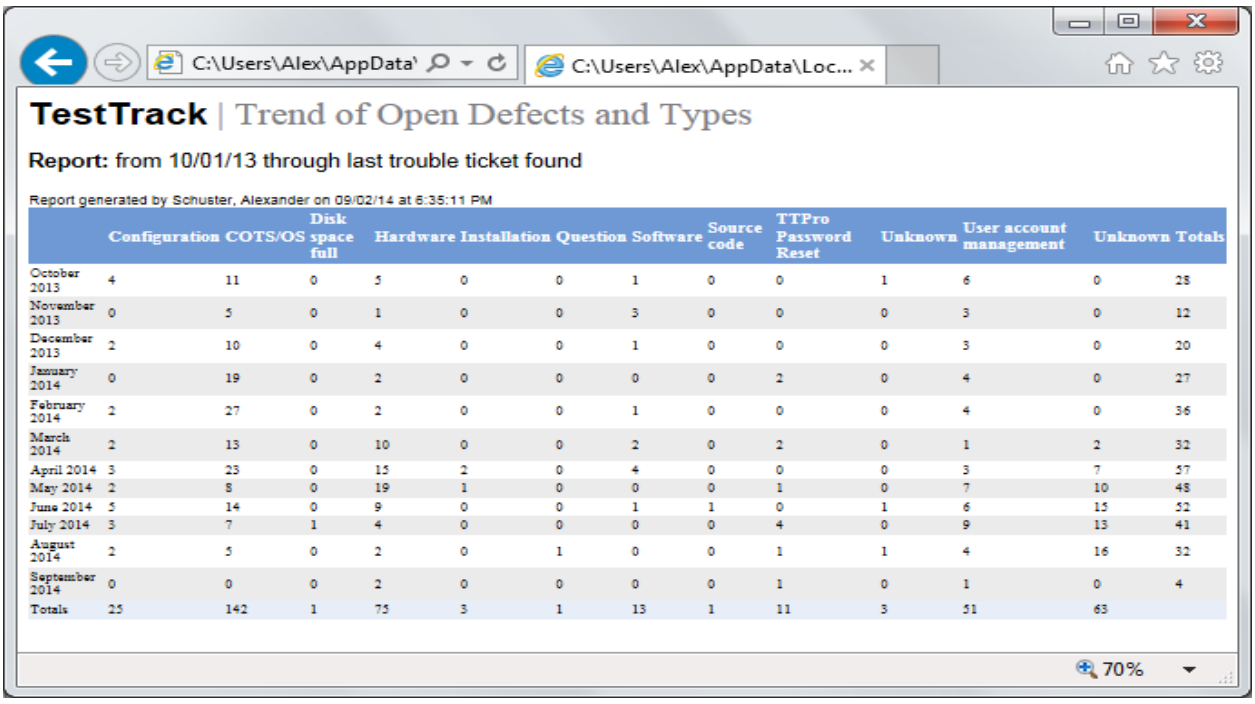


Figure 4.3.6-31. Summary of Problems Found/Modified Last Week Report



	Trouble Ticket Currently Assigned To
Acharya, Prashanth	2
Agha, Chukwuemeka	3
Auty, David	1
Baick, Joseph S	2
Best, Ron	7
Borodkin, Eugene	1
Bugenhagen, Karl	4
Choung, Bryant	2
Clarke, Derrick	7
Cohen, Arthur	1
Colglazier, Harold	7
Dadi, Upendra	1
Davu, Srikanth	1
Dobbins, Greg	8
Duma, Calin	2
Durbin, Chris	26
Faris, Hamid	13

Figure 4.3.6-32. Number of Tickets by Submitter Report



TestTrack | Trend of Open Defects and Types

Report: from 10/01/13 through last trouble ticket found

Report generated by Schuster, Alexander on 09/02/14 at 6:35:11 PM

	Configuration	COTS/OS	Disk space full	Hardware	Installation	Question	Software	Source code	TTPro Password Reset	Unknown	User account management	Unknown	Totals
October 2013	4	11	0	5	0	0	1	0	0	1	6	0	28
November 2013	0	5	0	1	0	0	3	0	0	0	3	0	12
December 2013	2	10	0	4	0	0	1	0	0	0	3	0	20
January 2014	0	19	0	2	0	0	0	0	2	0	4	0	27
February 2014	2	27	0	2	0	0	1	0	0	0	4	0	36
March 2014	2	13	0	10	0	0	2	0	2	0	1	2	32
April 2014	3	23	0	15	2	0	4	0	0	0	3	7	57
May 2014	2	8	0	19	1	0	0	0	1	0	7	10	48
June 2014	5	14	0	9	0	0	1	1	0	1	6	15	52
July 2014	3	7	1	4	0	0	0	0	4	0	9	13	41
August 2014	2	5	0	2	0	1	0	0	1	1	4	16	32
September 2014	0	0	0	2	0	0	0	0	1	0	1	0	4
Totals	25	142	1	75	3	1	13	1	11	3	51	63	

Figure 4.3.6-33. Trend of Open Defects and Types Report

4.3.6.8.2 Report Customization

Reference the TestTrack User Guide or TestTrack Web User Guide for information on creating and customizing reports. The manuals are installed along with the product. They can be accessed separately or by selecting Help on any TestTrack screen.

This page intentionally left blank.

4.4 Security and Accountability

This section describes the security and accountability tools used by DAAC operators:

1. TCP Wrappers and Xinetd
2. OSSEC
3. Cryptographic Management Interface (CMI)

This page intentionally left blank.

4.4.1 TCP Wrappers and Xinetd

TCP Wrappers allow the operator to control access to various network services through the use of access control lists. They also provide logging information of wrapped network services, which can be used to prevent or monitor network attacks. It intercepts incoming network connections and verifies if the connection is allowed before passing the connection onto the actual network daemon. TCP Wrappers allows the operator to monitor and filter incoming requests for the systat, finger, ftp, telnet, rlogin, rsh, exec, tftp, talk, and other, older network services. TCP Wrappers is not used directly, however. It is used in conjunction with the Linux super internet daemon xinetd (pronounce zye-net-d). Xinetd supports older daemons that typically require in-the-clear authentication such as wu-ftpd. Most of the available daemons are disabled. Full descriptions of these Linux services can be obtained using the "man" command, e.g., man systat.

NOTE: The only DAACs that still use TCP Wrappers are NSIDC and ASDC.

TCP Wrappers perform the following functions automatically:

- **Access control**: access can be controlled per host, per service, or combinations thereof.
- **Host name spoofing**: verifies the client host name that is returned by the address->name DNS server, by asking for a second opinion from a local DNS server.
- **Host address spoofing**: the wrapper programs can give additional protection against hosts that claim to have an address that lies outside their own network.
- **Client username lookups**: the protocol proposed in RFC 931 provides a means to obtain the client user name from the client host. The requirement is that the client host runs an RFC 931-compliant daemon. The information provided by such a daemon is not used for authentication purposes but it can provide additional information about the owner of a TCP connection.
- **Multiple ftp/gopher/www archives on one host**: `daemon@host' access control patterns can be used to distinguish requests by the network address that they are aimed at. Judicious use of the `twist' option (see the hosts_options.5 file supplied with TCP Wrappers, `nroff -man' format) can guide the requests to the right server. These can be servers that live in separate chroot areas, or servers modified to take additional context from the command line, or a combination.
- **Sequence number guessing**: client username lookup protocol can help to detect host impersonation attacks. Before accepting a client request, the wrappers can query the client's IDENT server and find out that the client never sent that request.

Additional information on TCP Wrappers can be obtained at the following URL:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-TCP_Wrappers_and_xinetd.html#sect-Security_Guide-TCP_Wrappers_and_xinetd-TCP_Wrappers

TCP Wrappers is used to perform the operator functions listed in Table 4.4.1-1.

Table 4.4.1-1. Common ECS Operator Functions Performed with TCP Wrappers

Operating Function	Command/Action	Description	When and Why to Use
Monitor potentially malicious attempts to access network services.	Check TCP Wrappers log using a text editor.	Program continuously runs in the background appearing to malicious external client service requests as a normal inetd daemon process.	To check for evidence of an attempt of breaking-in.

4.4.1.1 Quick Start Using TCP Wrappers/Xinetd

TCP Wrappers provides a library of tiny daemon wrapper programs which are integrated into the xinetd application. The daemons each correspond to a service provided by the host operating system. The daemons are registered with the service, which results in the operating system invoking the daemon each time that service is invoked. The daemons perform their function(s) and terminate. A common function is to log the name of the client host and requested service. They do not exchange information with client or server applications, and impose no overhead on the actual conversation between the client and server applications. Optional features include: access control to restrict what systems can connect to what network daemons; client user name lookups with the RFC 931 protocol; additional protection against hosts that pretend to have someone else's host name; and additional protection against hosts that pretend to have someone else's host address.

4.4.1.1.1 Command Line Interface

One may check if a service is using TCP Wrappers by using the command:

ldd <binary-name> | grep libwrap

The TCP Wrappers cannot be invoked or accessed from the command line. The TCP Wrapper daemons are invoked by the operating system service to which they are registered. The daemons terminate upon completing their function.

4.4.1.2 TCP Wrapper Main Screen

TCP Wrapper does not have a graphical user interface.

4.4.1.3 Required Operating Environment

For all COTS packages, appropriate information on operating environments, tunable parameters, environment variables, and a list of vendor documentation can be found in a CM controlled document for each product. To find the documentation for TCP Wrappers, refer to the Release Notes for Secure Shell posted on the EED Baseline Information System web page at your local site. Also refer to the Linux hosts.allow man page.

4.4.1.4 Databases

None

4.4.1.5 Special Constraints

None

4.4.1.6 Outputs

Check /var/log/messages for xinetd references.

4.4.1.7 Event and Error Messages

The log file provides the following information for each entry: data and time; host sever name; type of service requested and port that provides that service; answer given to the request connection (connect/refused); client host name.

4.4.1.8 Reports

None

This page intentionally left blank.

4.4.2 OSSEC

OSSEC is an open source host-based intrusion detection system. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.

OSSEC is a scalable, multi-platform, open source host-based intrusion detection system (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response.

It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows. Notable features include:

- Multi platform
  - OSSEC lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms such as Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac and VMware ESX.
- Real-time and Configurable Alerts
  - OSSEC lets customers configure incidents they want to be alerted on which lets them focus on raising the priority of critical incidents over the regular noise on any system. Integration with SMTP, SMS and syslog allows customers to be on top of alerts by sending these on to e-mail and handheld devices such as cell phones and pagers. Active response options to block an attack immediately are also available.
- Centralized management
  - OSSEC provides a simplified centralized management server to manage policies across multiple operating systems. Additionally, it also lets customers define server specific overrides for finer grained policies.
- Agent and agentless monitoring
  - OSSEC offers the flexibility of agent based and agentless monitoring of systems and networking components such as routers and firewalls. It lets customers who have restrictions on software being installed on systems (such as FDA approved systems or appliances) meet security and compliance needs.
- File Integrity checking
  - File integrity checking (or FIM - file integrity monitoring) is to detect changes and alert you when they happen. Any file, directory, or registry change will be alerted and logged.
- Log Monitoring
  - OSSEC collects, analyzes, and correlates logs to let you know if something wrong is going on (attack, misuse, errors, etc).

- Rootkit detection
  - You can be notified when trojans, viruses, etc change your system in any way.

4.4.2.1 Configuration

The configuration file consists of the following configuration sections:

- global - default options used everywhere in the system.
- email_alerts - granular e-mail alerting options.
- rules - list of .xml rule files to be included.
- Each .xml rule file includes the format for matching what services to be monitored. The file structure includes "rule id", "level" of the alert, "match" what string were trying to match, "description" of the alert, and the group that the alert belongs to.
- There is a .xml file for each type of service monitored
- Rules or .xml files are located in /usr/ecs/OPS/COTS/ossec/rules/
- syscheck - configuration related to the syscheck - integrity check.
- Configuration includes the frequency that syscheck is executed, the directories to check and the files that should be ignored.
- rootcheck - configuration related to the rootcheck - rootkit detection.
- Includes pointers to the rootkit detection configuration files and system audit information. Rootkit files are located under /usr/ecs/OPS/COTS/ossec/etc/shared
- localfile - options related to the log files to be monitored.
- remote - configuration related to what is monitored to log remote connections.
- alerts - e-mail and log alerting options.
- client - agent related options.
- Currently has the HIDS server ip address configured.
- database_output - Database output options.
- command - active-response configuration.

4.4.2.2 CLI-based Administrative commands

- agent-control – give you an agent list, status or extract information from an agent, and initiates scans.
- List_agents – list all agents, inactive and connected (active) agents.
- Manage_agents – tools to add/remove agents on the management server
- ossec-control – get status, start and stop the ossec daemon.
- Rootcheck_control – manages the policy and auditing database.

- Lists available or active agents, Clears the database, print resolved or outstanding issues

- Syscheck_control – manages the integrity checking database
  - Lists available or active agents, clears the database, prints information about modified files, lists modified files or registry entries for the agent.
- Syscheck_update – update syscheck database for all agents or specific agents. Update syscheck database locally.
- Ossec logs are located in /usr/ecs/OPS/COTS/ossec/logs. You can manually check the logs for resolved and outstanding issues using the rootcheck_control command and check modified files using the syscheck_control command.

4.4.2.3 GUI-base operation

- OSSEC uses a web based interface for normal operation. From an approved browser, use the URL:

  http://x4msl10:8001

  where x is the prefix for your DAAC

  (l = ASDC, n=NSIDC, l=LP DAAC, p=PVC)

OSSEC is used to perform the operator functions listed in Table 4.4.2-1.

Table 4.4.2-1. Common ECS Operator Functions Performed

Operating Function	Command	Description	When and Why to Use
Change the configuration file.	Edit the specific configuration file using the vi editor.	Specify which file(s) should be monitored.	When another file needs to be monitored. Checks the integrity of the file system specified when the daemon is started.
Verify that OSSEC agents are functioning	OSSEC list-agents	Compares files' current signatures against the database and emails the operator a notification for changed files.	As necessary to verify that agents are running on required platforms.
Change configuration on an agent	OSSEC manage-agent	Updates working configuration of agent	As necessary to maintain operation.

4.4.2.4 Required Operating Environment

OSSEC runs on all Linux hosts.

For all COTS packages, appropriate information on operating environments, tunable parameters, environment variables, and a list of vendor documentation can be found in a CM controlled document for each product. To find the documentation for OSSEC, refer to the Release Notes posted on the EED Baseline Information System web page at your local site.

4.4.2.5 Databases

OSSEC uses an internal data store of captured information. The user can update this data store through the command line interface.

4.4.2.6 Special Constraints

None

4.4.2.7 Outputs

OSSEC generates the outputs presented in Table 4.4.2-2 below in the filename specified on the command line invocation. A sample of the generated report is shown in Section 4.4.2.8, Figure 4.4.2-1.

Table 4.4.2-2. OSSEC Outputs

Output	Description and Format
Click on "Stats"	See below.

4.4.2.8 Event and Error Messages

Not available.

4.4.2.9 Reports

A statistics report is available from the GUI by clicking on “Stats”.

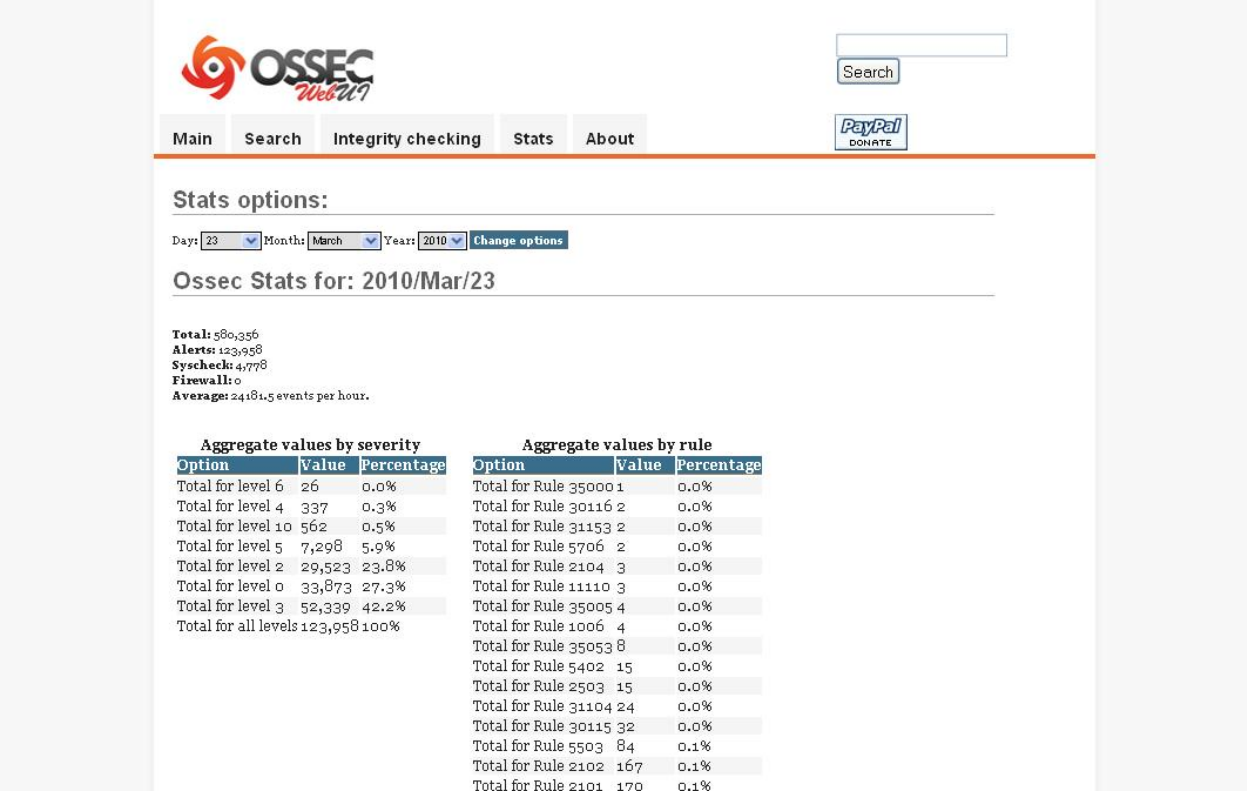


Figure 4.4.2-1. OSSEC Sample Statistics

This page intentionally left blank.

4.4.3 Cryptographic Management Interface (CMI)

The Cryptographic Management Interface (CMI) GUI program, EcSeAuthnProg, is used by operations personnel to generate a randomized username and password (though only the password is currently used) given a key. There is one key for each EED server and is the same as the Program ID stored in a server's configuration file. This tool is most often used to generate passwords for Sybase and FTP user accounts. It is therefore recommended that access to this tool be restricted to Sybase and Unix System Administrators only.

CMI is used to perform the operator functions listed in Table 4.4.3-1.

Table 4.4.3-1. Common ECS Operator Functions Performed with CMI

Operating Function	Command / GUI	Description	When and Why to Use
Start *CMI* program.	*EcSeAuthnProg*	This brings up the *ConnectAuth* GUI.	In order to obtain the user password for a given application key.
Generate password.	*CMI Main Screen (ConnectAuth GUI)*	This causes the program to generate a randomized username and password.	This is only needed when an EED server requires a new user account.

4.4.3.1 Quick Start Using CMI

The CMI Main Screen is a custom developed GUI utility and should be used only by operations personnel.

To execute CMI from the command line prompt, enter:

> **EcSeAuthnProg**

4.4.3.2 CMI Main Screen

Figure 4.4.3-1 is the CMI GUI Screen, which comes up when the CMI program is run. It contains three fields:

- Application Key field
- User Id field
- Password field

Operations personnel fill out the first field by entering the application key. In response, CMI returns a user name and password, which are displayed in the associated fields.

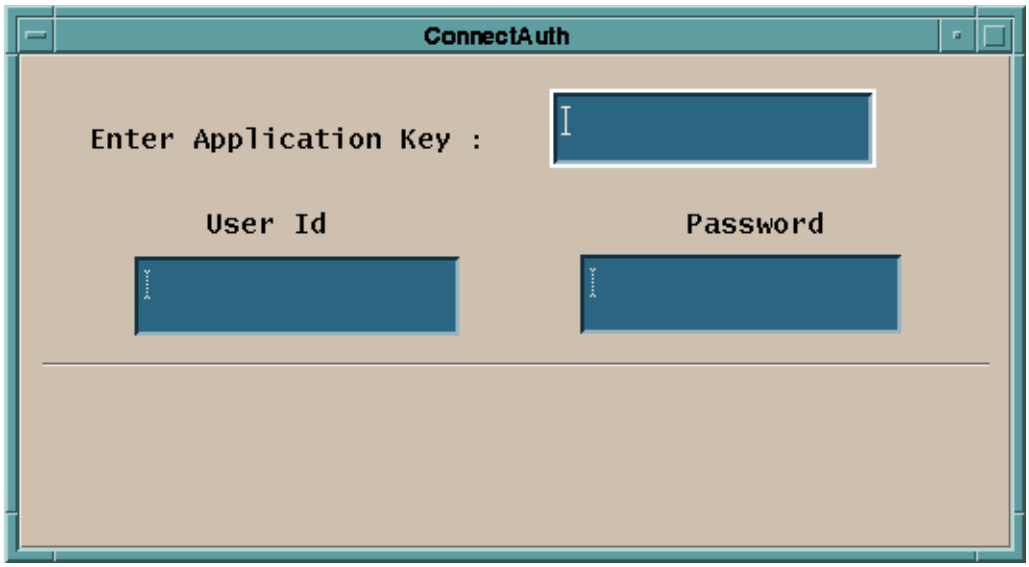


Figure 4.4.3-1. CMI Main Screen

Table 4.4.3-2 describes all the fields found in the CMI Screen in Figure 4.4.3-1.

Table 4.4.3-2. CMI Field Descriptions

Field Name	Data Type	Size	Entry	Description
Application Key	Integer	1 to 10 digits	Required	Key identifying an application.
User Id	Character	8	Generated by *EcSeAuthnProg* program	Displays the randomized user id based on the key (this field is not used).
Password	Character	8	Generated by *EcSeAuthnProg* program	Displays the password to be used when creating the account.

4.4.3.3 Required Operating Environment

The EcSeAuthnProg depends on a data file, which must be called "data" and must exist in the directory from which the tool is invoked. The data file is the same file as the EcSeRandomDataFile located in **$ECS_HOME/<mode>/CUSTOM/security,** only with a different name. CMI requires no other configuration files. It can run on a Linux 2.x platform.

4.4.3.3.1 Interfaces and Data Types

CMI utilizes no special data types or interfaces.

4.4.3.4 Databases

None

4.4.3.5 Special Constraints

A data file called "**data**" must exist in the execution directory. The data file must be the same file as the EcSeRandomDataFile.

4.4.3.6 Outputs

All information is displayed on the CMI screen.

4.4.3.7 Event and Error Messages

The CMI program issues error messages.

4.4.3.8 Reports

None

This page intentionally left blank.

4.5 Science Software Integration and Test (SSI&T)

This section describes the tools used by DAAC operations personnel who are Science Software Integration and Test (SSI&T) specialists. The function of SSI&T is to prepare the science software received from the Instrument Teams for DAAC production. All the COTS tools/products are documented in separate product specific documentation. These tools are only identified in this section. Operators must verify that COTS documentation matches the product version in use. Finally, there are custom applications that are unique to the SSI&T activity. These tools are described in the following subsections:

4.5.1 Science Software Integration and Test (SSI&T)

This page intentionally left blank.

4.5.1 Science Software Integration and Test (SSI&T)

The SSI&T contains comparison tools, and COTS tools for comparing and analyzing environment programs. All programs can be invoked from the UNIX command line.

The HDF file comparison tool is contained in the SSI&T subset of tools.

4.5.1.1 Linux Platform

Table 4.5.1-1 lists the SSI&T command line interfaces for the Linux workstation.

Table 4.5.1-1. SSI&T Command Line Interfaces

Command Line Interface	Description and Format	When and Why Used
EcClHdiff	HDF file comparison (command line)	Compare 2 HDF files.

4.5.1.1.1 HDF File Comparison - hdiff

The HDF File Comparison hdiff tool (for HDF4 based files) is started from the command line **$ECS_HOME/CUSTOM/utilities/EcClHdiff**. The command line will prompt the user for input. There is no graphics screen for this function. It is run through the command line interface. The operator is also provided with a list of options for different kind of comparisons the tool can perform on HDF4 files (Figure 4.5.1-1). After the operator enters two HDF filenames (HDF4 based), the differences between the files are displayed.

Figure 4.5.1-1. HDF (hdiff) Options

The following is an example of the HDiff tool (Figure 4.5.1-2). After asking for options, there will be a prompt asking for the mode of operations. Next, the tool prompts the user for the locations of the HDF files to be compared. Full paths are required. Finally, the user will be prompted for where to store the resulting output as a text file (full path required).

Afterward, the user can press ENTER to compare two other files or <q> to quit.

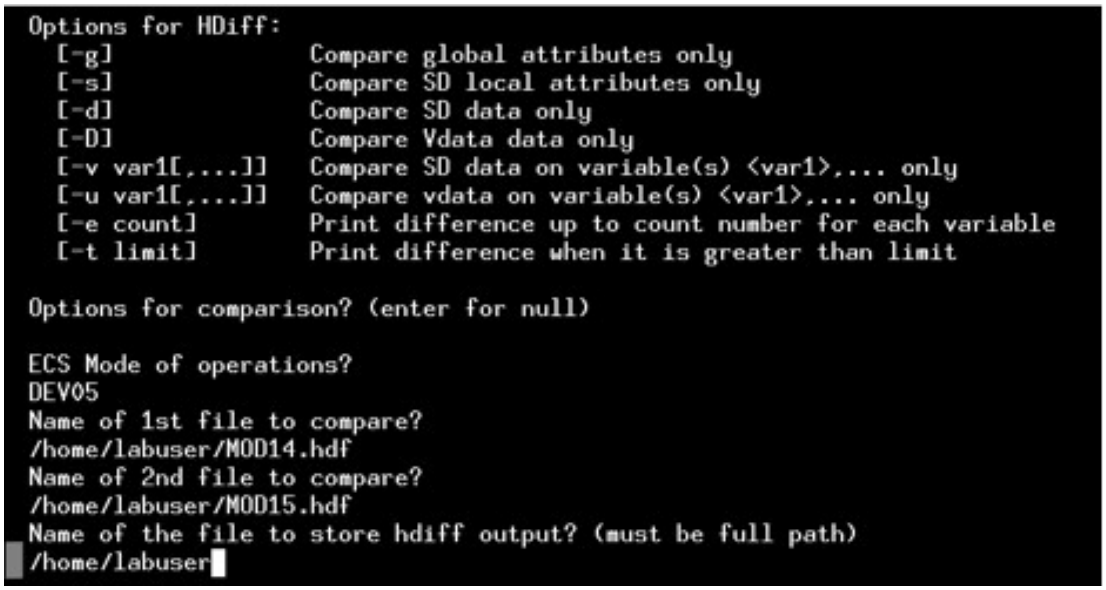


Figure 4.5.1-2. HDiff Example Output

4.6 ECS Data Pool Ingest

ECS Data Pool Ingest provides the software capability to acquire data by various protocols and transfer the data into the ECS system. The ECS Data Pool Ingest subsystem also stores and manages request information, performs data preprocessing, inserts data into the Online Archive, and copies data into the tape archive. The ECS Data Pool Ingest subsystem provides a GUI which allows the operator to view past ingest activities, monitor and control ingest requests and services, view operator alerts, disposition operator interventions, and modify system and external data provider parameters.

This page intentionally left blank

4.6.1 Data Pool Ingest GUI

The Data Pool (DPL) Ingest GUI is a web-based interface that allows operators to access and manipulate the DPL Ingest system. Using this GUI, an operator can monitor and fix Ingest requests, view system alerts, and see at a glance the status of the DPL Ingest system in part and in whole. The DPL Ingest GUI also allows in-depth configuration of the entire DPL Ingest system without the operator having to manually configure the DPL Ingest database. It provides a fast and secure way to easily manage the entire DPL Ingest system, complete with full operator permission configuration and management so that only authorized persons may perform actions or change configuration settings.

Since the DPL Ingest GUI is a web-based interface, it can be accessed from virtually anywhere there is access to the internal network. No custom software installation is required – all that is needed is a web browser (see Section 4.6.1.28 Browser Requirements). Because this is a web-based application, the DPL Ingest GUI can be run by any number of operators from any number of locations, even remote locations, provided that a remote connection is properly configured.

This document shows and explains in detail all of the available features and functionality of the DPL Ingest GUI, from the first login to complex operator actions and configuration, as well as tips for getting extra help.

4.6.1.1 Login Page

This page first appears when the application is loaded. The operator will be required to enter a pre-assigned user name and password, as shown in Figure 4.6.1-1. Once the operator is logged in, the home page will be displayed and the application will be enabled.

If the authorization scheme has been disabled, the home page (shown in Figure 4.6.1-2) would be displayed immediately instead of the login page, and the operator will not be required to log in.

Figure 4.6.1-1. Login Page

Using the GUI in Protected Mode

If your DAAC requires a password-protected login with different permission levels, the following applies:

- Sort settings are remembered for each session – that is, every time an operator logs in. They are reset when the operator logs off or a new session is started.
- Filter settings are always remembered for each operator, since these are stored in the database.

Using the GUI in Open Mode

If your DAAC does *not* require a password-protected login, then each operator essentially uses a single "virtual operator" which has all permissions and stores a single set of filter settings that are shared across all sessions. This means that an operator at one terminal can affect the filter settings of an operator at another terminal.

Sort settings are not stored in the database and are therefore remembered for each session. Please note however, that sort settings may be lost if the browser is closed of a new session is otherwise started.

Session Timeout

Depending on the installation of Tomcat at your particular site, the session timeout can vary and is not configurable through the GUI.

Miscellaneous Features

- **The Reset Button**: Throughout the GUI, you will see "Reset" buttons on some pages. These simply reset the form values so you can start over again – pressing/clicking Reset does not submit any changes to the database.
- **Whitespace in forms:** In general, whitespace is stripped from most text input fields unless it is meant to contain whitespace, like comment fields. For example, on the Provider Configuration page to add a new Data Provider, all of the input fields are stripped of any accidentally input whitespace when submitted.

4.6.1.2 Home Page

The Home Page provides a general overview of the Data Pool Ingest system status, as shown in Figure 4.6.1-2. This page includes the following:

- General system statistics
- The Data Pool Ingest statuses, which may be suspended if active, and resumed if suspended. These include:
    - General Ingest Status
    - Email Service Status
- The status of the Ingest services, which **cannot** be changed by the operator, including (see also Figure 4.6.1-2):
    - The Notification Service
    - The Polling Service
    - The Processing Service

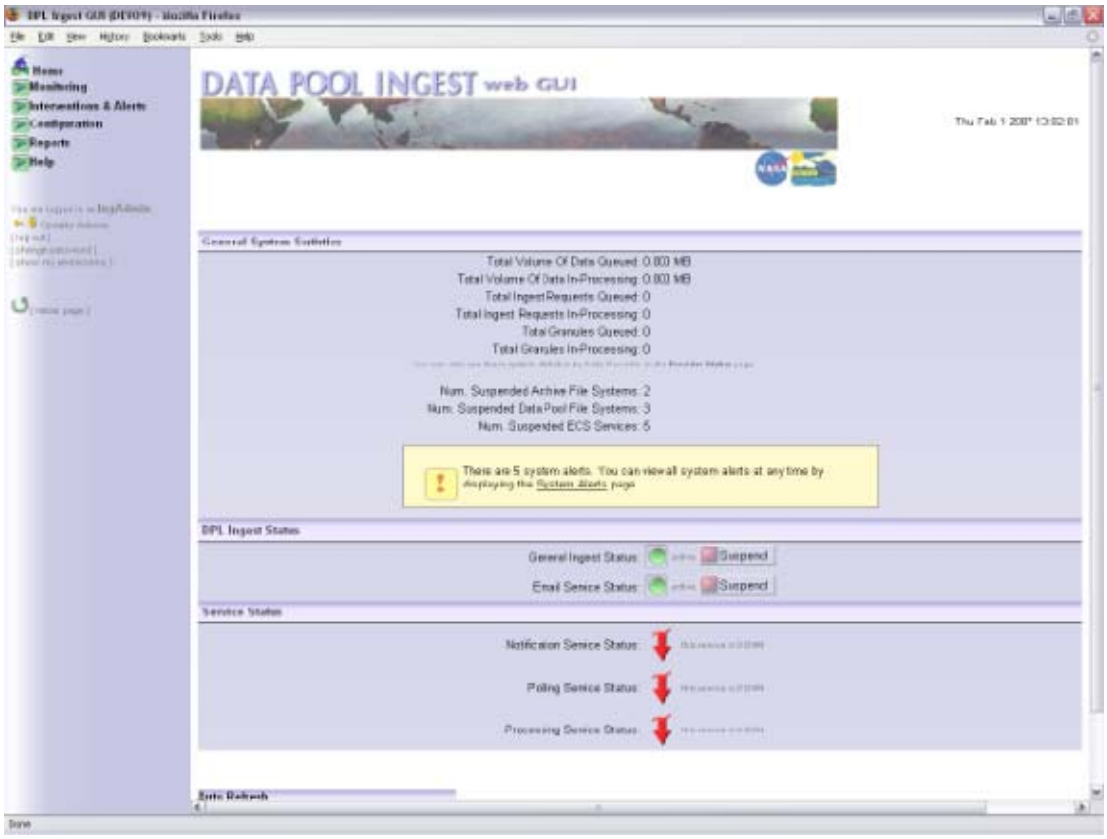


Figure 4.6.1-2. Home Page

4.6.1.2.1 General System Statistics

This section provides general information about current requests and granules in the system, as well as the various services and file systems used in processing. Summary information is not included about providers and transfer hosts, though this data can be found on the Provider Status page (Section 4.6.1.10) and the Transfer Host Status page (Section 4.6.1.13).

Detail descriptions of the data found in this section is available in Table 4.6.1-1.

Tabie 4.6.1-1. Home Page Field Descriptions

Field Name	Description
Total Volume of Data Queued	Sum of the size of all files of all granules that have not yet been activated
Total Volume of Data In-Processing	Sum of the size of all files of all granules that are currently active, and not suspended or in a terminal state
Total Ingest Requests Queued	Total number of requests that have not yet been activated
Total Ingest Requests In-Processing	Total number of requests that are currently active, and not suspended or in a terminal state
Total Granules Queued	Sum of all granules in active or queued requests that have not yet been activated
Total Granules In-Processing	Sum of all granules in active or queued requests that are currently active, and not suspended or in a terminal state
Num Suspended Archive File Systems	Total archive file systems that have been suspended, either automatically by the server or manually by operator
Num Suspended Data Pool File Systems	Total data pool file systems that have been suspended, either automatically by the server or manually by operator
Num Suspended ECS Services	Total ECS service hosts that have been suspended, either automatically by the server or manually by operator

4.6.1.2.2 DPL Ingest Status

This section consists of two buttons that enable the user to halt various actions throughout the data pool ingest system.

General Ingest Status – By pressing this button, the operator is able to stop polling from all polling locations and prevent any new granules from being activated. Any granules that are already active will complete ingest. These actions can easily be resumed by pressing the "Resume" button.

Email Service Status – By pressing this button, the operator will stop any further email notifications from being sent concerning completed, cancelled, failed, or terminated requests from any provider. Once the button is pressed again, email notifications will resume and emails will be sent for all requests from providers configured for email notifications that completed while email service was suspended.

4.6.1.2.3 Service Status

This page indicates the status of the three primary services that make up the Data Pool Ingest system.

The Ingest services cannot be started and stopped via the GUI. Instead, they are managed using start and stop scripts found in the utilities directory of the given mode. For the status of these services to be accurate, the IngestServiceMonitor script must also be running for each mode.

This script is installed in the utilities directory of each mode and can be started with the command: EcDlIngestServiceMonitorStart [MODE].

The services are as follows:

- *Notification Service Status* - Indicates whether the notification service is up or down. If up, no notifications will be sent, but a queue of notifications will be collected and distributed once the service is restarted.
- *Polling Service Status* - Indicates whether the polling service is up or down. If this service is down, PDRs will not arrive from any configured polling location, but any PDRs that remain in the directories will be added once the service is restarted.
- *Processing Service Status* - Indicates whether the processing service is up or down. If this service is down, no actions on any requests or granules will start, continue, or complete and Granules will "hang" in their current state.

4.6.1.3 The Navigation Panel

Navigation throughout the DPL Ingest GUI is accomplished through an Explorer-like menu in the left pane of the application, as shown in Figure 4.6.1-2 and Figure 4.6.1-3. These menus expand and contract to hide or view menu items under each category.

The navigation panel is static; it will not reload every time a new menu item is selected.

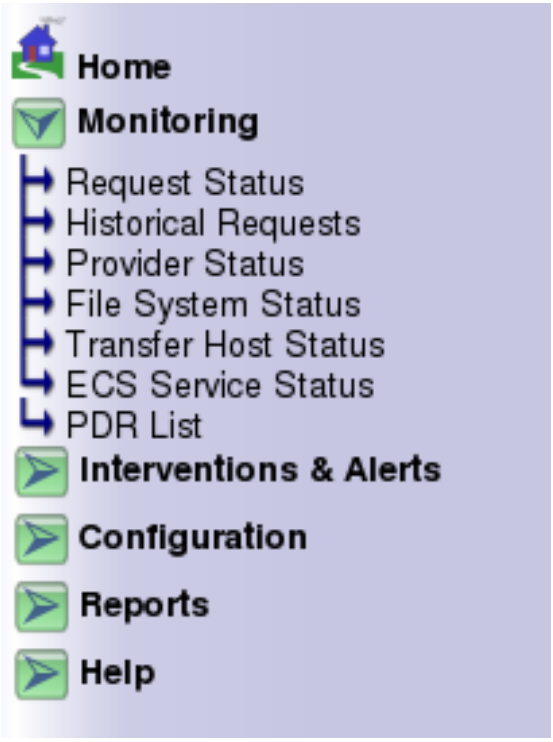


Figure 4.6.1-3. Navigation Panel

A Note on the Back and Forward Buttons

In order to properly navigate through the application, the operator should not use the browser's built-in back and forward browser buttons (Figure 4.6.1-4), as this may cause an error to occur in the application. All navigation should be accomplished through use of the navigation panel and list navigators (e.g., custom back and forward buttons for lists of requests and granules).

Figure 4.6.1-4. Built-in Back/Forward Browser Buttons

Error Pages

When errors occur (e.g., an invalid action was sent), the GUI will display such errors on the page for which it was generated and in most cases the items causing the error will be highlighted in red. An example is trying to resume an already active Provider, as shown in Figure 4.6.1-5.

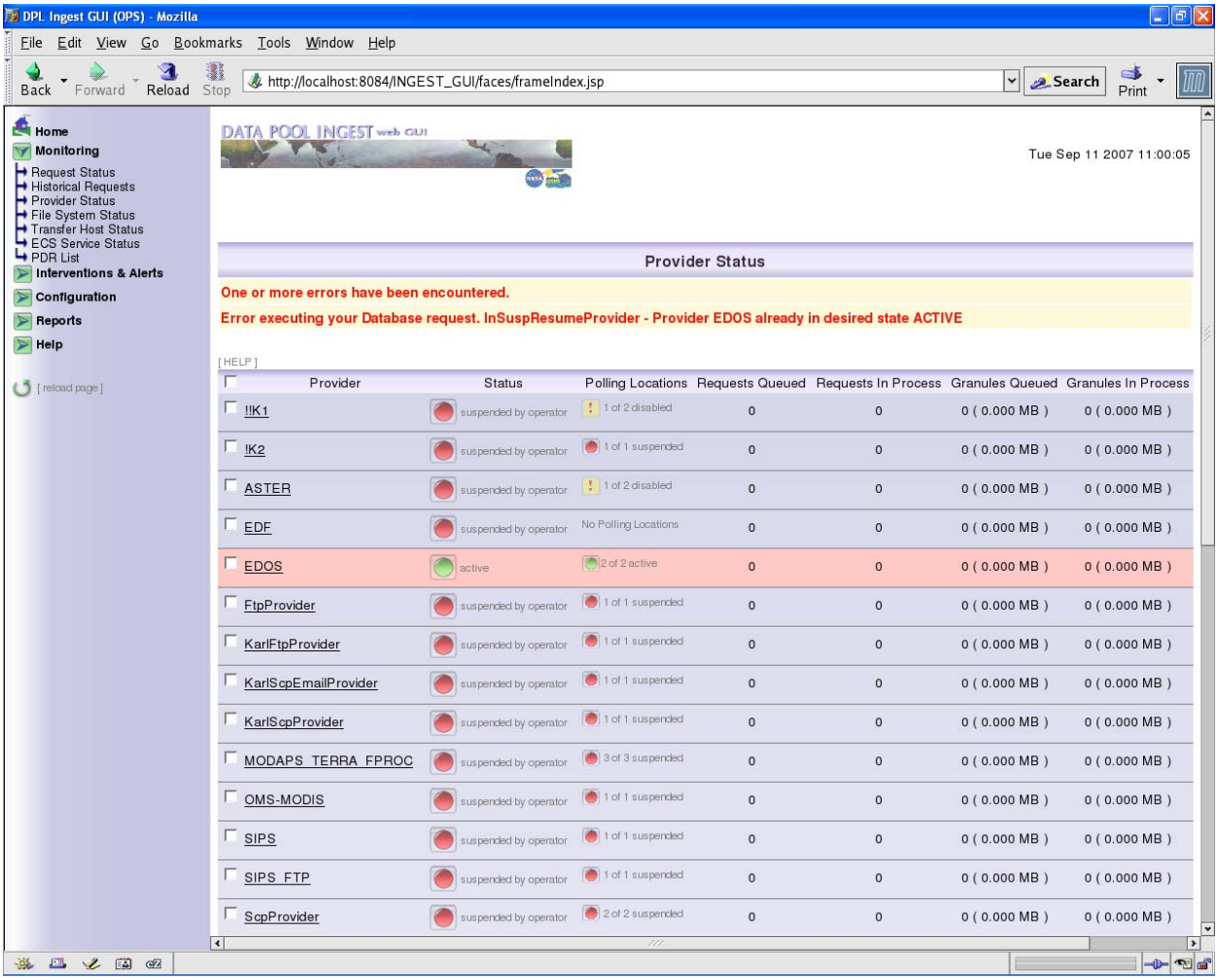


Figure 4.6.1-5. Error Indicators

In other cases, the GUI may have trouble processing an operator's action for an unknown reason. Although this is rare, an error screen will be displayed allowing you to reset your session so that the GUI can properly process further actions. See Figure 4.6.1-6 for an example. This error screen also displays the specific problem so that a detailed error message can be sent to a qualified person for analysis if the error occurs frequently.

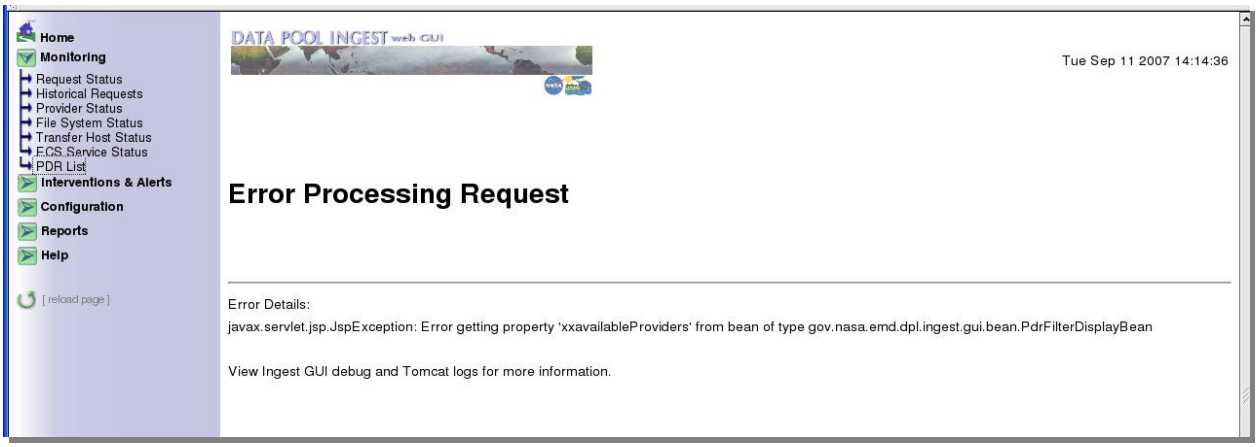


Figure 4.6.1-6. Error Processing Request

4.6.1.3.1 Current Operator Settings

The navigation panel also contains a section below the menus that allows the current logged-in operator to perform the following actions (see Figure 4.6.1-7):

- Log out
- Change your password
- Show all of your permissions

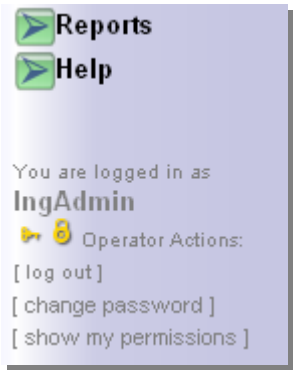


Figure 4.6.1-7. Operator Information Panel

Depending on the settings of the currently logged in operator, various functions of the DPL Ingest GUI will be disabled. An example of how disabled functions will appear is shown in Figure 4.6.1-8.

