PPM Solution Run Book

Standard Operating Maintenance Procedures

Document Title	PPM Clarity Standard Operations & Maintenance Procedures
Customer	Verizon Wireless
Project	Clarity Implementation
Last Saved Date	16-Apr-20
Version	1.0

Document Properties

Attribute	Value
Customer Name:	Verizon Wireless
Project Name:	Clarity Implementation
Document Name:	PPM Clarity Standard Operations & Maintenance Procedures
Document Version:	1.0
Version Date:	16-Apr-2020
Document Status:	Draft
Authors	Deborah Reece

Change History

Date	Version	Author	Description of Change
4/16/20	1.0	Deborah Reece	Initial document created

Referenced Documents

Related Project Documents
Clarity Implementation SOW
Clarity Product Documentation

Table of Contents

Glossary

Term	Definition of Terms
Availability	The backup/restore and fail-over characteristics of the Solution.
BG	Clarity Background service
Component	An instance of installable software which may contain executable(s) and/or data. The Solution Architecture Model will list the CA software, customer environment and project-developed components (if any) which are required for this Solution.
CSA	Clarity System Administrator
Physical Architecture	The structure that defines how product components are deployed to achieve the proposed Solution.
QoS	Quality of Service.
Reliability	Performance and throughput characteristics of the Solution.
Requirements	Part 1 (Sections 1 and 2) of the Detailed Design (SAS), or the Solution Requirements Specification.
SAO	Solution Architecture Overview - a work product delivered by CA Personnel for a customer to aid the production of a high level Solution design. The SAO is used to help the customer articulate requirements and project outcomes including functions, Solution Metrics, and scope. The SAO proposes an architecture, implementation, and validation approach for how CA products can help support the project outcomes. In the event of any conflict between a Project Statement of Work and a SAO, the Statement of Work takes precedence over the SAO.
Serviceability	A description of the Solution's administration and maintenance.
Solution	The proposed CA software implementation for the customer environment, which is detailed within this document.
Solution Calculator	A solution calculator is a spreadsheet which when completed by an architect will calculate work effort estimates for the implementation of CA Products in a customer environment. It contains provisions for those circumstances where there is a good SAO, an incomplete SAO or, worst case, where there is no SAO. The output from a calculator will give the most accurate project cost possible, dependent on the information available. It contains calculations for Parameters, estimation on the requirements for customization, plus required hours for the project team.
Solution Metric	A quantifiable measure of the project outcome.
Solution Metric Test	A test that helps validate that a Solution Metric has been achieved.

Term	Definition of Terms
Solution Requirement	One of the proposed functional outcomes of the solution.
Solution Run Book	Details the solution's routing maintenance procedures, key administrative functions, security and monitoring information. It also provides a troubleshooting guide for administrators and operations staff.
SOW	Statement of Work
VZW	Verizon Wireless

1 Solution Operational Environment

This document describes the various technical and functional procedures and guidelines necessary to operate and maintain the CA Clarity application at VZW.

Please refer to the Clarity r12 Installation Report document for a description of the Clarity production operational environment.

The installation reports are located at:
http://vzcentral.vzwcorp.com/sites/ITFL/Shared%20Documents/Clarity/Installation/Clarity/VerizonWireless%20-%20Clarity%20Install%20Report%20-%20Production.doc

2 Start-up and Shutdown Procedures

2.1 Start-up Procedures

2.1.1 Siteminder

1. The siteminder steps shown below only have to be performed on the user facing application instances:

    Tbleplmc01apdvg.tdc.vzwcorp.com
    Tbleplmc02apdvg.tdc.vzwcorp.com
    Tbleplmc03apdvg.tdc.vzwcorp.com
    Tbleplmc04apdvg.tdc.vzwcorp.com

2. Login to the each host and enter the following command to verify that the Apache Server is running:

    ps –ef | grep LLAWP

3. If the command returns something similar to below then the service is already running:

    /etc/httpd/conf/WebAgent.conf -APACHE22

4. If nothing like the above is returned, then you must restart the Apache service. Enter the commands below to restart Apache:

    a. **pbrun Clarity**
    b. **. ./.bash_profile (this sources the necessary environment variables)**
    c. **pbrun apachectl start (to stop the services, it is the same command but with a stop parameter)**
    d. **Enter the command below to verify that the services have started: ps –ef | grep LLAWP**

2.1.2 CA Clarity Startup

Clarity is made up of a cluster of nine (9) VMs with different services running. The table below displays which services are running on each VM.

Host	Beacon	NSA	APP	BG
tbleplmc01apdvg.tdc.vzwcorp.com	X	X	X	
tbleplmc02apdvg.tdc.vzwcorp.com	X		X	
tbleplmc03apdvg.tdc.vzwcorp.com	X		X	
tbleplmc04apdvg.tdc.vzwcorp.com	X		X	
tbleplmc05apdvg.tdc.vzwcorp.com	X		X	
tbleplcm06apdvg.tdc.vzwcorp.com	X			X
tbleplmc07apdvg.tdc.vzwcorp.com	X		X	
tbleplmc08apdvg.tdc.vzwcorp.com	X			X
tbleplmc10apdvg.tdc.vzwcorp.com	X			X

2.1.2.1 Verify Running Services

Before you start the services, enter the commands below to verify which services are already running.

1. Log into each host using the following commands:

   a. **pbrun clarity**
   b. **. ./.bash_profile**
   c. **niku status all**
   d. **Below an example of the return of the command on tbleplmc01apdvg:**
      [+] Niku Beacon [beacon] is stopped (PID:14378)
      [+] Niku Server [app] is stopped (PID:12304)
      [+] Niku System Admin Server [nsa] is stopped (PID:8063)

2. If a service is missing according to the table above, you will need to add and deploy the service using the following command:

   niku add deploy XYZ **(Replace XYZ with *app, bg, beacon, or nsa,* depending on which services is missing)**

3. Enter the following command to verify the services you need to view:

   niku status

4. Once all services are deployed, start them by entering the command:

   niku start all

5. Click the following URLs to verify that both Clarity and Siteminder are up:
   - http://tbleplmc01apdvg.tdc.vzwcorp.com/niku/app
   - http://tbleplmc02apdvg.tdc.vzwcorp.com/niku/app
   - http://tbleplmc03apdvg.tdc.vzwcorp.com/niku/app
   - http://tbleplmc04apdvg.tdc.vzwcorp.com/niku/app
   - http://tbleplmc05apdvg.tdc.vzwcorp.com:8080 (*to confirm that you can get to the login screen*)
   - http://tbleplmc07apdvg.tdc.vzwcorp.com:8080 (*to confirm that you can get to the login screen*)
   - http://clarity.tdc.vzwcorp.com
   - http://clarity-int.tdc.vzwcorp.com

2.1.2.2 Instances of Business Objects

Production Clarity has two instances of Business Objects (BO), as shown below.

1. One BO is a three (3) VM cluster:

   - **Tbleplmc11apdvg.tdc.vzwcorp.com**
   - **Tbleplmc12apdvg.tdc.vzwcorp.com**
   - **Tbleplmc13apdvg.tdc.vzwcorp.com**

2. The other BO is a ine (1) VM standalone, failover instance of BO found on:

   - **tbleplmc09apdvg.tdc.vzwcorp.com**

2.1.2.2.1 Starting Business Objects

1. Start Business Objects by entering the following commands on all four (4) BO hosts:
   a. **pbrun clarity**
   b. **. ./.bash_profile**
   c. **cd /ap_clarity_d01/SC/CommonReporting3/bobje**
   d. **./tomcatstartup.sh**
   e. **./startservers**
2. Verify that Business Objects is running by ensuring that you can get to the login screen for both the CMC and the InfoView for EACH instance using the following URLs:
   - http://tbleplmc11apdvg.tdc.vzwcorp.com:8080/CmcApp
   - http://tbleplmc09apdvg.tdc.vzwcorp.com:8080/CmcApp
   - http://tbleplmc11apdvg.tdc.vzwcorp.com:8080/InfoViewApp
   - http://tbleplmc09apdvg.tdc.vzwcorp.com:8080/InfoViewApp

2.2 Shutdown Procedures

Refer to the "***CA Clarity Administration Guide***" for more details.

3 Backup Requirements

3.1 Backup Schedules

3.1.1 Online Backups

The term online backup relates to backing up the Clarity Database (\niku, \bea folders) and Document filestore (\niku\clarity\searchindex and \niku\clarity\filestore) after hours and eventual storage of that backup on tape. The system is still active although data processing is reduced. This form of backup is not as thorough as an offline backup as data is still being processed by Clarity, and can result in certain information not being recorded during the backup process. The VZW data center has provided the listed documented processes relating to online backups.

3.1.2 Offline Backups

Offline backups are copies of the database (`\niku\clarity`, `\bea folders`) and document filestore (`\niku\clarity\searchindex` and `\niku\clarity\filestore`) performed when the application is stopped. An offline backup validates that the system database, the clarity folder and the filestore are a complete copy without any services running.

CA recommends that an offline backup be performed at least once a month. This form of backup is best as the services are static. An offline backup should be used for any troubleshooting or support activities when the vendor requires a copy of the database to try to duplicate an incident. The VZW data center has provided the listed documented processes relating to offline backups.

3.2 Storage Location

The VZW data center has provided the listed documented processes relating to storage.

3.3 Rotation for Backup Media

The VZW data center has provided the listed documented processes relating to backup media.

3.4 Log File Archive/Backup

The VZW data center has provided the listed documented processes relating to database transactional logs.

3.5 Restore Procedures

The VZW data center has provided the listed documented processes relating to database restore procedures.

3.5.1 Best Practices

- `CHARSETS` should be UTF-8 when exporting and importing. Using the wrong ones can convert your data in an undesirable manner. The best situation is when source and destination database have the same character sets, so that character conversion can be avoided.
- This behavior can be controlled by setting the `NLS_LANG` environment variable appropriately. When not set properly, "*Exporting questionable statistics*" messages may appear.
- After exporting, it is advisable to check the dump by importing with the parameter "`SHOW=Y`". This checks the validity of the dump file.