Figure 4.6.1-8. Disabled Permissions

Operator Actions Explained

Log Out

This allows you to log out of the current session (without closing the browser). The login page will be displayed upon successful logout (see Figure 4.6.1-9).

Figure 4.6.1-9. Log Out Button

Change Password

Click on "change password" to change the current operator's password – a box will appear below the link, as shown in Figure 4.6.1-10. Type the new password into the two boxes and click "Ok."

Figure 4.6.1-10. Operator Password Settings

Show My Permissions

Click on "show my permissions" to view or hide the current permissions – a box will appear below the link, as shown in Figure 4.6.1-11.

Figure 4.6.1-11. Operator Permission Settings

4.6.1.4 Pagination Arrows

On the Request Status page and details page, Historical Requests page and details page, and the Open Interventions page and details page, there are a set of pagination arrows used for maneuvering through the lists of requests and granules that are displayed. The maximum number of rows displayed at a time is configurable by the operator.

The items on the list that will be displayed on each page will be determined by the current sorting setting (see Section 4.6.1.6.3).

The pagination arrows are shown in the upper left-hand corner of any list of requests or granules, as shown in Figure 4.6.1-12.

Figure 4.6.1-12. Pagination Arrows on the Historic Requists Page

The meanings of these icons are as follows:

-  - Go to the first page of the list, as determined by the current sorting setting. If you are already on the first page, the button will be disabled.
-  - Go to the previous page in the list, as determined by the current sorting setting. If you are already on the first page, the button will be disabled.
-  - Go to the next page in the list, as determined by the current sorting setting. If you are already on the last group in the listing, the button will be disabled.
-  - Go to the last page in the list. If you are already on the last page, the button will be disabled.

4.6.1.5 Automatic Screen Refresh

The monitoring pages of the DPL Ingest GUI have an automatic screen refresh feature that allows the operator to control how often the page is automatically reloaded with new information. This is controlled by a small panel at the bottom of each screen, as shown in Figure4.6.1-13.

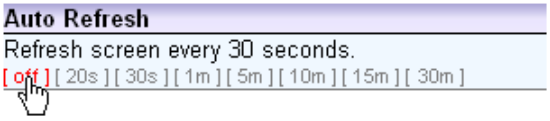


Figure 4.6.1-13. Auto Refresh Control Panel

The operator may change the refresh rate for any page or completely turn it off. Note that each page has an independent refresh rate and that these settings are remembered for the current session only – they are lost if the operator logs out or the application is restarted.

To change the refresh settings, click on the desired rate (or off). The page will reload and the new settings will take effect.

A dynamic clock will appear in the upper right-hand corner, informing the operator how long it will be until the next refresh, as shown in Figure 4.6.1-14.

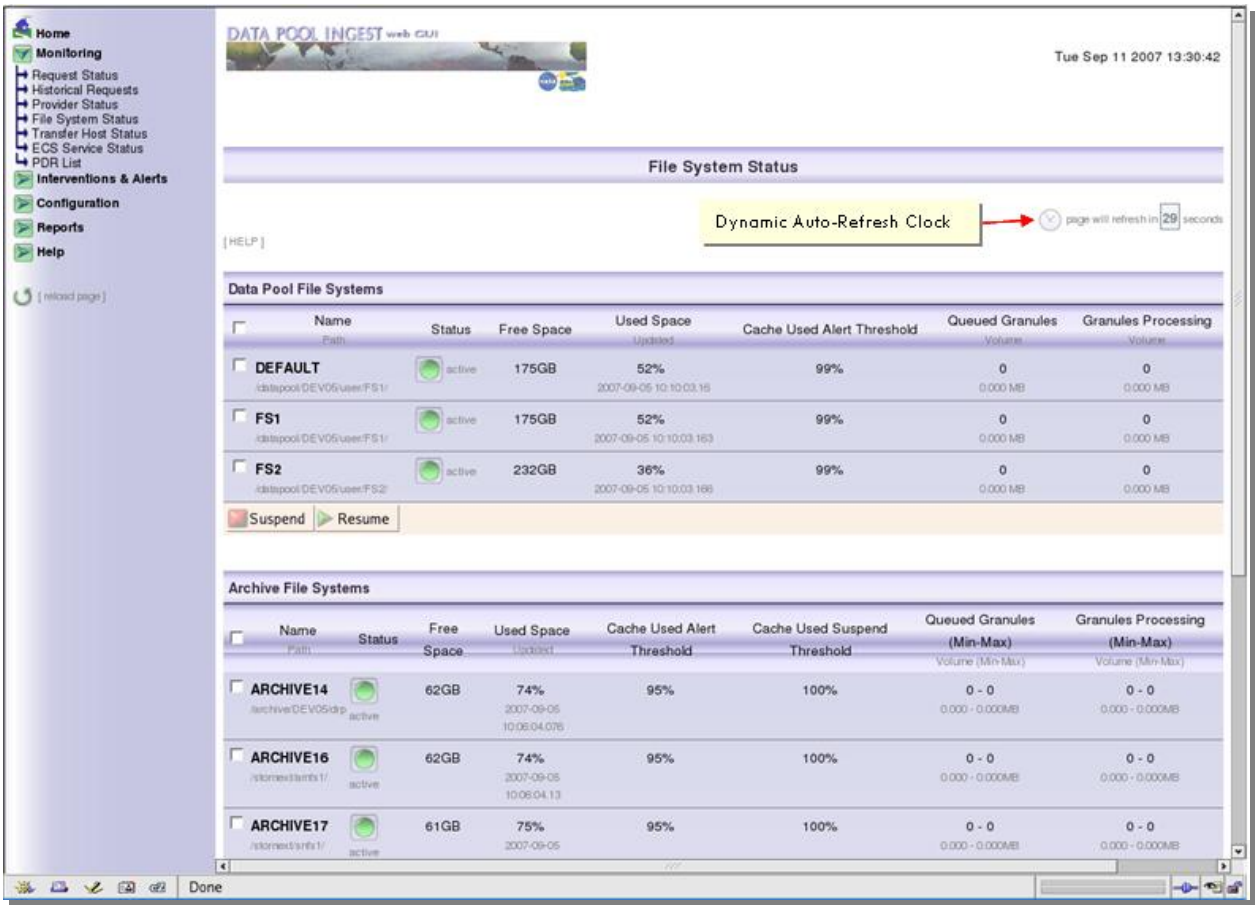


Figure 4.6.1-14. Dynamic Auto-Refresh Clock

The refresh counter will be paused whenever the mouse is in motion. This is to prevent a refresh from occurring when the operator is in the middle of an action, as shown in Figure 4.6.1-15.

Figure 4.6.1-15. Paused Auto-Refresh Clock

Note: Some pages have different available refresh rates. This is designed to reduce the load on the database for certain actions that could affect performance.

4.6.1.6 Ingest Requests Page

This page displays the current active ingest requests, as shown in Figure 4.6.1-16. The operator may select any eligible request and perform one of several actions:

- Cancel the request(s) – *This is an irreversible action, there is no way to 'un-cancel' a request.*

- Suspend the request(s) – *This action may be performed only if the selected requests are not already suspended or cancelled and is used to stop new granules from being activated. Active granules in suspended requests will continue through processing.*
- Resume the request(s) – *This action may be performed only if the selected requests are suspended.*
- Change the DPL Ingest Priority of the request(s) – *Requests in terminal states cannot have their priority changed. A default priority will be assigned to requests based upon the configuration of the request's provider.*

See Section 4.6.1.6.1 below for detailed explanations of each Request action. Table 4.6.1-2 contains descriptions of the Request Status page columns.

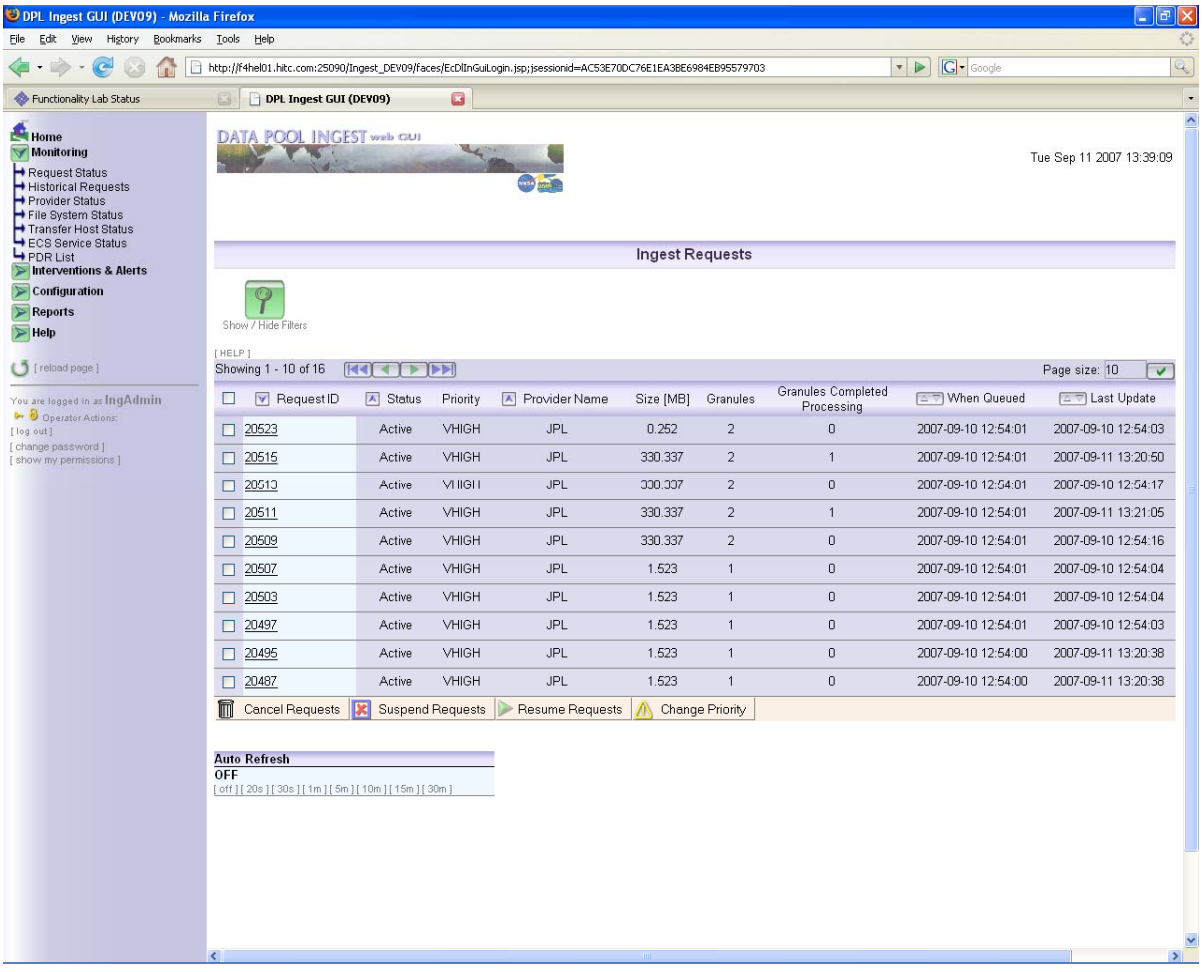


Figure 4.6.1-16. Request Status Page

Table 4.6.1-2. Request Status Page Column Descriptions

Field Name	Description
Request ID	Unique ID for an ingest request
Status	Status of the request (see Table for list of possible statuses)
Priority	The precedence which a request will have for activation and various processing actions.
Provider Name	Name of the provider from which the request was obtained
Size [MB]	Sum of the size of all granules in the request
Granules	Total granules included in the request
Granules Completed Processing	Total granules that have reached a successful state
When Queued	Time the request was encountered by the polling service
Last Update	Time of the last change made by the ingest services to the status of the request or its granules

Table 4.6.1-3 below describes the allowable actions that can be taken for Requests in their various states. A checkmark (✓) indicates that the action is allowed.

Table 4.6.1-3. Ingest Request Allowed Actions

Request Status	Request Actions				
	Suspend	Change Priority	Resume	Cancel	No Actions Allowed
New		✓		✓	
Validated		✓		✓	
Active	✓	✓		✓	
Partially_Suspended	✓	✓		✓	
Suspending / Suspended		✓	✓	✓	
Resuming	✓	✓			
Failed					✓
Partial_Failure					✓
Canceling					✓
Partially_Cancelled					✓
Successful					✓

4.6.1.6.1 Request Actions

Changing Request Statuses

To change the status of request(s) (cancel, suspend, or resume), select the desired request(s) by checking the boxes on the left side of the request list. You can also select or deselect all the requests by checking the box at the very top of the list. See Figure 4.6.1-17.

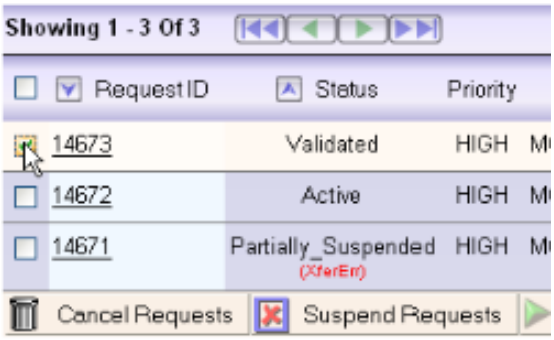


Figure 4.6.1-17. Canceling a Request

Some Requests may not have checkboxes because they are in a terminal state. Actions may not be processed for these requests. See Figure 4.6.1-18.

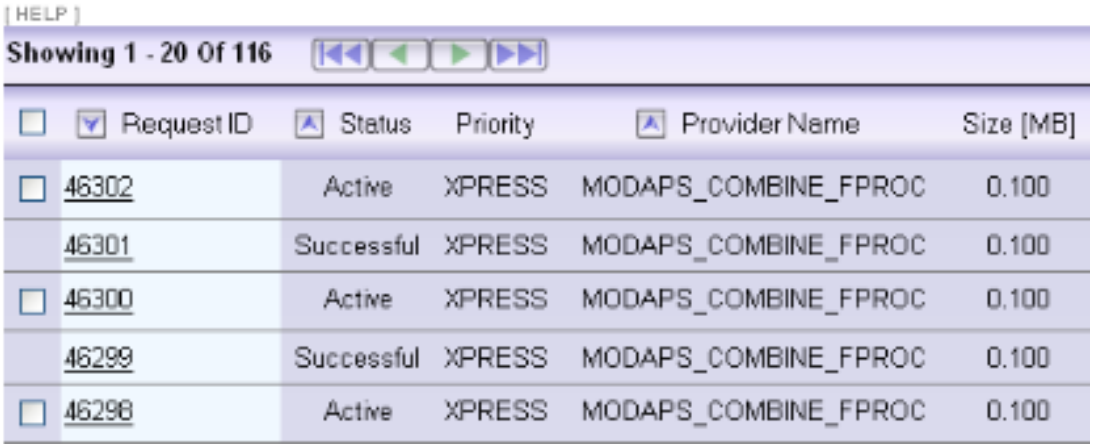


Figure 4.6.1-18. Request with No Checkboxes

Then click on the button of the desired status change action at the bottom of the list. A box will appear below to enter a reason for the status change. See Figure 4.6.1-19.

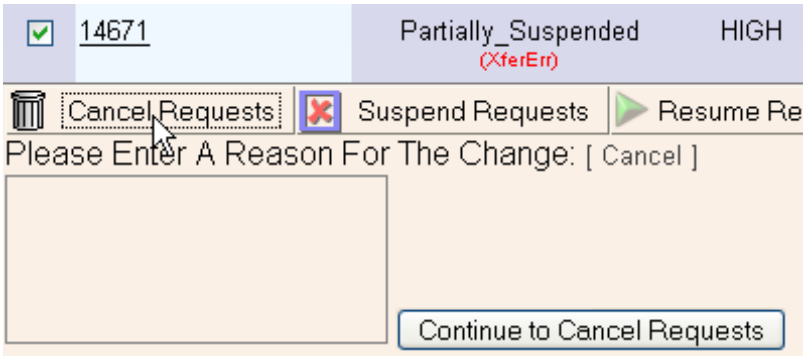


Figure 4.6.1-19. Explanation Field for Canceling Request

Once you have entered the reason, click on the button next to the text box to continue the action. You will be prompted for confirmation before the action is carried out.

Click on the [cancel] link to close the box if you do not wish to process the action.

Changing Request Priorities

To change the priority of ingest request(s), select the desired request(s) and click on the Change Priority button at the bottom of the list. A dropdown lists appears to select the new priority. See Figure 4.6.1-20.

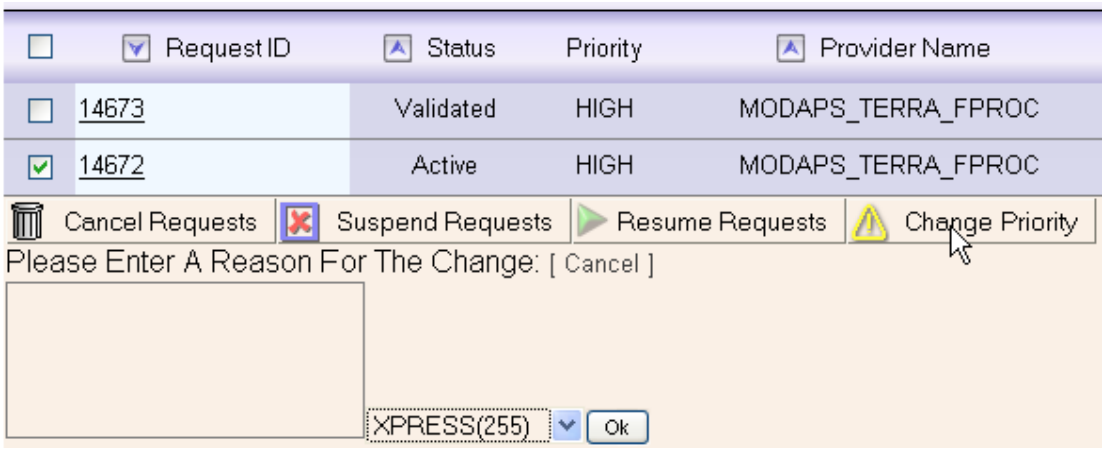


Figure 4.6.1-20. Changing Request Priorities

Enter a reason for the change in priority. Then select the desired priority from the drop down list and then click the OK button to continue the action. You will be prompted for confirmation before the action is carried out.

Click on the [cancel] link to close the box if you do not wish to process the action.

4.6.1.6.2 Filters

The request list on the Ingest Requests page can be filtered using the filter panel that appears on the same page. This is opened (or closed) by clicking on the green filter button at the top of the page, as shown in Figure 4.6.1-21. Filter settings are associated with an operator profile and are always remembered, even when logging out of the session.

Filter settings are shared among all operators if authentication is not enabled. See Section4.6.1.25 for more details on how this works.

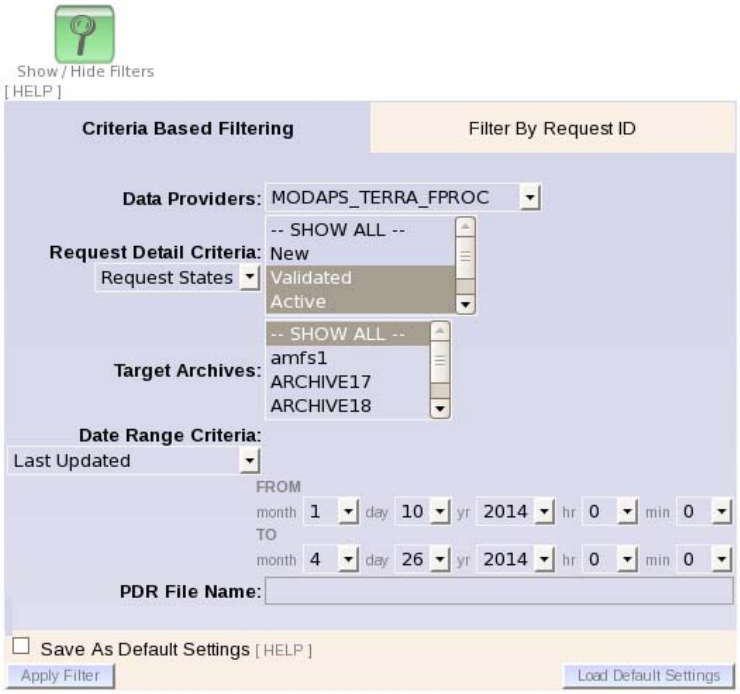


Figure 4.6.1-21. Ingest Request List Filter Panel

This panel shows the current filter settings and allows the operator to change them. There are two tabs on this panel, one that provides filter options based upon the attributes of the various requests (Criteria Based Filtering), as shown in Figure 4.6.1-21, and the other that will cause only a single request ID to be displayed (Filter By Request ID), as shown in Figure 4.6.1-22.

Under Criteria Based Filtering, there are several different types of filters that can be applied concurrently to the request list. These are as follows:

- **Data Providers –** By selecting a provider from the drop-down list, only requests from that provider will be displayed in the request list.
- **Request Detail Criteria** – The operator can either filter by a request state, or by an error state by selecting from the dropdown menu, as shown in Figure 4.6.1-22.

- *Request States* – If this option is selected, multiple states may be included in the filter by holding down the CTRL key and selecting all of the desired states. Only requests in the selected states will be displayed.
- *Error Types* – By selecting an error type, only requests in intervention with at least one granule currently in that error state will be displayed. Only one error type may be selected.

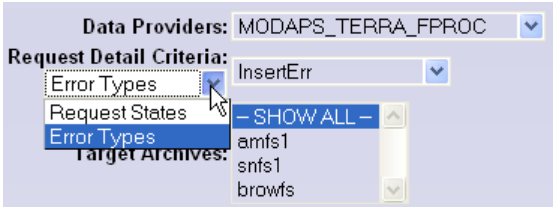


Figure 4.6.1-22. Selecting the Type of Request Detail Criterla

- **Target Archives –** Multiple archives may be included in the filter by holding down the CTRL key and selecting all of the desired archives. Only requests with granules from data types configured to be sent to the selected archives will be displayed.
- **Date Range Criteria** – The operator can either filter by the time when a request was last updated or when it was last queued, as shown in Figure 4.6.1-23.
  - *Last Updated* – Only requests that were updated from the "to" and "from" dates will be displayed. The *Last Updated* date/time of a Request is changed whenever the state of a granule or a request is changed.
  - *Queued* – Only requests that were added to the request list from the given date to the given date will be displayed
  - *Queued within Last Hour* – Only requests that were queued within the last one hour from the current time.
  - *None* – No date range filtering will be applied

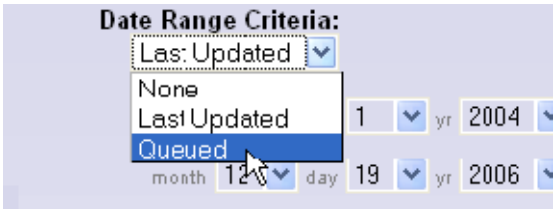


Figure 4.6.1-23. Selecting Date Range Criteria

- **PDR File Name** – The operatore can enter PDR File Name, and only requests with the specified PDR File Name will be displayed

To filter by a single Request ID, press on the "Filter By Request ID" tab. A single field for entering a Request ID number will appear, as shown in Figure 4.6.1-24. The request ID filter can only be applied by itself and not in combination with any other filter attributes.

Figure 4.6.1-24. Filtering by Request ID

Once the desired filter options are selected, the operator has the option of saving these settings as the default by selecting the "Save As Default Settings" box prior to clicking "Apply Filter" (seeFigure 4.6.1-25).Thereafter, the operator can click "Load Default Settings" to load the defaults. If no default is stored, the filters will be set so that all requests will be shown.

Figure 4.6.1-25. Saving Default Filter Settings

Once all settings are selected, press the "Apply Filter" button. A new page will appear showing only the requests meeting the filter criteria. Filtering options will be hidden until the green "Show / Hide Filters" button is pressed again.

4.6.1.6.3 Sorting

The request list on the Ingest Requests page can be sorted by clicking on the desired column at the top of the request list, as shown in Figure 4.6.1-26. The direction of the arrow next to the column indicates how that column may be sorted, either in ascending or descending order. All columns, unless they are date columns or the Request ID column, can be sorted in ascending order. The Request ID column is sorted in descending order. Date columns can be sorted in either ascending or descending order, as shown in Figure 4.6.1-27.

Unlike filter settings, sort settings are remembered for the session only.

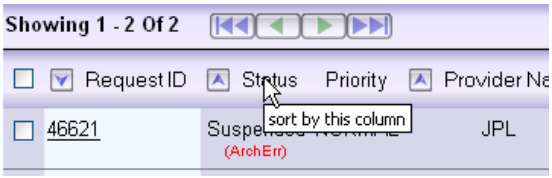


Figure 4.6.1-26. Request List Sorting

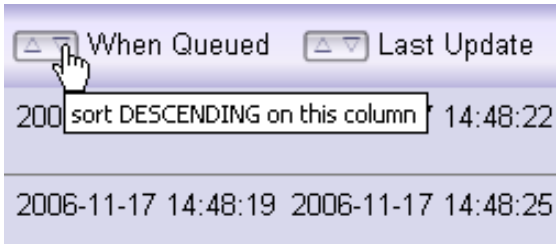


Figure 4.6.1-27. Date Sorts

4.6.1.7 Ingest Request Detail

To view the details of an ingest request (which also displays the list of associated granules), click on the desired request ID on the Ingest Request List, as shown in Figure 4.6.1-28.

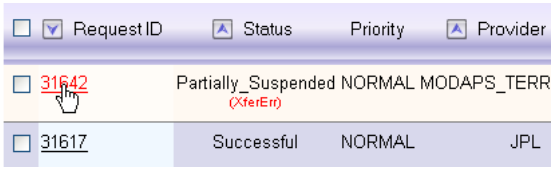


Figure 4.6.1-28. Viewing Request Details

The Ingest Request Detail page is shown below in Figure 4.6.1-29. Specific sections of this page are described in more detail in the following subsections. Table 4.6.1-4 contains descriptions for the Request Info Panel fields.

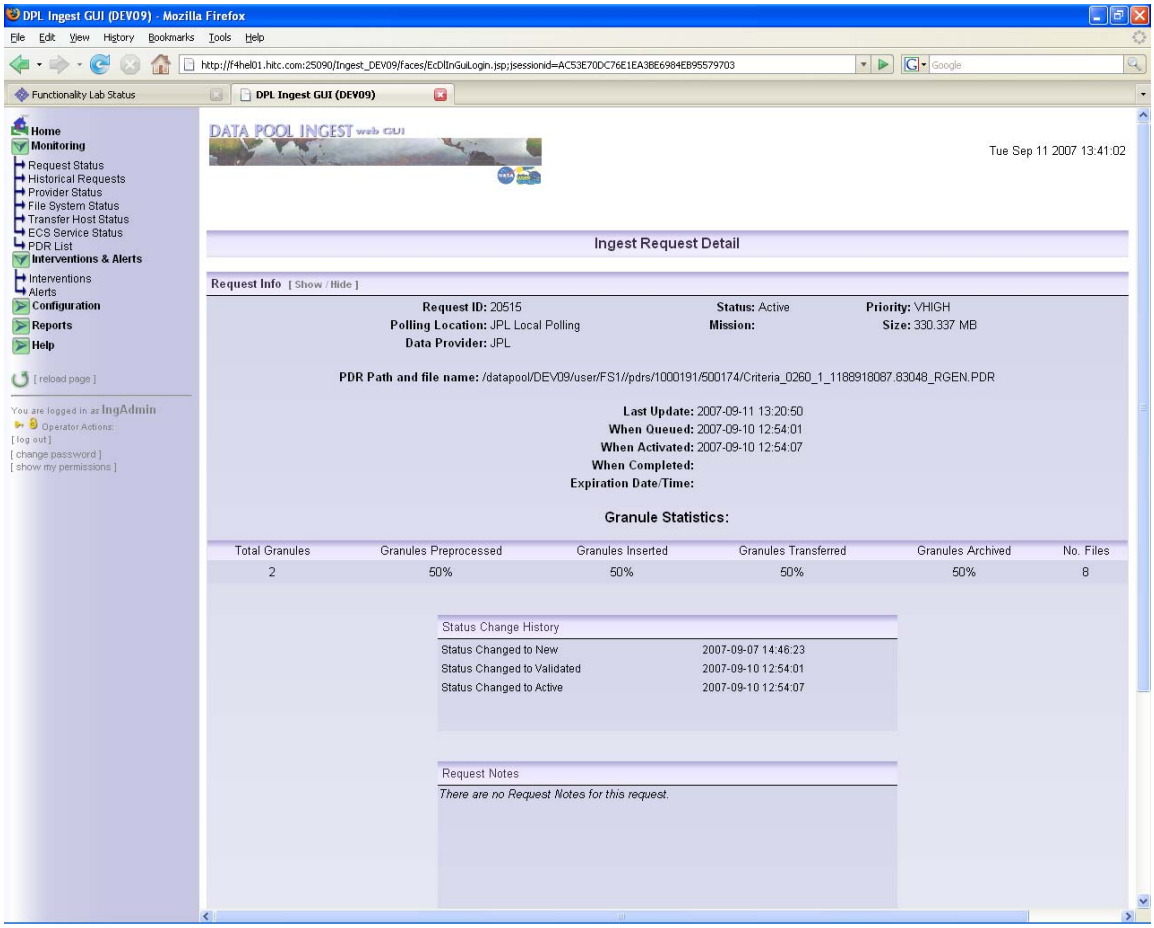


Figure 4.6.1-29. Ingest Request Detail Page

4.6.1.7.1 Request Info

The top of the Ingest Request Detail page shows the complete detailed information particular to the current request, including the complete date information of when major changes to the request were completed, as shown in Figure 4.6.1-30.

Figure 4.6.1-30. Request Info Panel

Table 4.6.1-4. Request Detail Page – Request Info Panel Field Descriptions

Field Name	Description
Request ID	Unique ID for an ingest request
Polling Location	Unique name assigned to the polling location from where the request was obtained
Data Provider	Unique name assigned to the provider associated with the polling location where the request was found
Status	The current state of the request (see Table 4.6.1-3 to see possible request states)
Mission	Satellite mission defined in the PDR associated with this request (this is not defined in most PDRs)
Priority	The precedence which a request will have for activation and various processing actions.
Size	Sum of the size of all granules in the request
PDR Path and file name	Temporary location and file name of the PDR after it was copied from the polling location. The PDR can be found in this location until the request completes ingest.
Last Update	The last time the status of the request or an associated granule changed
When Queued	The time the request was added to the request list
When Activated	The time the request was moved into the "Active" state
When Completed	The time all the granules in the request reached a terminal state
Expiration Date/Time	The date and time by which the corresponding ingest request must be completed

If there is an intervention pending against the request, then there will be a link to the intervention detail page, as shown in Figure 4.6.1-30. Click on the "[view details]" link to navigate to the intervention detail page. More information on intervention details can be obtained in Section 4.6.1.15.

4.6.1.7.2 Granule Statistics

This section of the request details shows the overall statistics for all of the granules associated with this request, as shown in Figure 4.6.1-31. Table 4.6.1-5 lists the granule statistics panel field descriptions.

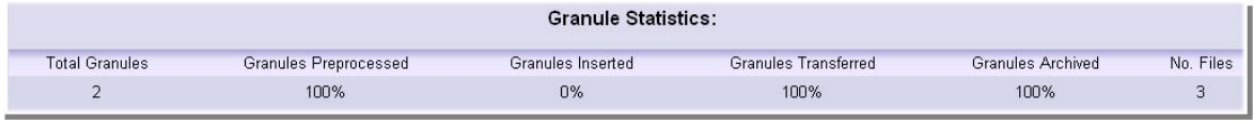


Figure 4.6.1-31. Granule Statistics

Table 4.6.1-5. Request Detail Page – Granule Statistics Panel Field Descriptions

Field Name	Description
Total Granules	Total number of granules included in the request
Granules Preprocessed	Percentage of granules that have moved from the preprocessing state to the archiving state
Granules Inserted	Percentage of granules that have been inserted into AIM
Granules Transferred	Percentage of granules transferred from the provider to the temp directories
Granules Archived	Percentage of granules that have been archived
No. Files	Total number of files associated with granules in the request

4.6.1.7.3 Status Change History

This section shows a complete record of the status changes for the request in a scrollable table, as shown in Figure 4.6.1-32.

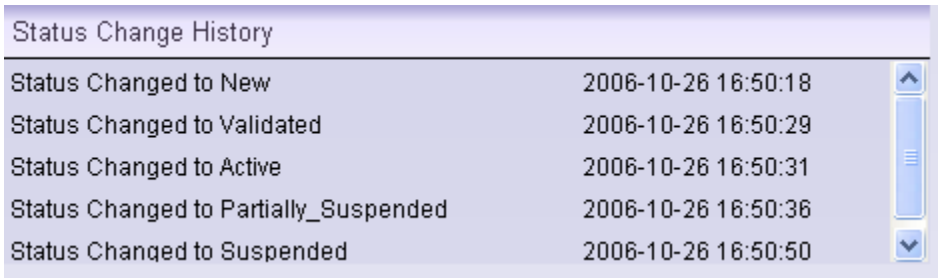


Figure 4.6.1-32. Status Change History

4.6.1.7.4 Request Notes

Requests notes are annotations that can be useful in tracking changes to the request. These will either be added automatically by the server or manually by the operator. Automatic annotations are added when the operator performs an action on the request or granules in the request.

In Figure 4.6.1-33 below, the first request note was automatically added after the operator "IngAdmin" failed one of the request granules. The second annotation was added manually by the operator "IngAdmin" to give more details on why the granule was failed.

You can add a request note, but not edit or delete one. To add a request note, click "[Add annotation...]" at the bottom of the annotation list, as shown in the figure below:

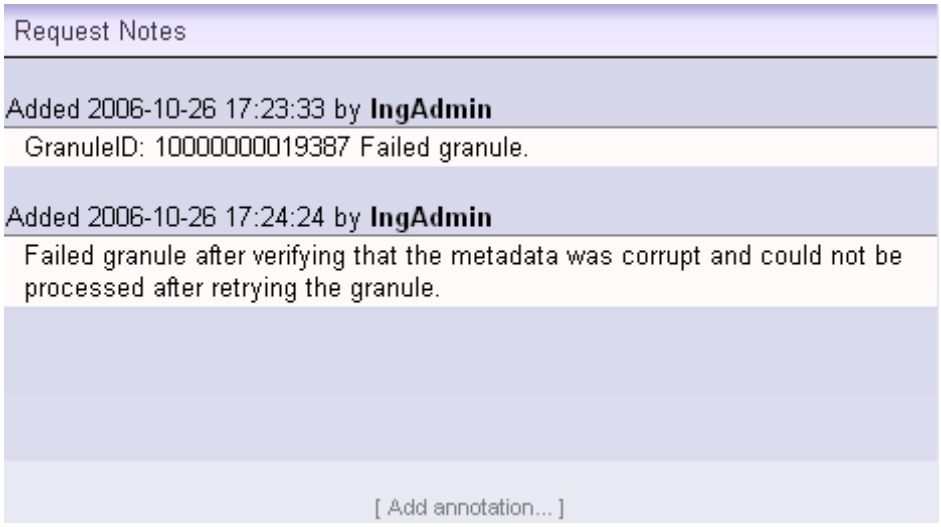


Figure 4.6.1-33. Request Notes

An area will appear below where you can add a new annotation. After you are finished, click "Add this Annotation," as shown in Figure 4.6.1-34. It will be time stamped after it is added.

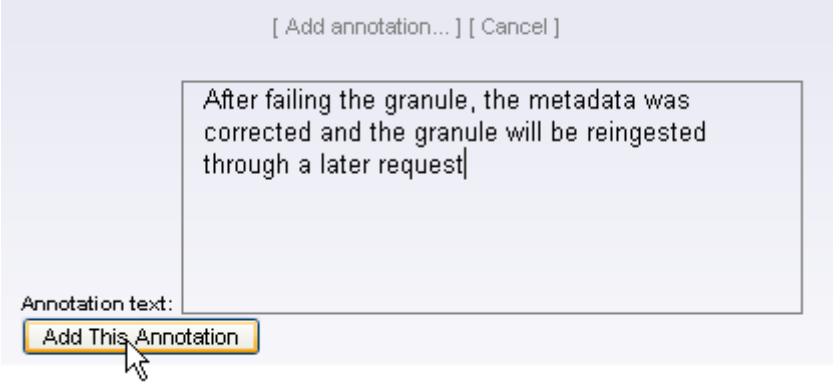


Figure 4.6.1-34. New Annotation Text Box

4.6.1.7.5 Granule List Panel

This is the list of all granules associated with this request, as shown in Figure 4.6.1-35. By default, this list is sorted in ascending alphabetical order by Granule status, always showing suspended granules first. The operator also has the ability to sort by other criteria, including:

- Descending granule states, with suspended granules last
- Granule sequence number

Figure 4.6.1-35. Granule List

Table 4.6.1-6 lists the granule list panel column descriptions.

Table 4.6.1-6. Request Detail Page – Granule List Panel Column Descriptions

Field Name	Description
Checkbox column	This column may contain a checkbox next to the granule, if the granule is not in a terminal state. This allows an action to be processed for the selected granule(s). The checkbox at the top of the column selects or de-selects all the granules in the list that have checkboxes.
File Detail	The column holds a link to display the detailed file information for each granule – this information appears for each granule at the top of the table when clicked on.
Seq. Number	The order in which a granule was found in the PDR
Ingest Gran ID	Unique Identifier assigned to the granule
Data Type	Data Type found in the PDR describing the granule
Version	Version found in the PDR describing the granule. The version will be extracted from the database if none is in the PDR
Status	Current granule status (see Table 4.6.1-7) and detailed error information
Granule Size (MB)	Sum of the size of all files associated with the granule
No. Files	Number of files found associated with the granule in the PDR
Last Status Change	Date and time the granule's status was last updated

A Note on Suspended Granules

Nearly all granules that encounter a problem during processing will eventually move into the "suspended" state. The only exception is if a granule fails checksum verification each of the configured number of retries. Except in the case of failed checksum verification or a PDR Validation failure, granules are not failed until the operator explicitly takes an action to fail suspended granules.

Granule Actions

The following actions listed in Table 4.6.1-7 may be performed on granules in the granule list, depending on granule state:

Table 4.6.1-7. Granule Allowed Actions

Granule Status	Status Type	Fail / Retry / Retry From Start	Cancel	No Actions Allowed
New	Queued		✓	
Transferring / Transferred	Active		✓	
Checksumming / Checksummed	Active		✓	
Preprocessing / Preprocessed	Active		✓	
Archiving / Archived	Active		✓	
Inserting	Active		✓	
Inserted	Active			✓
Suspending / Suspended	Error	✓	✓	
Resuming	Active		✓	
Canceling	Active			✓
Cancelled	Terminal			✓
Successful	Terminal			✓
Failed	Terminal			✓
Publishing / Published	Terminal			✓

Retry selected granules: This applies only to granules that are currently suspended and retries them from the last known good state of processing. Every time a granule is retried, an annotation is added identifying the time, operator, and action (see Figure 4.6.1-33).

Retry selected granules from START: This applies only to granules that are currently suspended and retries them from the beginning of processing. Every time a granule is retried, an annotation is added identifying the time, operator, and action.

Fail selected granules: This applies only to granules that are currently suspended and transitions the granule into a failed state, with the status indicating the type of error that originally caused the suspensions.

Error types are determined by what state the granule is in when it is failed. These states are: XferErr (transferring), ChecksumErr (Checksumming), PreprocErr (Preprocessing), ArchErr (Archiving), InsertErr (Inserting), and PubErr (Publishing).

NOTE: After a granule is failed, an annotation is added identifying the time, operator, and action.

To perform a granule action, select one or more granules by checking the box on the left side of the line for that granule (if available) and click on the desired action button at the top of the granule list. You will then be asked for confirmation before the action is carried out.

Cancel selected granules: This applies only to granules that are not yet in a terminal state. It manually cancels the granules. After a granule is cancelled it is expected that the granule will be re-ingested by the operator

View Granule File Information

Each granule has additional detailed information in the "File Detail" column. This column contains the list of files associated with that granule; if any of the files are in a failed or suspended state, the error details are also shown. To view this information, click the [show/hide] link for the desired granule, as shown in Figure 4.6.1-36. Table 4.6.1-8 lists the granule file information column descriptions.

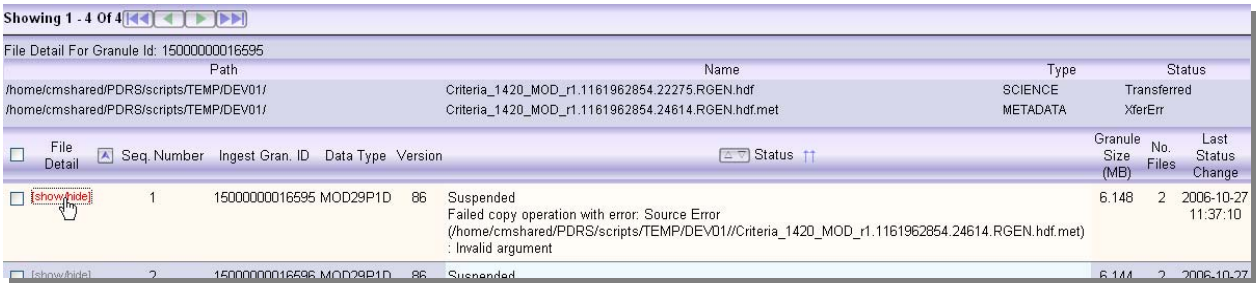


Figure 4.6.1-36. Granule File Information

Table 4.6.1-8. Granule File Information Column Descriptions

Field Name	Description
Path	Directory identified in the PDR where the file can be found
Name	Name of the file
Type	Internal file type of the file translated from the file type in the PDR according to a predefined table (e.g., SCIENCE, METADATA, BROWSE)
Status	Last action performed on the file or the most recent, unresolved, error encountered while processing the file

4.6.1.8 Historical Ingest Requests Page

This page shows all of the ingest requests that have reached a terminal state and have been moved from the active ingest requests list, which occurs after a configured interval has elapsed (configured on the Global Tuning page, Section 4.6.1.24). The DPL Ingest Database keeps a persistent record of *all* requests that have undergone ingest processing and can thus be viewed on this page (see Figure 4.6.1-37 below). The operator has the ability to configure how long this historical information is kept on the bottom of this page (see Figure 4.6.1-38) and can also be set on the Global Tuning Configuration page (Section 4.6.1.24). Table 4.6.1-9 lists the historical ingest requests column descriptions.