3.5.2 Other Considerations

- The Oracle client (where you are running `exp/imp`) may need to be patched to the same level as the Oracle server to prevent errors.
- When importing large amounts of data, consider dropping indexes prior to the import to speed up the process then re-creating them once the import is completed.
- The amount of archive-logs that may be created on a large import may fill up the disk.
- On `INSERT` triggers will fire: consider whether these need to be disabled.
- Increasing the `RECORDLENGTH` (max 65535) parameter can improve the length of time to perform an import/export as well as "`DIRECT=Y`" for export.

4 Risk Mitigation

4.1 Escalation Procedures

Assuming an issue has already been opened with CA Support, follow the steps below to escalate the issue to a CA Support Delivery Manager:

1. Log on to CA Support's web site at https://support.ca.com.
2. Select the case from **My Open Cases** on the home page.
3. Click **Change Priority**.
4. From the drop-down, select a higher priority value.
5. Describe the reason for the higher priority in the **Describe reason for change of priority** text box.
6. Click **Save**.

4.2 Fail-Over/High Availability

VZW has not configured Clarity as a high availability application.

4.3 Disaster Recovery/Business Continuity

The VZW data center has provided the listed documented processes relating to disaster recovery and business continuity.

5 Monitoring and Reporting

5.1 Processes

Inspect and verify that the following Clarity processes are running:

- `Niku System Administrator (nsa)`
- `Niku Application Server Service (app)`
- `Niku Background Service (bg)`
- `Niku service reports`

5.2 Log Management

5.2.1 System Logs

The following logs should be monitored daily and parsed for errors:

- `bg-niku.log`
- `bg-system.log`
- `admin.log`
- `nsa-niku.log`
- `nspider-niku.log`
- `beacon.log`

5.2.2 Application Logs

The following logs should be monitored daily and parsed for errors:

- `app-niku.log`
- `app-access*.log`
- `app-system.log`

5.2.3 Database Logs

The VZW DBA team is responsible for all matters related to monitoring database logs.

5.3 Ports

The VZW data center has provided the listed documented processes relating to monitoring ports.

5.4 Reporting

5.4.1 Report Types

Technical reporting is available using the Clarity system logs detailed above or from standard Oracle reporting utilities.

5.4.2 Frequency

System logs are generated automatically. They are available to the Clarity Application Owner via the Clarity NSA utility.

5.4.3 Distrbution

Distribution of all system reports will be at the discretion of the Clarity Application Owner.

> ***Note:*** *The Clarity Application Owner is* ***`$$Application Owner$$`*** *and is responsible and accountable for reviewing the logs.*

6 Security Controls

6.1 Securing the Solution

Access to Clarity is controlled by userid and password. Clarity Administrators are able to set password policies in the **Application Administration** pages, under **System Options**.

6.2 Security Monitoring

Security monitoring will be performed in accordance with established VZW policies and procedures.

6.3 Security Violation Reporting

Security violations will be reported following established VZW policies and procedures.

7 Troubleshooting Guide

7.1 Product Documentation Available

Please refer to the CA Clarity Administration Guide.

7.2 Solution On-Line Self-Help

Clarity users can click on the Help icon in the upper-right corner of each page to access Clarity self-help.

7.3 Product Customer Support

To open an issue with CA Clarity Support, log in to the web site at https://support.ca.com.

7.4 Internal Support Procedures

VZW internal support procedures will be followed for issue documentation and resolution.

7.5 Common Troubleshooting and Actions

1. Check the logs listed in "***Section 5.2 Log Management***" above for errors.
2. If a user can't access data they should be able to view, check their access rights.
3. Run a SQL Trace on a userid whose actions are resulting in an error.
4. If a Clarity process stops working for no apparent reason, try recreating the process from scratch.
5. If projects that are newly created from templates have the wrong attribute values, check the values in the templates.

7.6 Handling Incidents

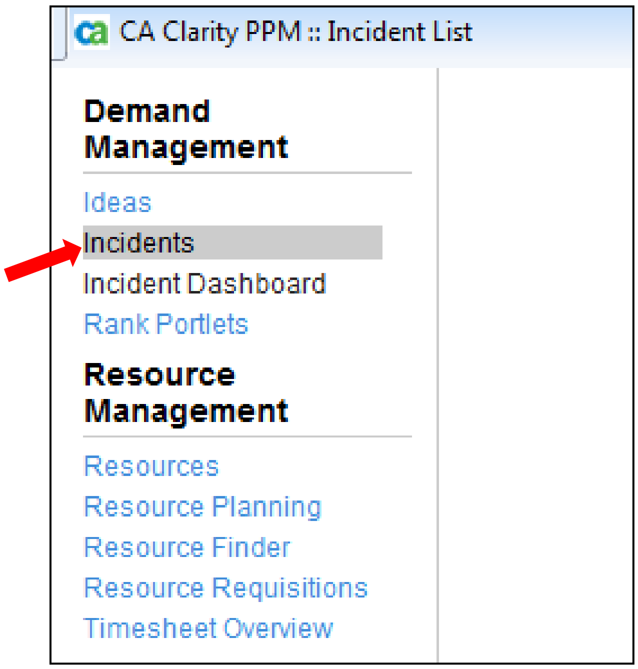
The **Demand Management** menu functions in Clarity can be used to assess costs incurred due to unplanned work and view resource utilization. The definition of an incident is any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to or a reduction in the quality of that service. Incidents can include hardware or software, but may also include service requests.

The **Incidents List** portlet displays all outstanding incidents. The **Incident Dashboard** portlets allows you to prioritize and manage all unplanned work on a daily basis, which may include troubleshooting any outstanding incidents that have been reported and require resolution. Incidents also may include requests for enhancements to run applications, assets, projects, products, services, support activities, and other investments. Functional Maintenance Procedures

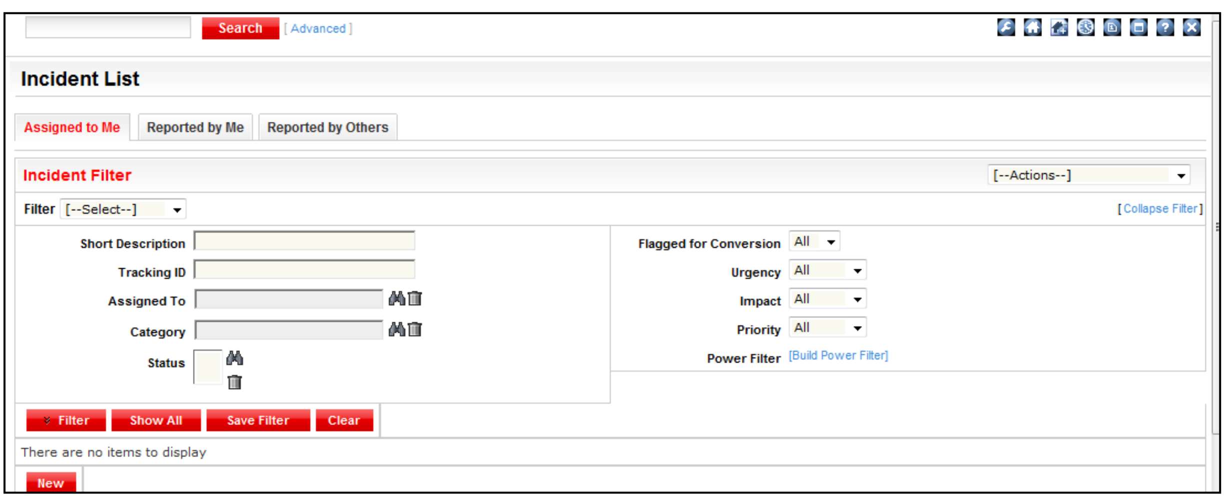
7.6.1 Viewing Incident List

Perform the following steps to view any outstanding incidents:

1. Login to Clarity.
2. Go to the left-hand navigation menu on the **Clarity Overview: General** screen.
3. Scroll down to the **Demand Management** menu and click the **Incidents** link.



4. The **Incident List** portlet displays as shown on the screen below.



5. You can view incidents in any of the following categories:

    - *Assigned to Me*
    - *Reported by Me*
    - *Reported by Others*
    - *Sort by Filter*

7.6.1.1 Assigned to Me Incidents

To view all incidents that are currently assigned to the logged on userid, click the **Assigned to Me** tab on the **Incident List** page. This tab displays by default when you view the **Incident List** page.

This portlet also displays incidents if any the following conditions are true:

- You have reported incidents
- You have been assigned incidents
- You have the *Incidents - Manage Category Incidents* access right for at least one incident category

You can specify how you are notified of new incidents or incidents that have been assigned to you by using the account settings on the **Account Settings: Notifications** page.

Note: Refer to the "Common Features and Personal Options User Guide" for more information.

7.6.1.2 Reported by Me Incidents

To view all incidents that were created by the logged on userid, click the **Reported by Me** tab on the **Incident List** portlet.

The tab will also display for you under the following conditions:

- You have reported incidents
- You have been assigned incidents
- You are a requestor or IT manager

7.6.1.3 Reported by Others Incidents

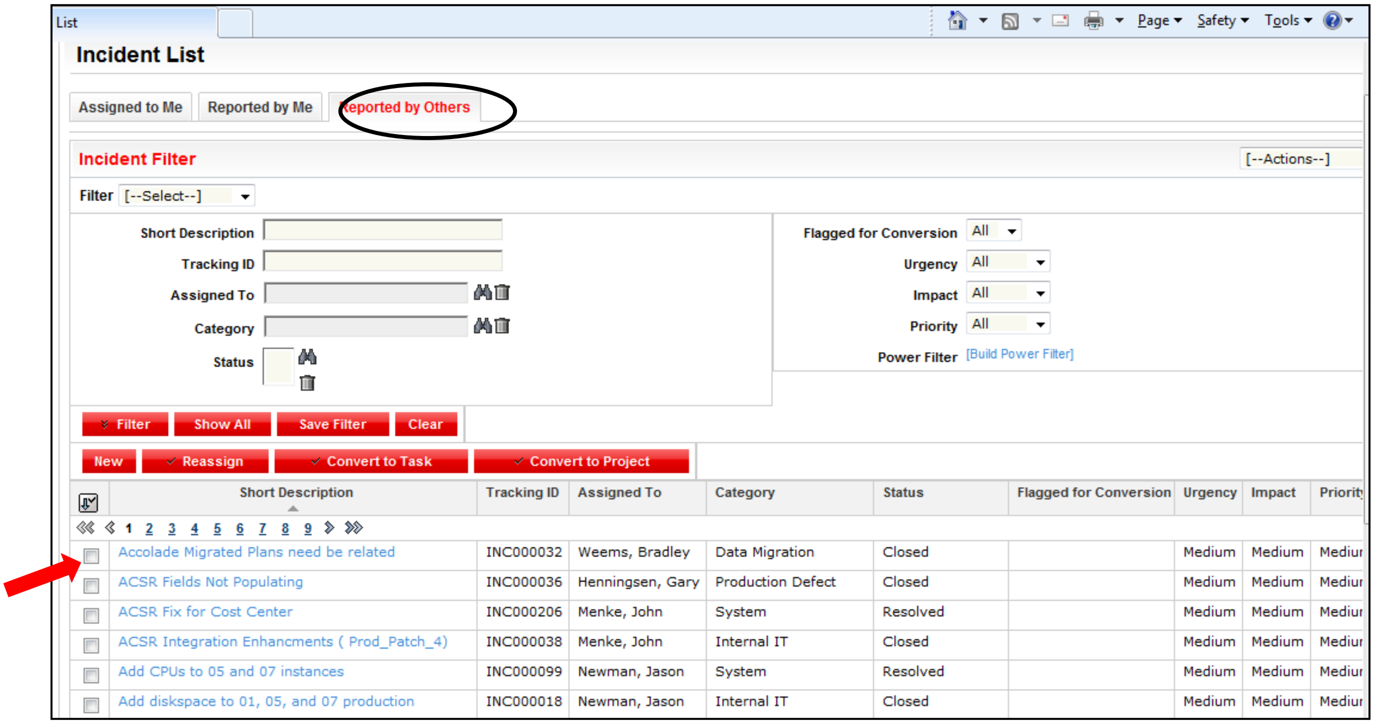
To view all incidents which were reported by other resources, click the **Reported by Others** tab on the **Incident List** portlet.

This incidents list includes the following:

- Any incidents mapped to incident categories to which you have access rights (i.e., either directly or by your association to a group)
- Any incidents assigned to you
- Any incidents reported by you

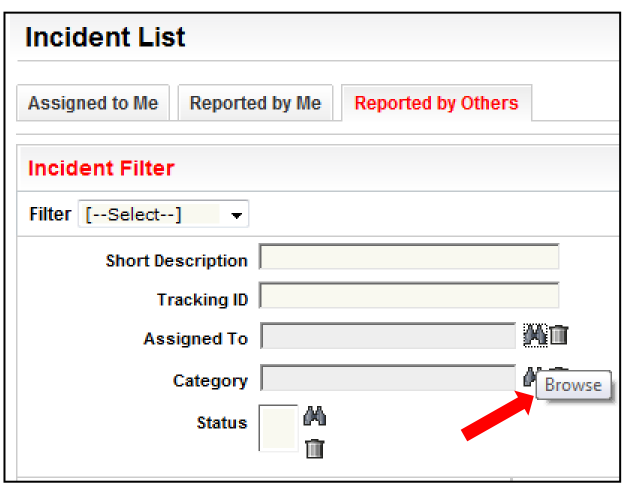
This tab only appears if you have the **Incidents - Create/Edit - All** access right or the **Incidents - Manage Category Incidents** access right.

This list of incidents displays as shown on the screen below.

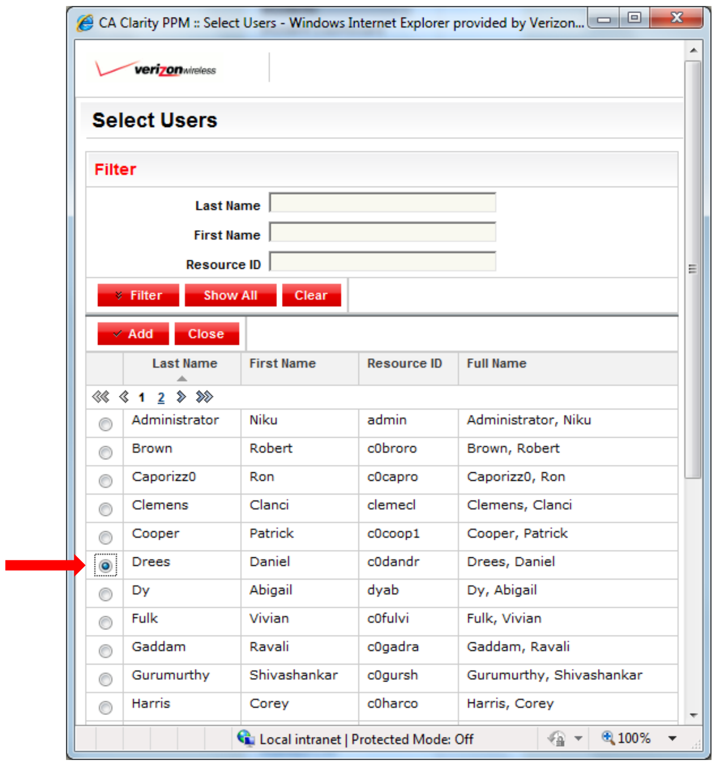


7.6.1.4 Sort by Filter

1. Click one of the tabs in the **Incident List** portlet (as shown in sections "7.6.1.1.1" through "7.6.1.1.3" above) to view the appropriate category of incidents.
2. Click the **Browse** button ("binoculars" icon) in the field (e.g., the **Assigned To** attribute) that you want to sort by.



The pop-up filter screen displays for the selected attribute (refer to the example in Step 2 above). Click the **userid** of the resource that you want to filter on.



All incidents that are assigned to the selected name will display.

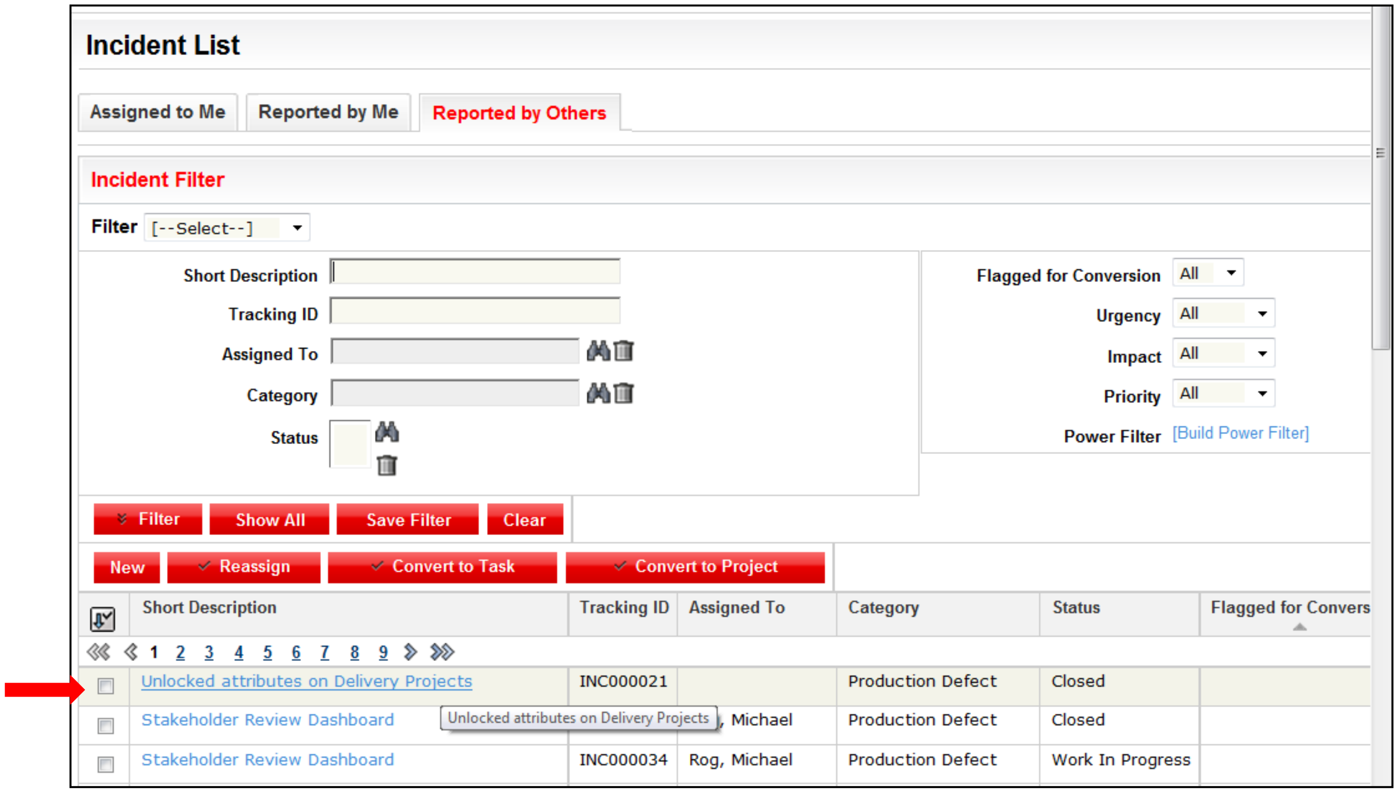
7.6.2 Viewing Incident Properties

The **Incident Properties** page allows the user to define and view incident basics, such as its short description, category, status, urgency, and impact. You can also convert the incident into a project or project task.