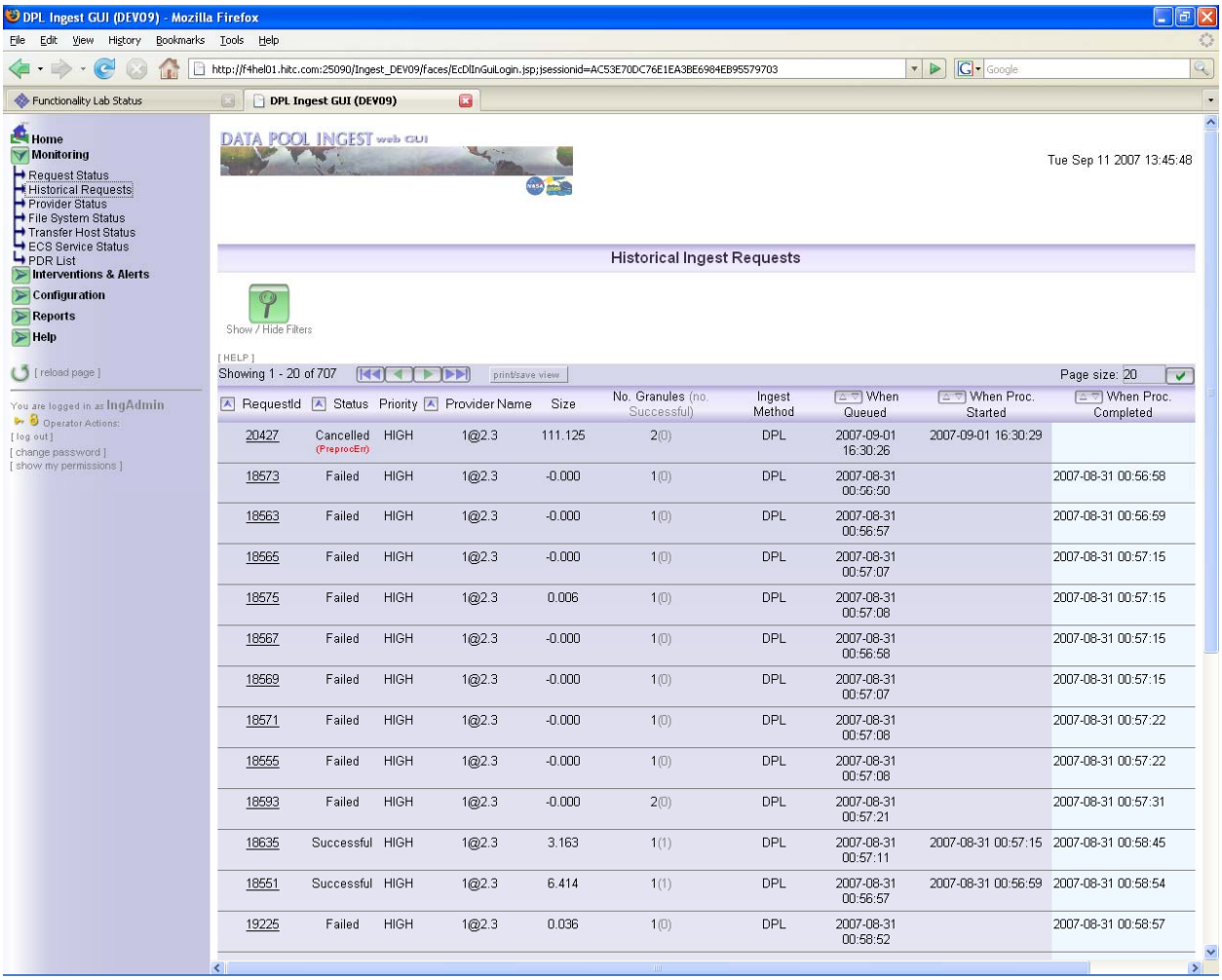


Figure 4.6.1-37. Historical Requests Page

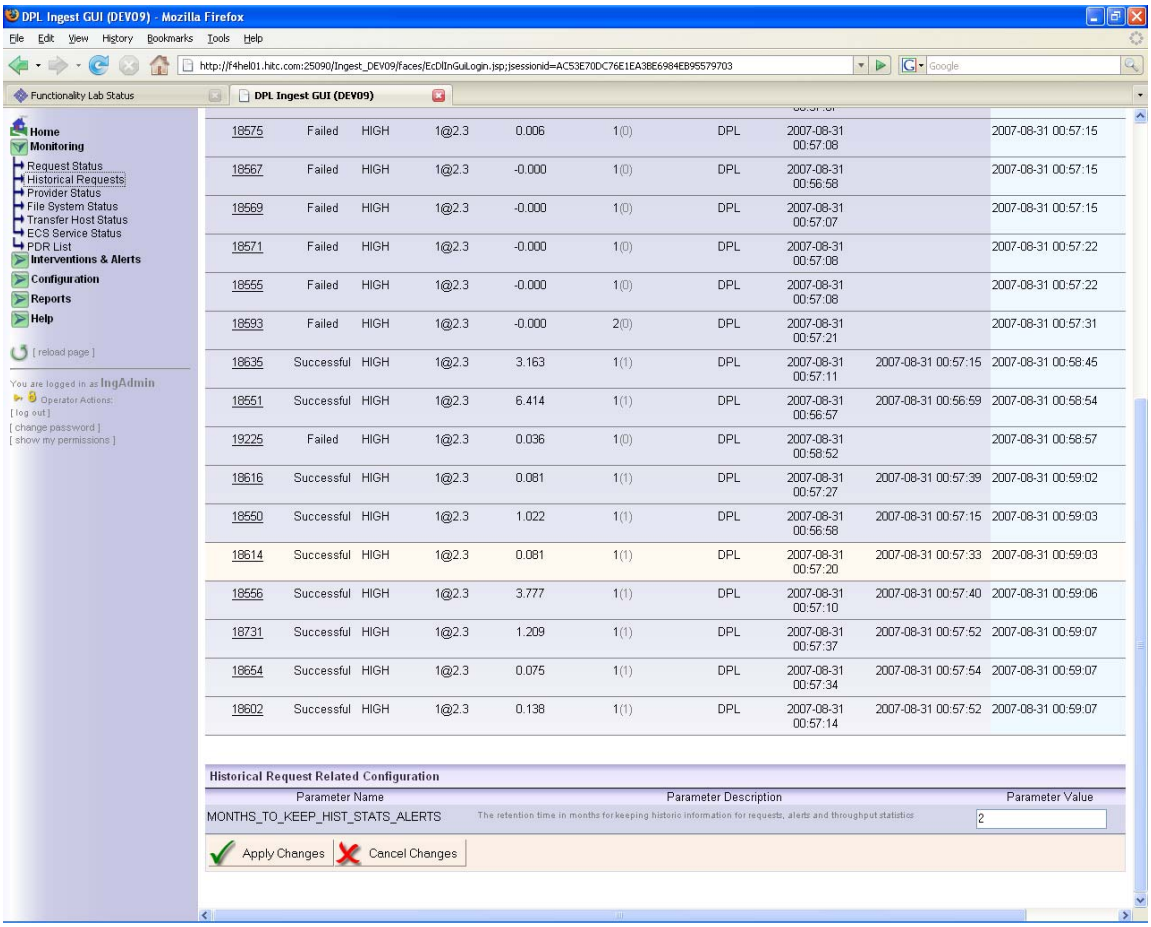


Figure 4.6.1-38. Historical Request Related Configuration

Table 4.6.1-9. Historical Ingest Requests Column Descriptions

Field Name	Description
Request ID	Unique ID for an ingest request
Status	Terminal state reached by the request
Priority	The final priority assigned to the request during processing
Provider Name	Name of the provider from which the request was obtained
Size	Sum of the size in MB of all granules in the request
No. Granules	Total granules included in the request
Ingest Method	Whether the request was processed by Classic Ingest, or the new DataPool Ingest system. "DPL" indicates Data Pool Ingest, while "CLASSIC" indicates Classic Ingest.
When Queued	Time the request was encountered by the polling service
When Proc. Started	Time the request was activated by processing
When Processing Completed	Time the request reached a terminal state

4.6.1.8.1 Viewing Historical Request Details

To view request details, click on a request ID, which displays a request detail page similar to that for an Active Ingest Request, as shown in Figure 4.6.1-39.

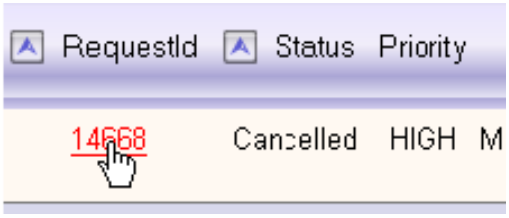


Figure 4.6.1-39. Viewing Historic Request Details

4.6.1.8.2 Printing and Saving Historical Request Lists as Reports

The operator can view the entire Historic Request list by clicking the "print/save view" button next to the pagination arrows at the top of the Historic Request List, as shown in Figure 4.6.1-40.

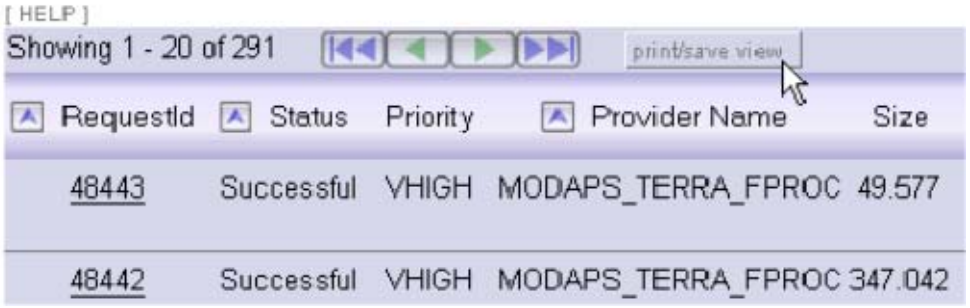


Figure 4.6.1-40. Print/Save View Button

This will display a complete list of all the historic requests, though this list will be restricted by current filter settings. A new window will be opened and you will be prompted to continue, as shown in Figure 4.6.1-41.

Because the list could potentially contain thousands of records, it may take several minutes to load the entire list into the browser window. At this point, the window will display "Processing Your Request" (see Figure 4.6.1-42) while the web server retrieves the data – this page may be displayed for several minutes. Once the entire list is loaded, the page will display the list as normal (Figure 4.6.1-43).

Saving and Printing

From here you can save the list as HTML by using the browser's built-in save functionality (usually File > Save As...). Most browsers will also allow you to save the page as text only. To print, either press the "Print This Report" button directly on the page, or use the menu (File > Print...); this will load your browser's built-in print dialog box, an example of which is shown in Figure 4.6.1-44.

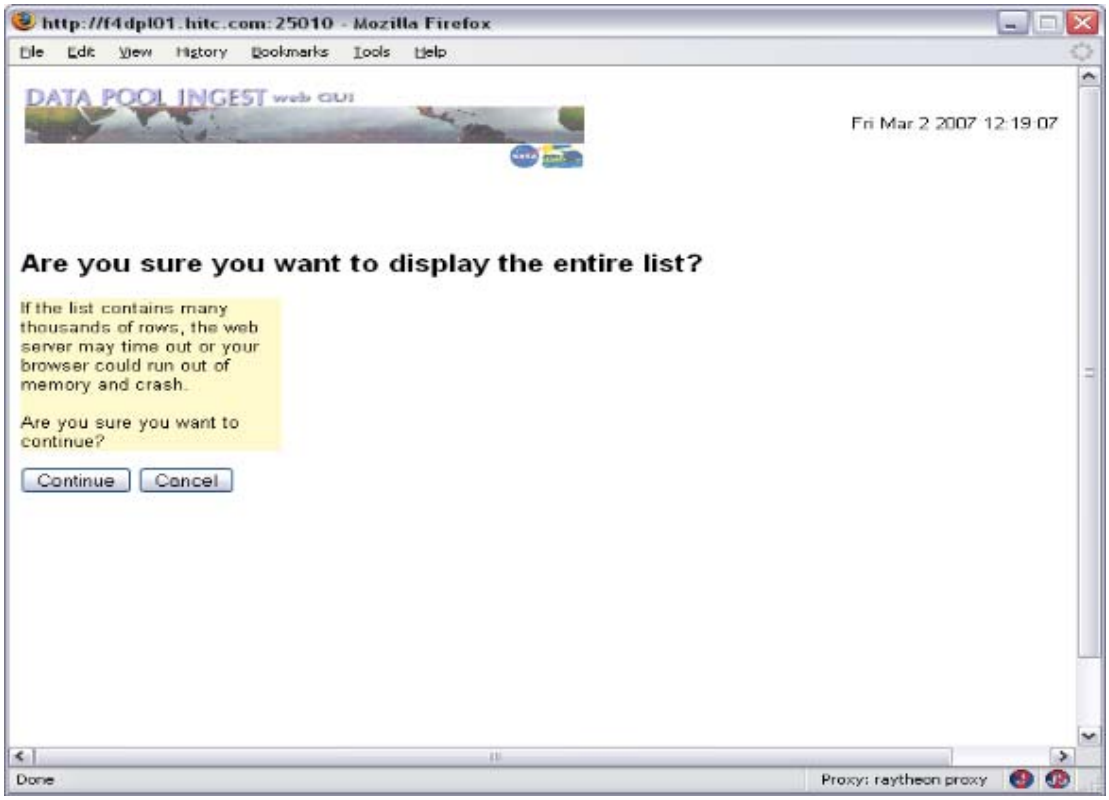


Figure 4.6.1-41. Prompt to Display Entire Historic Request List

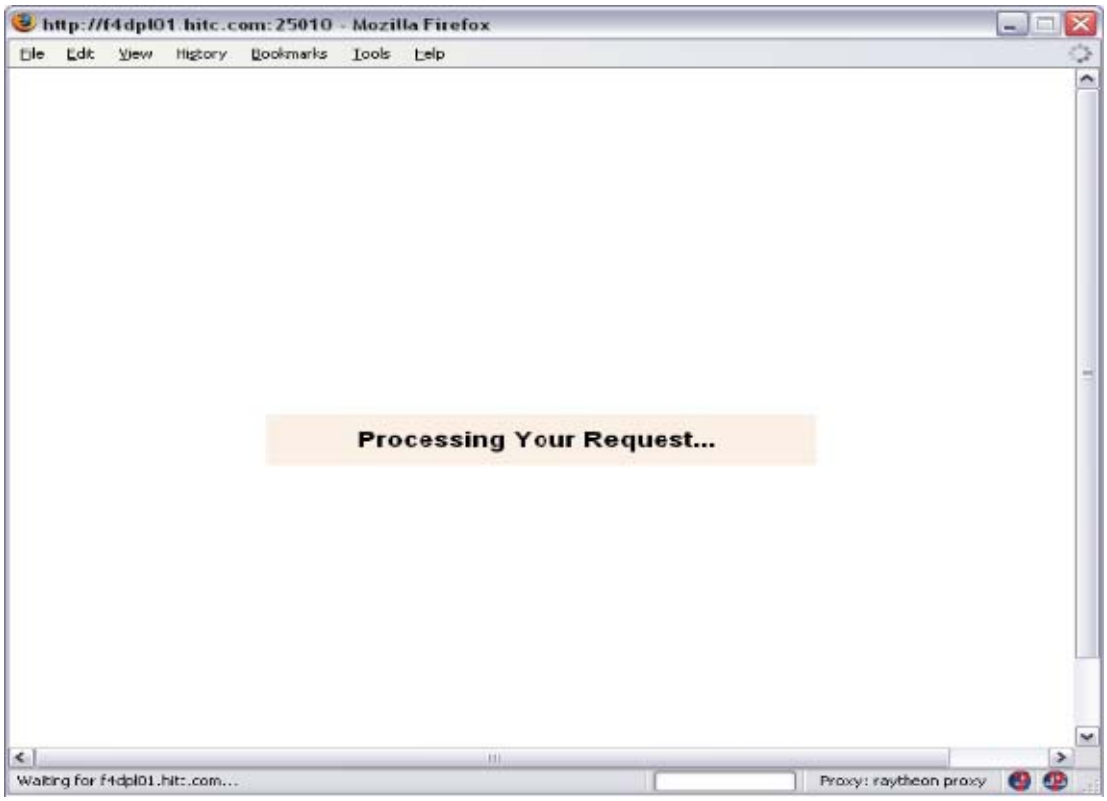


Figure 4.6.1-42. "Processing Your Request" Wait Screen

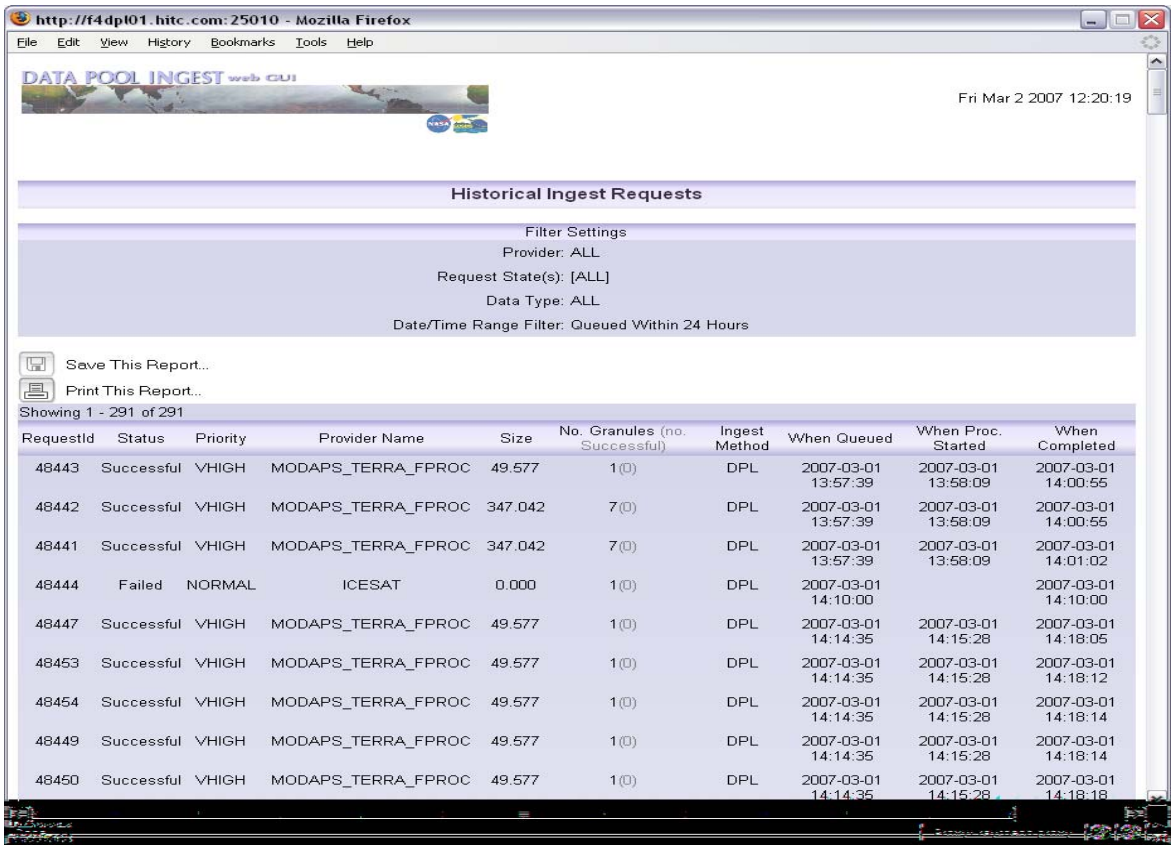


Figure 4.6.1-43. Print/Save View of Historical Ingest Requests

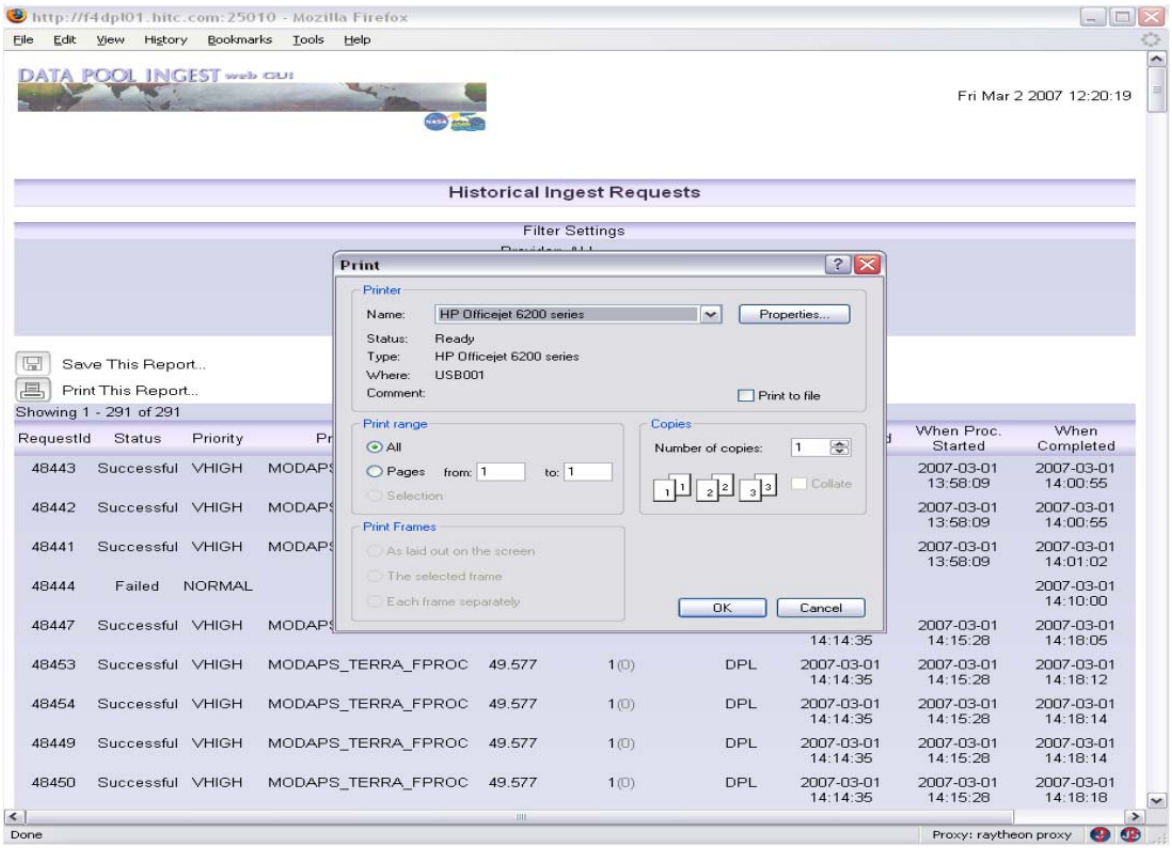


Figure 4.6.1-44. Print Dialog Box

4.6.1.8.3 Historical Request Filters

The historic request list on this page can be filtered using the filter panel that appears on the same page. This is opened by clicking on the green filter button at the top of the page, as shown in Figure 4.6.1-45. If authentication is enabled, filter settings are always remembered, even when logging out of the session. They are never lost unless the operator profile is completely removed or authentication is disabled.

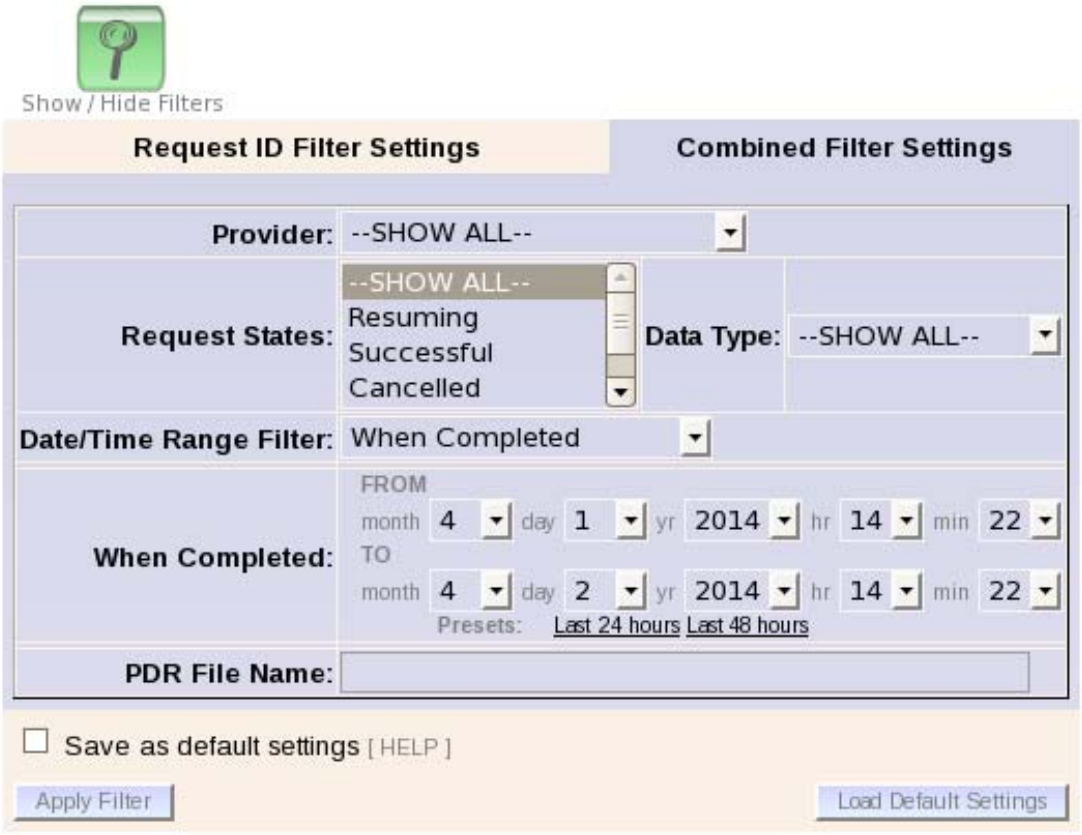


Figure 4.6.1-45. Filter Panel

This panel shows the current filter settings and allows the operator to change them. There are two tabs on this panel, one that provides filter options based upon the attributes of the various requests ("Combined Filter Settings"), as shown in Figure 4.6.1-45, and the other that will filter by a single request ID ("Request ID Filter Settings"), as shown in Figure 4.6.1-47.

Under Criteria Based Filtering, there are several different types of filters that can be applied concurrently to the request list. These are as follows:

- **Data Providers –** By selecting a provider, only requests from that provider will be displayed in the request list.
- **Request States** – If this option is selected, multiple states may be included in the filter by holding down the CTRL key and selecting all of the desired states. Only requests in the selected states will be displayed.
- **Data Type** – By selecting a data type, only requests with granules of the selected data type will be displayed
- **Date/Time Range Filter** – The operator can either filter by the time when a request was last updated or when it was last queued, as shown in Figure 4.6.1-46.

- *When Completed* – Only requests that completed from the given date to the given date will be displayed. Completion time is recorded once all granules reach a terminal state.
- *When Queued* – Only requests that were added to the request list from the given date to the given date will be displayed
- *Queued Within 24 Hours* – Only requests that were added to the request list within the last 24 hours from the current date
- *None* – No date/time range filtering will be applied

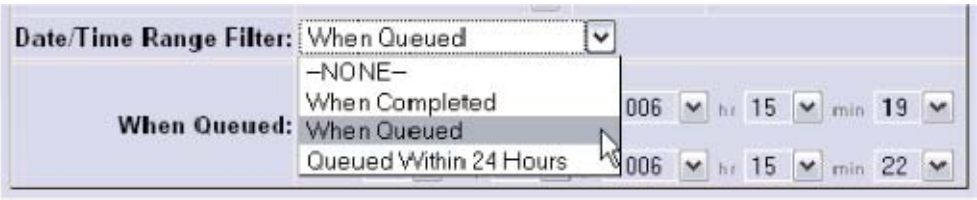


Figure 4.6.1-46. Selecting a Date Range Criteria

- **PDR File Name** – The operatore can enter PDR File Name, and only requests with the specified PDR File Name will be displayed

To filter by a single Request ID, press on the "Request ID Filter Settings" tab. A single field for entering a Request ID number will appear, as shown in Figure 4.6.1-47. The request ID filter can only be applied by itself and not in combination with any other filter attributes.

Figure 4.6.1-47. Filtering By Request ID

Once the desired filter options are selected, the operator has the option of saving a set of default settings by selecting the "Save As Default Settings" box prior to clicking "Apply Filter" (see Figure 4.6.1-48). Thereafter, the operator can click "Load Default Settings" to restore these saved defaults. If no default is stored, all requests will be shown by default. If authentication is disabled, there will be no option for saving or loading default settings.

Figure 4.6.1-48. Saving Default Filter Settings

Once all settings are selected, press the "Apply Filter" button. A new page will appear with showing only the requests meeting the filter criteria. Filtering options will be hidden until the green "Show / Hide Filters" button is pressed again.

4.6.1.9 Historical Ingest Request Detail Page

The request detail page for a historical request (Figure 4.6.1-49) is similar to the one for an Active Ingest Request, with the request details followed by a granule list. The details on this page are somewhat different in that information pertaining to historical data is shown. Since the request is in a terminal state, no actions can be processed for this request, so action buttons are not present. Tables 4.6.1-10 through 4.6.1-12 contains information for the Historical Ingest Request Detail page such as the request info field descriptions, the request info column descriptions, and the granule list column descriptions.

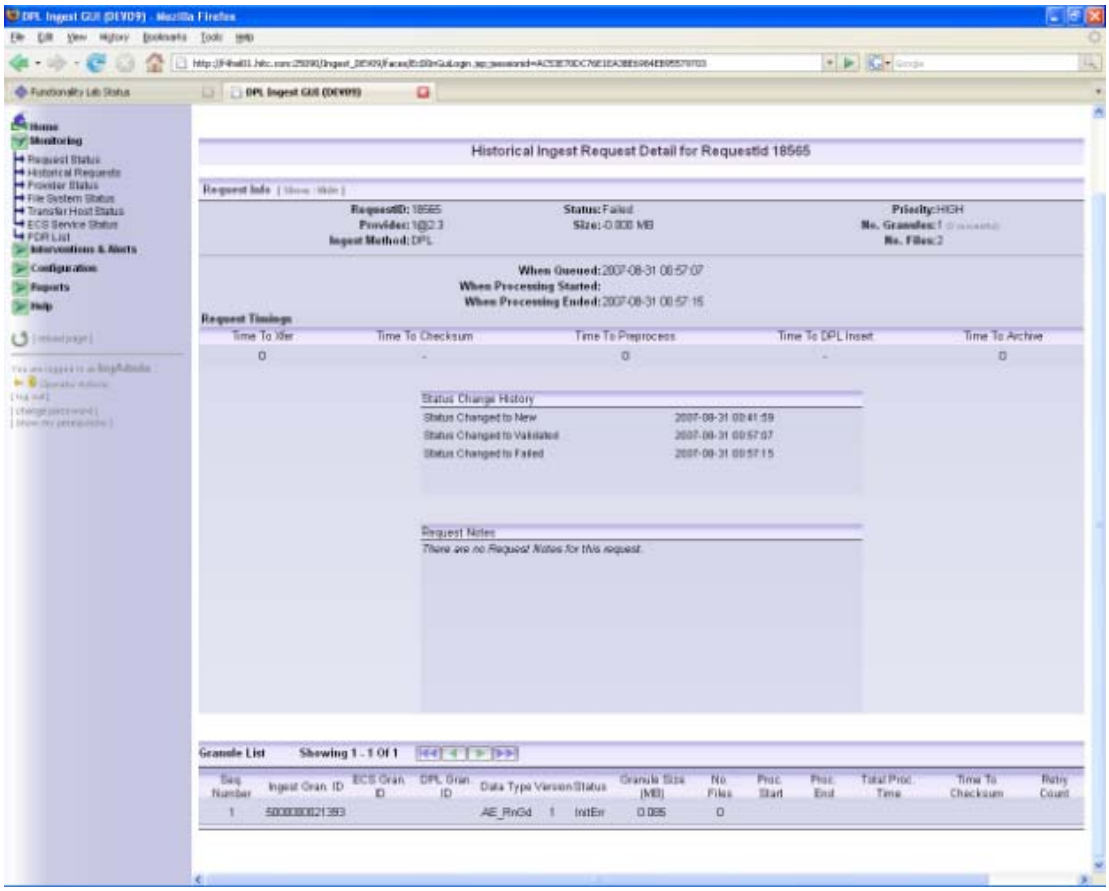


Figure 4.6.1-49. Historical Request Detail Page

Page Sections

- Request Info – *General information about the request*

Table 4.6.1-10. Historical Ingest Request Detail Page – Request Info Field Descriptions

Field Name	Description
Request ID	Unique ID for an ingest request
Status	The final state of the request (see Table 4.6.1-3for a list of possible request states)
Priority	The precedence which a request will have for activation and various processing actions.
Provider	Unique name assigned to the provider associated with the polling location where the request was found
Size	Sum of the size of all granules in the request
No. Granules	Total number of granules in the PDR
Ingest Method	Whether the request was processed by Classic Ingest, or the new DataPool Ingest system
No. Files	Number of files found associated with the granule in the PDR

- Request Timings – *Seconds of time that passed during various processing actions*

Table 4.6.1-11. Historical Ingest Request Detail Page – Request Timings Column Descriptions

Field Name	Description
Time to Xfer	Total seconds of time that passed during all granule transfers
Time to Checksum	Total seconds of time that passed during all granule checksum operations
Time to Preprocess	Total seconds of time that passed during all granule preprocessing operations
Time to Insert	Total seconds of time that passed to insert all granules into AIM
Time to Archive	Total seconds of time that passed to copy all granules into the archive

- Granule List – *Detailed granule information*

Table 4.6.1-12. Historical Ingest Request Detail Page – Granule List Column Descriptions

Field Name	Description
Seq Number	The order in which a granule was found in the PDR
Ingest Gran ID	Unique Identifier assigned to the granule by the DPL Ingest System
ECS Gran ID	Unique Identifier assigned to the granule for insert in AIM
DPL Gran ID	Unique Identifier assigned to the granule for registration in the Data Pool
Data Type	Data Type found in the PDR describing the granule
Version	Version found in the PDR describing the granule
Status	Terminal state reached by the granule
Granule Size (MB)	Sum of the size of all files associated with the granule
No. Files	Number of files found associated with the granule in the PDR
Proc. Start	Time of granule activation
Proc. End	Time granule reached a terminal state
Total Proc. Time	Total seconds that lapsed in between granule activation and completion
Time to Checksum	Total seconds that passed during granule checksum across all files
Retry Count	Number of times the granule was retried(or retried from start)

4.6.1.10 Provider Status Page

This page displays the status and information about each configured data provider in the Data Pool Ingest system (see Figure 4.6.1-50a and 4.6.1-50b for a general overview). Table 4.6.1-13 contains the Provider Status page column descriptions.

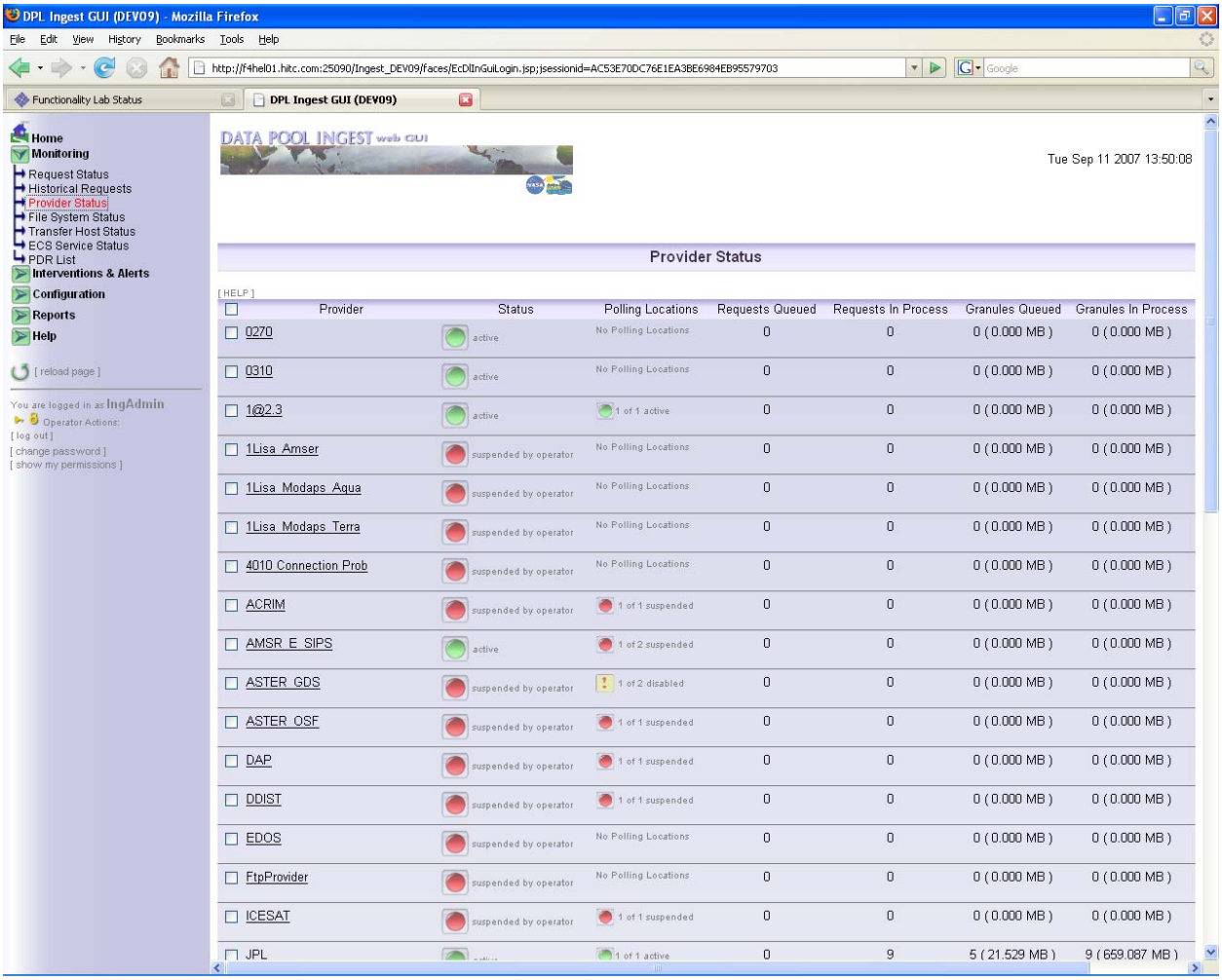


Figure 4.6.1-50a. Provider Status Page (General Overview)

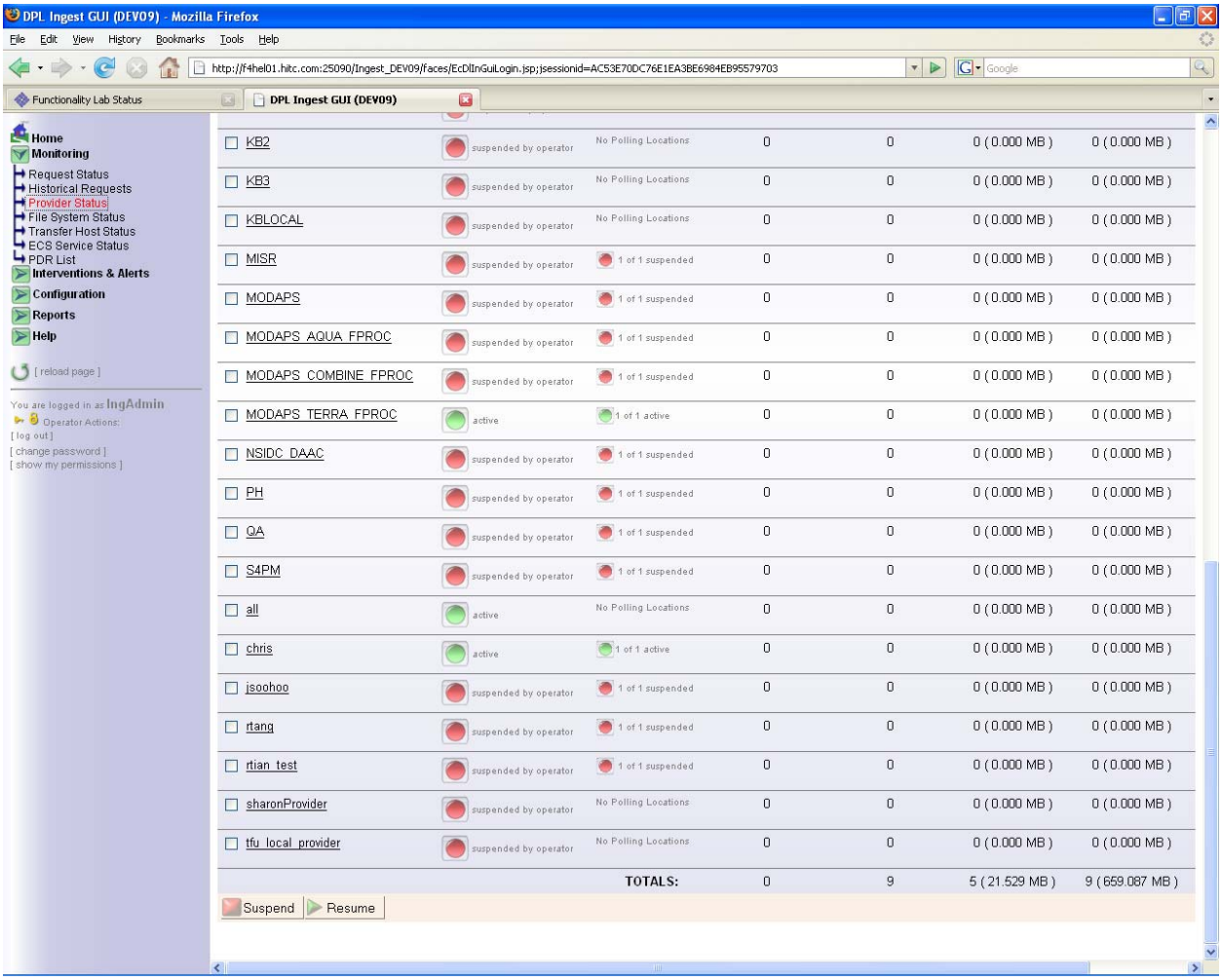


Figure 4.6.1-50b. Provider Status Page (General Overview)

Table 4.6.1-13. Provider Status Page Column Descriptions

Field Name	Description
Provider	Provider name configured to identify an External Data Provider
Status	Whether the provider is active, suspended by server, or suspended by operator
Polling Locations	Total number of active polling locations on the provider, or the number of polling locations that are suspended out of the total number configured
Requests Queued	Total number of requests waiting for activation from the provider
Requests In-Process	Total number of requests that are active and not suspended from the provider
Granules Queued	Total number and volume (in MB) of granules waiting for activation in requests from the provider
Granules In-Process	Total number and volume (in MB) of granules that are active and not suspended in requests from the provider

Possible Status Indicators

There are three possible status indicators for a provider.

- Active – at least one polling location is active

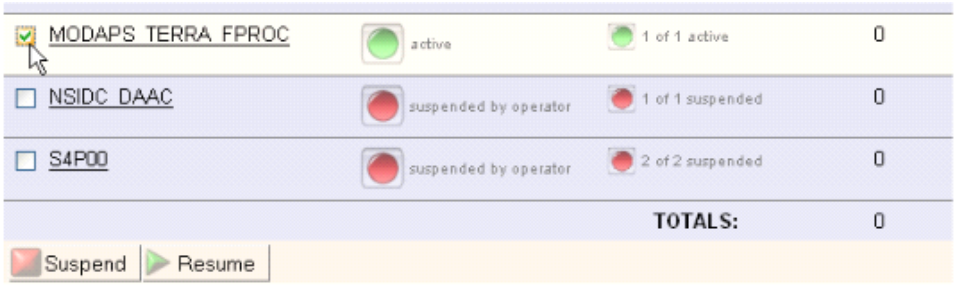
- Suspended by Server (indicating all polling locations are suspended) – the server has suspended the Polling Location automatically.

- Suspended by Operator (indicating all polling locations are suspended) – operator manually suspended the Polling Location from the GUI

4.6.1.10.1 Provider Status Actions

You can suspend or resume any of the Data Providers listed on this page. The status column shows a green (active) or red (suspended) icon. To change the status of one or more providers, do the following:

1. Select the desired provider; multiple providers may be selected at once:



2. Click the appropriate action button at the bottom of the list:

3. You will be prompted for confirmation. The page will reload with the status of the selected providers changed.

The Impacts of Suspending a Provider

Suspending a Data Provider will stop the activation of Ingest Requests from that Provider, but Ingest Requests that are already active will be completed. Ingest will also stop polling all of the Polling Locations associated with that Data Provider; The impact then is that no new Requests

from that suspended Data Provider will be queued except if a polling cycle is in progress, in which case the polling cycle will be completed.

4.6.1.11 Provider Status Detail

The detail page of a provider shows the detail information of the Provider, the configured Notification Types, and the individual status of each polling location associated with the provider, as shown in Figure 4.6.1-51, and allows the operator to suspend or resume the Polling Locations accordingly.

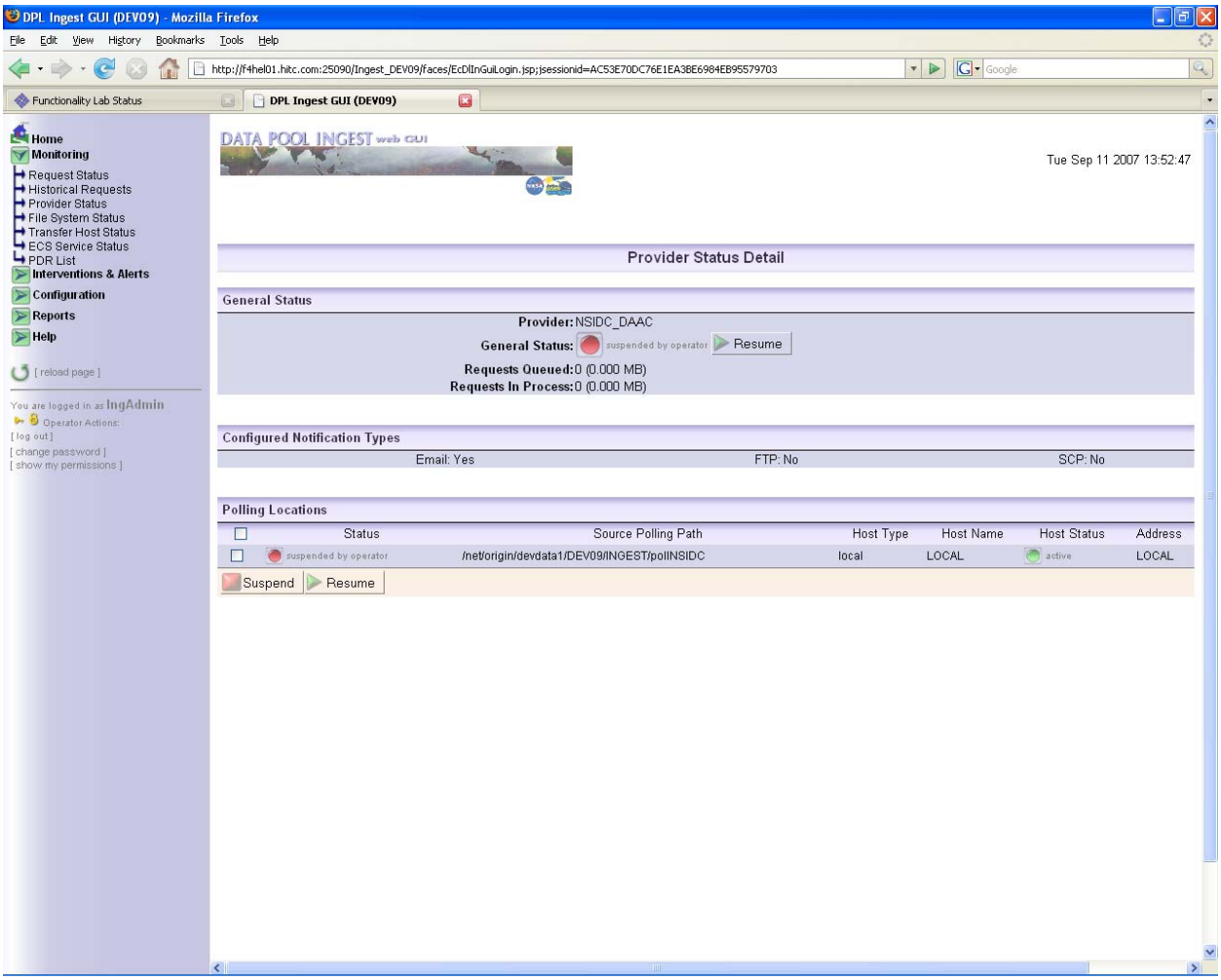


Figure 4.6.1-51. Provider Status Detail Page

4.6.1.11.1 General Status

This section of the Provider Status Detail page provides an overview of current processing through the provider, as shown in Figure 4.6.1-52. Table 4.6.1-14 contains the general status field descriptions for the Provider Status detail page.

Figure 4.6.1-52. General Status for a Provider

Table 4.6.1-14. Provider Status Detail Page – General Status Field Descriptions

Field Name	Description
Provider	Unique name for this external data provider
General Status	Whether the provider is active, or has been suspended either manually by the operator or automatically by the server
Requests Queued	Total number of requests waiting for activation from the provider, as well as the total size of those requests
Requests In-Process	Total number of requests that are active and not suspended from the provider, as well as the total size of those requests

4.6.1.11.2 Configured Notification Information Types

The Provider Status detail page shows the configured notification types for a provider and its notification method, as shown in Figure 4.6.1-53, Figure 4.6.1-54, and Figure 4.6.1-55. The operator cannot suspend or resume these for an individual provider.

Figure 4.6.1-53. Notification Information

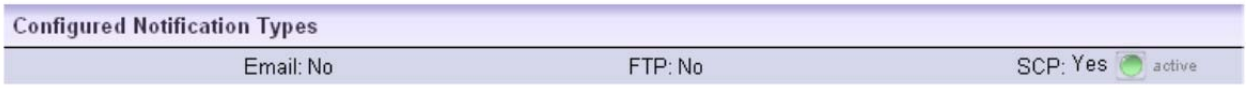


Figure 4.6.1-54. Notification Information w/ SCP active

Figure 4.6.1-55. Notification Information w/ FTP active

A Data Provider may have SCP, FTP, HTTP, email, or a combination of these methods of notification. There is no status for an email notification method or for a notification method that is not enabled.If any of the methods are not used, then "No" will appear next to the notification method name.

Note that operators or the Ingest Service can suspend all traffic to and from a Remote Transfer Host (e.g., if the host or the connection to the host will be taken down or is experiencing problems). In that case, notifications for a provider that use that host will be shown as suspended. Operators can suspend email notifications as a whole via the Ingest Status page (e.g., when the local e-mail service needs to be shut down for maintenance), in which case all email notifications for all providers will be shown as suspended. For more information on that functionality, see Section 4.6.1.2.2.

The overall status of Remote Transfer Hosts is shown on the Transfer Host Status Page (see Section 4.6.1.13). The status of email notifications is shown on the Ingest Status Page (Section 4.6.1.2).

4.6.1.11.3 Polling Location List

Each Data Provider has a list of associated Polling Locations, which are directories on remote or local Hosts that can be suspended or resumed. These can be suspended or resumed in order to halt or resume data to be sent through (Ingested from) these providers, without impacting the status of the Host on which that polling location resides (see Figure 4.6.1-56). To suspend or resume a polling location, check the boxes of the desired locations in the list and click the action button at the bottom of the list. You will be prompted for confirmation before the action is carried out. Table 4.6.1-15 contains the polling locations column descriptions for the provider status detail page.

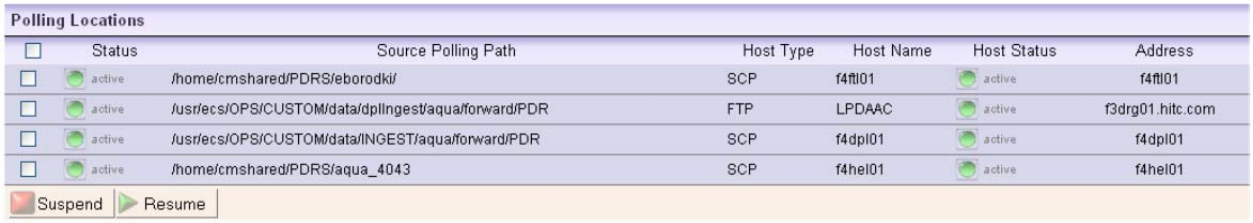


Figure 4.6.1-56. Polling Location List

Table 4.6.1-15. Provider Status Detail Page – Polling Locations Column Descriptions

Field Name	Description
Status	Whether the polling location is active, suspended by server, or suspended by operator
Source Polling Path	Full path of directory being polled
Host Type	Method being used for polling – Local, FTP, HTTP, or SCP
Host Name	Label assigned to the host on which the polling location is found
Host Status	Whether the host where the polling location is found is active or suspended. The polling location itself can be suspended, but this does not affect the state of the host.
Address	IP address or DNS name where the polling directory can be found

4.6.1.12 File System Status

This page displays the status of each of the Archive File Systems and Data Pool File Systems, as shown in Figure 4.6.1-57. Table 4.6.1-16 contains the file systems status page column descriptions.

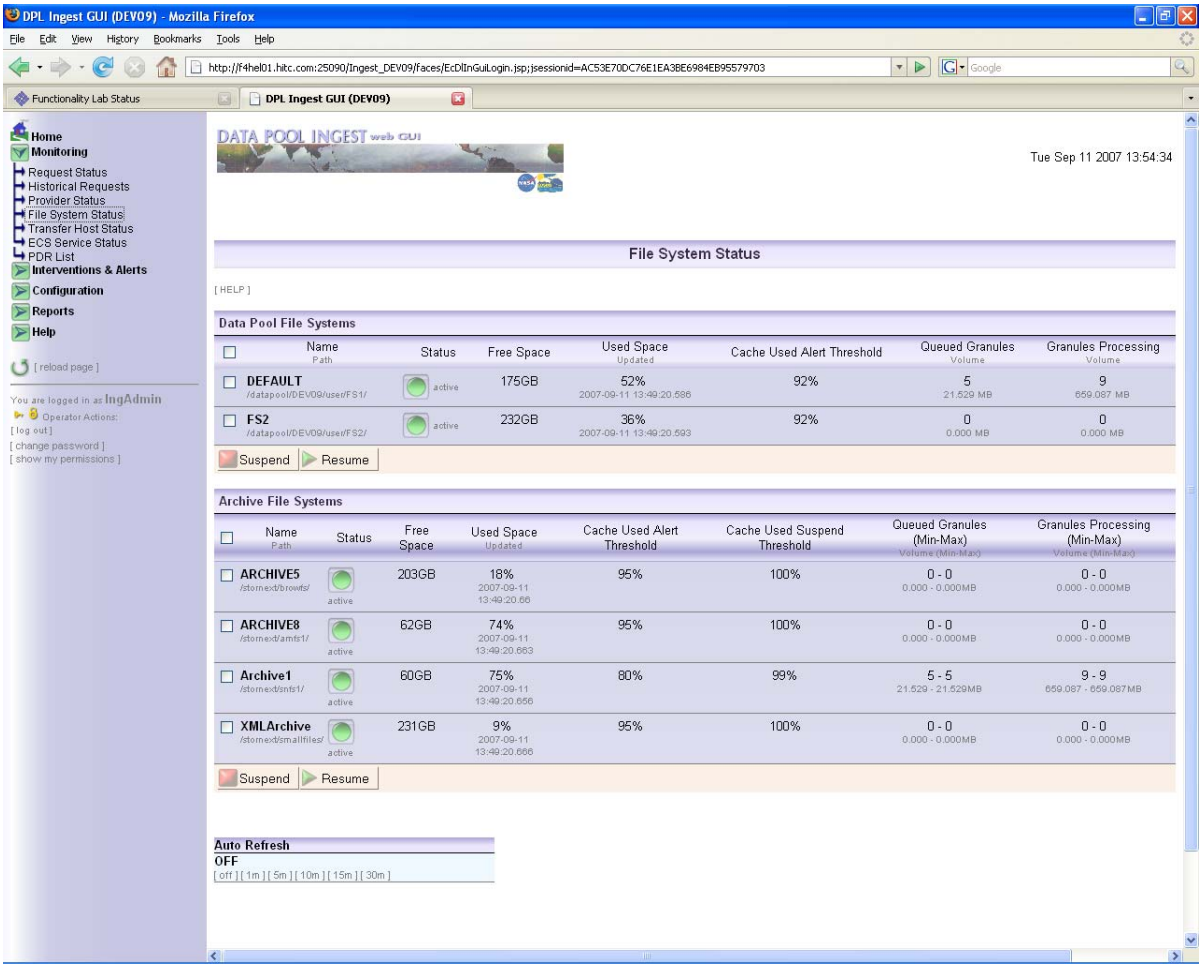


Figure 4.6.1-57. File System Status Page Screen Shot

Table 4.6.1-16. File System Status Page Column Descriptions (1 of 2)

Field Name	Description
Name	Unique name assigned to the file system and the directory where the file system is found
Status	Whether the file system is active, suspended by operator, or suspended by server
Free Space	The amount of free space (in GB) on the File System.
Used Space	Percentage of space used on the file system and the time this information was last checked
Cache Used Alert Threshold	The percentage of used space in the cache at which point an alert would be raised for the Archive or Data Pool File System. For example, if the threshold was set to 80%, an alert would be raised as soon as more than 80% of the cache was used. No requests or file systems will be suspended as a result of this threshold being reached

Table 4.6.1-16. File System Status Page Column Descriptions (2 of 2)

Field Name	Description
Cache Used Suspend Threshold *Archive File Systems only*	The percentage of used space in the cache at which point the Archive or Data Pool File System would be suspended. For example, if the threshold was set to 90%, the Archive File System would be suspended as soon as more than 90% of the cache was used
Queued Granules	Total granules waiting for activation set to ingest on the file system and the sum of the size of those granules
Processing Granules	Total granules active set to ingest on the file system and the sum of the size of those granules

Actions on this page:

As with other pages that display services or providers, each of these archive file systems can also be suspended or resumed. The status column shows a green (active) or red (suspended, either by operator or server) icon. To change the status of one or more file systems, do the following:

1. Select the desired Data Pool File System or Archive File System (multiple selections may be made):

2. Click the desired action button at the bottom of the list
3. You will be prompted for confirmation. The page will reload with the status of the selected archives changed.
4. The application will not allow the same action to be taken twice on an Archive File System. For example, an already active status can not be resumed. However, an Archive File system that was suspended by the server may be manually suspended by the operator.

4.6.1.13 Transfer Host Status

The Transfer Host Status page shows the status of each configured Remote Transfer host, as well as the status of Local Host Transfers. The status is further broken down into the individual polling, processing, and notification statuses for each provider which uses the host. The operator can manually suspend all operations on the host and can resume all operations on the host. See Figure 4.6.1-58 for a general overview.

When an operator suspends the host, the Ingest Service will complete any ongoing transfers, polling cycles, or notifications with that host, but not start any new ones. When an operator resumes the host, this will resume all traffic with that host. It is possible that not all providers will be returned to active when resuming the host depending on the current status of the polling location and data provider.

If the polling, processing, or notification status of a host is suspended by the Ingest Service, an Alert will also be generated and displayed on the System Alerts page (e.g., a connection could not be established with a host because it is down, or there were too many errors while trying to transfer PDR files).

If a PDR is sent through processing with a host configured in the PDR that does not show up on the GUI, a new host will automatically be added to the lists of Remote Transfer Hosts with the name UNDEFHOST_[Provider]_[RequestID] (See Figure 4.6.1-58). The provider status on a host will be displayed if the operator has configured a polling location for that provider on the host, a PDR for the provider references the host, or the provider has configured notifications to be delivered to that host. It is possible that a host is not used for all three servers in which case the status for that particular server(s) will be displayed as not applicable. If more than one polling location is configured for a provider on the host, the number of polling locations will also be displayed next to the polling status. Table 4.6.1-17 contains the transfer host status page column descriptions.

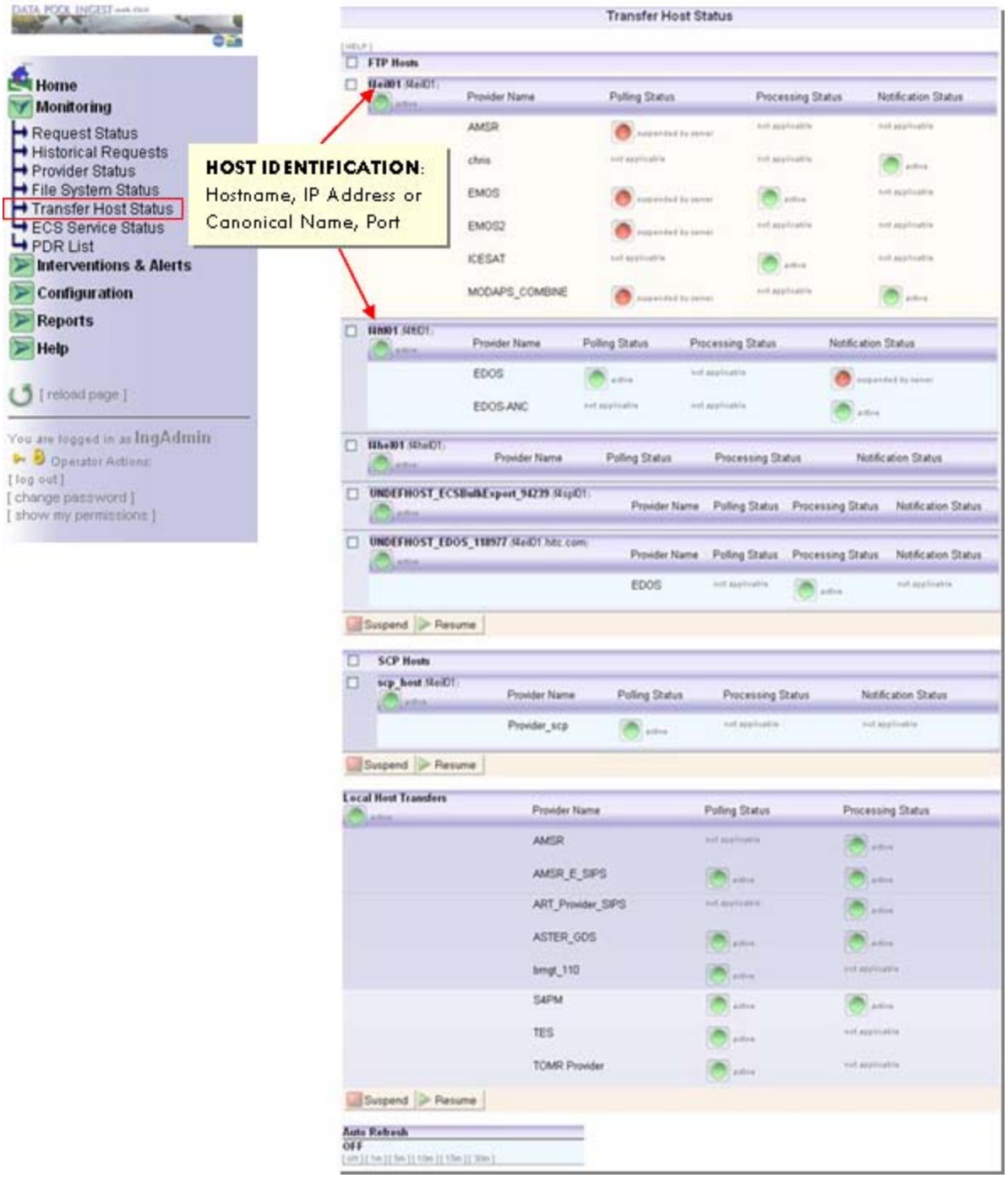


Figure 4.6.1-58. Transfer Host Status Page (General Overview)

Table 4.6.1-17. Transfer Host Status Page Column Descriptions

Field Name	Description
"Host identification"	Display name for the host in bold, followed by the IP address or the canonical name and port of the host in parenthesis, followed by the overall status of the host. Possible statuses are "active" or "suspended by operator".
Provider Name	Name of a provider which uses this host.
Polling Status	Whether or not polling for this provider on this host is active. Possible states are "active", "suspended by operator", "suspended by server", or "not applicable".
Processing Status	Whether or not file transfers for the provider on this host are active. Possible states are "active", "suspended by operator", "suspended by server", or "not applicable".
Notification Status	Whether or not notifications for this provider on this host are active. Possible states are "active", "suspended by operator", "suspended by server", or "not applicable".

Actions on this page:

Each of the Remote Transfer hosts, as well as Local Host Transfer, can be suspended or resumed. The status columns show a green (active) or red (suspended by server or operator) icon and indicate which operations (polling, processing, notification) are suspended for each provider on the host.

To change the status of one or more hosts, do the following:

1. Select the desired host; multiple selections may be made
2. Click the Suspend or Resume button at the bottom of the list, as shown in Figure 4.6.1-59. You will be prompted for confirmation. The page will reload with the status of the selected hosts changed.
3. All operations for all providers will be suspended as a result of suspending the host. Polling will stop on polling locations that use this host for transfers. No notifications will be sent to the host until it is resumed, at which time all notifications halted during the suspension will be later sent.

Figure 4.6.1-59. Suspending a Remote Transfer Host

4.6.1.14 ECS Services Status

The ECS Service Status page shows the status of each of the various ECS Services. There are two types of ECS Services:

1. Services that run on the same host as the Ingest processing service – the GUI only shows that the service is up or down.
2. Services that can run on any number of hosts that have been configured for that purpose. Examples are checksumming, archiving, and transfers. The service on each host is independent of the same type of service on the other hosts, in that its configuration and status is host specific. For example, checksumming on one host may be suspended but may be operating just fine on the other. As a result, the GUI shows the status information for that service separately for each host. These services are called *Hosts Used For ECS Services*.

Host-specific ECS Services can be individually suspended and resumed for that particular host. The XVU, DPIU, and ODL2XML services are listed separately and can only be resumed. See Figure 4.6.1-60 for the general page overview.

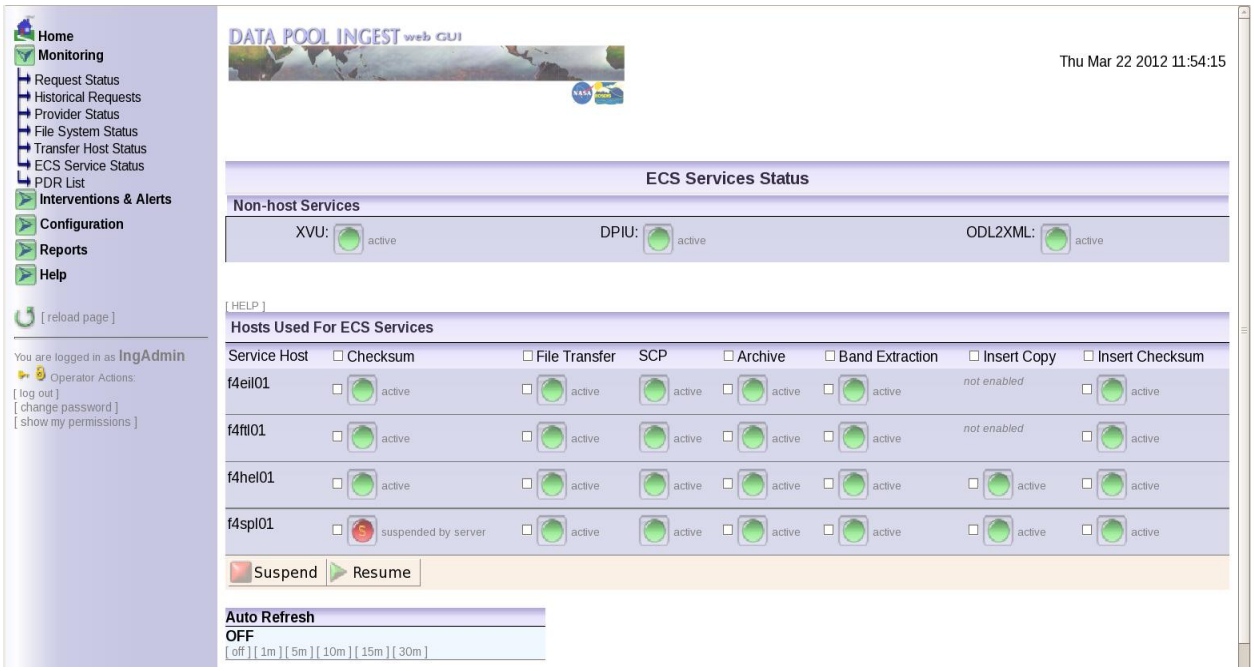


Figure 4.6.1-60. ECS Services Status Page

4.6.1.14.1 Non-host Services

This page shows the status of each of the services which do not run on an ECS Service host. The XVU service performs the XML Validation for granule metadata files, the ODL2XML service converts ODL files into XML files, and the DPIU service registers the granule metadata into the Data Pool database. Each of these services runs on the same host as the processing service and will either be "active" or "suspended by server". If any of the services is suspended it will prevent any ingest from completing because every granule requires these services.

4.6.1.14.2 Hosts Used for ECS Services

These are services that are tied to a specific host. Each of the services can be suspended or resumed on that particular host. The services are:

- Checksum
- File Transfer
- Archive
- Band Extraction
- Insert Copy
- Insert Checksum

To suspend or resume a service on a host, check the box next to the status and click on the desired action button (Suspend or Resume), as shown in Figure 4.6.1-61. You will be prompted for confirmation before the action is carried out. The checkboxes at the top of each column allow the selection of *all* of that particular service for all hosts.

Figure 4.6.1-61. Host-Specific Services

Suspending a service on a host will let all service operations of that type that are currently executing on that host complete on that host, but no new requests for that service will be dispatched to that host. For example, if the Checksum service is suspended for HOST_A, ongoing check summing operations will complete, but then no more check summing operations will be dispatched on that host (regardless of the type of checksum involved). Checksum on other active hosts will continue. Table 4.6.1-18 contains the field descriptions for hosts used for ECS services.

As a rule, checksum operations must take place on a different host that the one on which a granule was transferred. If all but one checksum host is suspended, all granules transferred on that same host will go into a suspended state until another checksum host is activated.

Table 4.6.1-18. Field Descriptions for Hosts Used for ECS Services

Field Name	Description
Service Host	The label of the host used for the ECS Services.
Checksum	The status of the Checksum Service.
File Transfer	The status of the File Transfer Service.
Archive	The status of the Archive Service.
Band Extraction	The status of the Band Extraction Service.
Insert Copy	The status of the Insert Copy Service.
Insert Checksum	The status of the Insert Checksum Service.

Note that for all of these services, *not enabled* may appear as the status; this indicates that the service has not been enabled for that host in the ECS Services Configuration page, therefore no real status exists for that service.

4.6.1.15 PDR List

The PDR List page shows the PDR information retrieved from the Ingest database. The PDR information is shown in Figure 4.6.1.62) with the first column listing the polling location for the PDR and the second column listing the PDR file name.

There is a check box displayed for each of the PDRs listed in the table. By checking the box and applying the Ingest Selected PDRS Again button at the bottom, the corresponding PDR will be re-ingested.

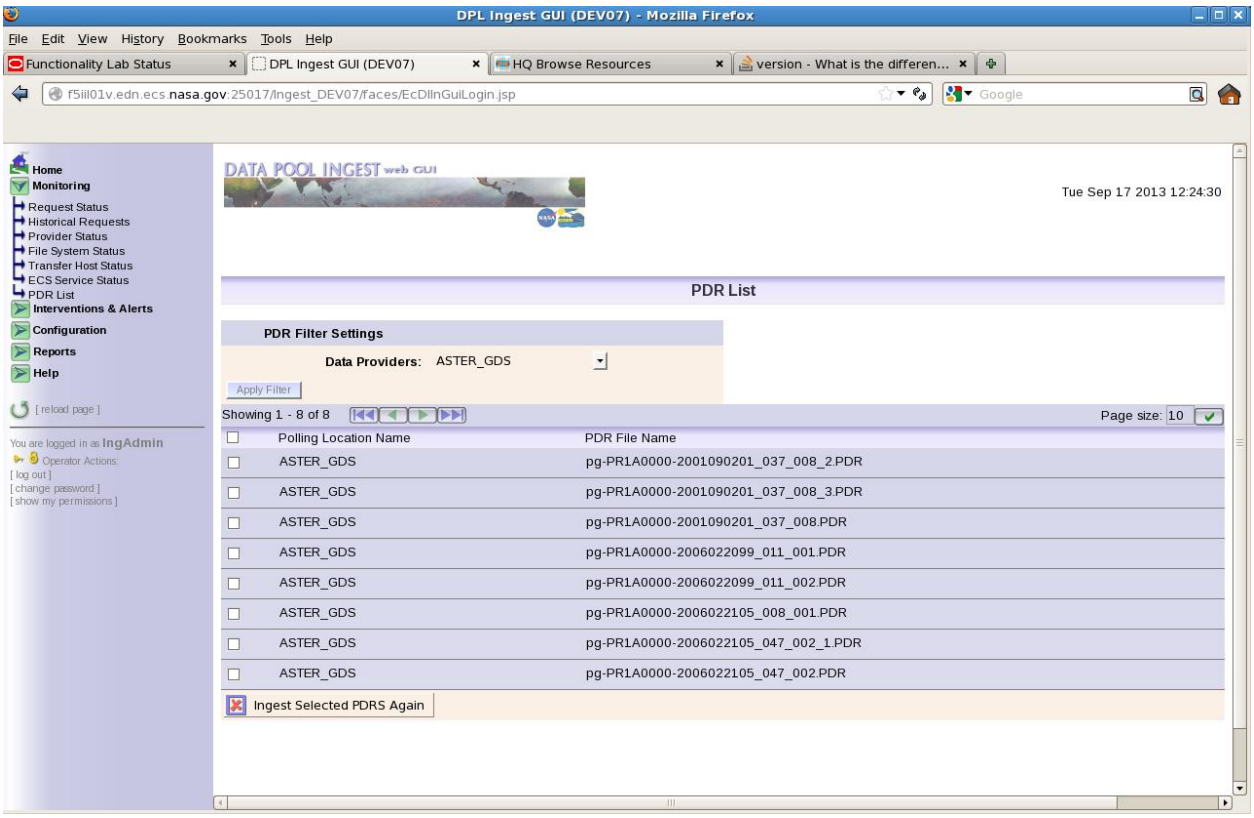


Figure 4.6.1-62. PDR Listing

4.6.1.16 Open Interventions

This page displays the list of Ingest Requests with open interventions, as shown in Figure4.6.1-63. The operator may select any eligible request and perform one of two actions:

- Cancel Active Ingest Request(s) – *This is an irreversible action. There is no way to 'un-cancel' a request.* Processing for this ingest request will be terminated and any granules that did not yet complete processing will be cancelled. If cancelled prior to the "Inserted" state, the granule will be removed from data base entries and files will be removed from temporary locations and the data pool database. A PAN will be sent to the provider that will report failed or cancelled granules and the failure reasons (the specifics depend on the Interface Control Document that covers this interface).
- Resume Active Ingest Request(s) – *only if the selected requests are suspended. Cancelled Requests can not be resumed.* Resuming a request will resume processing for all granules that are currently suspended, restarting each from the last known good state. To disposition individual granules differently, the operator needs to access the intervention detail page. Table 4.6.1-19 contains the descriptions of the open interventions listing page column.

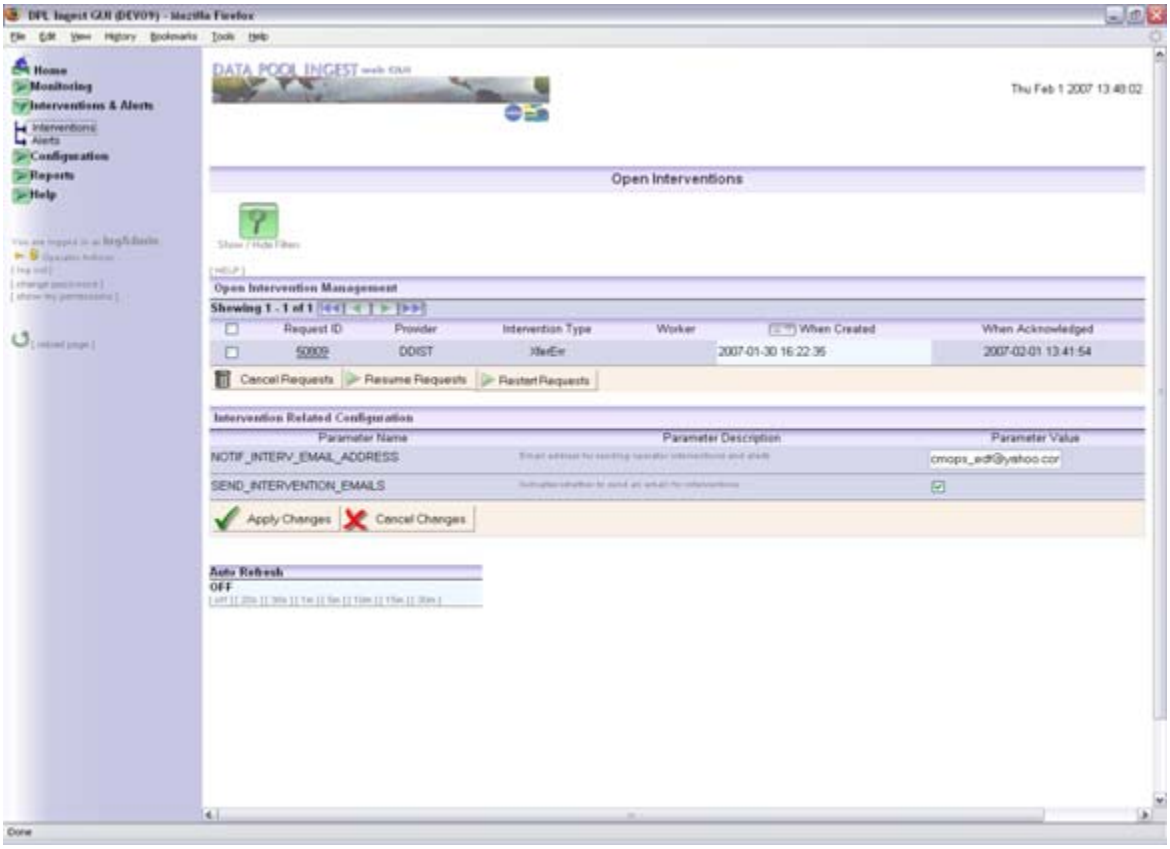


Figure 4.6.1-63. Open Interventions Listing (General Overview)

Table 4.6.1-19. Open Interventions Listing Page Column Descriptions

Field Name	Description
Request ID	Unique Data Pool Ingest identifier assigned to the request in intervention
Provider	Name of the provider from which the request was obtained
Intervention Type	Type of error encountered during processing of at least one of the request granules (if there are multiple error types encountered in a single request, the type will be "MULTIPLE")
Worker	Name of a worker assigned to address the intervention
When Created	Time the intervention was generated (which may have been after several retries after the error was first encountered)
When Acknowledged	Time the intervention was first viewed by an operator

The information on this page is similar to the Request Status page (see Section 4.6.1.6). To view intervention details, click on the Request ID link to open the intervention detail page.

4.6.1.17 Request Actions

Changing Request Statuses

A request is suspended and goes into Operator Intervention Status when at the completion of its processing; at least one of its granules is suspended because it ran into some error. Note that operators can disposition suspended granules before the request goes into intervention, as explained in Section 4.6.1.7.5 . As a result, when a request goes into intervention, some granules may already be in a failed state (if they have been failed by the operator before).

From this page, one can resume suspended requests regardless of the failures. Otherwise, the operator can view the suspended granules of the request and disposition them individually. See the Intervention Detail section below (4.6.1.16) for more details on how Interventions are processed.

To perform a request action, select the desired requests by checking the boxes on the left side of the request list. You can also select or deselect all the requests by checking the box at the very top of the list. See Figure 4.6.1-64.

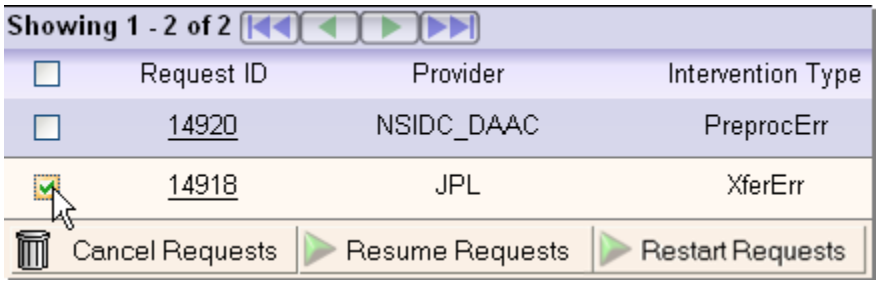


Figure 4.6.1-64. Selecting a Request for Action

Then click on the button of the desired action at the bottom of the list. A box will appear below to enter a reason for the status change. See Figure 4.6.1-65.

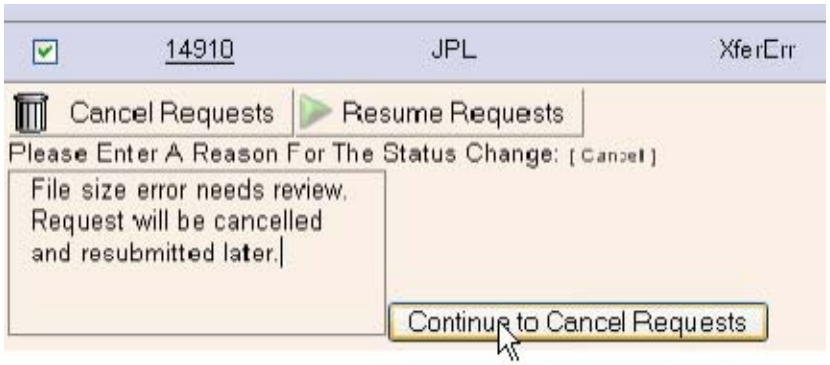


Figure 4.6.1-65. Explanation Field for Changing Request Status

Once you have entered the reason, click on the button next to the text box to continue the action. You will be prompted for confirmation before the action is carried out.

If you do not wish to process this action, click on the [cancel] link to close the box.

4.6.1.17.1 Filters

The Intervention list on this page can be filtered using the filter panel that appears on the same page. This is opened by clicking on the green filter button at the top of the page, as shown in Figure 4.6.1-66. Filter settings are associated with an operator profile and are always remembered, even when logging out of the session. They are never lost unless the operator profile is completely removed or authentication is disabled.

The operator has the option of saving a set of default settings by selecting the "Save As Default Settings" box prior to clicking "Apply Filter." Thereafter, the operator can click "Load Default Settings" to restore these saved defaults. If no default is stored, all Interventions will be shown by default.

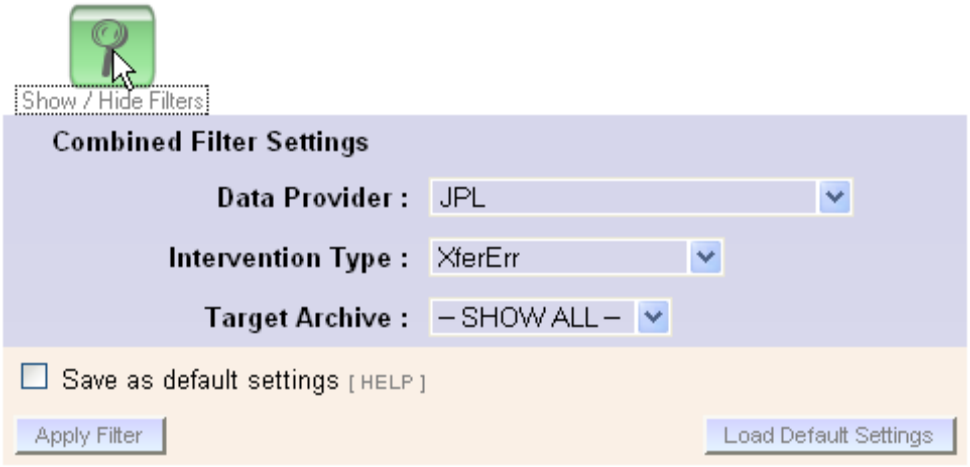


Figure 4.6.1-66. Intervention List Filter Panel

This panel shows the current filter settings and allows the operator to change them. Each of the filters shown in the figure has a SHOW ALL option that effectively does not filter by that field.

Multiple filter settings can be applied at the same time (i.e., the filters are ANDed), thus the operator could opt to see only requests from JPL with an XferErr intervention type, or he could just filter to only see interventions from a single provider.

4.6.1.17.2 Sorting

The Intervention list on this page can only be sorted by the creation date (i.e. the date and time the intervention was created) in ascending or descending order, as shown in Figure 4.6.1-67.

Unlike filter settings, sort settings are remembered for the session only, and are lost when the operator logs out or the application is closed.

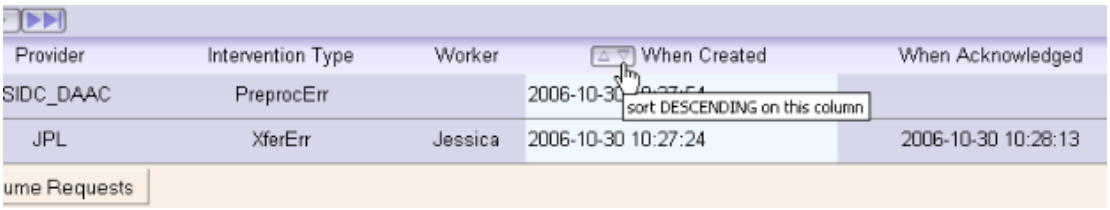


Figure 4.6.1-67. Intervention List Sorts

4.6.1.17.3 Intervention Related Configuration Panel

In addition to being displayed on the Data Pool Ingest GUI, interventions can also be sent as email to a specified operator email address.

To set the email address and permit email notification of Interventions, enter an address next to the "NOTIF_INTERV_EMAIL_ADDRESS" parameter, check the box next to the "SEND_INTERVENTION_EMAILS" parameter, and click the "Apply Changes" button, displayed at the bottom of the "Intervention Related Configuration" section, as shown in Figure 4.6.1-68.

Figure 4.6.1-68. Intervention Related Configuration Panel

The configured email address will receive notifications for all interventions as they are opened.

4.6.1.18 Open Intervention Detail Page

This page displays all of the information as in the general open intervention listing, as well as the granule list. In addition, actions may be taken for the intervention on this page. This page is shown in Figure 4.6.1-69.