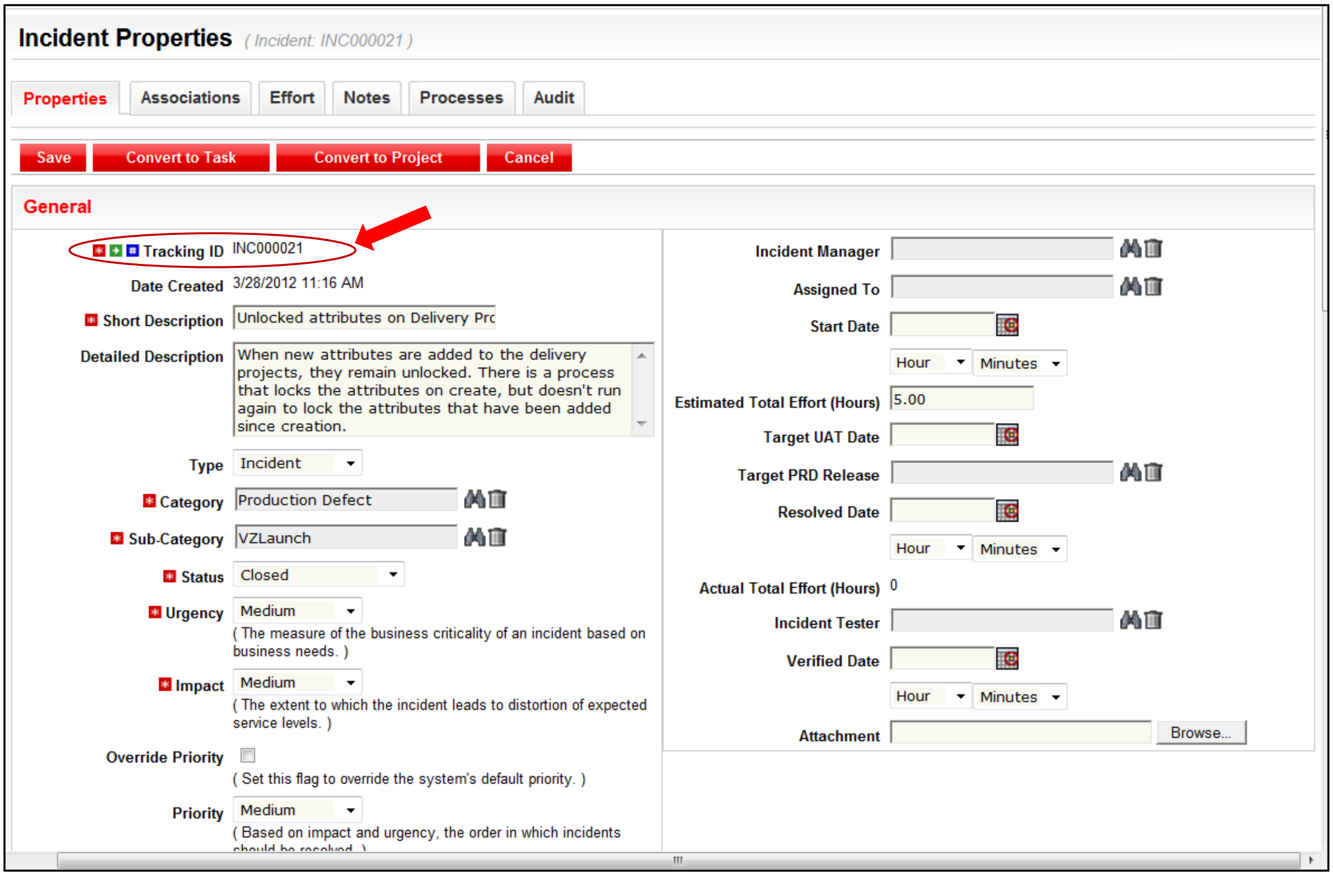
7.6.2.1.1 Incident Properties

Perform the steps below to view the **Incident Properties** page:

1. Select **Incidents** from the **Demand Management** menu as shown in "***Section 7.6.1 Viewing Incident List***". The **Incident List** page appears.
2. Click the **Short Description** of the incident you want to view.



The **Incident Properties** page displays for the selected incident.



You can also change attributes shown on this page for the selected incident.

> ***Note:*** *For more information, refer to "**Section 7.6.3 Change Incident Properties**".*

7.6.2.1.2 Incident Properties Tabs

You can access the tabs on the **Incident Properties** page as shown below.

7.6.2.1.2.1 Associations Tab

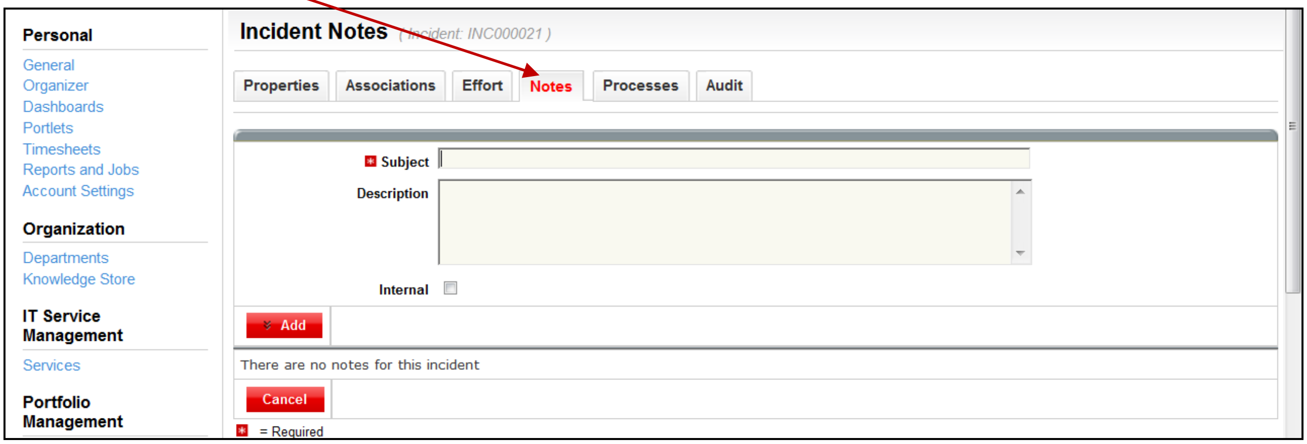
Click the **Associations** tab to view a list of projects and project tasks which were created for a specific incident.

7.6.2.1.2.2 Effort Tab

Click the **Effort** tab to view the list of efforts that resources entered on timesheets to resolve this incident.

7.6.2.1.2.3 Notes Tab

Click the **Notes** tab to add notes to an incident or view notes that have already been posted.

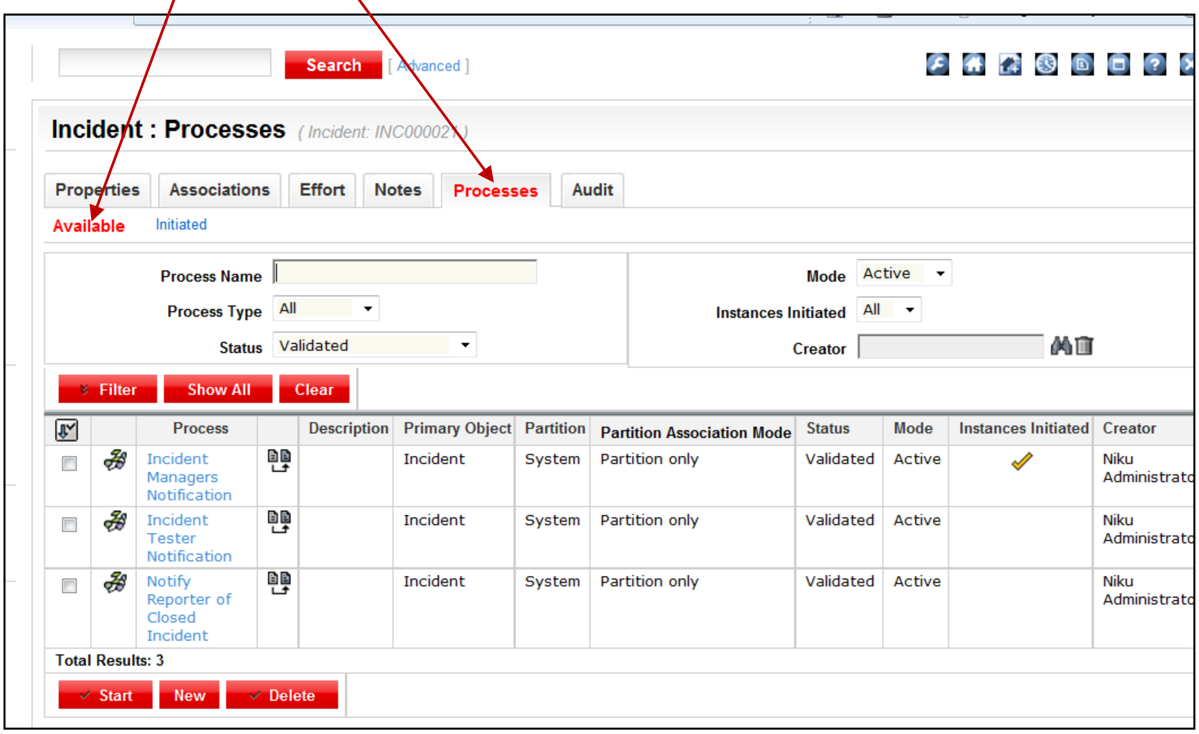


7.6.2.1.2.4 Processes Tab

Click the **Processes** tab to view the **Available** and **Initiated** processes for an incident.