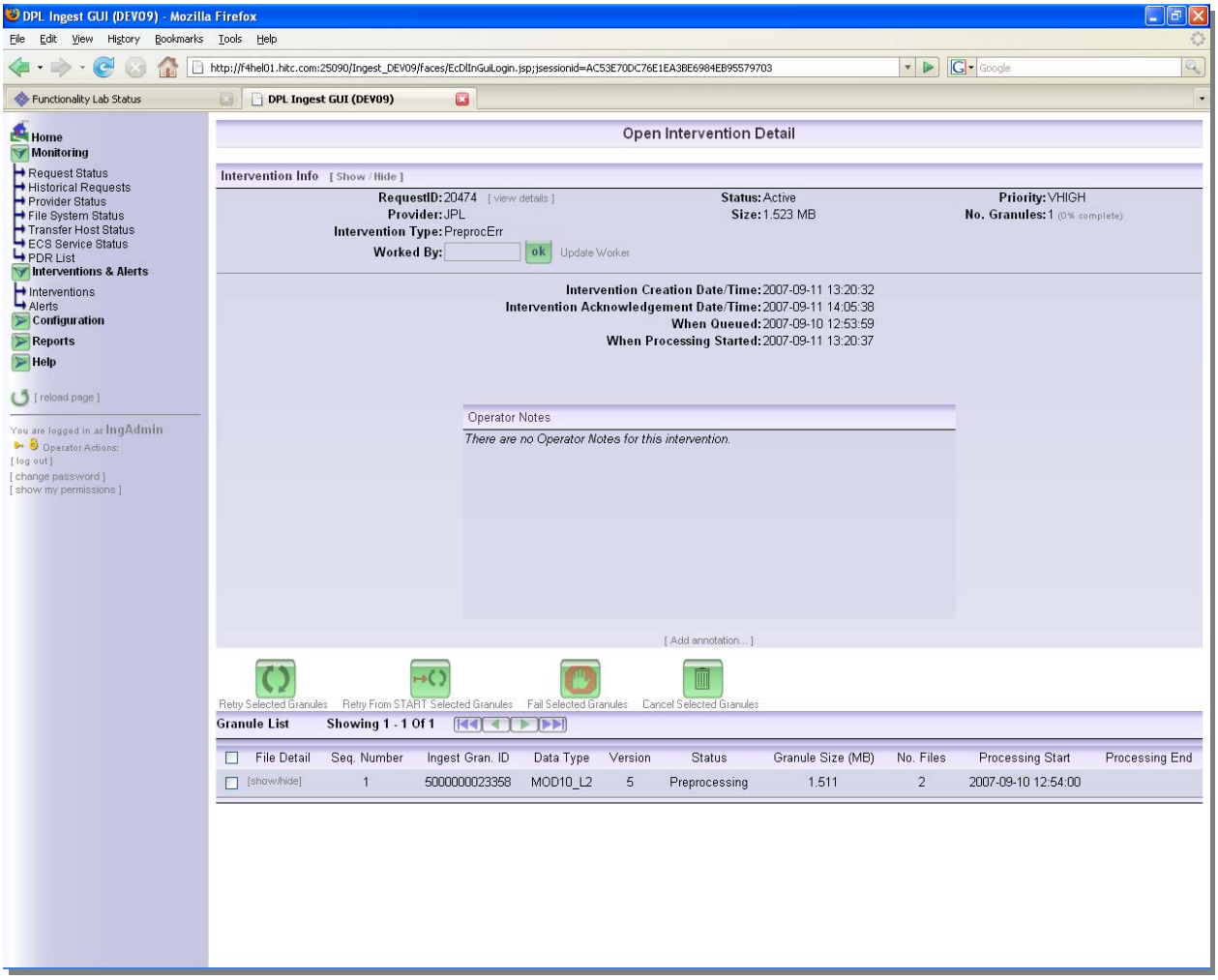


Figure 4.6.1-69. Open Intervention Detail (General Overview)

How Interventions are processed:

An Operator Intervention for an Ingest Request remains open as long as there are suspended granules in the Request. The operator can take one of several actions to 'close' the intervention (i.e., take the request out of suspension and allow the Ingest Request to be processed normally):

- **Retry selected granules:** This applies only to granules that are currently suspended and retries them from the last known good state of processing. Every time a granule is retried, an annotation is added identifying the time, operator, and action (see Figure 4.6.1-69).

- **Retry from START selected granules:** This applies only to granules that are currently suspended and retries them from the beginning of processing. Every time a granule is retried, an annotation is added identifying the time, operator, and action.

- **Fail selected granules:** This applies only to granules that are currently suspended and transitions the granule into a failed state, with the status indicating the type of error that originally caused the suspensions.

Error types are determined by what state the granule is in when it is failed. These states are: XferErr (transferring), ChecksumErr (Checksumming), PreprocErr (Preprocessing), ArchErr (Archiving), InsertErr (Inserting), and PubErr (Publishing).

NOTE: After a granule is failed, an annotation is added identifying the time, operator, and action.

To perform a granule action, select one or more granules and click on the desired action button at the top of the granule list. The operator will be asked for confirmation before the action is carried out.

- **Cancel selected granules:** This applies only to granules that are not yet in a terminal state. It manually cancels the granules. After a granule is cancelled it is expected that the granule will be re-ingested by the operator

Working on an Intervention

The operator must have Ingest Control permission to perform any actions on this page. A worker name is not explicitly required on this page because the logged-in operator name will be used by default. However, an operator may override this by entering a different name into the "worked by" text box. This is allowed because more than one operator may be using the same login during a session, though this practice is not recommended if authentication is enabled.

Closing the Intervention

Once all granule issues have been resolved, the open intervention status will automatically be removed. No explicit action on the part of the operator is required to do this.

If an open intervention is not resolved after being viewed, it will remain in the open intervention list and can be worked on at any time after navigating to a different page or even logging out of the session.

Viewing Request Details:

The operator can navigate to the details for a request by pressing the "[view details]" link next to the Request ID in the upper left-hand corner of the page, as shown in Figure 4.6.1-70. More information on the Request Details page can be found in Section 4.6.1.7.

Figure 4.6.1-70. Viewing Request Details from Intervention Details

Information on this page:

Figure 4.6.1-71 explains the various features and information available on this page. The second part of the page, the granule panel, is described in the subsection 4.6.1.18.2.

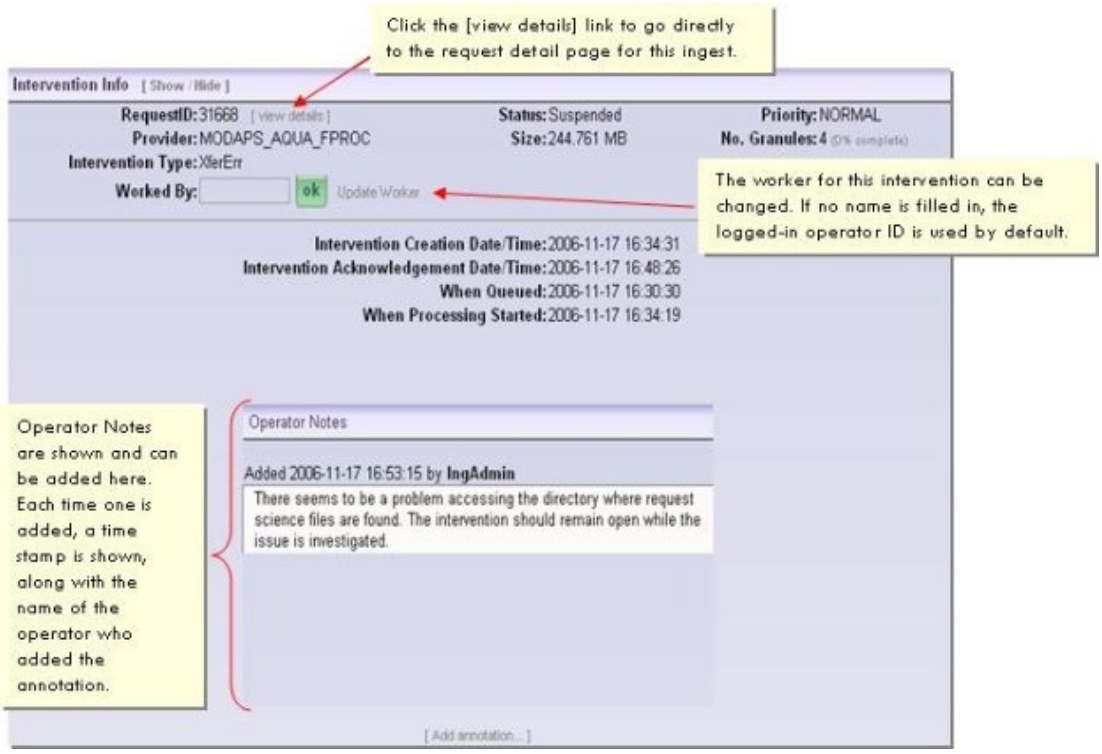


Figure 4.6.1-71. Intervention Detail: Request Information Panel Diagram

4.6.1.18.1 Operator Notes

This section shows operator notes added by the operator. Operator notes are annotations that can be useful in tracking changes to the request or recording information affecting the intervention. The operator notes are kept separately from the request notes (see Section 4.6.1.7.4), though they will be appended to request notes after the intervention is closed.

An operator note can be added, but not edited or deleted. To add an operator note, click [Add annotation...] at the bottom of the annotation list, as shown in Figure 4.6.1-72.

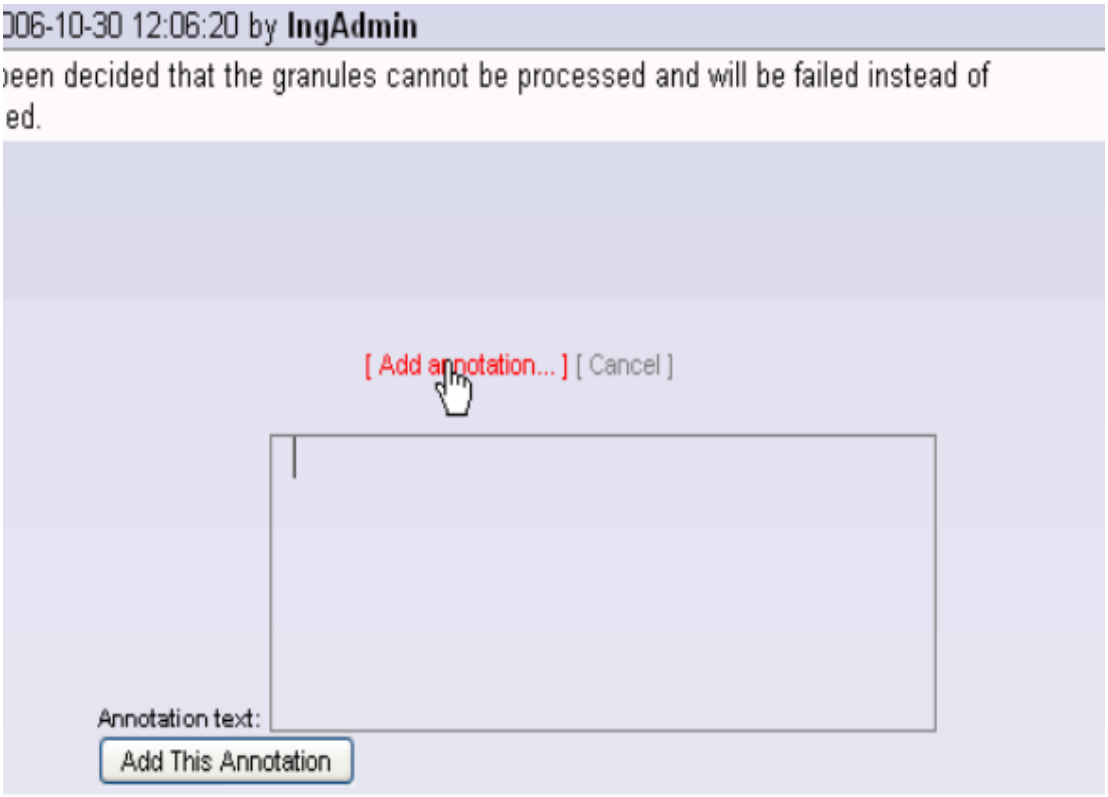


Figure 4.6.1-72. Adding an Annotation

4.6.1.18.2 Granule List Panel

The Granule List Panel is shown immediately below the Intervention Information panel. By default, the list is sorted by suspended granules first. Detailed error information for all suspended and failed granules will be displayed in the granule status, along with the associated error type.

The diagram in Figure 4.6.1-73 below explains the various features and information available on this panel. For more details about the fields in the granule list and file details, see Section4.6.1.7.5.

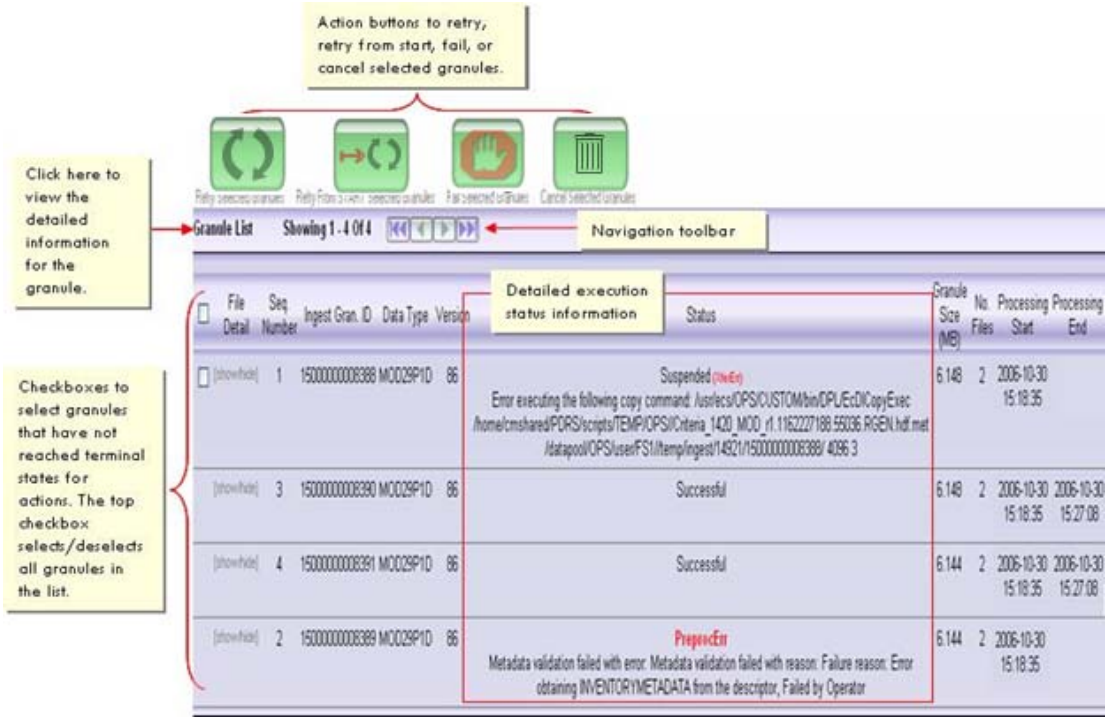


Figure 4.6.1-73. Intervention Detail: Granule List Diagram

4.6.1.18.2.1 Granule Details

Each granule has detailed file information that can be viewed directly on this screen by clicking the [show / hide] button next to a granule. The information will appear above the granule list in sections identified by the Granule Id. The information includes for each file, the full path, file name, file type associated with the granule, and the file status, as shown in Figure 4.6.1-74.

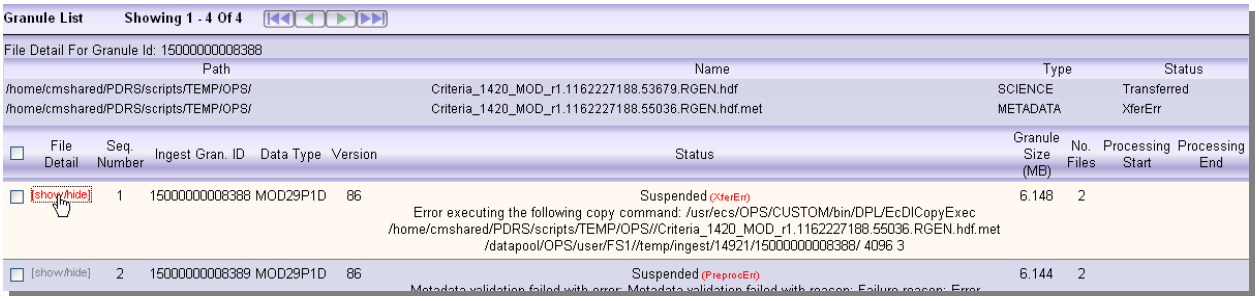


Figure 4.6.1-74. Granule Details

The information can be hid by clicking [show / hide] beside the granule.

4.6.1.19 Alerts

This page (Figure 4.6.1-75) displays the Ingest alerts as they are raised in the Ingest database. These warn the operator when the Ingest Service runs into a problem that is with a resource or service it is using.

Alerts will usually only be generated after a configured number of retries on the failed action, or after a configured number of occurrences of a particular error. After raising an alert, the Ingest Service will check at regular intervals whether the problem has been resolved and clear the alert if that is the case. Table 4.6.1-20 contains the alerts page column descriptions.

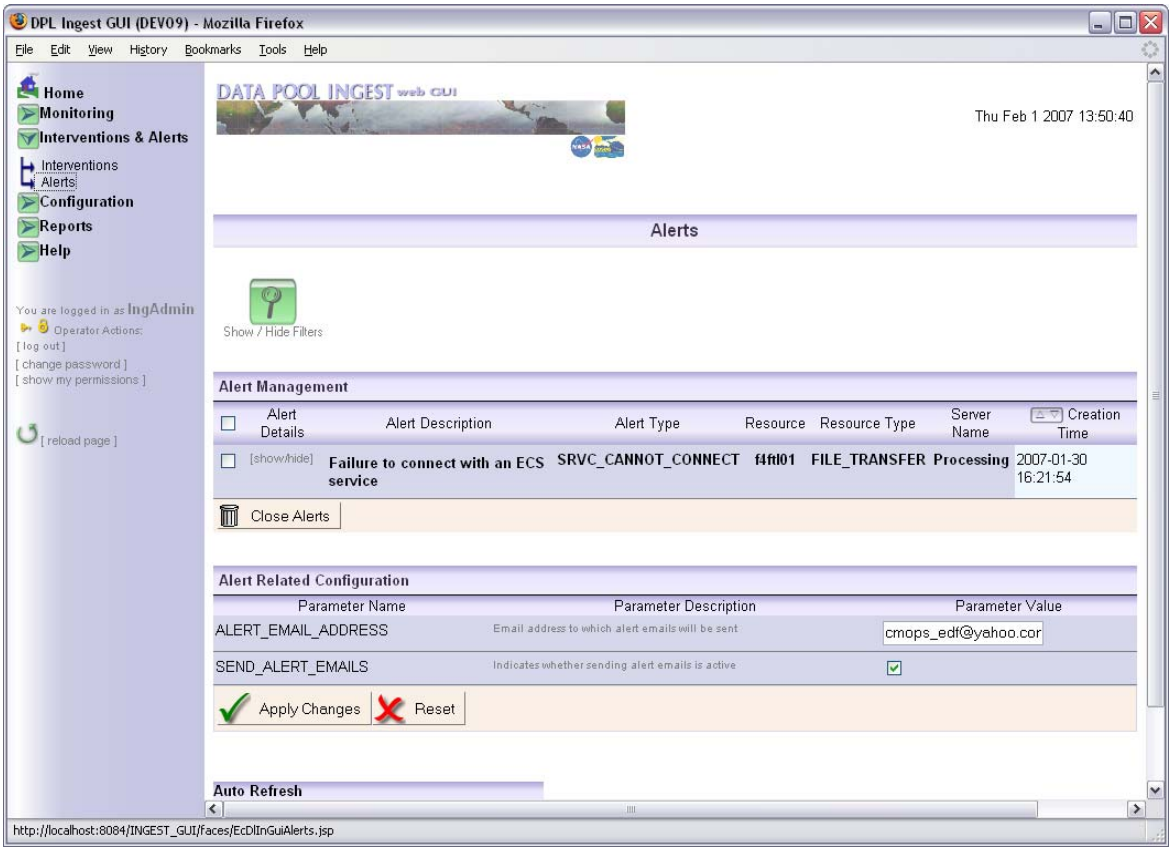


Figure 4.6.1-75. Alerts Page (General Overview)

Table 4.6.1-20. Alerts Page Column Descriptions (1 of 2)

Field Name	Description
Alert Details	Buttons for displaying detailed alert information.
Alert Description	Basic description of the error that generated the alert.
Alert Type	Unique name for the type of error that was encountered.
Resource	The name of the resource affected by the alert.

Table 4.6.1-20. Alerts Page Column Descriptions (2 of 2)

Field Name	Description
Resource Type	The type of resource affected by the alert, such as SCP/FTP/HTTP Host, Polling Location, or Archive.
Server name	The name of the server affected by the alert.
Creation Time	Time the alert was generated (which may have been after several retries after the error was first encountered).

Alert-Related Configuration

In addition to being displayed on this page, alerts can also be sent as email to a specified address.

To set the email address and permit email notification, enter an address next to the "ALERT_EMAIL_ADDRESS" parameter, check the box next to the "SEND_ALERT_EMAILS" parameter, and click the "Apply Changes" button, displayed at the bottom of the "Alert Related Configuration" section. See Figure 4.6.1-76.

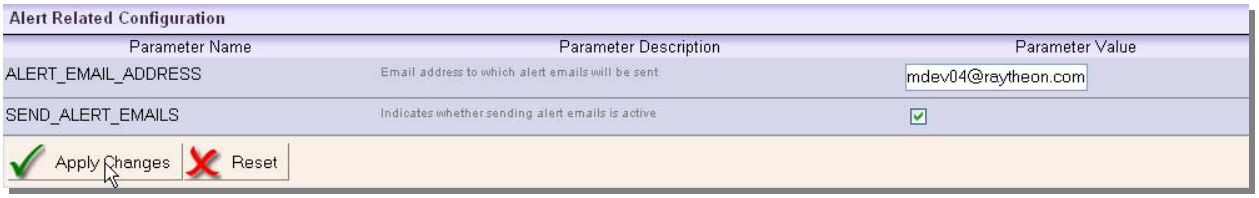


Figure 4.6.1-76. Alert-Related Configuration

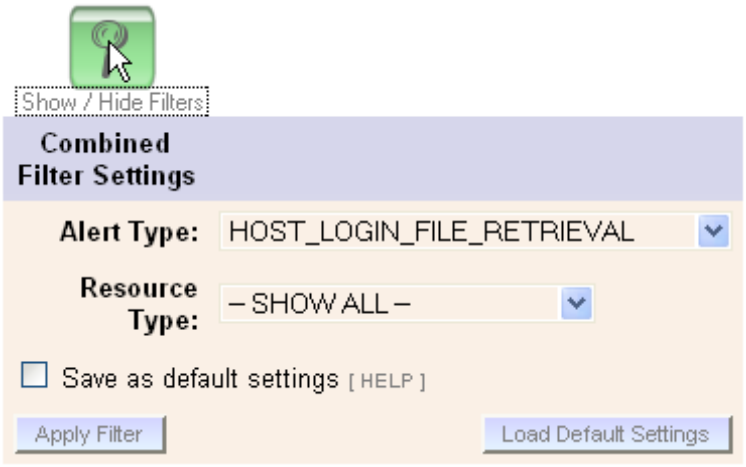
4.6.1.19.1 Filters and Sorts

Alerts are sorted in descending order (most recent first) by creation time. To sort in the opposite direction, click on the sort icon under the "Creation Time" column. See Figure 4.6.1-77.

Figure 4.6.1-77. Sorting the Alert List

This page shows all alerts by default. If you want to see only specific types of alerts, you can set a filter:

1. Click [Show / Hide Filters] at the top of the alert listing:

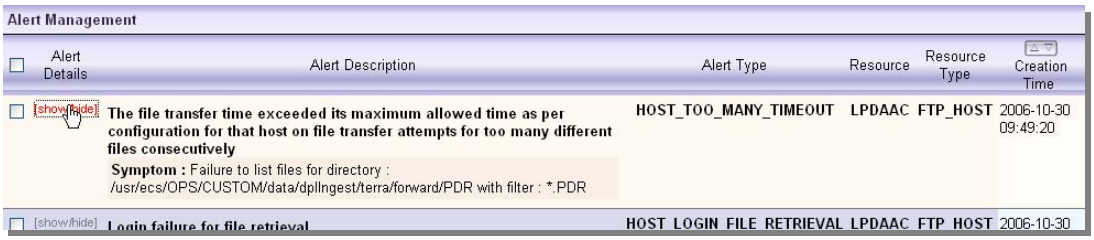


2. Click "Apply Filter" to apply the filter:
3. The page will reload; only alerts matching the filter criteria will be shown.

Note that these filters combined (ANDed). Also, each of the drop down lists has a SHOW ALL option, allowing all Alerts for that particular field to be shown.

4.6.1.19.2 Alert Details

The details of the alert will appear under the alert description (a new page will not be loaded). To view this detailed information, click [show / hide] under the Alert Details column to expand the detail area:



Click [show / hide] again to hide the details.

If the Resource Type for the Alert is an archive or file system, the alert details will show the Data Providers affected by the alert condition, as well as the number of PDRs, ingest granules, total queued data, and total in-process data affected. See Table 4.6.1-21.

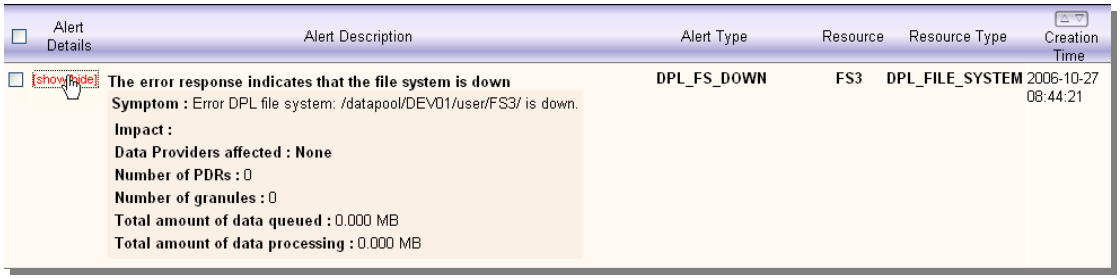


Table 4.6.1-21. Alert Description Details Field Descriptions

Row Name	Description
Symptom	Information about the specific action or item that caused the alert.
Impact	The resource affected by the Alert (if applicable). An example of an impacted resource would be a SCP, FTP or HTTP Transfer Host. This field is only shown if the Alert could potentially impact a Resource. Otherwise, for Alerts like "**Email Notification is down**" or "**Login failure for PAN/PDRD transfers**", this field is not shown.
Data Providers affected	List of providers that will be suspended as a result of the alert. This is only shown if Data Providers could potentially be affected, for example if connection to a Transfer Host could not be established.
Number of PDRs	Total number of PDRs active or queued on a provider affected by the suspended resource. This is only shown if the Alert affects Ingest Requests.
Number of granules	Total number of granules active or queued on a provider affected by the suspended resource. This is only shown if the Alert affects Ingest Requests.
Total amount of data queued	Sum of the size of the files in the granules that require the file system and will not be activated while it is suspended. This is only shown if the Alert affects Ingest Requests.
Total amount of data processing	Sum of the size of the files in the granules that require the file system, but will get "stuck" in an active state as a result of the alert. This is only shown if the Alert affects Ingest Requests.

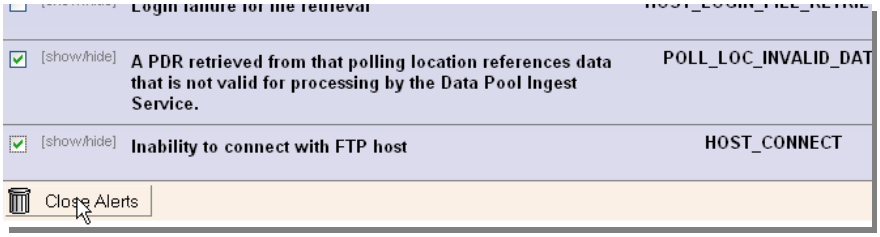
4.6.1.19.3 Clearing an Alert

An alert may be cleared manually at any time, though this should only be done once the operator is certain the problem has been resolved. In response, the Ingest Service will resume using that resource and all the associated resources, for example, the FTP Host to which it could not connect and all the polling locations on that host. The Ingest Service may find that it is still unable to use the resource (e.g., still cannot connect), in which case the alert will be raised again.

It is not necessary for an operator to clear an alert manually. Normally, the Ingest Service will test in regular intervals whether the error situation has been resolved and if so, clear the alert automatically. However, it may be appropriate to clear an alert manually, for example, if the operator took some manual steps to resolve the reported problem (such as restarting an ECS Host) and then wants the Ingest Service to try using that resource immediately.

To clear an alert from the list manually, do the following:

1. Select the desired alerts from the list by checking the boxes on the line for the Alerts; multiple selections may be made:



2. Click the "close alerts" icon at the bottom of the alert list. You will be prompted to confirm the clearing of the alert(s):
3. The page will be reloaded with the selected alerts no longer appearing on the list.

4.6.1.20 Provider Configuration Page

This page lists all of the Data Providers for the DPL Ingest System, along with selected attributes of each to get a general overview of each provider. From this list, the operator may also add or remove a Data Provider. By clicking on the provider name, the operator may also view the Provider details. This page is shown in Figure 4.6.1-78. Explanations of the fields on this page are found in Table 4.6.1-22.

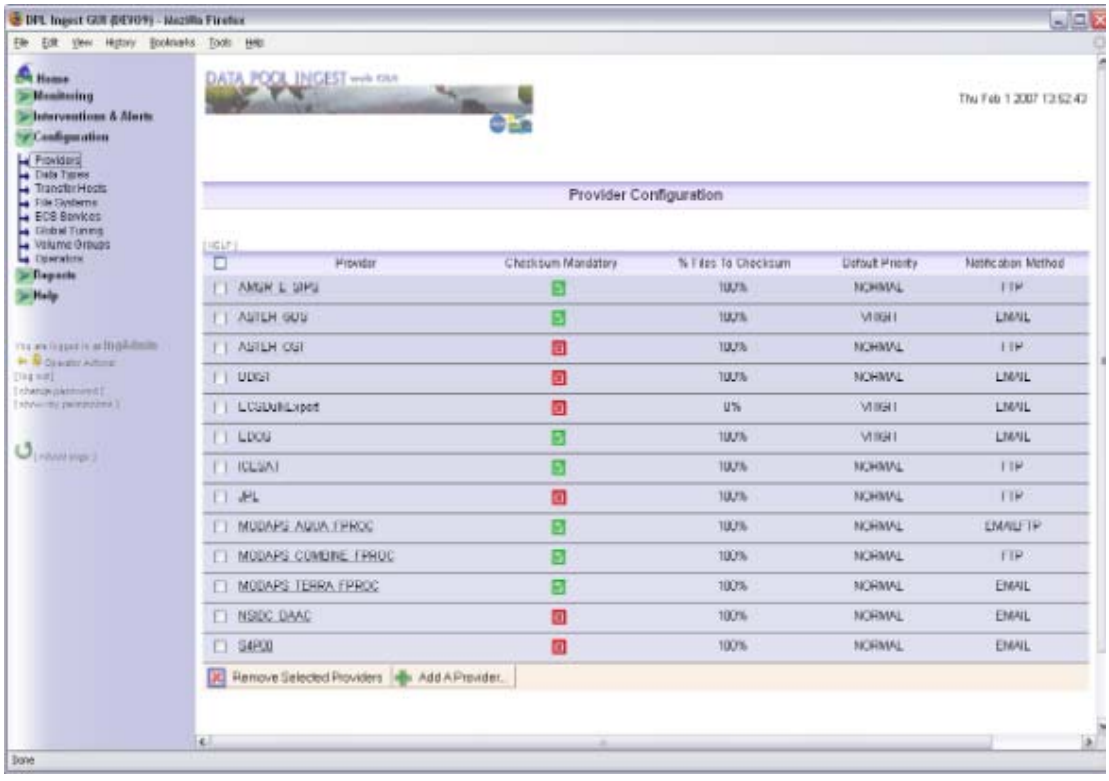


Figure 4.6.1-78. Provider Configuration Page (General Overview)

4.6.1.20.1 Edit a Provider Page

The "Edit a Provider" page shows all of the settings for a data provider, including the notification method and the polling locations, as shown in Figure 4.6.1-79. This page is displayed when the operator clicks the provider name on the Provider Configuration List page (previous section).

Note: Trailing and leading white space will be removed from values entered into any text fields on this page, or any of the sub pages under it.

Table 4.6.1-22 contains the provider configuration detail field descriptions.

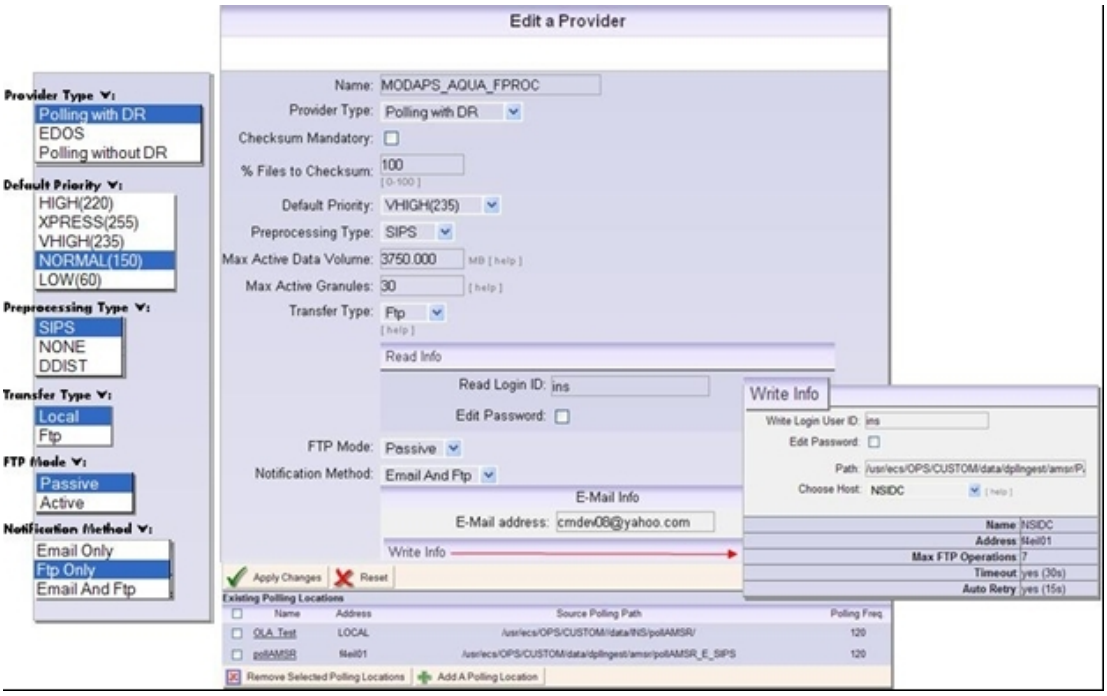


Figure 4.6.1-79. Provider Configuration Detail (General Overview)

Table 4.6.1-22. Provider Configuration Detail Field Descriptions (1 of 2)

Field Name	Entry	Description
Name	Required	Name for an external data provider.
ProviderType	Required	Indicates the type of the provider (such as Polling with DR, Polling without DR, EDOS).
Checksum Mandatory	Optional	Indicates that the Data Provider *must* provide checksum information in the PDR.
% Files to Checksum	Required	Percent of requests to checksum for this provider.
Default Priority	Required	Default priority for ingest requests for this provider.

Table 4.6.1-22. Provider Configuration Detail Field Descriptions (2 of 2)

Field Name	Entry	Description
Preprocessing Type	Required	Type of ingest processing to occur (such as SIPS or DDIST).
Max Active Data Volume	Required	Maximum total volume that will be active on a provider if requests for other providers are pending.
Max Active Granules	Required	Maximum total granules that will be active on a provider if requests for other providers are pending.
Transfer Type	Required	Method used for obtaining files from the external data provider (local, FTP, HTTP, or SCP with various cipher types).
Notification Method	Required	Method for providing notifications to the provider (email, SCP, FTP, HTTP, or combination of SCP/FTP/HTTP and email).
Email Address	Required if email is the notification method	Address to which to send notifications after a granule on the provider completes ingest.
Write Login User ID	Required if FTP or SCP is the notification method Optional if HTTP is the notification method	User Id for getting write permissions on the provider's notification directory.
Write Info: Password	Required if FTP or SCP is the notification method Optional if HTTP is the notification method	Checkbox displays a password and verify password field that are used to provide access to the provider's notification directory.
Path	Required if FTP, HTTP, or SCP is the notification method	For FTP or SCP, Directory where notifications will be sent on the provider. For HTTP, URL location where notifications will be sent on the provider.
Choose Host	Required if FTP, HTTP, or SCP is the notification method	Host where the notification path can be found (list is generated from hosts configured on the Host Configuration page).
Read Login Id	Required if a polling location uses FTP or SCP Optional if HTTP is the polling method	User Id for getting read permissions on the provider's polling directories.
Read Info: Edit Password	Required if a polling location uses FTP or SCP Optional if HTTP is the polling method	Checkbox displays a password and verify password field that are used to provide access to the provider's polling directories.

Existing Polling Locations

A list of pre-existing polling locations is displayed at the bottom of the page. You can add or delete polling locations on this list. For instructions on how to add a Polling Location (when adding a Data Provider), see Section 4.6.1.20.3, steps 12-19.

To edit a polling location, select the location name (see Figure 4.6.1-80).

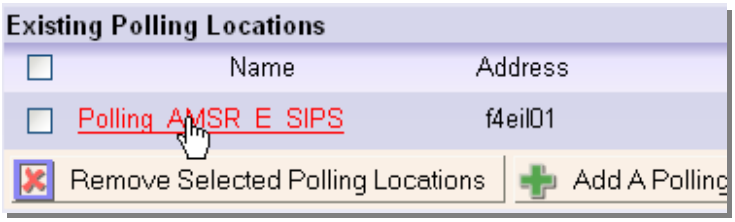


Figure 4.6.1-80. Editing a Polling Location

A page will appear much like the "Add a Polling Location page," except all the fields will be populated, as shown in Figure 4.6.1-81. Table 4.6.1-23 contains the polling location detail page field descriptions.

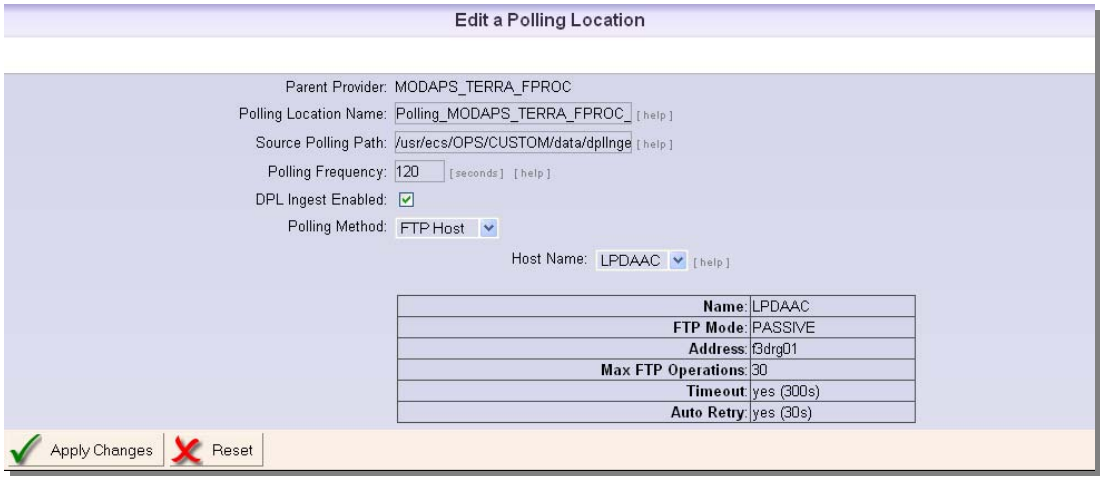


Figure 4.6.1-81. Polling Location Detail

Table 4.6.1-23. Polling Location Detail Page Field Descriptions

Field Name	Entry	Description
Parent Provider	Not Editable	Name of the provider with which this polling location is associated.
Polling Location Name	Required	Name used to uniquely identify the polling location.
Source Polling Path	Required	Directory that will be polled.
Polling Frequency	Required	Number of seconds the ingest service will wait between scanning the polling path for new PDRs.
DPL Ingest Enabled	Optional	Indicates whether this polling location is enabled for ingest via DPL.
Polling Method	Required	Transfer method used for obtaining PDRs from the polling location.
Host Name	Required if using a remote transfer method	Host where the polling directory is found.

Enter the desired modifications and click "Apply Changes."

Deleting Polling Locations

To remove a polling location, click the check the box next to the location's name; multiple selections may be made. Click "Remove Selected Polling Locations"; you will be prompted to confirm the deletion. See Figure 4.6.1-82.

Under some circumstances, a Polling Location may not be able to be removed. For example, if there are pending requests with PDRs that use the Polling Location, you will see a database error if you try to remove it. In order to successfully remove a Polling Location, ensure that no requests using this Polling Location are pending and that the Processing Service has been shut down.

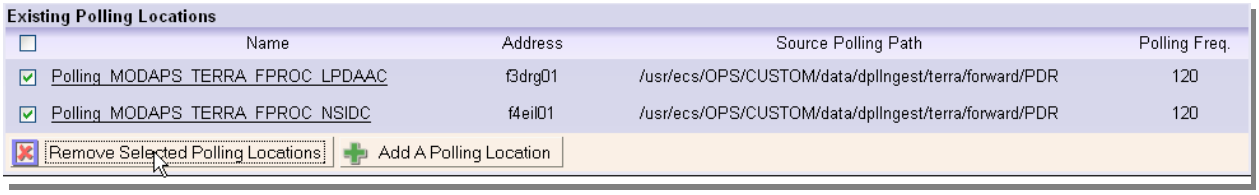


Figure 4.6.1-82. Polling Location List

Adding a Polling Location

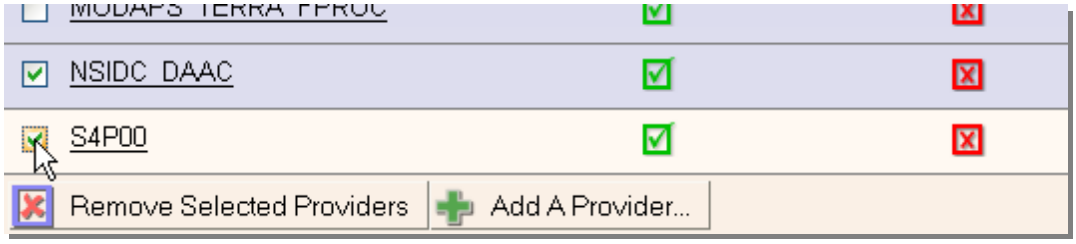
See Section 4.6.1.18.3 for complete details on how to add a Polling Location for a Provider.

4.6.1.20.2 Removing a Data Provider

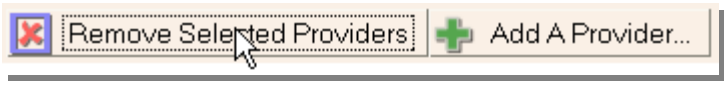
You can only remove an existing Data Provider if all of its Polling Locations have been removed.

To remove a provider:

1. Select a provider by checking the box next the provider name; multiple selections may be made:



2. Click the remove button at the bottom of the list:



3. You will be prompted for confirmation. The page will reload and the selected providers will n4.6.1.20.3o longer be displayed.

4.6.1.20.3 Add a Provider Page

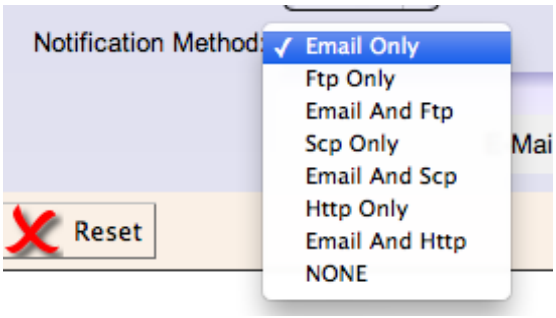
This page enables an authorized operator to add a Data Provider and associated Polling Location. Adding a data provider involves several complex steps. Below is a step-by-step guide to the process involved in adding a provider.

Note that EDOS providers have some special rules:

- A Processing Type is not allowed (it is automatically set to NONE in the GUI and is enforced when adding the Provider)
- An EDOS Provider can only use an FTP Transfer Type and an FTP Notification method. This selection is also enforced in the GUI.

The general steps are:

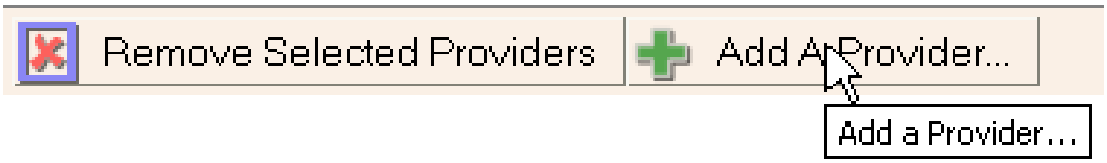
1. Setting the provider's name and its configuration parameters. If you are not authorized to change configuration parameters, you cannot add a provider.
2. Selecting the notification method and configuring the attributes of each method (if more than one applies). Again, if you are not authorized to change configuration parameters, you cannot configure the notification methods. A provider may have one of the following notification methods:
    a. Email only
    b. SCP only
    c. FTP only
    d. HTTP only
    e. Email and FTP
    f. Email and SCP
    g. Email and HTTP



3. Adding a Polling Location (this involves several sub-steps – see the detailed instructions below).

Detailed illustrated instructions for adding a provider:

1. On the Provider Configuration page, Press "Add Provider" at the bottom of the existing provider list:



2. A new page will be loaded, which will guide you through configuring the provider; it contains a blank form to add your parameters (see Figure 4.6.1-83). Explanations of the fields on this page may be found in Table 4.6.1-22.

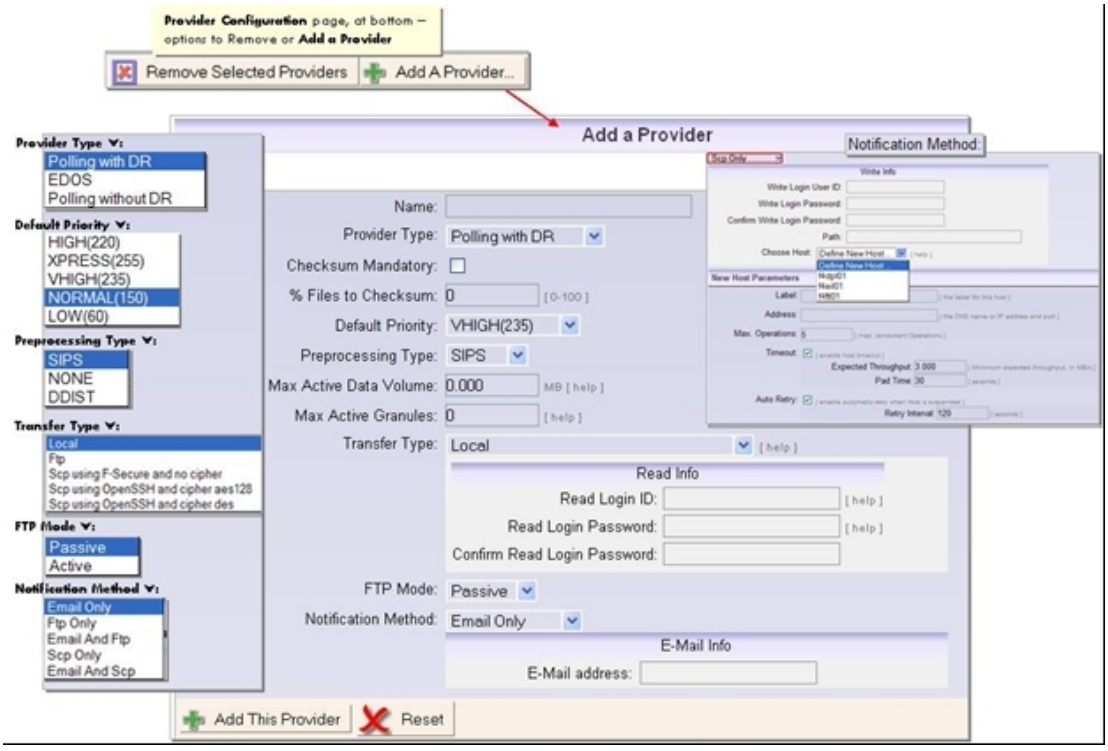
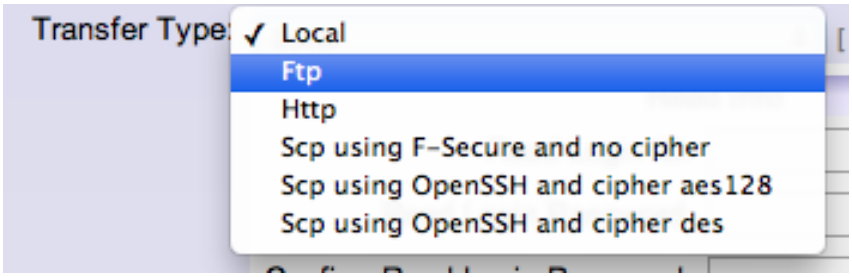


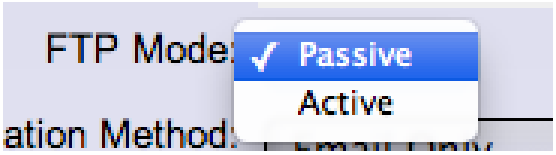
Figure 4.6.1-83. Add Provider Page

3. Provide a unique name for this provider. Already existing names will be rejected by the database.
4. Select the correct type of the provider which is one of "Polling with DR", "EDOS" or "Polling without DR". If you select EDOS, Preprocessing Type will become NONE, Transfer Type will become FTP and Notification method will become FTP Only. These options cannot be changed. If you select "Polling without DR", a VersionedDataType drop-down list will appear on the page for operator to select the ESDT this provider will ingest from a predefined list of polling without DR ESDTs, the "Checksum Mandatory" checkbox will be unchecked and disabled, the "% Files to Checksum" will be set to 0 and disabled, the Preprocessing Type will become NONE and Notification Method will become NONE.
5. If applicable, check the box for "Checksum Mandatory"; if this box is checked, this indicates that the Data Provider must provide checksum information in the PDR.
6. If "Checksum Mandatory" is checked, you may specify the percentage of files to be checksummed in the "% Files to Checksum" text box.
7. Select a default priority from the following options: LOW (60), NORMAL (150), HIGH (220), VHIGH (235), XPRESS (255).
8. Enter the maximum data volume (in MB) that can be processed at the same time on this provider.
9. Enter the maximum number of granules that can be processed at the same time for this Provider. The Ingest Service uses the maximum data volume and number of granules to limit the amount of the work which it will activate for a provider. Ingest will activate a new granule for an active ingest request only until the amount of work for the provider that is currently in progress reaches one of the configured limits. New granules will be activated as granules complete and slots are opened up.

   Only active granules are counted as work in progress and will count against provider limits; granules that completed ingest, failed, were cancelled, or are suspended are not considered 'in progress'. Note that, in addition, there are overall limits on the total amount of work in progress, across all providers, which may further limit how much work is activated.
   Ingest will ignore the provider limits if there is insufficient work queued for the other providers. In this case, granules will be activated until system limits, instead of the provider's limits, are reached.
10. Select the transfer type.



Choose the FTP Mode if the data transfer is FTP:

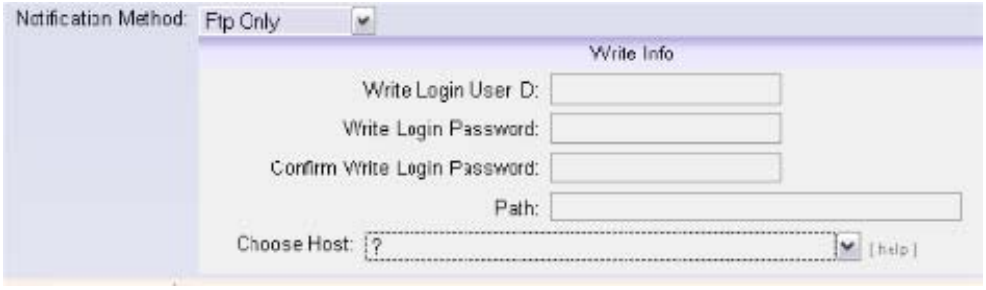


If data transfer will be FTP or SCP, the operator must enter the Read Info parameters, as shown in Figure 4.6.1-84. If this information is not filled out, when a polling location is added, the operator will not be able to select ftp as the transfer method. The Read Info is optional if the data transfer is HTTP providing the user authentication may not be needed.

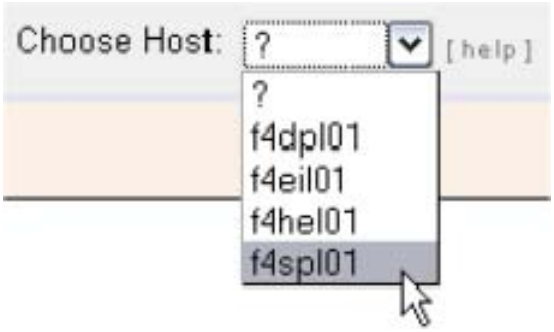
Figure 4.6.1-84. Read Info

11. Select the notification method. Depending on your selection, the appropriate boxes for the related parameters will appear below the drop-down list:
    a. Email only: enter a valid Email address

    b. FTP only, HTTP only, or SCP only (the same form shows up for either): enter the Write login information (Required for FTP and SCP, optional for HTTP), the path, and select a host from the dropdown list (see next step).

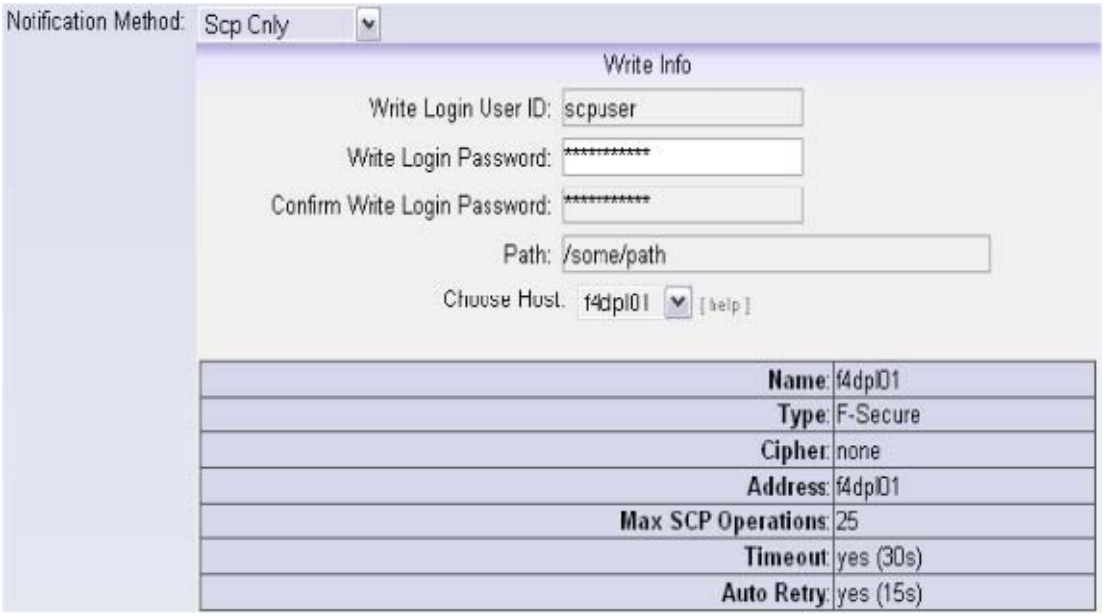


    c. Pick an existing, pre-configured FTP host as defined in the FTP Host Configuration page; a drop-down list will appear with the available configured hosts:

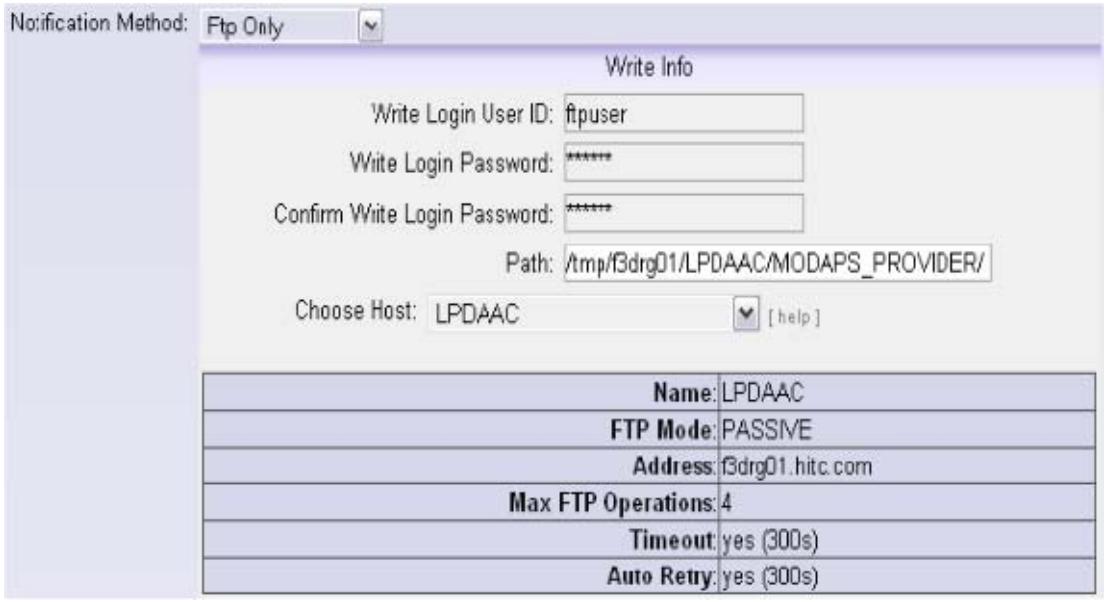


When you select the desired host, an information box is displayed, showing the host's name, IP address, and other details, as applicable to the type of host (FTP, HTTP or SCP – see the figures below):

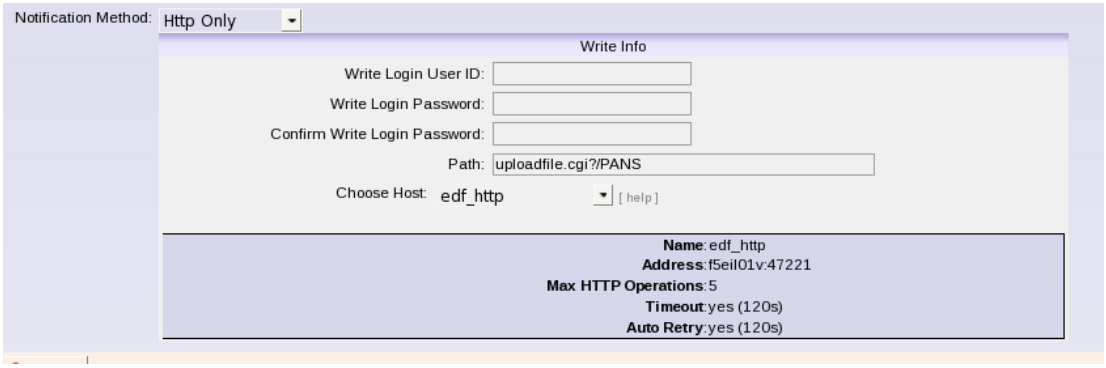
An example of an SCP host:



An example of an FTP host:



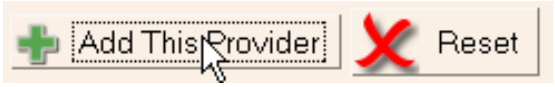
An example of an HTTP host:



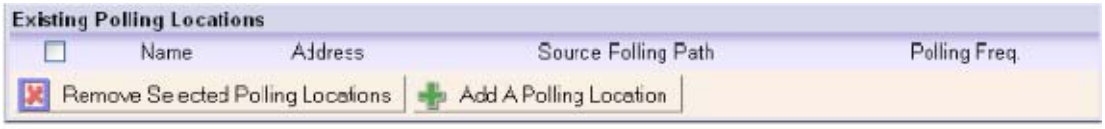
d. If you are configuring a Polling Location with Transfer Type of "local", no path or Read Info entry is required.

e. Email and FTP, or Email and SCP: If you select this option, you must enter parameters for both the Read and the Write Info. Email and HTTP: If you select this option, the Read and the Write Info are optional providing the user authentication may not be needed.

12. Now add this provider by clicking the "Add This Provider" button at the bottom of the screen. Note that polling locations can not be added until the provider has been added. You will be prompted to confirm the addition of a new provider.

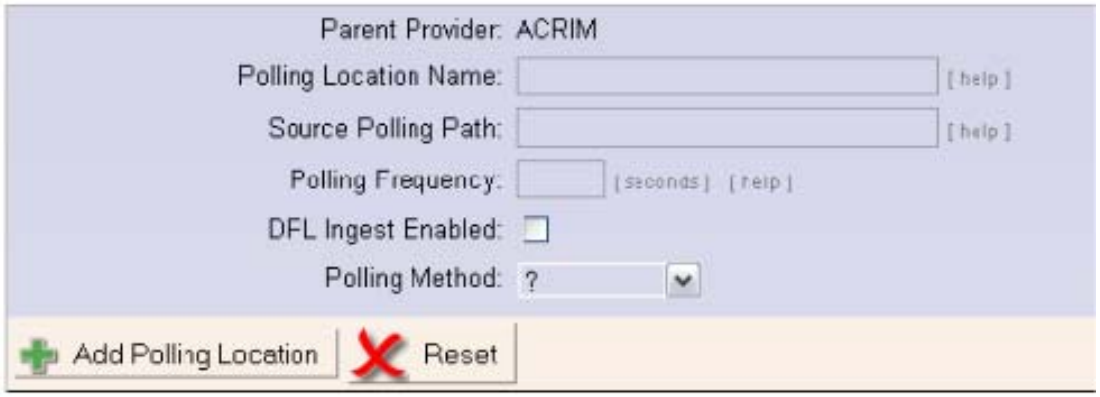


13. You will be taken back to the Provider Configuration page. Select the new provider to view its details. At the bottom of the Provider Detail page, click "Add a Polling Location":

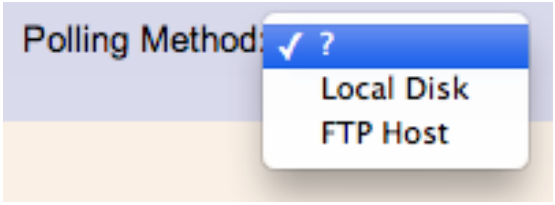


Note: This step is not necessary to complete the provider configuration; the operator may come back and edit this provider and add or remove polling locations at any time. The Data Provider, however, will not become active (i.e., polling will not begin) until at least one polling location is added.

14. A new screen will be displayed that will guide you through configuring the parameters of the polling location:

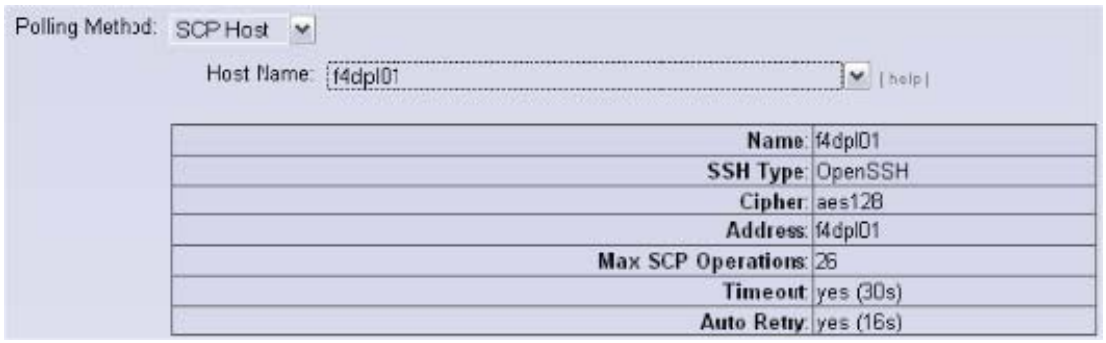


15. Enter a unique name for the location; names that already exist will be rejected.
16. Enter the Source Polling Path- this is the pathname from which to transfer the PDR files.
17. Enter the polling frequency in seconds – the minimum value is 120 seconds.
18. Select whether or not this Polling Location is DPL Ingest Enabled.
19. Choose the type of host on which this polling location resides:
    a. Pick pre-configured FTP, SCP or HTTP host as defined in the Host Configuration page; a drop-down list will appear with the available configured hosts. The available configured hosts are based on the Transfer Method of the parent provider. For example, if the Transfer Method is FTP for the provider, then the available Polling Methods will be Local Disk, FTP Host:

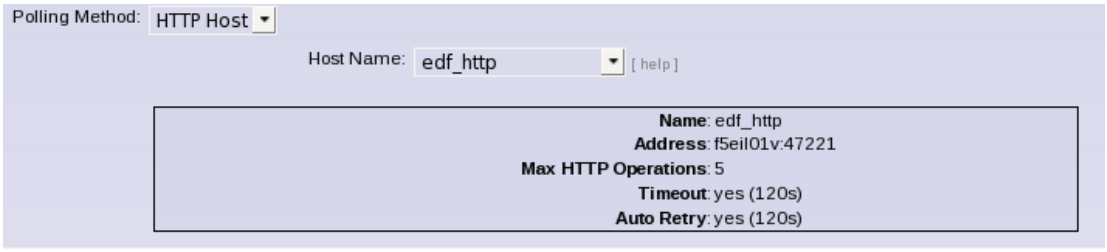


When you select the desired host, an information box is displayed, showing the host's login information, IP address, and other details. The following is an example of what is displayed for an FTP host:

The following is an example of what is displayed for an SCP host:



The following is an example of what is displayed for an HTTP host:



b. Or...configure as a local disk directory; No further information is required (the path is already provided at the top of the page).

20. When you're done, click the "Add Polling Location" button at the bottom of the screen. Now you're done adding the polling location! Repeat the steps above to add more polling locations.

4.6.1.21 Data Type Configuration

Any ECS Collection is eligible for DPL Ingest. ECS collections are added via ESDT Maintenance GUI and Data Pool Maintenance GUI. These configuration screens allow DAAC users to override some assumptions about these Data Types. The default assumptions are:

- By default, granules of ECS collections are archived but not inserted into the public Data Pool upon successful ingest. The operator can change this so all granules associated with an ECS Collection are inserted into the public Data Pool as soon as they are successfully ingested. This would take the place of an unqualified subscription for Data Pool insert and is more efficient.

- By default, HDF map granules are not created for all science granules. The operator can change this so that HDF map granules for the science granules associated with an ECS collection are created and inserted into online-archive after those science granules are successfully ingested. The creation of HDF map granules are handled by a separate Map Generation Utility (MGU).
- By default, if there is a metadata validation warning for any granule during ingest, the operator will be notified via an email. This can be changed on "Data Type Configuration" page so that all metadata validation warnings will be ignored and the operator won't receive emails because of it for all granules associated with an ECS collection.
- By default, the duplicate granule detection rule for the granules of all data types is "File Collision Only". The operator can change it to another established rule for a data type (or a group of data types) on "Data Type Configuration" page. The change of duplicate detection rule is not allowed for QA/PH/Browse/HDF4 Map.

This page displays the data types whose configuration has been altered to support non-default options. To change options for these data types, check the box next to each Data Type short name you wish to modify, and set the options in the Modify Selected Data Types panel at the bottom of the list. To set non-default options for other Data Pool data types, select 'View / Configure Additional Data Types' at the top of the list and select the additional data types from the resulting list.

See Figure 4.6.1-85 for a general overview of this page. Explanations of the fields on this page may be found in Table 4.6.1-24.

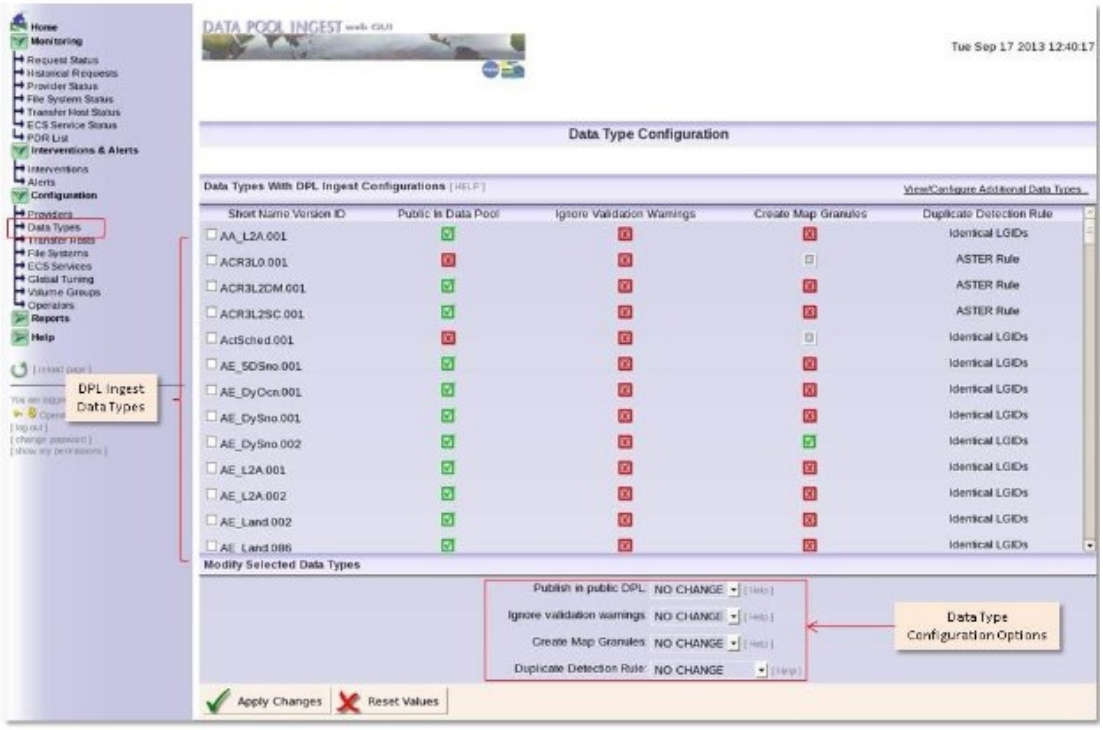


Figure 4.6.1-85. Data Type Configuration Page

Editing Data Types

To configure the attributes of any of the listed data types here, check the box next to the desired data types (multiple selections may be made) and enter the new parameters (or choose "No Change" to keep the current parameters) in the form below labeled **Modify Selected Data Types** and click on **Apply Changes**, as indicated by the red arrows in Figure 4.6.1-85.

Note: Trailing and leading white space will be removed from values entered into any text fields on this page, or any of the sub pages under it.

Table 4.6.1-24. Data Type Configuration Page Field Descriptions

Field Name	Entry	Description
Short Name.Version ID	Not Editable	The Short Name and Version Id for the collection.
Public in Data Pool	Editable	Indicates whether or not to publish data for this data type in the public Data Pool following successful Ingest.
Ignore Validation Warnings	Editable	Determines whether the operator will be notified via email if there are metadata validation warnings for a granule belonging to the given collection.
Create Map Granules	Not Editable if there is a gray X box for the data type; Editable otherwise.	Indicates whether or not HDF map granules are created for science granules of this data type.
Duplicate Detection Rules	Not Editable for QA/PH/Browse/Map; Editable for others.	Indicates the duplicate granule detection rule for this data type.

4.6.1.22 Transfer Host Configuration

This page allows the operator to manage SCP, FTP, HTTP, and Local Hosts for general use in the Data Pool Ingest system. These hosts can be referenced when defining polling locations or notification hosts.

In addition, if the host ip-addresses are referenced within PDRs as the source locations for granule files, DPL Ingest will automatically refer to their definition to obtain time out and retry parameters.

The DAAC will be able to define default time-out and retry parameters for Remote Transfer hosts, to be used if a host is referenced that has not been explicitly defined. If a request is sent through processing with a host referenced in the PDR that does not show up on the GUI as a configured host, a new host will automatically be added to the list of Remote Transfer Hosts with the name UNDEFHOST_[Provider]_[RequestID]. Default host configuration parameters will be applied to the new host until the operator chooses to modify them.

On the Transfer Host Configuration page, you can add named Remote Transfer hosts and configure them to suit their purpose. You can also edit and remove existing hosts, and change the default parameters for all Remote Transfer hosts and for the LOCAL host.

This page is shown in Figure 4.6.1-86. Explanations of the fields on this page may be found in Table 4.6.1-25 and throughout this section.

Figure 4.6.1-86. Host Configuration (General Overview)

Viewing and Configuring Host Details

To view or configure the details for a host, click on the name of the desired host. The Remote Transfer Host Detail pages are explained in Section 4.6.1.20.3.

4.6.1.22.1 Removing a Remote Transfer Host

To remove a reference to a host, check the box next to the host name; multiple selections may be made. Then click "Remove Selected Hosts" at the bottom of the list – you will be prompted for confirmation before the host is removed. See Figure 4.6.1-87.

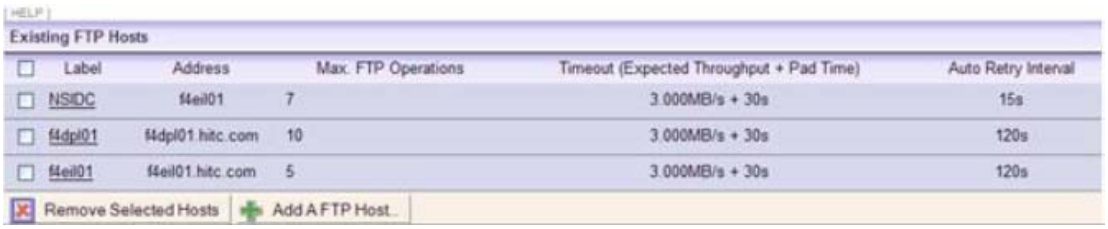


Figure 4.6.1-87. Removing a Remote Transfer Host

4.6.1.22.2 Adding a Remote Transfer Host

To add a named reference to a new host, take the following steps:

1. Click on "Add a [SCP, FTP, HTTP] Host..." at the bottom of the host list:

2. A new screen will be displayed with blank fields to add the host label (a unique name YOU give this host), IP address/DNS Name, and configuration parameters, as shown in Figure 4.6.1-88 and Figure 4.6.1-89.

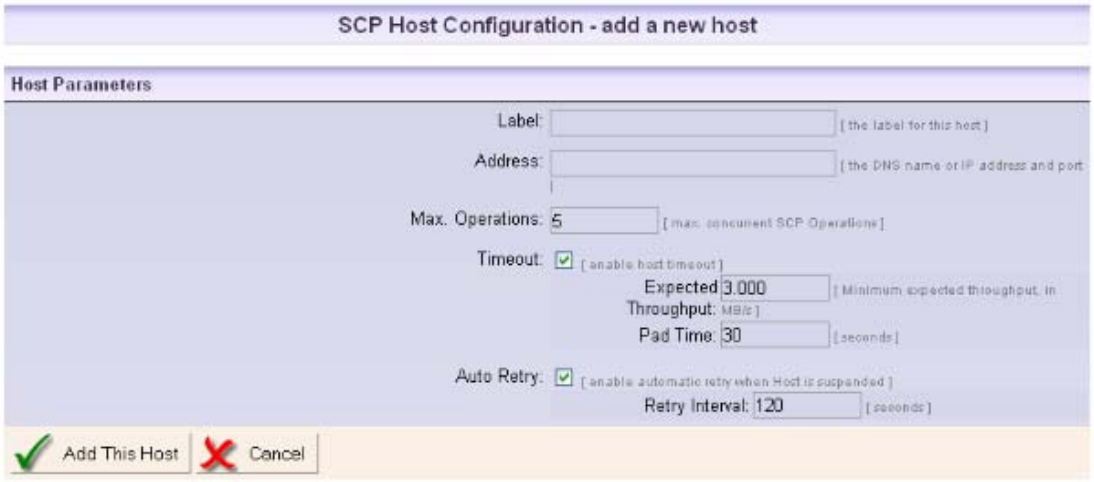


Figure 4.6.1-88. Adding a New SCP Host

Figure 4.6.1-89. Adding a New FTP Host

Figure 4.6.1-90. Adding a New HTTP Host

FTP, HTTP and SCP Hosts have similar but slightly different fields. Table 4.6.1-25 explains these fields.

Table 4.6.1-25. Add a Remote Transfer Host Page Field Descriptions (1 of 2)

Field Name	Entry	Description
Label	Required	A unique identifier for the host.
Address	Required	The IP address (e.g., 192.168.2.1:23) or DNSname (e.g., f4eil01.hitc.com:22) and port of the SCP, FTP, or HTTP host. The port is not required, but if none is supplied, the default ports of 21 for FTP and 22 for SCP will be used.

Table 4.6.1-25. Add a Remote Transfer Host Page Field Descriptions (2 of 2)

Field Name	Entry	Description
Max Operations	Required	Total number of operations that can occur simultaneously on the host. If this field is left empty a default value will be supplied.
Timeout	Optional	Whether or not to allow a host to timeout if operations of a particular size take too much time to complete.
Expected Throughput	Required if timeout is flagged	Expected amount of data in MBs of a granule to be processed during the configured pad time. If this field is left empty a default value will be supplied.
Pad Time	Required if timeout is flagged	Time (in seconds) a configured chunk of data should be processed before raising a timeout alert. If this field is left empty a default value will be supplied.
Auto Retry	Optional	Whether or not to retry an action that failed or generated an error on the host.
Retry Interval	Required if Auto Retry is flagged	Time in between retries on the host. If this field is left empty a default value will be supplied.

3. Enter a unique labelfor the host – existing labelswill be rejected.
4. Enter the I.P. (e.g., 192.168.2.1) address or the DNS name (e.g., f4eil01.hitc.com) and port number on the same line, separated by a colon. If no port is provided, the default ports of 21 for FTP and 22 for SCP will be used.
5. If you're configuring an FTP host, select active or passive mode
6. Set "Max. Operations" - the maximum number of concurrent transfer operations this host may initiate.
7. Set the timeout flag. If this box is checked, text boxes will be displayed for the Expected Throughput (in MB/s) and Pad Time values:

8. Set the Auto Retry flag. If this box checked, a textbox will be displayed to set the Retry Interval value - the number of minutes to wait between retries of this host if it becomes suspended by the server:

9. Click "Add This Host" at the bottom of the screen to add this host. It will now appear as a new entry in the Transfer Host Configuration page.

4.6.1.22.3 Remote Transfer Host Configuration Detail

To view and edit an existing Remote Transfer Host, click on the name of the desired host on the Host Configuration page. A new page will be displayed, allowing the operator to view and edit (if authorized) the parameters of the host, as shown in Figure 4.6.1-90. Explanations of the fields on this page may be found in Table 4.6.1-26.

Note: Trailing and leading white space will be removed from values entered into any text fields on this page, or any of the sub pages under it.

Figure 4.6.1-90. FTP Host Configuration Detail

Table 4.6.1-26. Remote Host Configuration Detail Field Descriptions

Field Name	Entry	Description
Label	Required	A unique identifier for the host.
Address	Required	An IP address or the canonical name and port (if needed) of a Remote Transfer host.
Max Operations	Required	Total number of operations that can occur simultaneously on the host. If this field is left empty a default value will be supplied.
Timeout	Optional	Whether or not to allow a host to timeout if operations of a particular size take too much time to complete.
Expected Throughput	Required if timeout is flagged	Expected amount of MBs of a granule to be processed during the configured pad time. If this field is left empty a default value will be supplied.
Pad Time	Required if timeout is flagged	Time a configured chunk of data should be processed before raising a timeout alert. If this field is left empty a default value will be supplied.
Auto Retry	Optional	Whether or not to retry an action that failed or generated an error on the host.
Retry Interval	Required if Auto Retry is flagged	Time in between retries on the host. If this field is left empty a default value will be supplied.

4.6.1.22.4 Local and Default Host Configuration

Local Host configuration parameters are used during any local transfer operations. The *Max. Local Operations* limits how many local copies will occur concurrently. The timeout values apply to each individual local copy operation.

Default Remote Transfer Host configuration values are used to fill in default values whenever a new Remote Transfer Host is added, or if a field is left empty when updating an existing Remote Transfer Host.

To edit local host or default Remote Transfer Host configuration, click "Edit" beneath the "Local Host Configuration" or "Default SCP/FTP/HTTP Host Configuration" sections of the Transfer Host Configuration page. See Figure 4.6.1-91.

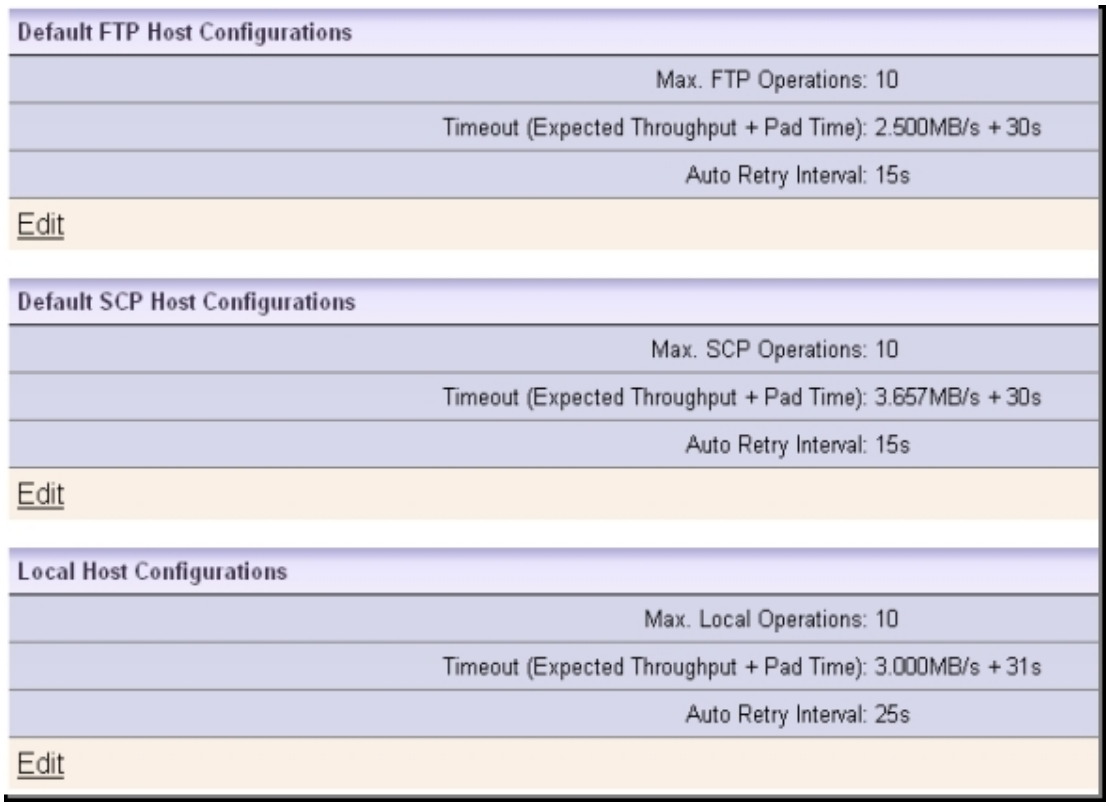


Figure 4.6.1-91. Default Remote and Local Host Configuration

A configuration page will appear exactly like the SCP/FTP/HTTP Host Configuration Detail page, except the Label will not be an editable field (as shown in Figure 4.6.1-92). Explanations of the fields on this page may be found in Table 4.6.1-26.

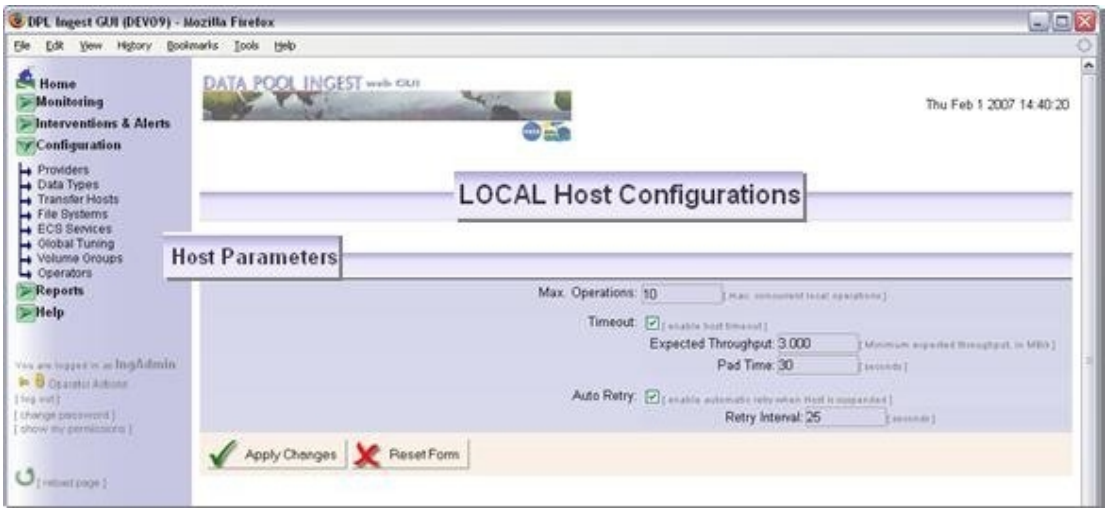


Figure 4.6.1-92. Local Host Configuration

Enter your configuration changes and then press "Apply Changes."

4.6.1.23 File System Configuration

The File System Configuration page allows the operator to configure warning and suspension thresholds for any configured Archive or Data Pool File Systems, as shown in Figures 4.6.1-93 and 4.6.1-94. This page shows both types, starting with the Archive File Systems at the top and Data Pool File Systems at the bottom. Table 4.6.1-27 contains the archive file system configuration page field descriptions and Table 4.6.1-28 contains Data Pool file systems configuration page field descriptions.

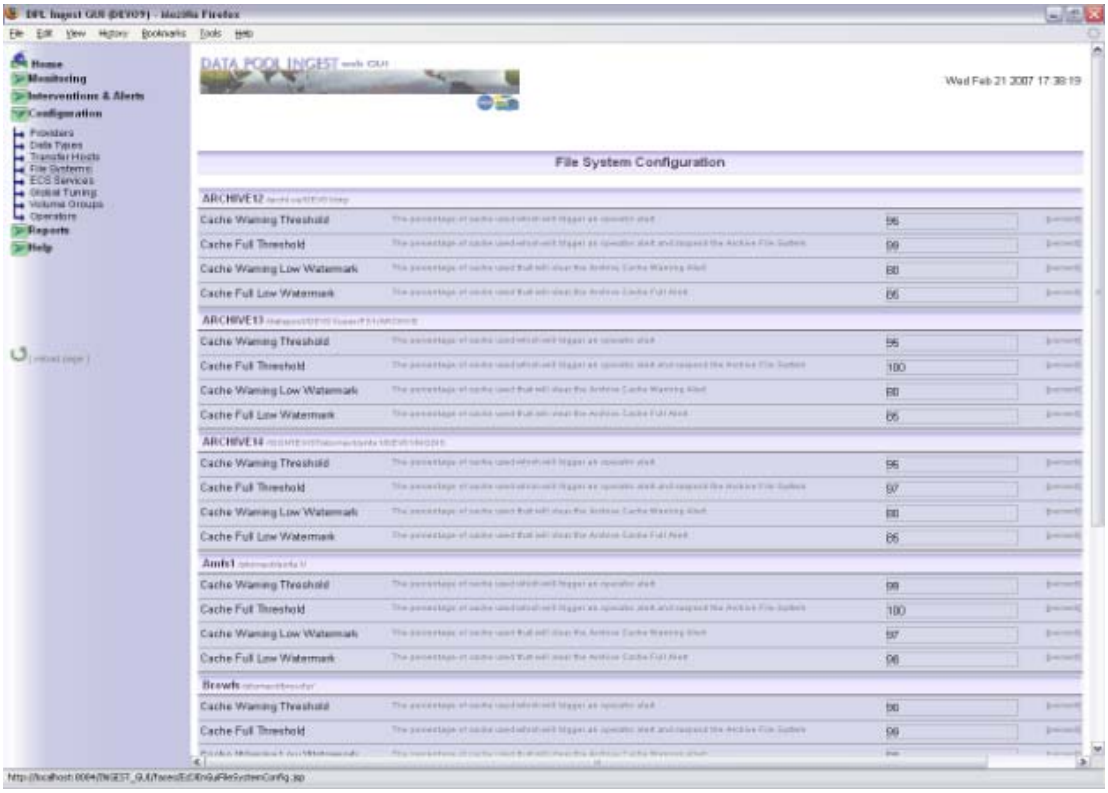


Figure 4.6.1-93. File System Configuration (Archive File Systems Only)

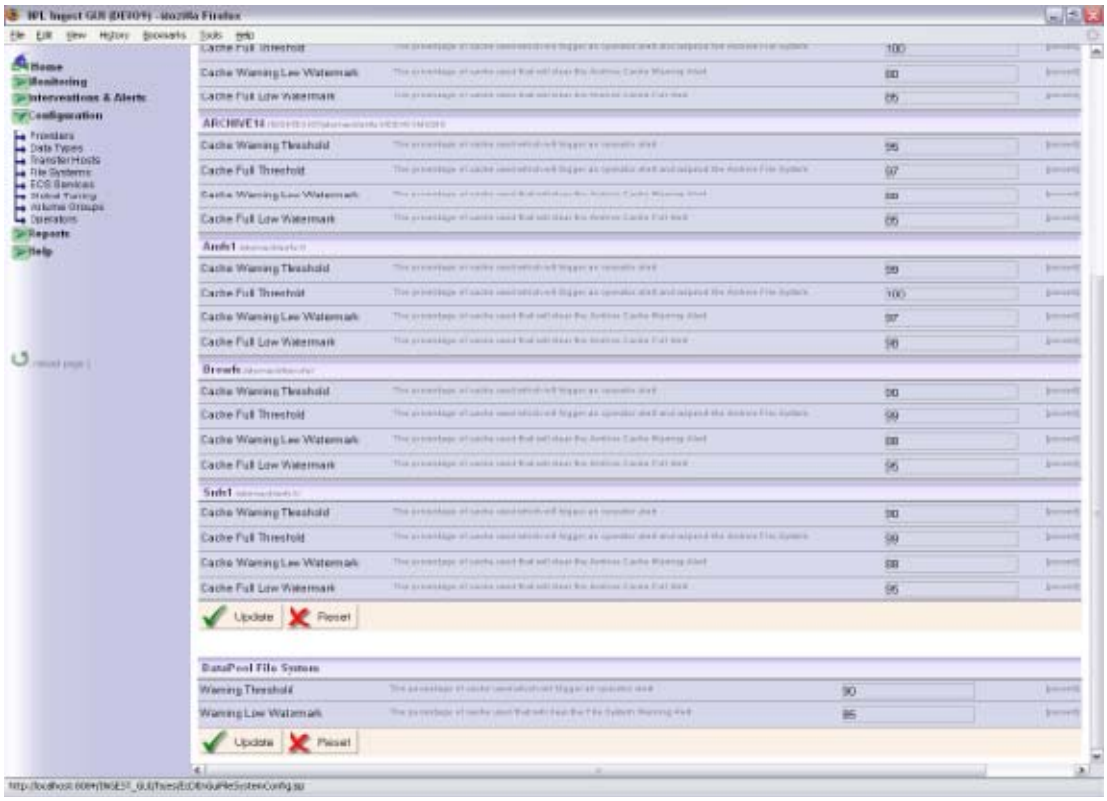


Figure 4.6.1-94. File System Configuration (DataPool File Systems at the Bottom)

Table 4.6.1-27. Archive File Systems Configuration Page Field Descriptions

Field Name	Description
Cache Warning Threshold	The percentage of cache used which will trigger an operator alert. This must be below the Cache Full Threshold and above the Cache Warning Low Watermark.
Cache Full Threshold	The percentage of cache used which will trigger an operator alert and suspend the Archive File System. This must be above the other threshold and watermarks.
Cache Warning Low Watermark	The percentage of cache used that will clear the Archive Cache Warning Alert. This must be below the Cache Warning Threshold and the Cache Full Low Watermark.
Cache Full Low Watermark	The percentage of cache used that will clear the Archive Cache Full Alert. This must be below the other watermark and thresholds.