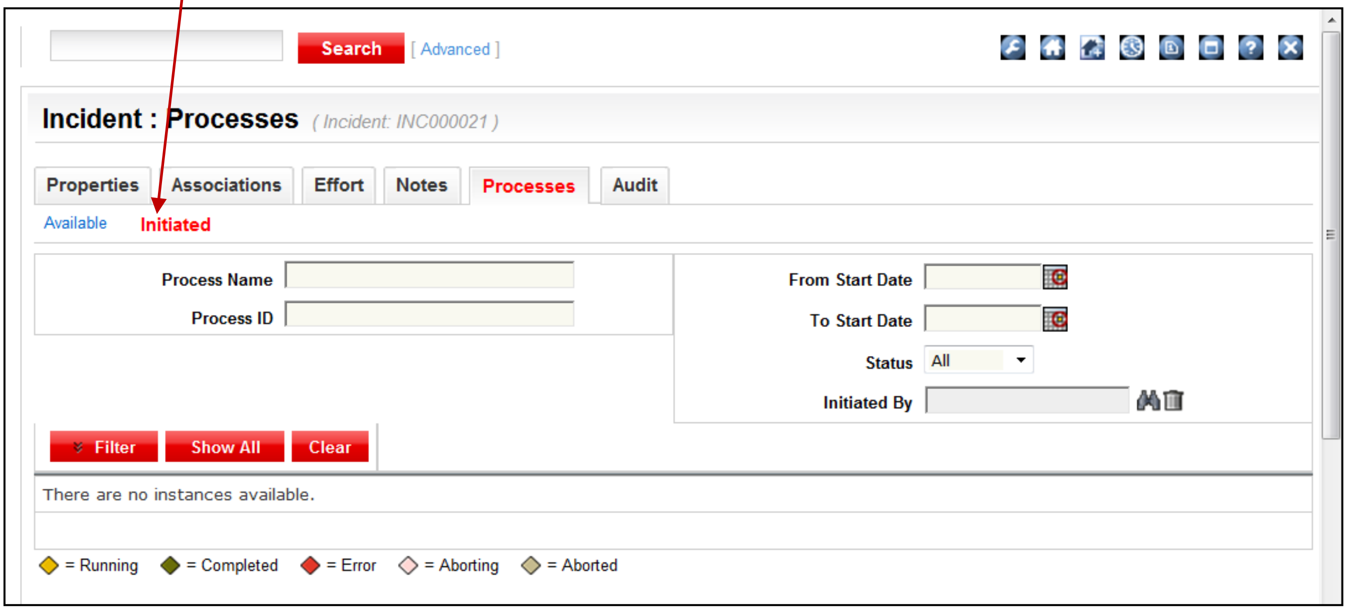
7.6.2.1.2.5 Available Page Link

Click the **Available** tab to view all processes that were created for an incident.



7.6.2.1.2.6 Initiated Page

Click the **Initiated** tab to display the **Initiated** page where you can create and run processes that automate specific elements of demand management.



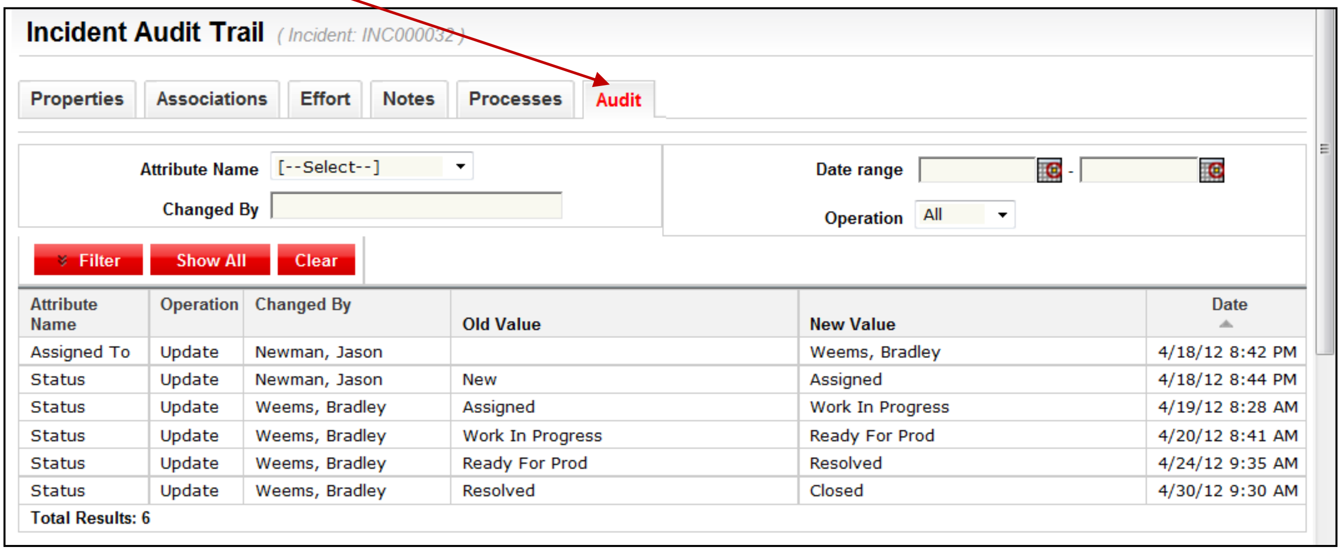
For example, you can create a process that notifies the incident manager when the incident status changes to "**Resolved**".

The PPM administrator can also define processes that take action on the incident, such as setting the urgency to "**High**".

> ***Note:*** *Refer to the "**CA Clarity Project & Portfolio Manager Administration Guide**" for more information.*

7.6.2.1.2.7 Audit Tab

Click the **Audit** tab to view the history of specific activities that occur for an incident. The **Audit Trail** page includes a log that details the change, addition, and deletion records of any fields chosen for auditing.



Attribute Name	Operation	Changed By	Old Value	New Value	Date
Assigned To	Update	Newman, Jason		Weems, Bradley	4/18/12 8:42 PM
Status	Update	Newman, Jason	New	Assigned	4/18/12 8:44 PM
Status	Update	Weems, Bradley	Assigned	Work In Progress	4/19/12 8:28 AM
Status	Update	Weems, Bradley	Work In Progress	Ready For Prod	4/20/12 8:41 AM
Status	Update	Weems, Bradley	Ready For Prod	Resolved	4/24/12 9:35 AM
Status	Update	Weems, Bradley	Resolved	Closed	4/30/12 9:30 AM

On this page you can view the previous and new values of changed fields, the resource who changed the fields, and the date that the changes were made.

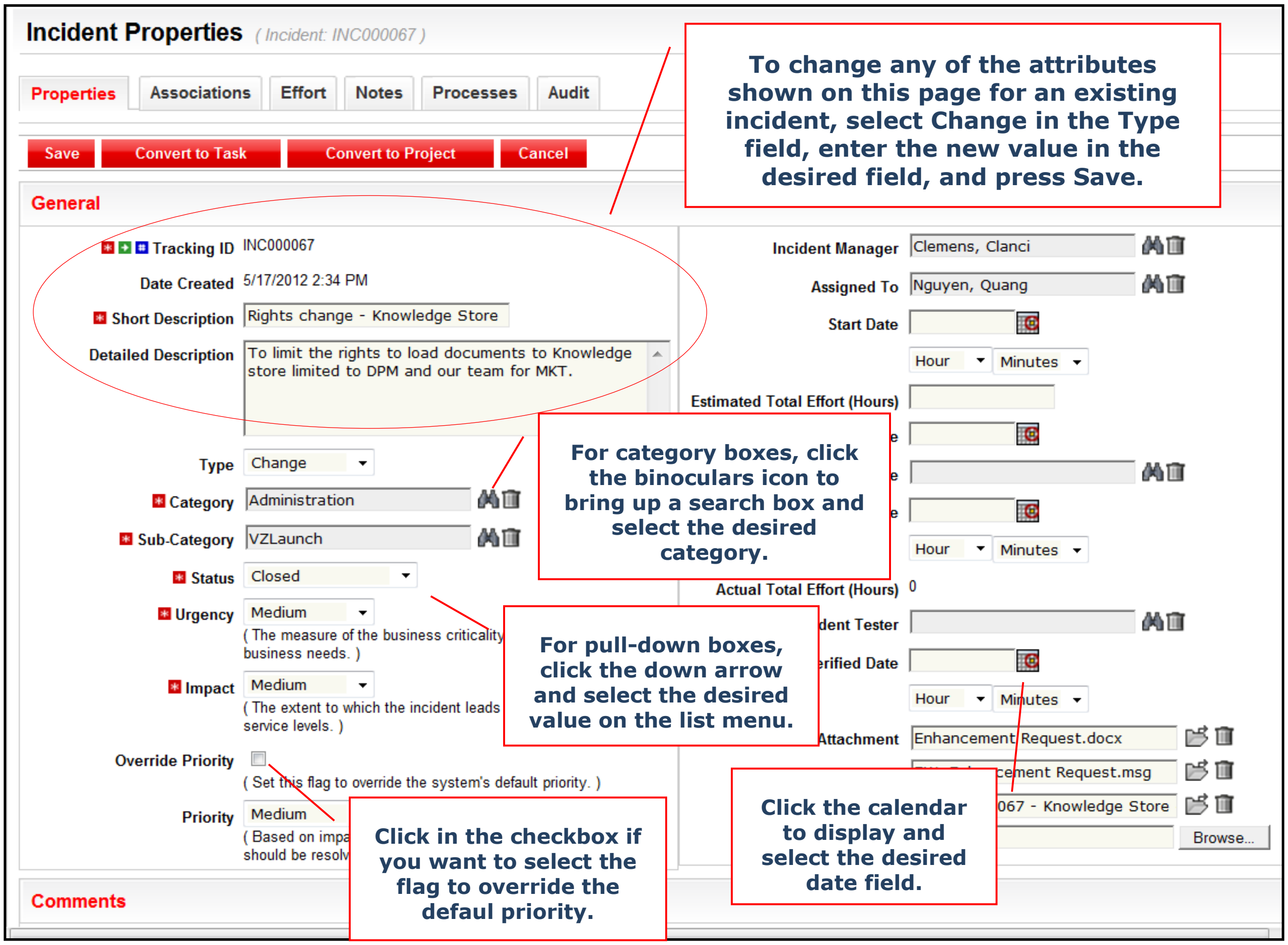
You can also filter the view based on the **Attribute Name**, **Changed By**, **Date Range**, and **Operation** fields. These fields display on the bottom half of the **Incident Audit Trail** page.

Auditing must be set up by the Clarity PPM administrator, who determines which fields are audited and what information is stored in the audit trail.

> ***Note:*** *Contact your Clarity PPM administrator or refer to the* ***"CA Clarity Project & Portfolio Manager Administration Guide"*** *for more information.*

7.6.3 Change Incident Properties

The user can change the values of all attributes shown on the **Incident Properties** page for a particular incident. In addition, you can create comments in the **Comments** box.



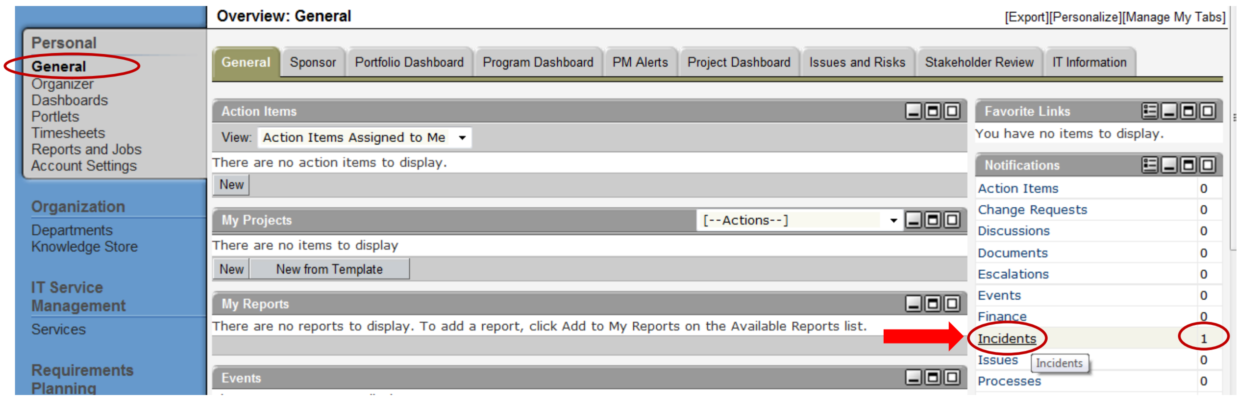
Refer to the text boxes shown above for information on changing data values in the corresponding attribute field boxes.

7.6.4 View Newly Assigned Incidents from the Notifications Portlet

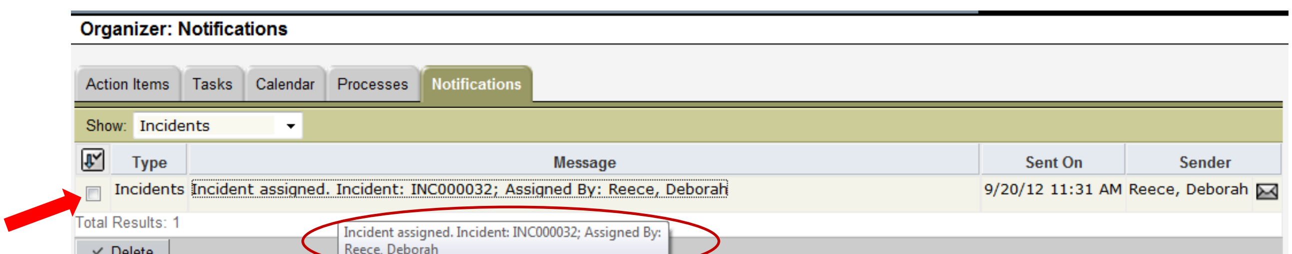
You will receive new notifications whenever an IT manager assigns work to you on an incident. This assignment notifications can be viewed on the **Notifications** portlet on the **Overview: General** page.

7.6.4.1 Steps to View Notifications

1. Click the **General** link on the **Personal** menu and the **Notifications** portlet displays along with other portlets. The number of incident notifications you have received displays.



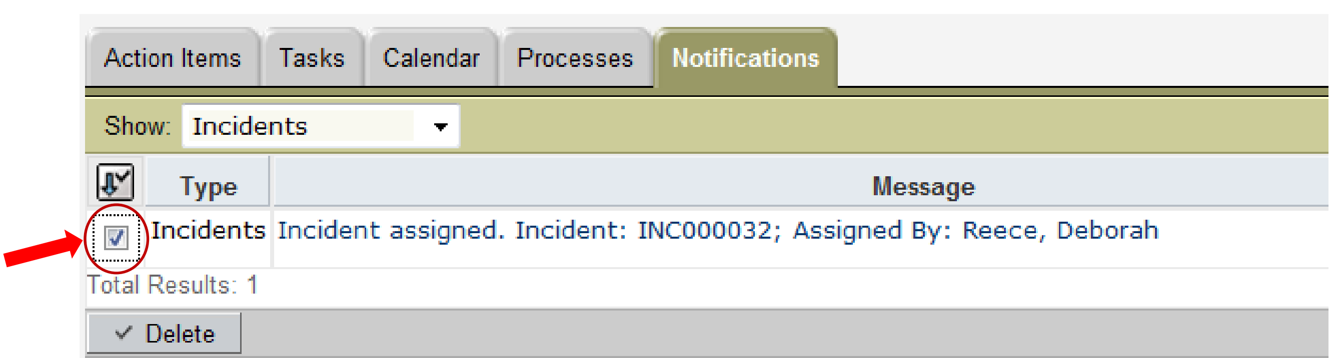
2. Click the **Incidents** link in the right-hand **Notifications** column (shown above) and the **Organizer: Notifications** page displays your assigned incidents.



__Note:__ Refer to the __"Common Features and Personal Options User Guide"__ for more information.

7.6.4.1.1 Deleting Notifications

If you want to delete your notification(s), click the checkbox next to the notification(s) you want to delete under the **Notifications** tab, then click **Delete**.



7.6.5 Create New Incidents

You can access the **Create Incident** page from the **Demand Management** menu and use it to report new incidents or work requests. You can also create a new incident directly from the investment.

> *Note: You must have Incidents - Create and Incidents Select Category access rights for at least one incident category in order to create an incident.*

Perform the following steps to report a new incident or work request:

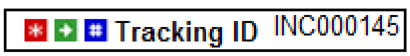
1. Click the **Incidents** link on the **Demand Management** menu.
2. The **Incident List** page displays. Click **New.**
3. The **Create Incident** displays. Complete the fields in the **General** section as shown in "***Section 7.6.4.1.1. Incident Properties Attributes***" below.

7.6.5.1 Incident Properties Attributes

Enter the following field values on the **Incident Properties** page to create new incidents:

- **Tracking ID**

  Allows you to define the tracking number for this incident. If auto-numbering is enabled, this field will be read only (i.e., it will be generated automatically).



- **Date Created**

  After an incident is submitted, this read-only field displays the date and time that the incident was created.

- **Short Description**

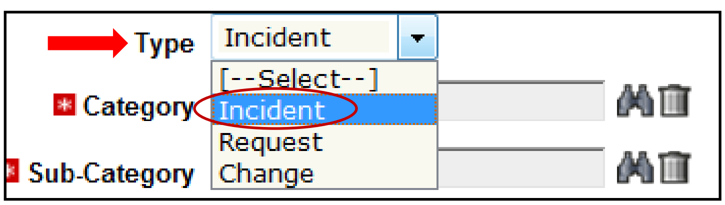
  Allows you to type a short, descriptive name for the incident.

- **Detailed Description**

  Allows you to type a detailed description for the incident.

- **Type**

  Allows you to indicate a type for the selected incident. Select "**Incident**", "**Service Request**" or "**Change**" on the drop-down box.

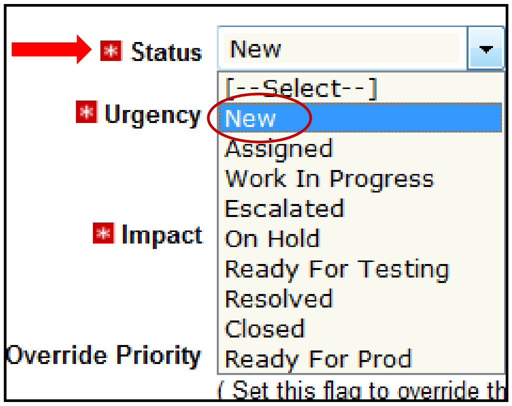


- **Category**

  Allows you to define the classification for this incident (i.e, this helps trace costs for unplanned work). Click the **Browse** icon to display and select the incident category for this incident.

Status

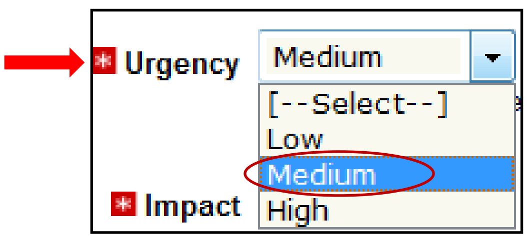
Allows you to indicate a status for the incident. Select one of the following values from the drop-down list to change the status: "**New**", "**Assigned**", "**Work In Progress**", "**Escalated**", "**On Hold**", "**Resolved**", "**Closed**" or "**Ready for Prod**".



Note: The status of a new incident is set to "New" by default when you click the Save button.