Table 4.6.1-28. DataPool File Systems Configuration Page Field Descriptions

Field Name	Description
Warning Threshold	Warning Threshold The percentage of cache used which will trigger an operator alert.
Warning Low Watermark	The percentage of cache used that will clear the File System Warning Alert.

To modify File System parameters, enter the desired changes in the configurable fields and click "Update" – these buttons are located at the bottom of each of the DataPool and Archive File Systems sections.

4.6.1.24 ECS Service Configuration

This page (see Figure 4.6.1-95) allows the operator to configure the parameters of ECS services on a host-specific basis. A default checksum type and algorithm can also be set for use by the checksumming service hosts. Further, this page also allows the operator to select the host from which AIM will be run. This must be configured to ensure proper functionality of the DPL Ingest system.

An authorized operator can change any of the fields (they would otherwise be disabled for unauthorized or view-only operators).

Note that you cannot suspend or resume these services from this page – you must do this from the ECS Services Status Page (see Section 4.6.1.14). The initial page is a listing page only on which modifications cannot be made. The list shows which services are enabled for each host.

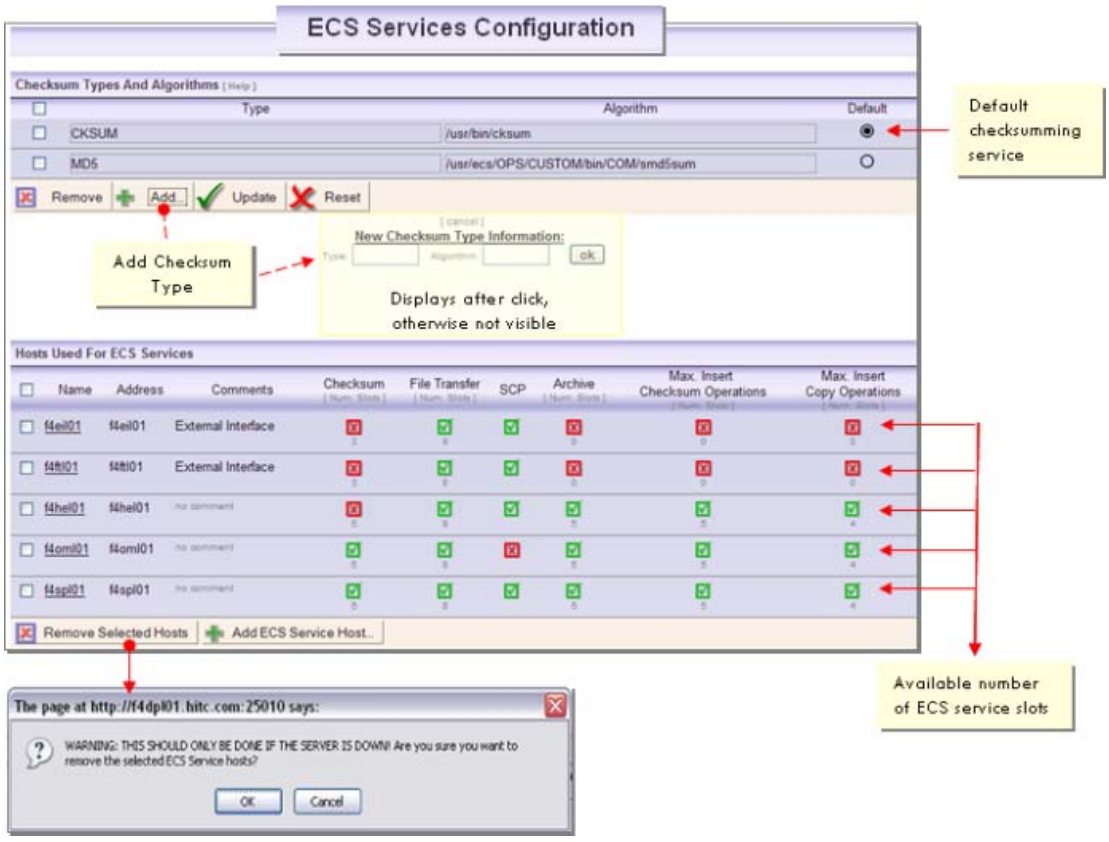


Figure 4.6.1-95. ECS Service Configuration (General Overview)

This page contains three sections:

- Checksum Type and Algorithm Configuration – *The operator can add, edit, and delete checksum types and their specific algorithms, and specify if the checksum type will be used as the default type.*
- Hosts used for ECS Services – *The operator can view, add, and edit the attributes of the ECS Service host and can configure each of the services that run on that host (see Table 4.6.1-29).*

Table 4.6.1-29. ECS Services Configuration Field Description

Field Name	Description
Name	The unique name given for this ECS Service Host.
Address	The IP address or DNS Name and port of the host.
Comments	Any descriptive comment text given for this host.
Max. Insert Checksum Operations	The maximum number of Insert Checksum Operations that will be performed by this host (checksum performed before archiving).
Max. Insert Copy Operations	The maximum Insert Copy operations that will be performed by this host.
Checksum	Each of these ECS Services are indicated by checkmark as enabled (green ☑) or disabled (red ☒) for each host. NOTE: The numbers under each of the indicators are the number of available slots for this service.
File Transfer	
Archive	
Band Extractions	
SCP	☑ 10

4.6.1.24.1 Adding an ECS Service Host

Authorized operators can add new ECS Service Hosts and configure each of their associated services from this page. To add a Service Host, do the following:

- On the ECS Services page, click "Add an ECS Service Host" at the bottom of the list:

- A new page will load with a blank form, as shown in Figure 4.6.1-96.

Table 4.6.1-30 contains the ECS services configuration field.

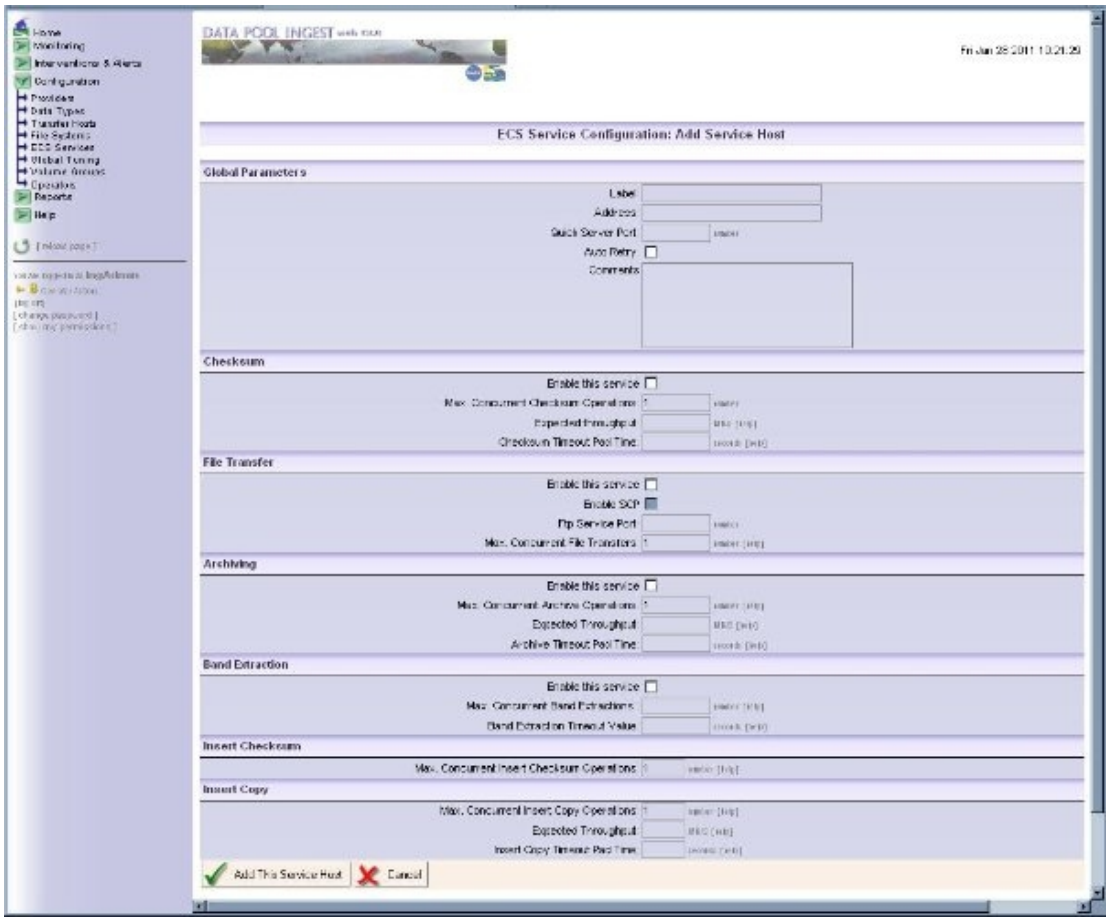


Figure 4.6.1-96. Adding a New ECS Service Host

Table 4.6.1-30. ECS Services Configuration Field Descriptions (1 of 2)

Field Name	Entry	Description
Global parameters:		
Label	Required	A unique name for the ECS Service host, preferably based on the actual host name.
Address	Required	The IP address (e.g., 127.5.2.88) or canonical name (e.g., f4eil01.hitc.com) of the host.
Quick Server Port	Required	The Quick Server port number associated with this service. Hint: the Quick Server port can be determined by looking at the Quickserver's configuration file.
Auto Retry	Optional	Whether or not to automatically retry processing of actions for all services enabled on this host.
Comment	Optional	The description of the host and its services.

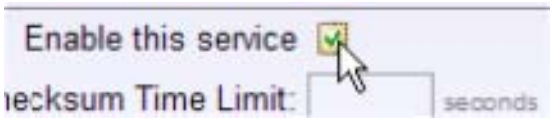
Table 4.6.1-30. ECS Services Configuration Field Descriptions (2 of 2)

Field Name	Entry	Description
Checksum:		
Enable this service	Optional	Whether or not to use this service.
Max. Concurrent Checksum Operations	Required if enabled	The maximum number of concurrent checksum operations that may be performed on this host at any one time.
Expected Throughput	Required if enabled	The expected data throughput for checksum operations. This is to identify stuck operations.
Checksum Timeout Pad Time	Required if enabled	The additional delay for a checksum operation before it is considered timed-out.
File Transfer:		
Enable this service	Optional	Whether or not to use this service.
Enable SCP	Optional	Whether or not to use SCP as the file transfer method. This will only take effect if "Enable this service" is checked.
Ftp Service Port	Required if enable	The Ftp Service port number associated with this service. Hint: the Ftp Service port can be determined by looking at the FtpService's configuration file.
Max. Concurrent File Transfers	Required if enabled	The maximum number of concurrent file transfers that may be executed on this host.
Archiving:		
Enable this service	Optional	Whether or not to use this service.
Max. Concurrent Archive Operations	Required if enabled	The maximum number of concurrent archive operations that may be executed on this host.
Expected Throughput	Required if enabled	The expected data throughput for archive operations. This is to identify stuck operations.
Archive Timeout Pad Time	Required if enabled	The additional delay for an archive operation before it is considered timed-out.
Band Extraction:		
Enable this service	Optional	Whether or not to use this service.
Max. Concurrent Band Extractions	Required if enabled	The maximum number of concurrent band extraction operations that may be executed on this host.
Band Extraction Timeout Value	Required if enabled	The number of seconds for a band extraction operation before it is considered timed-out.
Insert Checksum:		
Max. Concurrent Insert Checksum Operations:	Optional	The maximum number of concurrent Insert Checksum operations that may be executed on this host.
Insert Copy:		
Max. Concurrent Insert Copy Operations	Required	The maximum number of concurrent Insert Copy operations that may be executed on this host.
Expected Throughput	Required	The expected data throughput for Insert Copy operations. This is to identify stuck operations.
Insert Copy Timeout Pad Time	Required	The additional delay for an Insert Copy operation before it is considered timed-out.

- Under the Global Parameters section, enter the parameter values for that server:

You can also add comments here to describe the server's purpose.

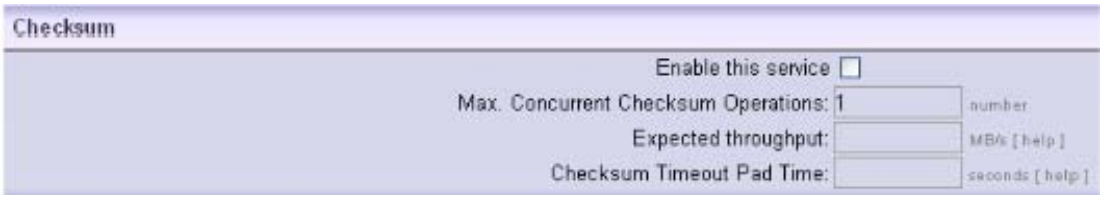
- Configure the parameters for each of the available services on this server. Some services can be enabled or disabled (e.g., Checksum and File Transfer). By default, services are *not* enabled unless you specifically enabled them by checking "Enable this service" above the parameter boxes:



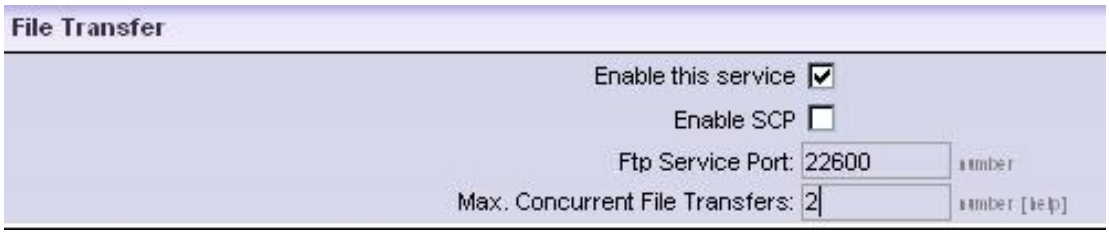
- Configure the settings for the Checksum service. Note that these are parameters for *all* types of checksum operations that run on this host. To add and configure checksum types, go to the main ECS Service Configuration page.

  Here and for all other services, there are two time-out parameters that the Ingest Service uses to determine when an operation should be considered overdue (i.e., timed-out) and cancels it. The two parameters are: (1) the expected throughput; (2) the time out pad time.

  The Ingest Service will calculate the expected time of the operation for a granule by dividing the granule size by the expected throughput, and then add the time out padding. These parameters are only used to determine when an operation should be considered hung, so both the expected throughput and the time-out padding should be chosen pessimistically to avoid canceling operations that are just slow because of concurrent heavy workload.

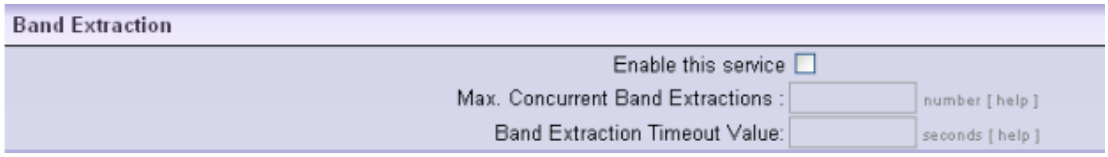


- Configure the settings for the File Transfer service. If this service is enabled, then specify the Ftp Service Port, and configure the maximum number of concurrent file transfers. The timeout parameters are configured separately for each of the FTP hosts. If you wan to enable SCP as a transfer service in addition to FTP, check "Enable SCP":

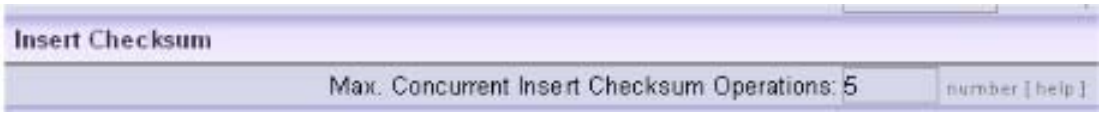


- Configure the Archive Service:

- Configure the Band Extraction Service:

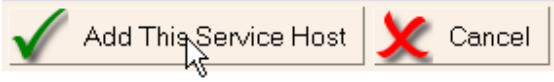


- Configure the Insert Checksum Service:



- Configure the Insert Copy Service:

- Click "Add This Service Host" at the bottom. The host will be added and the listing page will be displayed:



4.6.1.24.2 Editing an ECS Service Host

To edit an ECS Service Host and its associated services, click on the name of the host (as shown in Figure 4.6.1-97) and the detail page for that host will be displayed. This page is similar to the "Add ECS Service Host" page and contains all of the same fields. See Section 4.6.1.22 for details on how to configure an ECS Service Host.

Figure 4.6.1-97. Selecting an ECS Service Host to Edit

4.6.1.24.3 Removing an ECS Service Host

To remove an ECS Service Host, check the box next to the host name (as shown in Figure4.6.1-98) and click "Remove Selected Hosts" at the bottom of the list. A warning will pop up stating that the Server (the Processing Server) must be first shut down, as shown in Figure4.6.1-99.

Figure 4.6.1-98. Selecting an ECS Service Host for Removal

Figure 4.6.1-99. Warning for Removing ECS Service Host

4.6.1.25 Volume Group Configuration

The Volume Group configuration in the DPL Ingest GUI is meant to duplicate the functionality in the decommissioned STMGT GUI tab with some refinements and enhancements. This configuration page is shown in Figure 4.6.1-100. Table 4.6.1-31 contains the volume groups configuration page field descriptions.

4.6.1.25.1 Volume Group Configuration Page

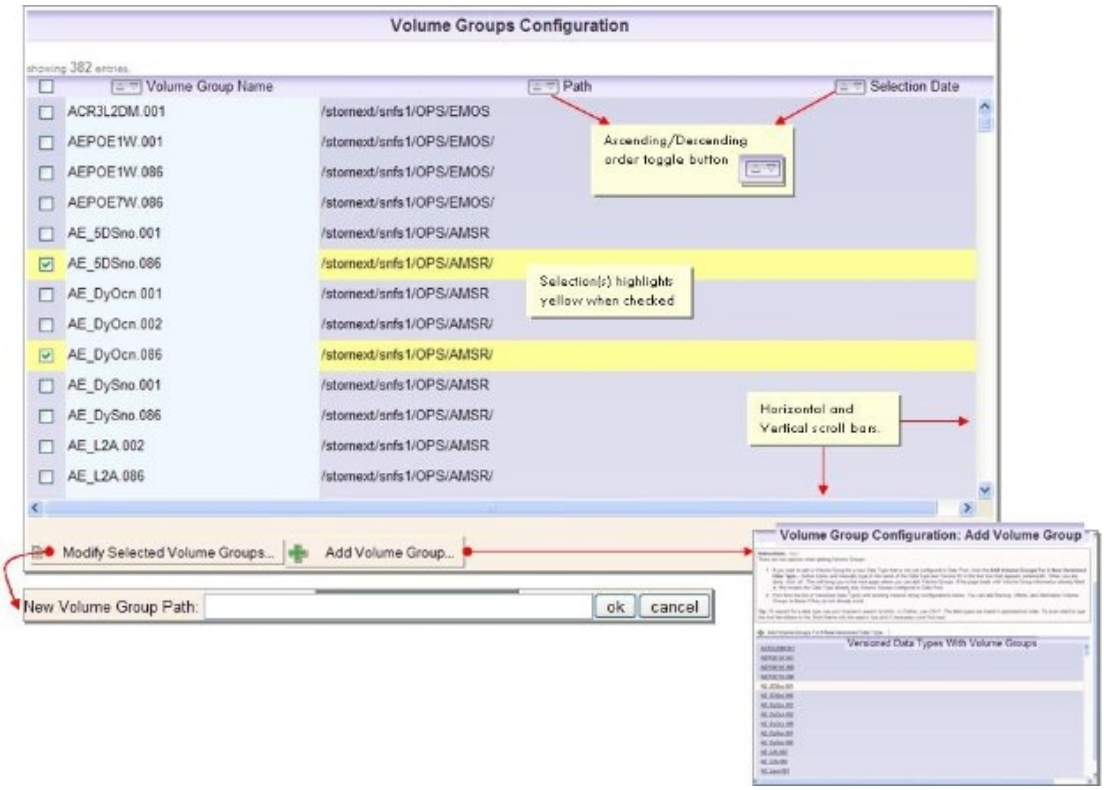


Figure 4.6.1-100. Volume Groups Configuration (Listing Page)

Table 4.6.1-31. Volume Groups Configuration Page Field Descriptions (1 of 2)

Field Name	Data Type	Size	Entry	Description
Volume Group Name	Character	255	System Generated	The name of the Volume Group based on a Data Type shortname with version identifier.
Path	Character	255	System Generated	The fully qualified Unix path to where data is stored for the specified data type.

Table 4.6.1-31. Volume Groups Configuration Page Field Descriptions (2 of 2)

Field Name	Data Type	Size	Entry	Description
Selection Date	Character	32	System Generated	A selection date (if applicable) defined for the Data Type version of which there are two volume group history sets: one defined for forward processing and the other for reprocessing data.
New Volume Group Path	Text	255	Operator	A hidden field that is displayed when the operator clicks "Modify Selected Volume Groups".

This page displays the list of currently configured volume groups. This list is displayed all on one page and not broken into chunks. By default, the entries are listed alphabetically by Data Type name. You can search for a desired data type by using the browser's built-in search function.

The bottom of the list has a buttons to add a new volume group configuration or edit multiple selections of existing volume groups. Below are more detailed screen shots that explain the features available on this page.

4.6.1.25.1.1 Column Sorting

All columns on the Volume Groups Configuration page can be sorted in ascending or descending order. To sort on a column, click on the up or down arrow at the top of the column, as shown in Figure 4.6.1-101. The sorted column will be highlighted.

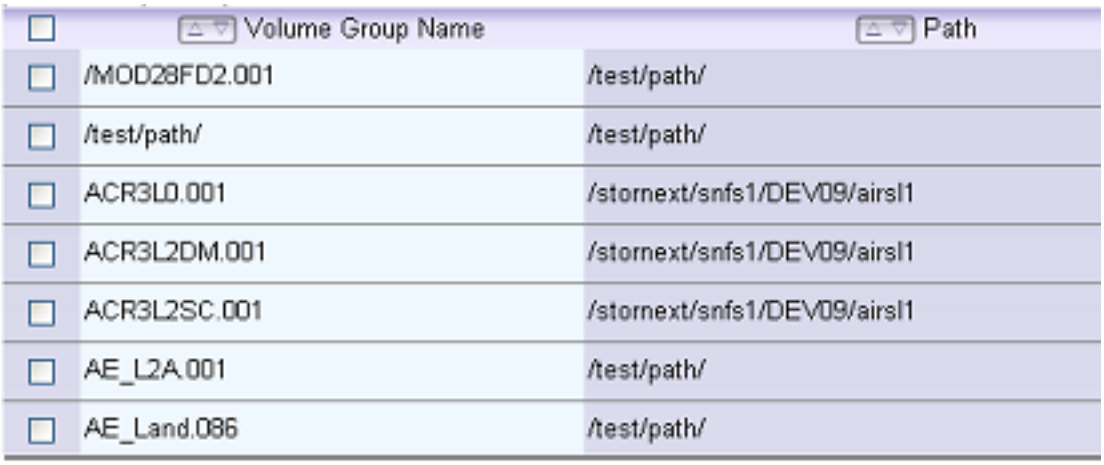


Figure 4.6.1-101. Sort-able Columns

4.6.1.25.1.2 Modifying Volume Groups

Several Volume Groups may be modified at once by checking the boxes next to each Volume Group name and then clicking "Modify Selected Volume Groups..." at the bottom of the list. The checkbox at the very top of the list allows the operator to select all of the Volume Groups on the page, as shown in Figure 4.6.1-102. Operators will not be able to modify more than one volume group at a time when there are Volume Groups selected from a Data Type version that has an alternative Volume Group History Set defined.

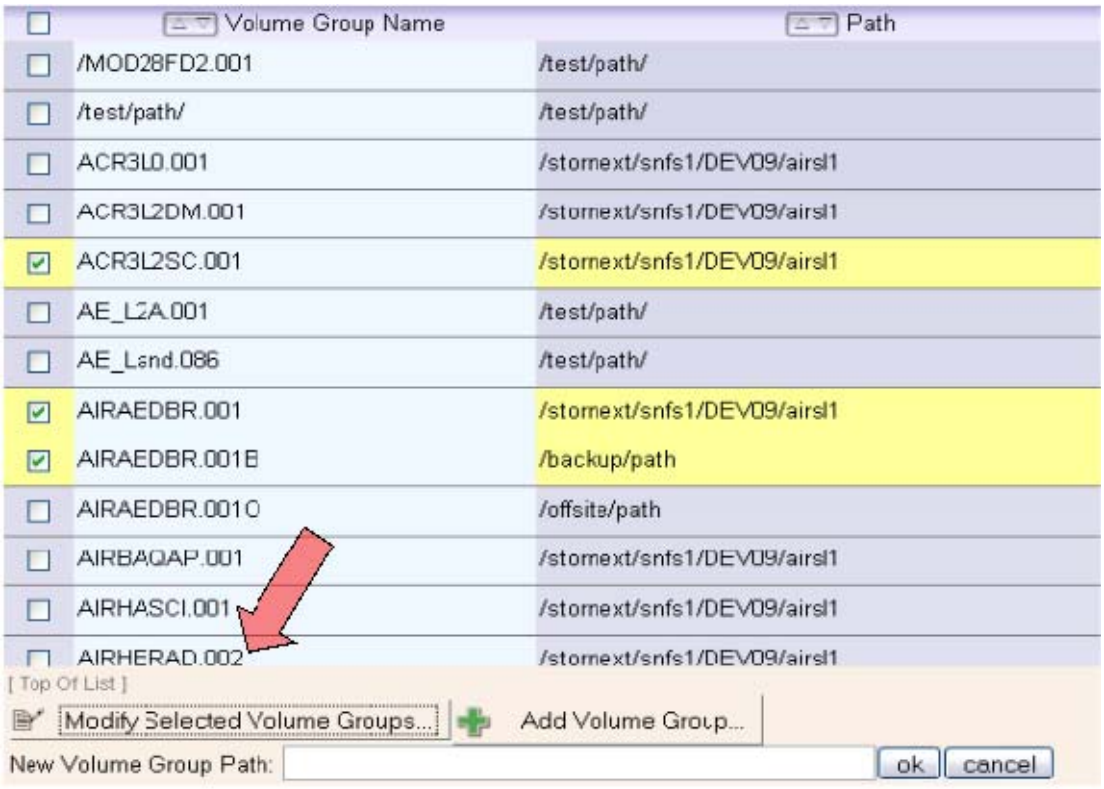


Figure 4.6.1-102. Modify Selected Volume Groups

When the desired Volume Groups are selected, they are highlighted to give a clear visual indication of which Volume Groups will be changed. When the "Modify Selected Volume Groups" button is clicked, a path input field appears below – here you can enter the new path to be applied to all selected Volume Groups. Click "ok" to apply the changes. Before any change takes place, you will be prompted for confirmation.

4.6.1.25.1.3 Adding New Volume Groups

To add a new Volume Group, click "Add Volume Group" at the bottom of the list, as shown in Figure 4.6.1-103.

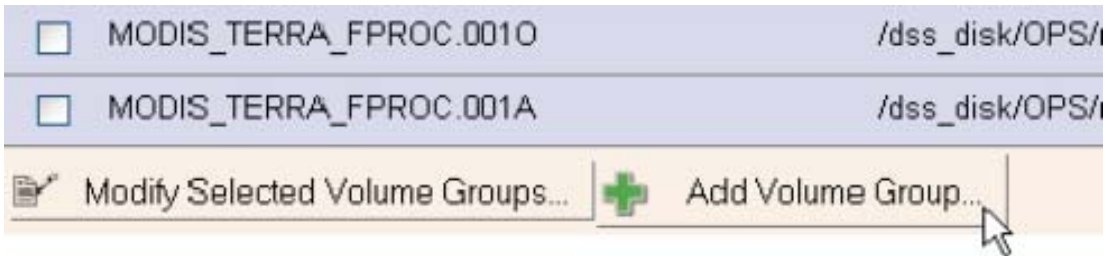


Figure 4.6.1-103. Add Volume Group Button

This will display the Add Volume Groups page.

The list of Volume Groups displayed on this page have already been entered and configured in the STMGT Database. There are two paths one can take when adding a Volume Group:

1. The operator can add volume groups, to a new a Data Type version (a Data Type version that has not already been configured)
2. The operator can add Volume Groups to an existing Data Type version (a Data Type Version that has at least one Volume Group History Set). For example, if a primary volume group exists for AST_L1B.003, the operator may add a backup Volume Group, which would create a Volume Group named AST_L1B.003B (appending a "B" to the original name). If the backup already exists, the operator would not be able to add another backup Volume Group.

See Section 4.6.1.23.1.4 for more details on how Volume Groups get named.

4.6.1.25.1.4 Volume Group Naming Conventions

When a Volume Group is added, the name will be created based on the type of Volume Group that was added. There are six types, as explained in Table 4.6.1-32. Note that "R" indicates an alternative Volume Group for reprocessing. There is no explicit suffix for forward processing.

Table 4.6.1-32. Volume Group Naming

Volume Group Type	Extension	Example
Primary	*none*	AST_L1B.003
Primary Alternative	R	AST_L1B.003R
Backup	B	AST_L1B.003B
Backup Alternative	BR	AST_L1B.003BR
Offsite	O	AST_L1B.003O
Offsite Alternative	OR	AST_L1B.003OR

4.6.1.25.2 Add Volume Group Page

The Add Volume Group page allows an authorized operator to add a volume group for a new Data Type version or to add new volume group to an existing Data Type version. See

Figure4.6.1-105. To add a Volume Group for a new Versioned Data Type, you must first type in the name of the Versioned Data Type. The sequence is as follows:

1. Click on the **Volume Groups** tab in the navigation menu
2. Click on **Add Volume Group...** at the bottom of the list
3. Follow the instructions on the next page. To add a Volume Group for a *new* Versioned Data Type, click **Add Volume Groups For A New Versioned Data Type...** at the top page, as show in Figure 4.6.1-105.
4. Manually type in the Versioned Data Type into the text box. Click ok. A new page will load (Figure 4.6.1-104), allowing you to configure the Versioned Data Type as explained below.

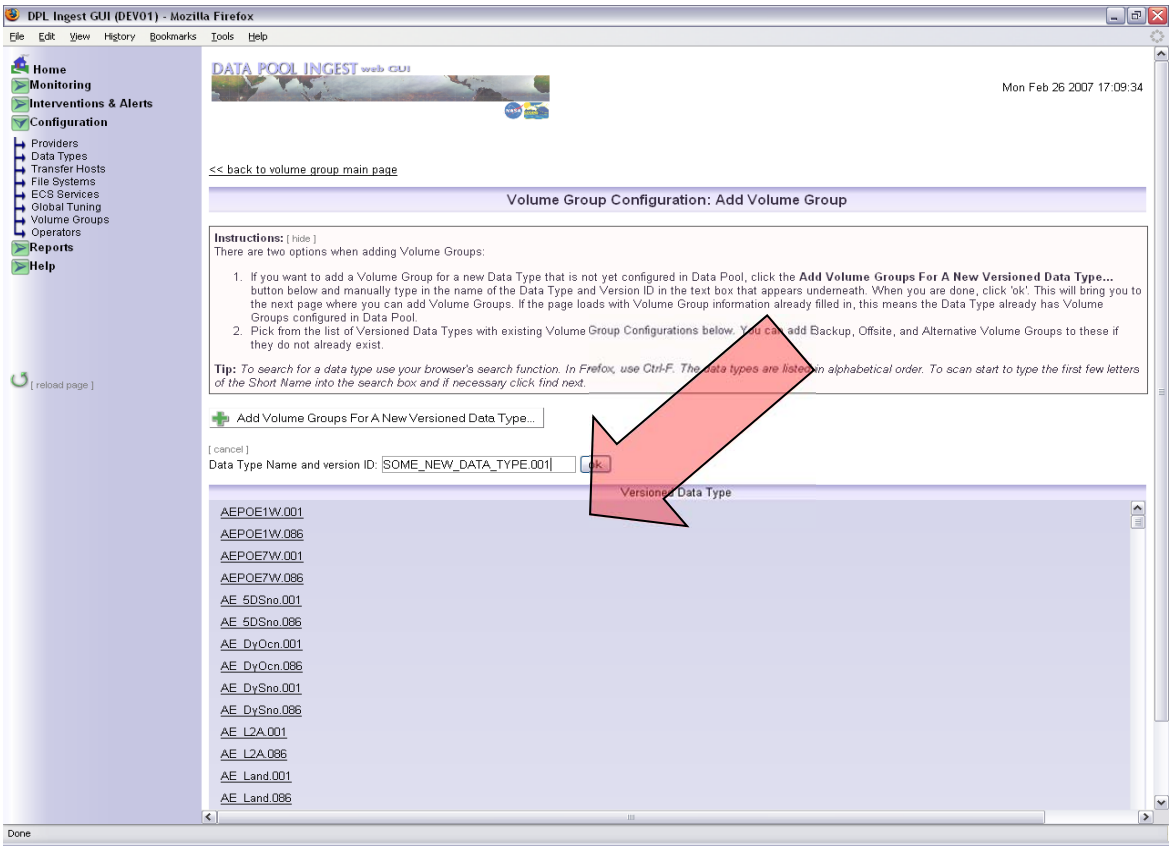


Figure 4.6.1-104. Entering a New Versioned Data Type

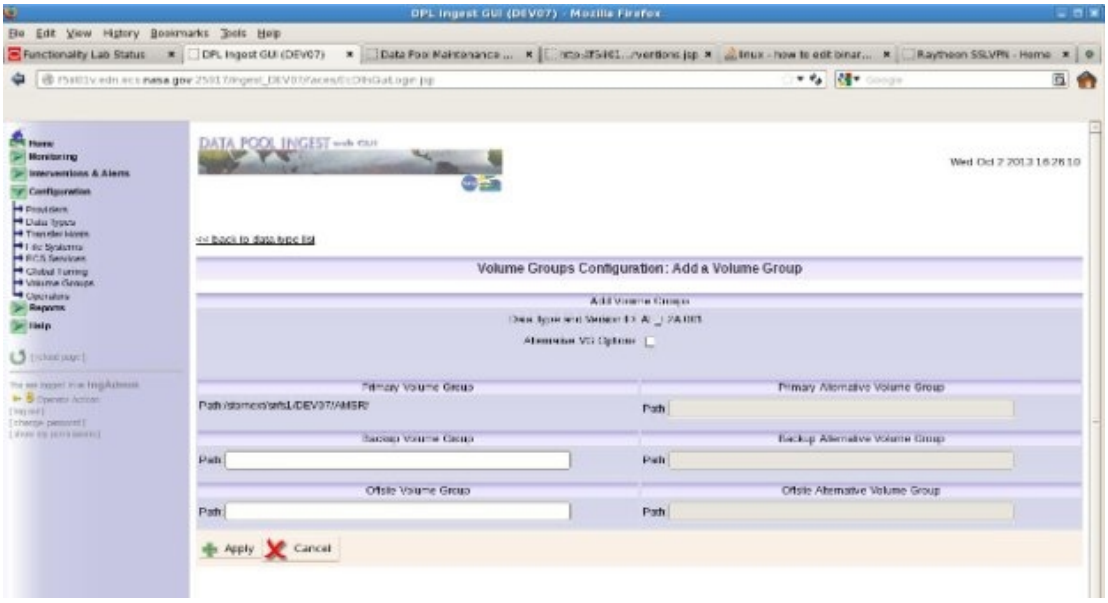


Figure 4.6.1-105. Volume Groups: Add a Volume Group Page

Adding a Volume Group for a New Data Type Version

The following rules apply when adding a volume group for a new Data Type Version:

1. The Primary path information *must* be entered.
2. The addition of Backup Volume Group, Offsite Volume Group, or Alternative Volume Group History Set, are optional and may be entered at a later time, however they can be entered all at once on this page as shown in Figure 4.6.1-106.

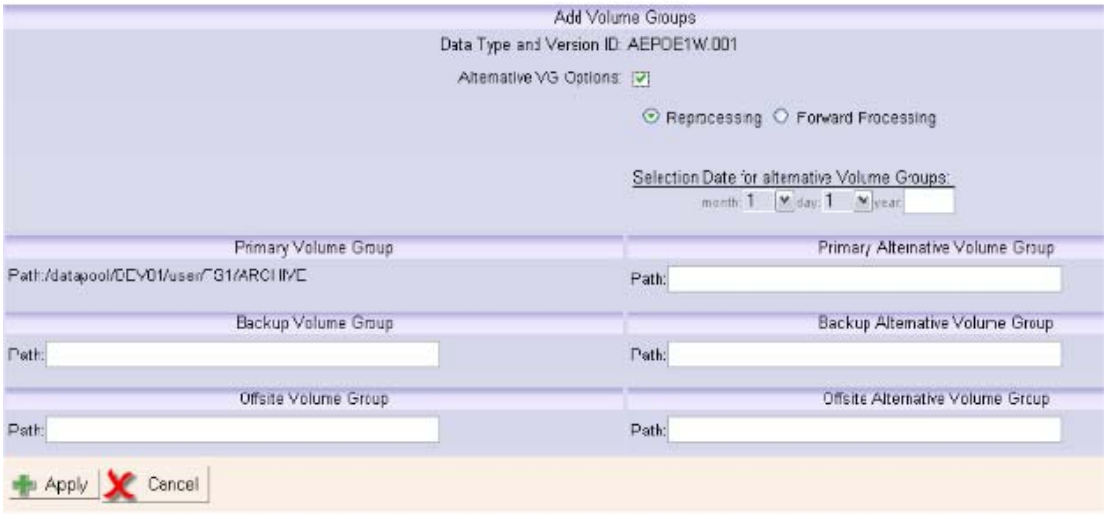


Figure 4.6.1-106. Alternative Volume Groups

Table 4.6.1-33 contains the add volume group page field descriptions.

Table 4.6.1-33. Add Volume Group Page Field Description (1 of 2)

Field Name	Entry	Description
Data Type and Version ID	Required	A Data Type short name and version identifier.
Alternative VG Options	Not Required	Allows operator to enter options for alternative Volume Groups. This can only be checked if an Alternative Volume Group was specified, otherwise, the checkbox is disabled.
Selection Date for alternative Volume Groups	Required if adding Alternative Volume Group History Set	When the alternative check box is selected, the Selection Date section is enabled and is required to be filled out by the user. Selection Date is a separate date to guide Archive Server to select an appropriate Volume Group History set for storing / retrieving data. When acquisition date is not null and less than the Selection Date, Reprocessing Volume Group history set will be used, otherwise, forward processing Volume Group history set will be used.
Reprocessing, Forward Processing	Required if adding Alternative Volume Group History Set	Alternative volume groups can be configured either for reprocessing or even for forward processing. The default is for reprocessing. Although the flexibility to add a new alternative for forward processing is supported, it should be used withcaution.
Volume Group Path (For Primary)	Required	The fully-qualified Unix path to where data is currently being stored for the specified data type to the Primary Archive.
Volume Group Path (For Backup)	Required if Backup enabled	The fully-qualified Unix path to where data is currently being stored for the specified data type to the Backup Archive.
Volume Group Path (For Offsite)	Required if Offsite enabled	The fully-qualified Unix path to where data is currently being stored for the specified data type to the Offsite Archive.
Volume Group Path (For Primary Alternative)	Required if Primary Alternative enabled	The fully-qualified Unix path to where reprocessing data is currently being stored for the specified data type to the Primary Alternative Archive.
Volume Group Path (For Backup Alternative)	Required if Backup Alternative enabled	The fully-qualified Unix path to where data is currently being stored for the specified data type to the Backup Alternative Archive.
Volume Group Path (For Offsite Alternative)	Required if Offsite Alternative enabled	The fully-qualified Unix path to where data is currently being stored for the specified data type to the Offsite Alternative Archive.

Figure 4.6.1-107 shows the List of Versioned Data Types w/ Existing Volume Group Page.