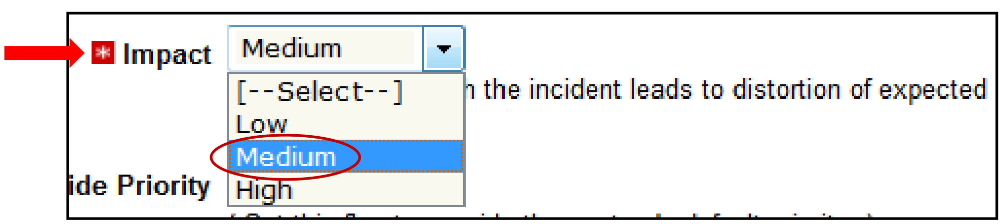
Urgency

Allows you to indicate the critical measure that the incident requires based on business needs. Select one of the following values: "**Low**", "**Medium**", and "**High**".



Impact

Allows you to define the degree of impact expected for service levels relating to the incident. Select one of the following from the drop-down: "**Low**", "**Medium**", and "**High**".

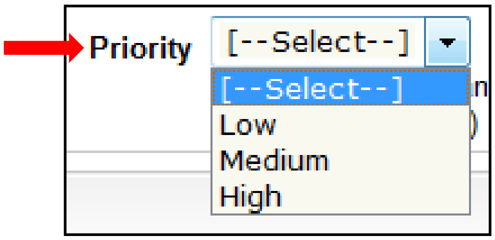


Override Priority

Select this box if you want to override the priority of the incident. This field will only display if you have the **Incidents - Override Priority** access right. Incident priority is ranked by the *Incident Priority* matrix based on urgency and impact selections.

- **Priority**

  Allows you to define the order in which incidents should be resolved (i.e., based on the impact and urgency). If you do not have the *Incidents - Override Priority* access right, the priority will be system-generated and read-only. Otherwise, select the **Override Priority** checkbox and click one of the following priorities on the drop-down list: "**Low**", "**Medium**", and "**High**".



  Submit this incident. Then re-open the incident and select this checkbox.

- **Incident Manager**

  Allows you to define the resource assigned as the Project Manager (PM) for this incident. To enable this incident for conversion into a project or project task, complete all required fields and submit this incident. Re-open this incident and click the **Browse** icon to select the PM.

- **Start Date**

  Allows you to define the date when the user is expected to start working on this incident. You must have the *Incident - Create/Edit* access right to view this field.

- **Estimated Total Effort (Hours)**

  Allows you to define the estimated total amount of effort needed to resolve this incident. You must have the *Incident - Create/Edit* access right to view this field.

- **Target PRD Release**

  Allows you to enter the targeted production release date (i.e., after the incident is resolved).

- **Resolved Date**

  Allows you to define the date when the user is expected to complete the work and mark the incident as "**Resolved**".

- **Actual Total Effort (Hours)**

  Displays the total hours entered for individual effort on the incident.

  - **Resolved Date**

    Allows you to select the date when the incident **Status** field is set to "**Resolved**".

    - **<u>Hour</u>**

      Allows you to enter the hour when the incident **Status** field is set to "**Resolved**".

    - **<u>Minutes</u>**

      Allows you to enter the minutes when the incident **Status** field is set to "**Resolved**".

- **Incident Tester**

  Allows you to select the name of the person who will be responsible for testing the incident.

- **Verified Date**

  Allows you to define the date that the incident's resolution is accepted and the incident is verified to be closed.

- **Attachment**

  Allows you to indicate if you want to attach a file relating to this incident. Click the **Browse** icon and attach the file. You can add up to ten (10) file attachments.

- **Primary Contact**

  Allows you to enter contact info for the created incident. You must complete the following fields in this section:

  - **Name**

    Enter the contact name for this incident or it will default to the resource currently logged in. Click the **Browse** icon to select another resource as the contact.

  - **Email**

    Enter the primary contact's email address.

  - **Home Phone**

    Enter the primary contact's home phone number.

  - **Work Phone**

    Enter the primary contact's work phone number.

  - **Mobile Phone**

    Enter the primary contact's mobile phone number.

7.6.6 Assign and Reassign Incidents

The *Assign Incidents* process starts automatically when an incident is logged by a requestor. The incident approval process is used by process administrators to manage the assignment, review, and completion of incidents. This process must be activated by a process administrator from the **Administration Tool** before it can be started.

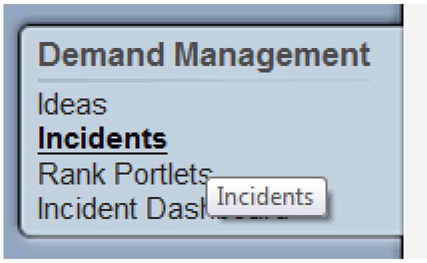
7.6.6.1 Assign Resources to Incidents

All incidents must be assigned to a resource (i.e., userid) using the **Assign To** field on the **Incidents List** page. This field displays on the page after you initially create the incident. (***Note:*** *Refer to "**Section 7.6.5 Create New Incidents**".)* When you assign an incident, a notification will be sent to that resource. The method in which notifications are received depends on the assigned resource's personal notification settings.

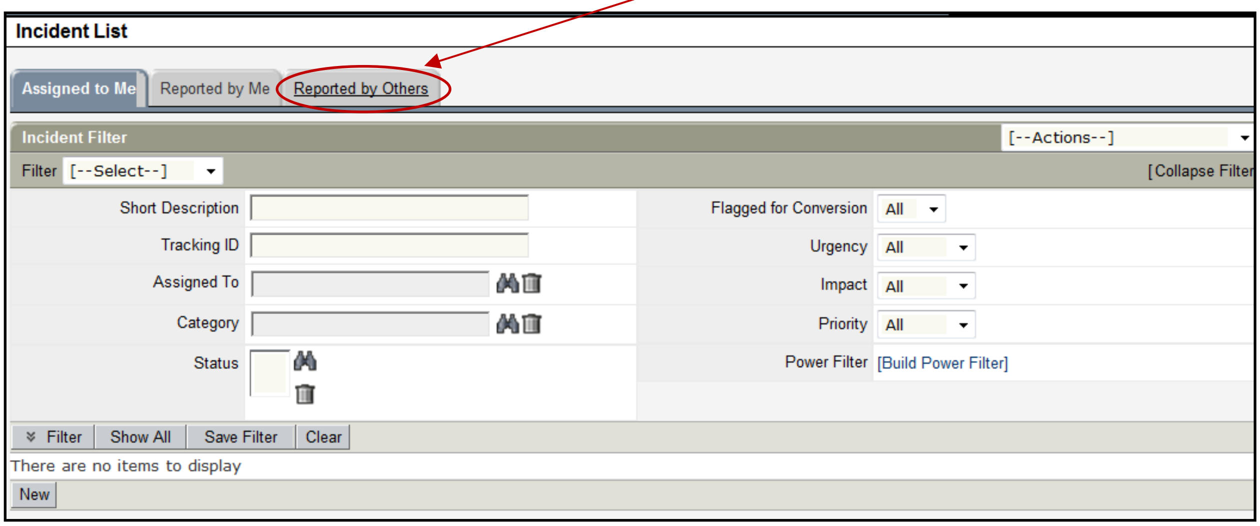
Note: Refer to the "Common Features and Personal Options User Guide" for more information.

7.6.6.1.1 Assignment Steps

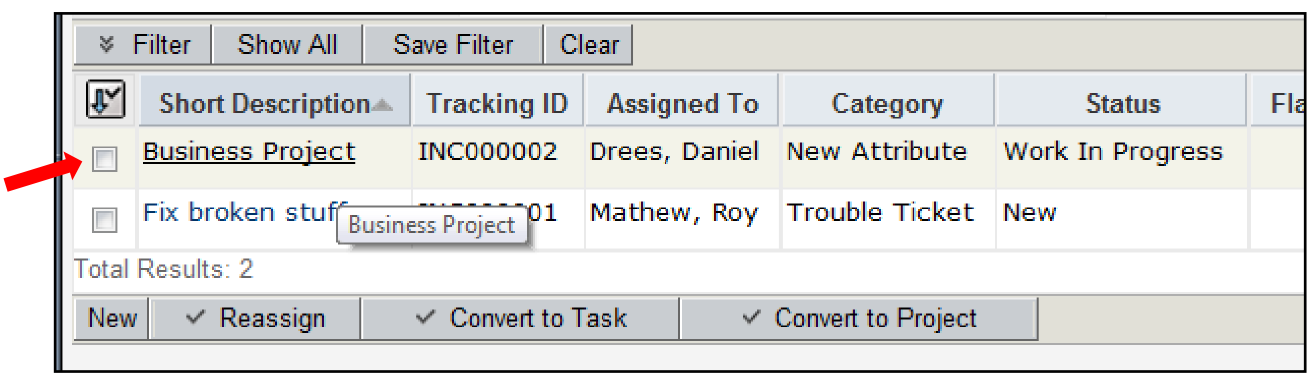
1. Click the **Incidents** link on the **Demand Management** menu and the **Incident List** page displays.



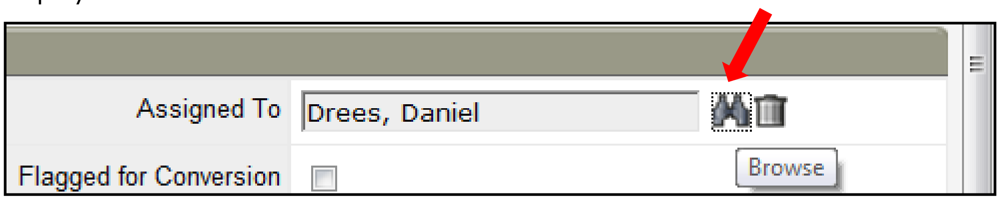
2. Click the **Assigned to Me**, **Reported by Me**, or **Reported by Others** tab to display the appropriate incident that you want to assign to a resource.