Adding a Volume Group to an existing Data Type Version

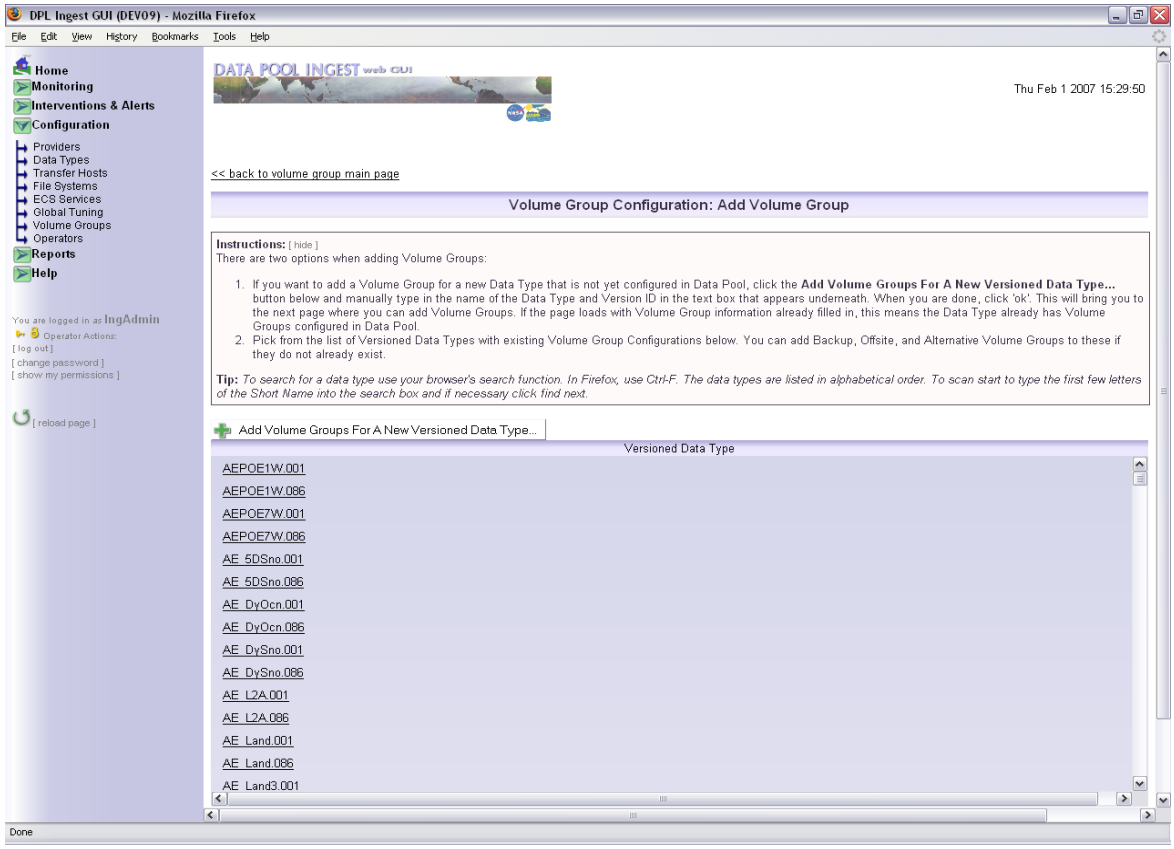


Figure 4.6.1-107. List of Versioned Data Types w/ Existing Volume Groups

The following rules apply when adding Volume Groups to an existing Data Type version (e.g., Backup, Offsite, etc.):

1. The Volume Group name will be selected from the Add Volume Group page (see Figure4.6.1-107). When the link for the desired Versioned Data Type is clicked, the Data Type is displayed at the top of the next page.
2. Any previously added Volume Group will be displayed, but will not be editable. For example, if a Backup Volume Group has already been added, the Volume Group path will be shown, but the operator will not be able to edit this path.
3. Similarly, if any Alternative Volume Groups have been specified, the Alternative VG options and Volume Groups will be displayed, but not editable.
4. If the operator is adding the Alternative Volume Group History Set for the first time, the Alternative Options must be selected and the operator may choose the processing type (Forward Processing or Reprocessing) for the Alternative Volume Group History Set, as well as a selection date to be applied to the Reprocessing Volume Groups.

Adding Volume Groups

Multiple Volume Groups for a Data Type version may be added at once on the Add Volume Group page. For each volume group you wish to specify, enter a path for that Volume Group, as show in Figure 4.6.1-108.

Figure 4.6.1-108. Adding the Primary Volume Group

4.6.1.25.3 Authorization

For DAACs that have security enabled for the DPL Ingest GUI, an operator would have to have Ingest Admin permission to add or configure volume groups as described in this document. No special permissions are needed to view current configurations or generate the Volume Groups History report page.

4.6.1.26 Global Tuning Configuration

This page allows the operator to configure the global tuning parameters in the Data Pool Ingest database. The parameters are listed along with their descriptions and a text box to change the values, as show in Figure 4.6.1-109.

There are two sections of the Global Tuning page, each editable by different permission levels. The first section, "Global Admin Tuning Parameter Configuration," is editable with Ingest Admin or Ingest Tuning privileges. The second section, "Global Tuning Parameter Configuration," requires Ingest Tuning privileges. If the logged in operator does not have permission to edit a section, the fields and buttons for that section will be disabled.

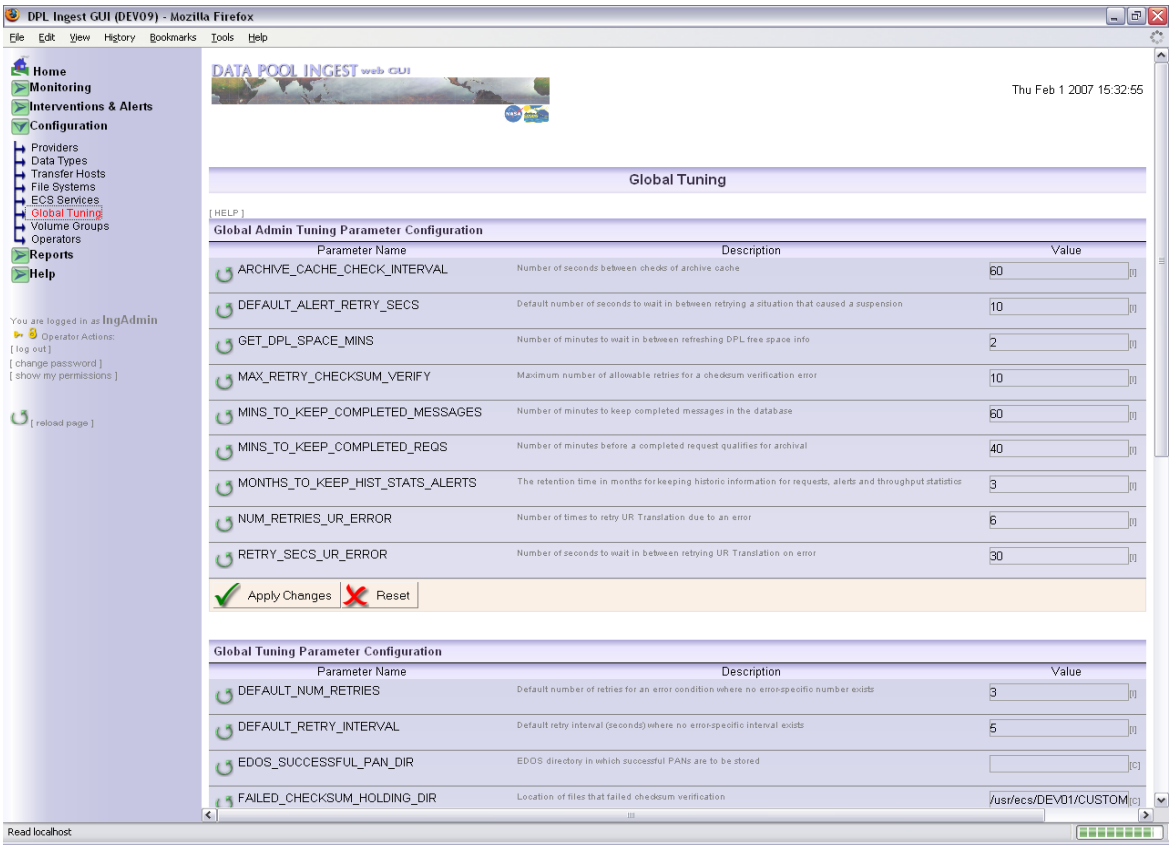


Figure 4.6.1-109. Global Tuning Configuration Page

Dynamic vs. Static Parameters

Dynamic parameters are those that are applied to the Ingest Service without having to restart it. The Ingest Service will automatically apply these parameters within 1 minute of having been set on the GUI. Static parameters are those that require the Ingest Service to be restarted before a change in the parameter value can take effect. Each parameter on this page is preceded by an icon indicating whether parameter is dynamic or static, as shown in Figure 4.6.1-110.

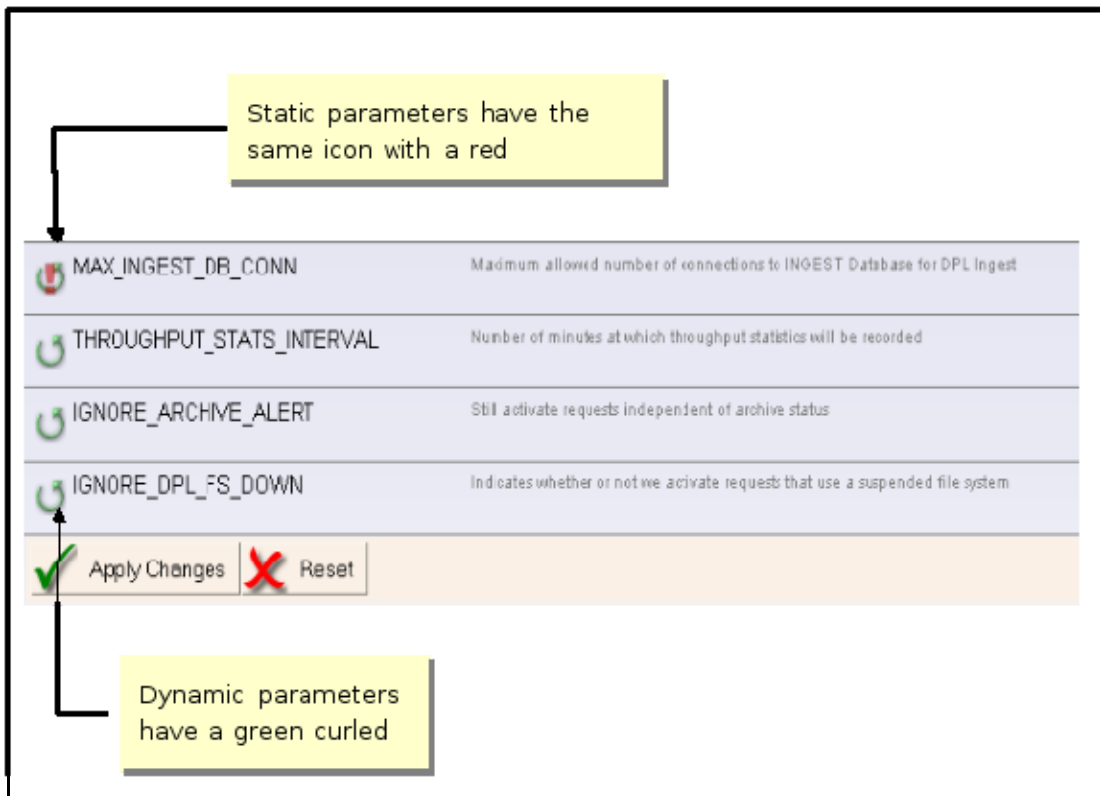
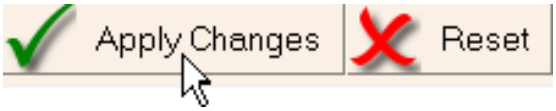


Figure 4.6.1-110. Dynamic and Static Configuration Icons

Descriptions of each parameter are displayed on the GUI and will not be included in this document.

To modify parameters, fill in the desired values in the appropriate fields and press the "Apply Changes" button.



Note: Parameters must be edited section by section. If parameters are changed in the "Global Admin Tuning Parameter Configuration" section and then the "Apply Changes" button is pressed in the "Global Tuning Parameter Configuration," modifications in the first section will be ignored.

4.6.1.27 Operator Configuration

This page consists of a list of operator names and their current permission settings and allows an Ingest Security operator to configure the authorized users for the Data Pool Ingest GUI. Here operators can be added, edited, or removed. Figure 4.6.1-111 shows the general overview of this page.

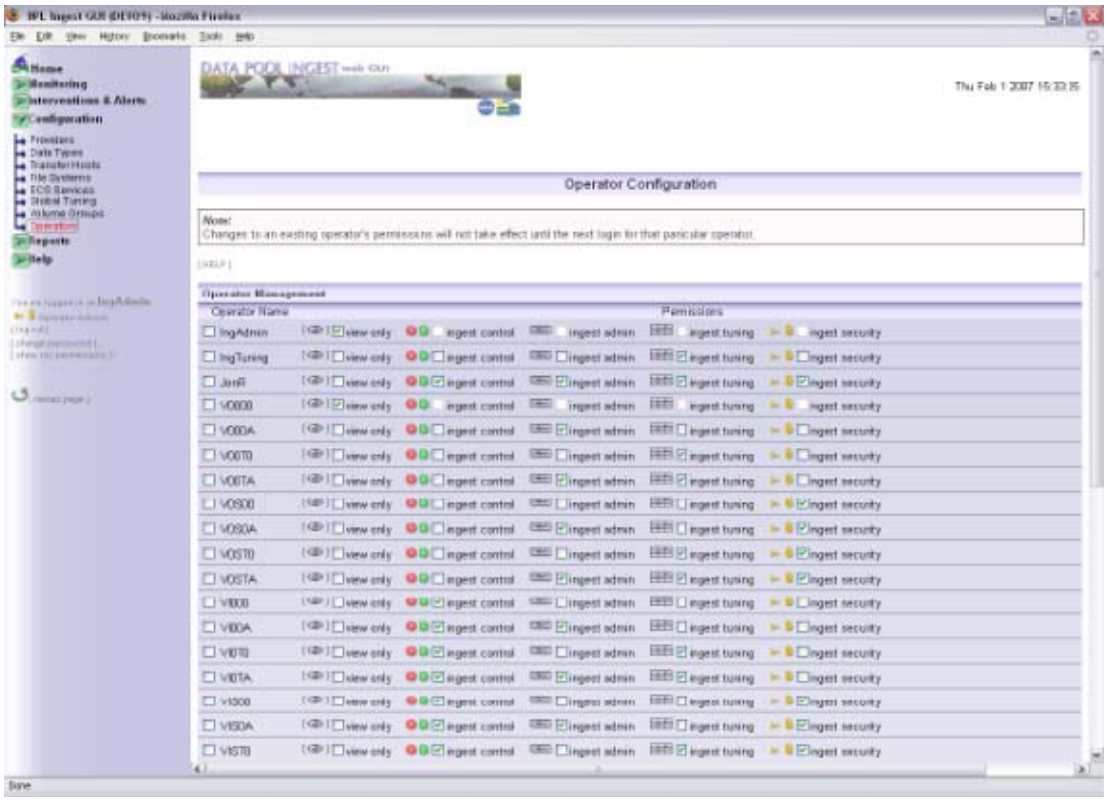


Figure 4.6.1-111. Operator Configuration Page

Permission Levels Explained

There are 5 different permission levels. View Only is a special case: if an operator is assigned the View Only permission level, it may not have any other permissions. In any other case, the other 4 levels can be combined together as they represent the ability to manage an exclusive set of properties associated with data pool ingest. For example, an operator may be assigned Ingest Control and Ingest Admin permissions simultaneously, but not View Only and Ingest Admin. See Table 4.6.1-34 for the available permission levels and their descriptions.

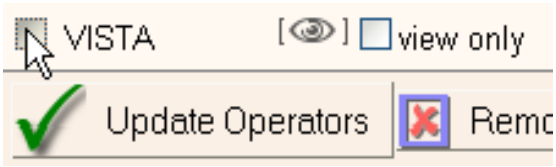
Table 4.6.1-34. Operator Permissions

Icon	Permission Level	Description
	**View Only**	The operator cannot modify any field nor take any actions on the GUI. Most buttons, textboxes, checkboxes, drop-down lists, etc. are disabled, with the exception of filters and sorts. View Only operators can also generate reports.
	**Ingest Control**	For Ingest Requests or Interventions, the operator can: Suspend, resume, cancel, or change the priority of Ingest Requests Suspend, resume, cancel, or retry Granules associated with an Ingest Request Add annotations to an Ingest Request or Intervention The operator can also suspend or resume the General Ingest Status, the Email Service, Providers, Polling Locations, File Systems, Transfer Hosts, and ECS Services, and can also clear Alerts.
	**Ingest Admin**	The operator can add, edit, and deletethe following configurable items: Providers and Polling Locations, Data Types, Transfer Hosts, File Systems, ECS Services, and Volume Groups.
	**Ingest Tuning**	The operator can modify Global and host-specific tuning configuration parameters.
	**Security Admin**	The operator can add, edit, or delete operators and change operator permissions.

4.6.1.27.1 Configuring an operator

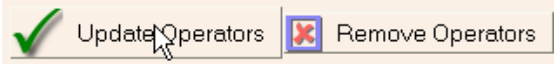
To change an operator's permission settings, do the following:

1. Next to the operator name, check the box next to the operators you would like to update.



2. Select any combination of permissions for each checked operator. Note how that when **View Only** is checked, the other permission checkboxes are automatically unchecked and disabled; this permission setting must be exclusive of the others.

3. Click the "Update Operators" button at the bottom:



4.6.1.27.2 Deleting Operators

To remove an operator from the list, do the following:

1. Select an operator by checking the box next to the operator name (more than one may be selected):

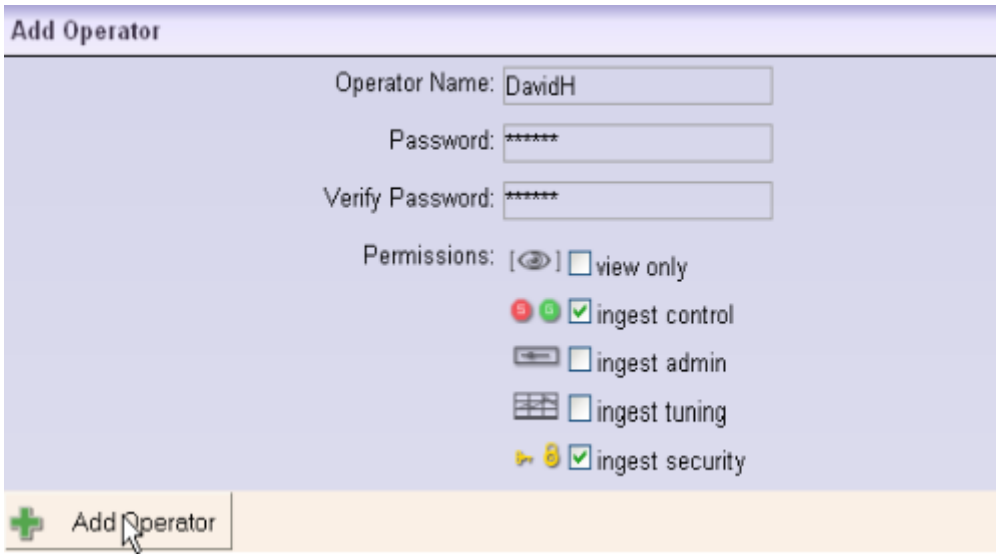
2. Click the "Remove Operators" button. You will be prompted for confirmation:

3. The page will reload, with the selected operator(s) no longer appearing on the list.

4.6.1.27.3 Adding Operators

To add an operator, do the following:

1. Under the "Add Operator" section of the page (located at the bottom of the operator list), enter in the operator name and password, and then select the desired permissions. At least one permission level must be selected.
2. Click the "Add Operator" button at the bottom of the page.



3. You will be prompted for confirmation. The page will reload with the new operator added to the list.

4.6.1.28 Reports

The reporting capability of the Ingest GUI offers the ability to view detailed reports on data providers and data types, as well as Request summary, Granule summary, and Volume Group history reports. The report pages are located under the Reports menu in the navigation pane.

4.6.1.28.1 Report Formats and Layouts

This report pages display the information across several data providers or data types. An example of the Detailed Report page is shown in Figure 4.6.1-112. As with all types of reports, the operator must select a date range (presets are provided for the last 24 and 48 hours), as well as criteria for the search. These include one or more data providers, one or more data types, and one or more final request statuses. All Data Criteria fields are optional, but at least one selection of one field must be made to generate the report.

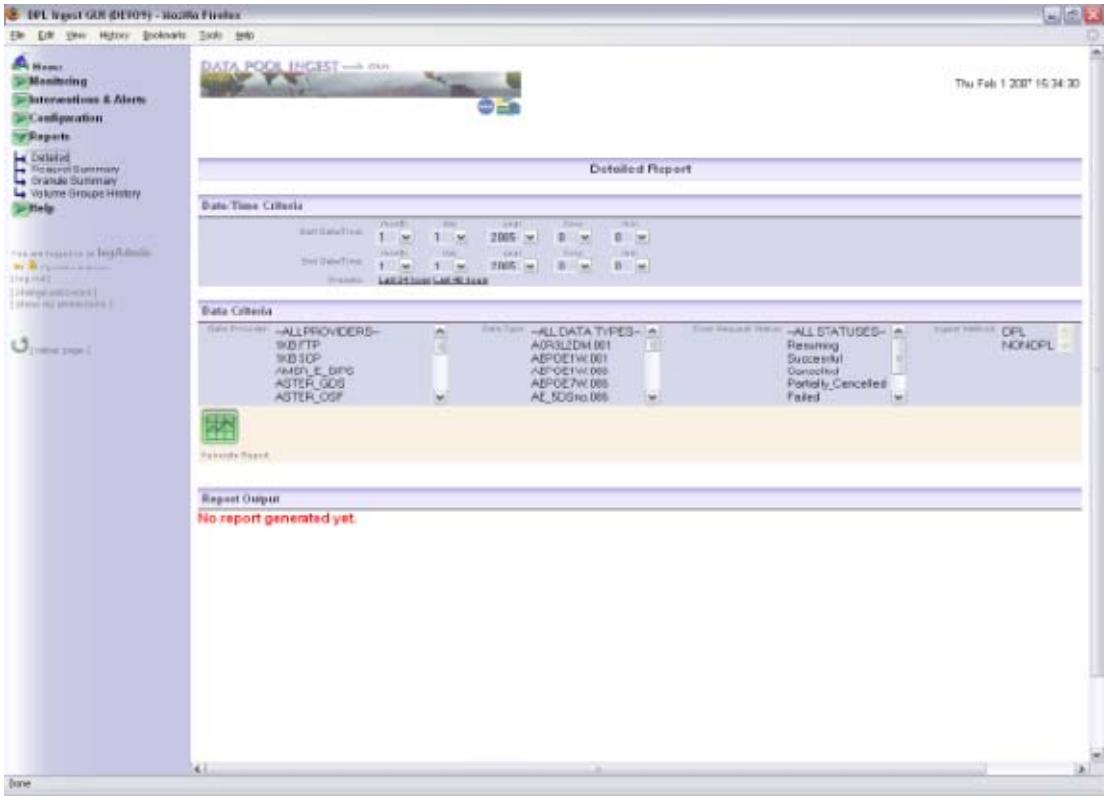


Figure 4.6.1-112. Detailed Report Page

4.6.1.28.2 Generating the report

Due to the large volume of data that may be in the database, reports can sometime take a while to process and be displayed. Immediately upon pressing the "Generate Report" button, a transitional screen is loaded with the message "Processing Your Request...", as show in Figure 4.6.1-113.

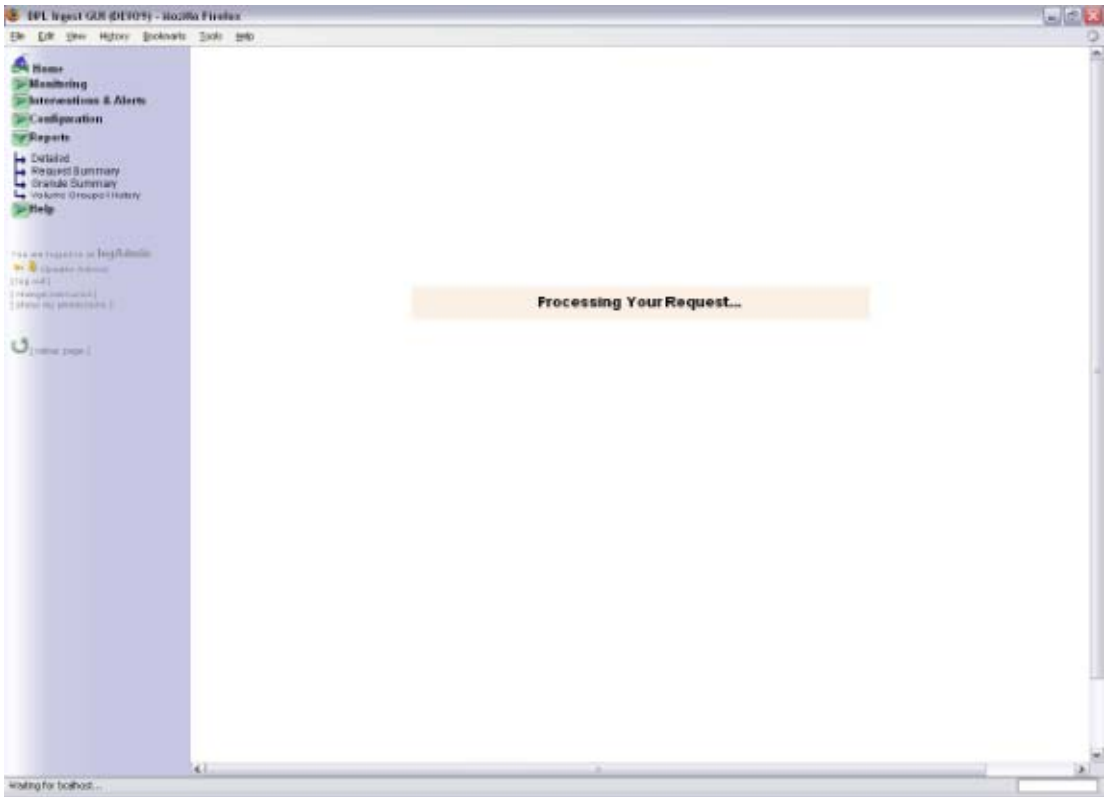


Figure 4.6.1-113. Report Page Processing a Report Request

4.6.1.28.3 Fields Generated Reports

The various report pages look similar at first glance, but they all produce different fields. The following figures (Figure 4.6.1-114, Figure 4.6.1-115, and Figure 4.6.1-116) display the headers generated for each particular report type. Some example data is also shown along with the headers.

Reports containing averages (e.g., "size avg." on the Request Summary Report) actually contain weighted averages, which is in effect an average of averages. For example, "size avg." is an average of all of the granules, weighed against the average of all the other averages for each Data Provider.

Note that the current search criteria (data and date/time) are always shown at the top of the report output.

Current Report Criteria:

Data Provider(s): [ALL] Data Type(s): [ALL]

Final Request Status: [ALL] Start Date/Time: 1/11/2006 15:18

End Date/Time: 31/10/2006 15:18

Report Output

Req.ID	Data Provider	Ingest Type	Ingest Method	Start Date/Time	End Date/Time	Tot.# grans.	# Succ. grans.	Vol (MB)	File Count	Time to xfer (mins)	Time to preproc (min)	Time to Archive (min)	Priority	Restart Flag
21307	S4P00	Polling_w/DR	DPL	2006-11-31 08:21:07	2006-11-01 08:21:19	1	1	6.311	2	0	0	0	VHIGH	
21308	S4P00	Polling_w/DR	DPL		2006-11-01 00:29:06	1		6.245	2	0	0	0	VHIGH	
21309	ASTER_GSF	Polling_w/DR	DPL	2006-11-31 10:03:09	2006-11-01 10:03:10	1		0.473	2	0	0	0	NORMAL	
21310	ASTER_GSF	Polling_w/DR	DPL	2006-11-31 10:03:09	2006-11-01 10:03:10	1		0.473	2	0	0	0	NORMAL	
21311	ASTER_GSF	Polling_w/DR	DPL	2006-11-31 10:03:09	2006-11-01 10:03:10	1		0.473	2	0	0	0	NORMAL	

Figure 4.6.1-114. Detailed Report Layout

Current Report Criteria:

Data Type(s): [ALL] Final Request Status: [ALL]

Start Date/Time: 1/11/2006 15:21 End Date/Time:31/10/2006 15:21

Report Output

Data Provider	Ingest Type	Ttl. Reqs	Ttl. Errors	Gran Avg	Gran Max	File Avg	File Max	Size Avg (MB)	Size Max (MB)	Xfer time Avg (mins)	Xfer time Max (mins)	Preproc time Avg (mins)	Preproc time Max (mins)	Archive Time Avg (mins)	Archive Time Max (mins)
ASTER_GSF		12	0	1	1	2	2	0.473	0.473	10	123	3	14	0	1
CH11_4150_2		10	0	1	1	2	2	0.473	0.473	0	1	1	2	0	0
MODAPS_TERRA_FPROC		1	0	1	1	2	2	0.473	0.473	0	0	2	2	0	0
S4P00		57	0	1	1	2	3	8.157	71.236	0	2	2	8	0	1

Figure 4.6.1-115. Request Summary Report Layout

Current Report Criteria

Data Provider(s): [ALL] Data Type(s): [ALL]

Final Request Status: [ALL] Start Date/Time: 1/11/2006 15:21

End Date/Time: 30/10/2006 15:21

Report Output

Data Provider	Ingest Type	Data Type	Ttl. Grans	Ttl. Errors	File Avg	File Max	Size Avg (MB)	Size Max (MB)	Xfer time Avg (mins)	Xfer time Max (mins)	Preproc time Avg (mins)	Preproc time Max (mins)	Archive Time Avg (mins)	Archive Time Max (mins)
ALL_ESDTS		AEPOE1W	2	0	2	2	0.046	0.046	0	1	18	27	1	3
ALL_ESDTS		AEPOE7W	2	0	2	2	0.100	0.100	0	1	11	15	1	1
ALL_ESDTS		AE_5DSno	2	0	2	2	0.100	0.100	1	2	18	21	0	0
ALL_ESDTS		AE_DyOcn	4	0	2	2	0.100	0.100	1	3	16	28	0	1
ALL_ESDTS		AE_DySno	4	0	2	2	0.100	0.100	0	1	18	29	1	4
ALL_ESDTS		AE_L2A	29	0	2	2	0.103	0.103	2	6	16	30	1	4
ALL_ESDTS		AE_Land3	4	0	2	2	0.100	0.100	2	3	11	17	0	3
ALL_ESDTS		AE_MoOcn	3	0	2	2	0.100	0.100	2	3	12	24	0	3

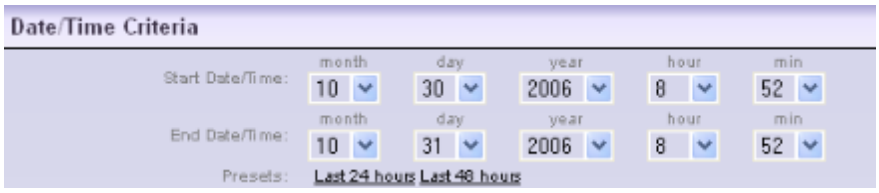
Figure 4.6.1-116. Granule Summary Report Layout

4.6.1.28.4 Generating the report

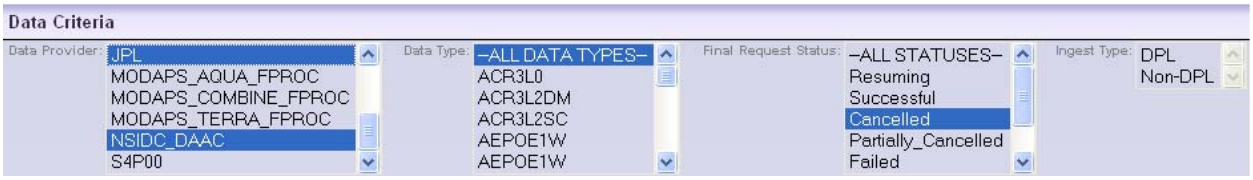
To generate a report, take the following steps:

1. Select the type of report you wish to see from the navigation panel. For this example, select Detailed, Request Summary, or Granule Summary. Volume Group History is covered in a separate section.

2. The report page will be loaded. Select the date/time range. If you leave the time fields at 0:00, it will be assumed that this will cover the entire 24-hour period:



3. Select the data criteria for the search. Several values of each criterion may be selected to narrow the search, but at least one field must selected (hold down the Ctrl key to select multiple items):



4. Click the green button to submit the query and generate the report.

5. A message will appear, alerting the operator that the system is processing the request. This may take a few seconds.
6. The report will be displayed on the bottom of the page (see Figure 4.6.1-114, Figure 4.6.1-115, and Figure 4.6.1-116 for report output examples).
7. If you want to save the report, use your browser's "Save Page As..." function to save the page in HTML format.

4.6.1.28.5 Volume Groups History Page

The Volume Groups History page displays the history of the configuration changes that have occurred to volume groups, as shown in Figure 4.6.1-117. To view the report for a particular Volume Group, select the Volume Group from the box at the top of the page and click the "retrieve" button. Once this button is clicked, the page will automatically refresh with the report

specific to that Volume Group (the page is initially blank when first loaded). Table 4.6.1-35 contains the volume groups history page field descriptions.

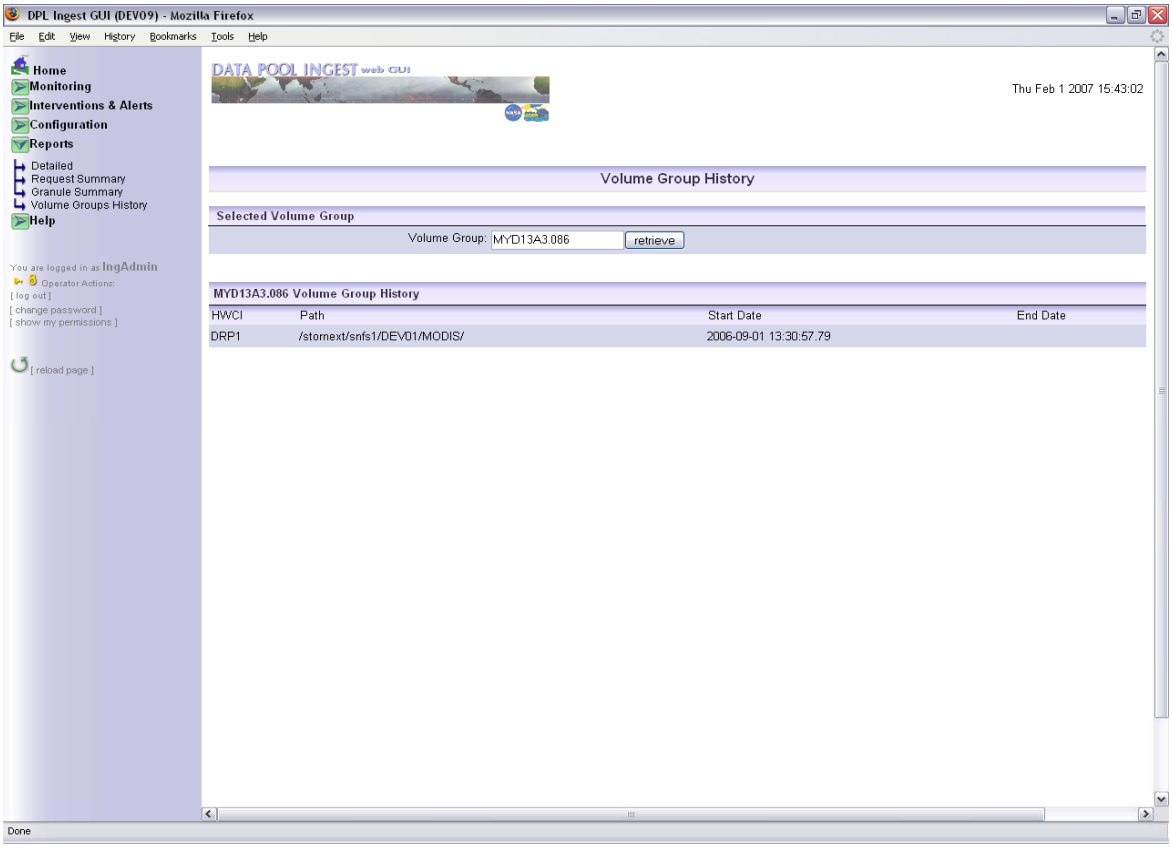


Figure 4.6.1-117. Volume Groups History

This page features a search-as-you-type input. Simply type in any characters of the Volume Group for which you want to see the history. A list of suggestions automatically pops up, and from there you may select a suitable Volume Group. Figure 4.6.1-118 shows how you can type the first three characters of a desired Volume Group and get suggestions for your search.

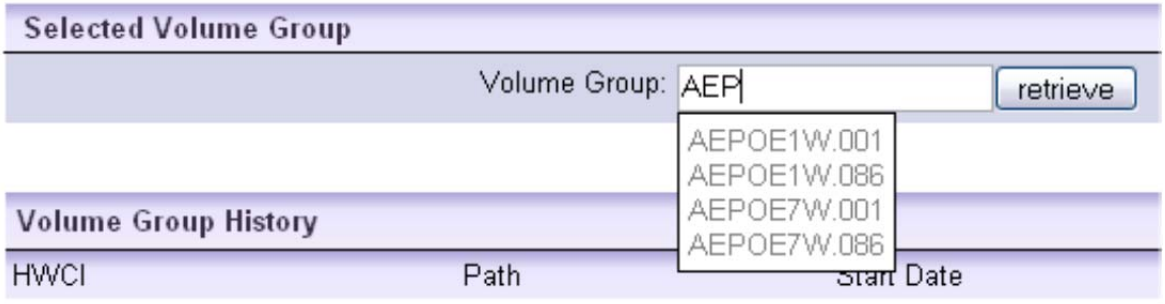


Figure 4.6.1-118. Volume Group History Page: Search-As-You-Type Input

The following figure shows how you can type any sequential characters of the Volume Group and get suggestions for your search (Figure 4.6.1-119).

Figure 4.6.1-119. Search-As-You-Type (Example 2)

Table 4.6.1-35. Volume Groups History Page Field Description

Field Name	Entry	Description
Volume Group (Data Type. Version ID + Volume Group Type Suffix)	Required	The name of the Volume Group for which the history report will be generated.
Path	System Generated	In reverse chronological order, the fully qualified Unix paths to where data has been stored for the specified data type. The current path is listed first.
HWCI	System Generated	The label of the Archive silo group instance that was responsible for storing data of the specified data type.
Start Date	System Generated	The date on which this configuration became active for the listed data type.
End Date	System Generated	The date on which this configuration was superseded by new configuration information. If blank, this row reflects the current configuration for the volume group. If any row has a blank end date, the volume group is closed, and no further data is accepted for that volume group.

4.6.1.29 Help Pages and Context Help

4.6.1.29.1 Help Pages

The last section found in the navigation bar, the "Help" section, contains information to which the operator can have ready access while operating the Data Pool Ingest GUI. Included in this section are three pages: General Topics, Context Help, and About, as shown in Figure 4.6.1-120.

Figure 4.6.1-120. Help Navigation Section

4.6.1.29.2 General Topics

This page includes an index of topics that should be useful to the operator in understanding how the GUI and Data Pool Ingest system work, and is shown in Figure 4.6.1-121. The operator can press on the name of a section from the index in order to jump to the section text.

Figure 4.6.1-121. Help - General Topics

4.6.1.29.3 Context Help

This page explains another tool provided by the operators to assist them in effectively using the Data Pool Ingest GUI. For more information about the details of this help page, see Section 4.6.1.27.5.

4.6.1.29.4 About

This page provides recommendations for software to use the GUI and a brief description of the development of the GUI.

4.6.1.29.5 Context Help

Throughout most pages on this GUI, you can get relevant, context-sensitive help by hovering your mouse (no need to click) over the **[help]** text. In many cases this is to explain the significance of a parameter or to provide instructions on what to do on the page. A blue pop-over window will appear and disappears as soon as the mouse is moved away, as shown in Figure 4.61-122, Figure 4.6.1-123, and Figure 4.6.1-124.

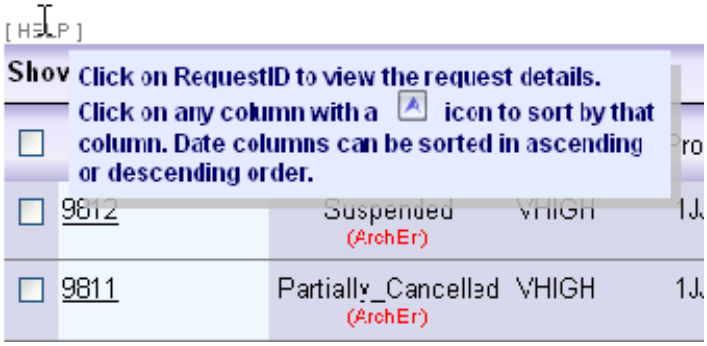


Figure 4.6.1-122. Request Detail Page - Instructions on How to View Request Details

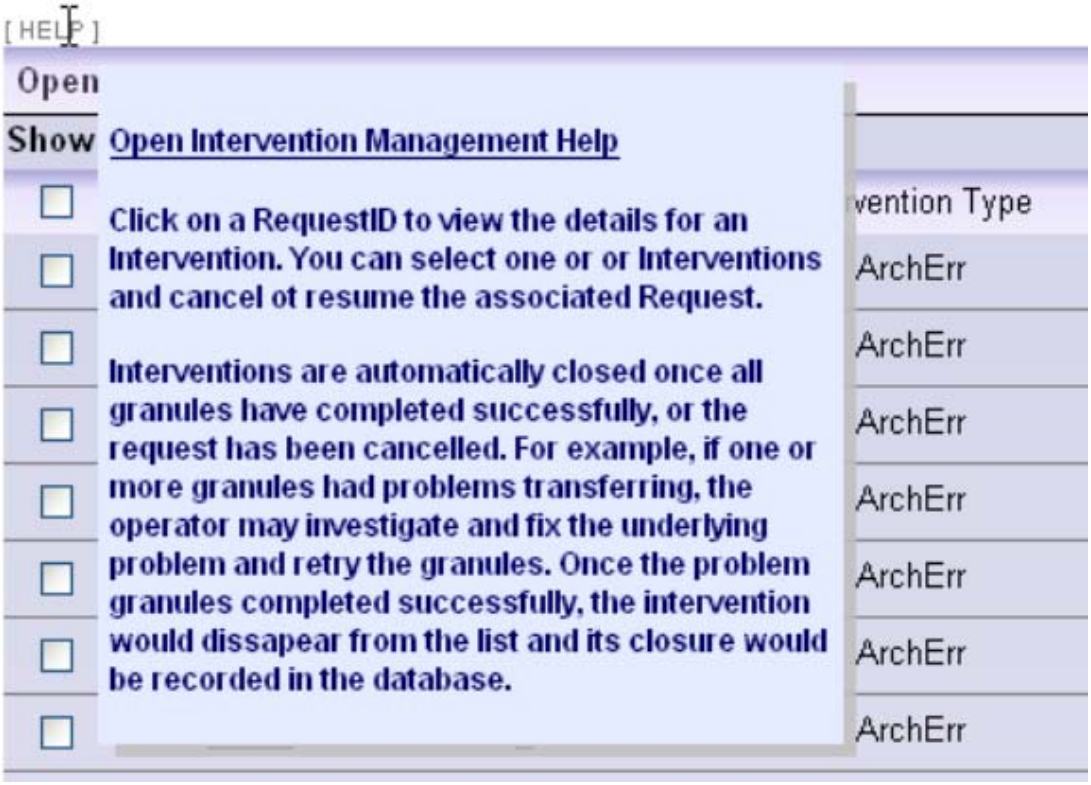


Figure 4.6.1-123. Intervention Monitoring Page - Assistance for Managing Interventions

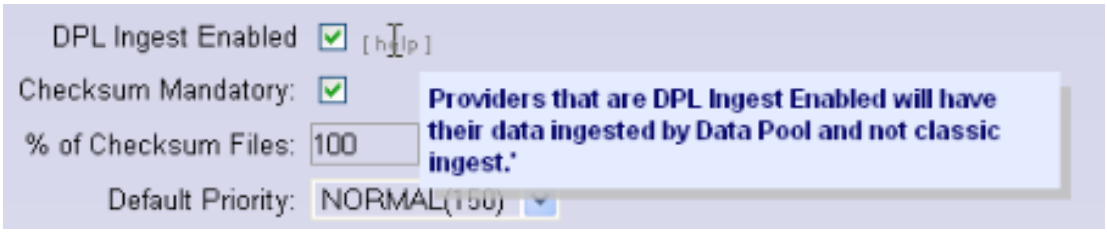


Figure 4.6.1-124. Provider Detail Configuration Page - Parameter Explanation

4.6.1.30 Browser Requirements

The specific browser requirements are stated elsewhere in this document. The recommended browsers are the only ones that should be used, as other browsers may not handle rendering and JavaScript correctly (for example, IE handles some JavaScript differently than Firefox).

JavaScript must also be enabled to run the application. In most cases, the cache size is automatically set and should be sufficient. Java is not required and need not be enabled in the browser to run the DPL Ingest GUI.

This page intentionally left blank.