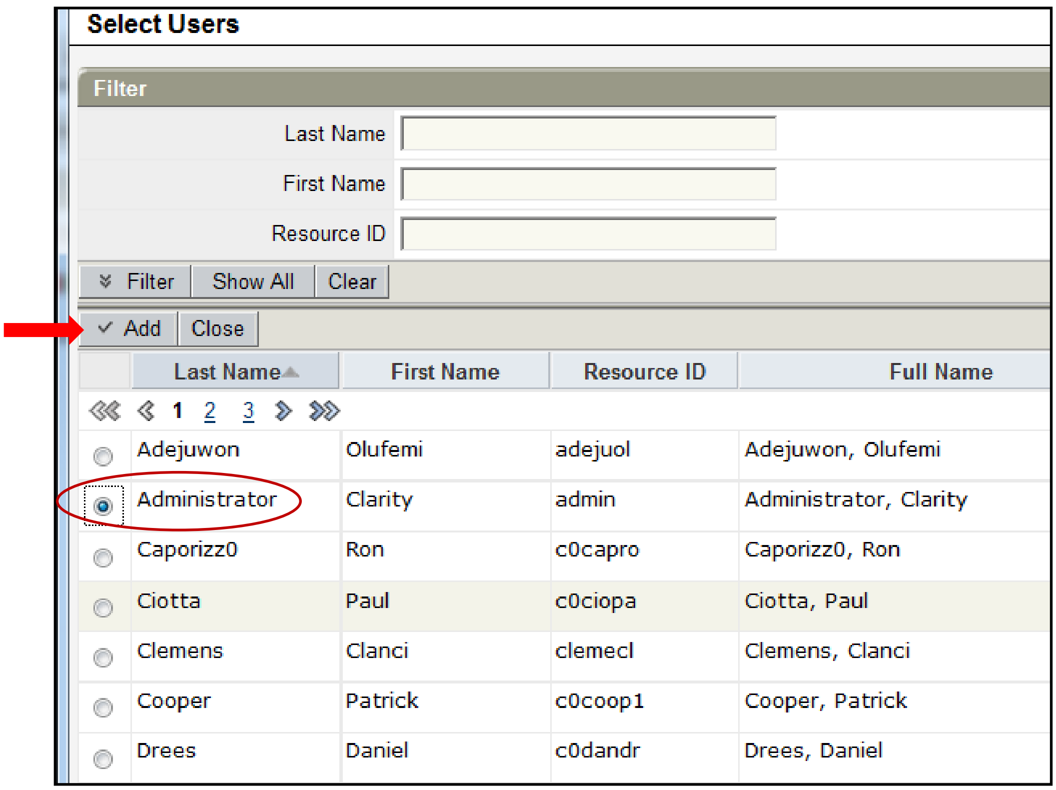
2. Click the incident's **Short Description** and the **Incident: Properties** page displays.



3. Click the **Browse** icon next to the **Assigned To** field and the pop-up **Select Users** window displays.



5. Select the desired resource and click **Add**. The selected resource is assigned to the incident.



5. Click **Save** on the **Incident Properties** page to save your changes.

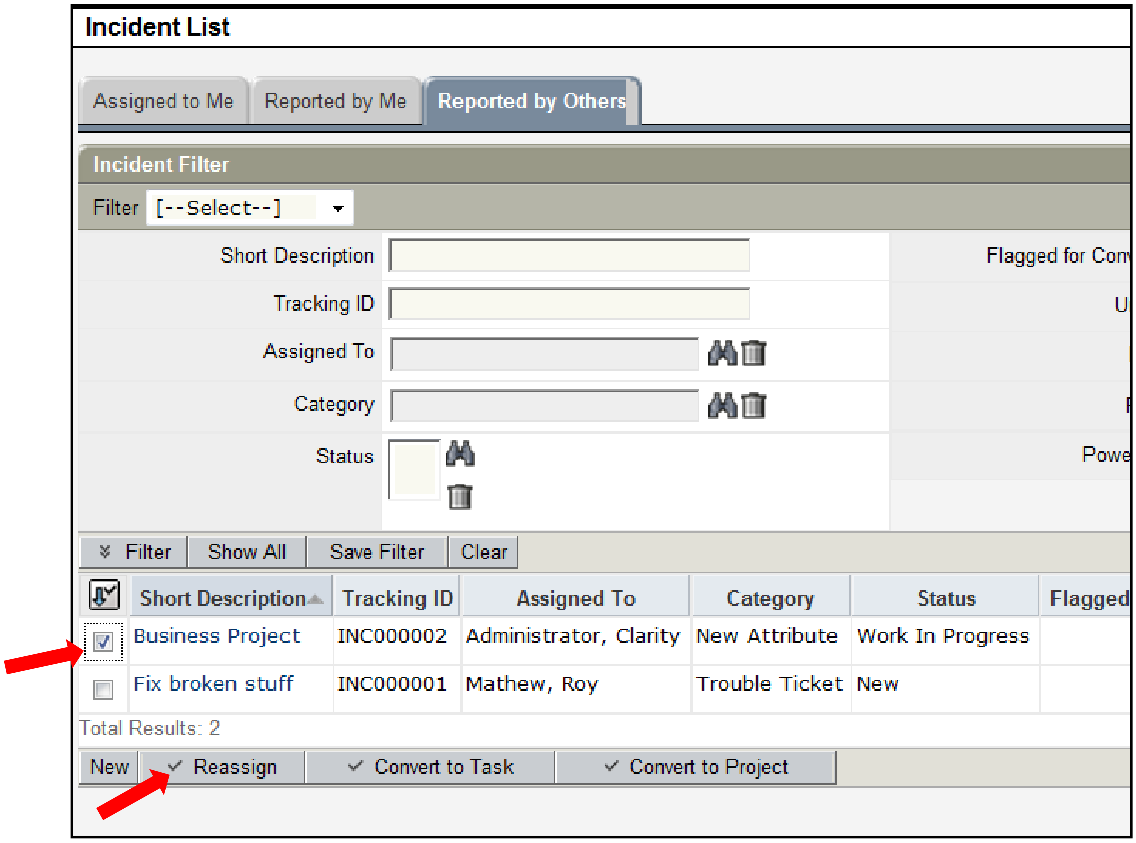
7.6.6.2 Reassign Incidents

You can reassign incidents that are unresolved to another resource using the **Incident List** page. Alternatively, you can reassign incidents from the **Incident Properties** page. When you assign an incident, a notification is sent to that resource. The method in which notifications are received depends on the assigned resource's personal notification settings.

Note: Refer to the "Common Features and Personal Options User Guide" for more information.

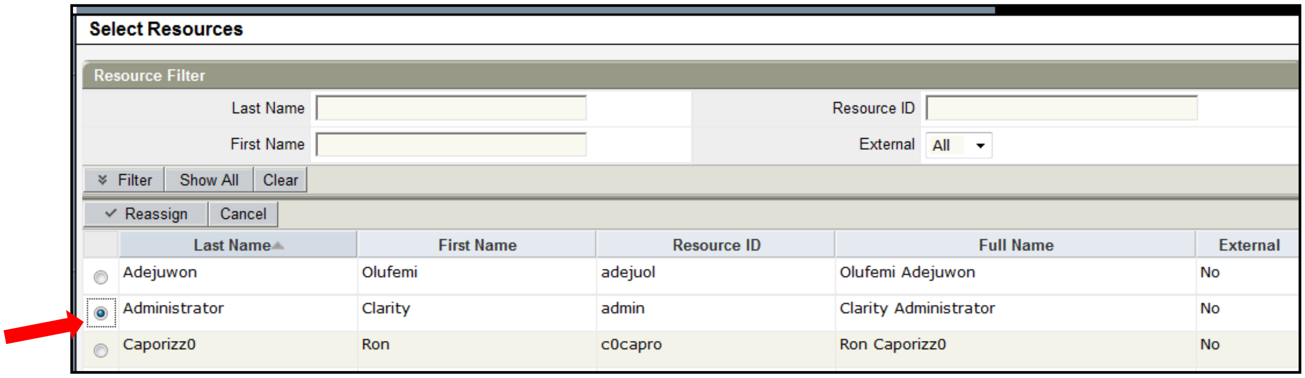
7.6.6.3 Reassignment Steps

1. On the **Incident List** page, check the box next to the incident you want to reassign.

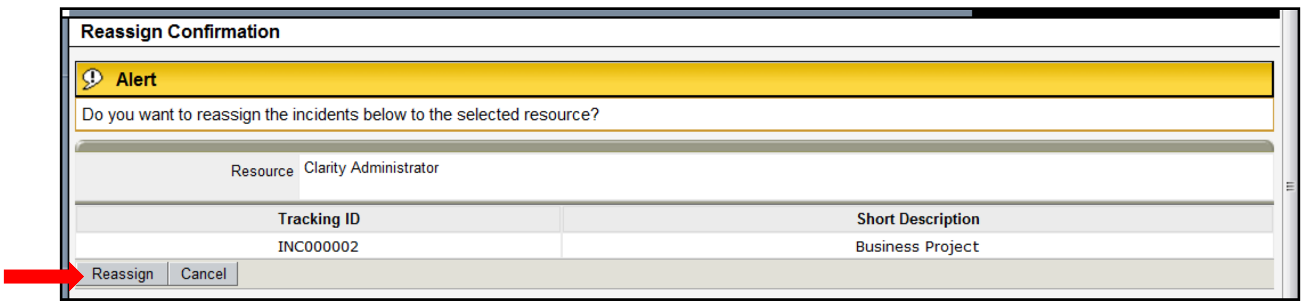


2. Click **Reassign**.

3. The **Select Resources** page displays. Select the resource (i.e., userid) you want to assign to this incident.



4. Click **Reassign** and the **Reassign Confirmation** page displays.



5. Click **Reassign** to reassign the incident to the selected resource, or click **Cancel** to cancel out of the screen without saving.

7.6.7 Daily Maintenance

Perform the following steps to ensure that all application services are running:

1. Login to the Clarity NSA.
2. Monitor the services.
3. Run the health-check report.
4. Monitor all log files (parse for "error").

7.6.8 Check Available/Scheduled Reports and Jobs

Users and administrators can click the **Reports and Jobs** link on the Clarity left-hand navigation menu to run and schedule reports and jobs.

They also can view generated report output and job logs.

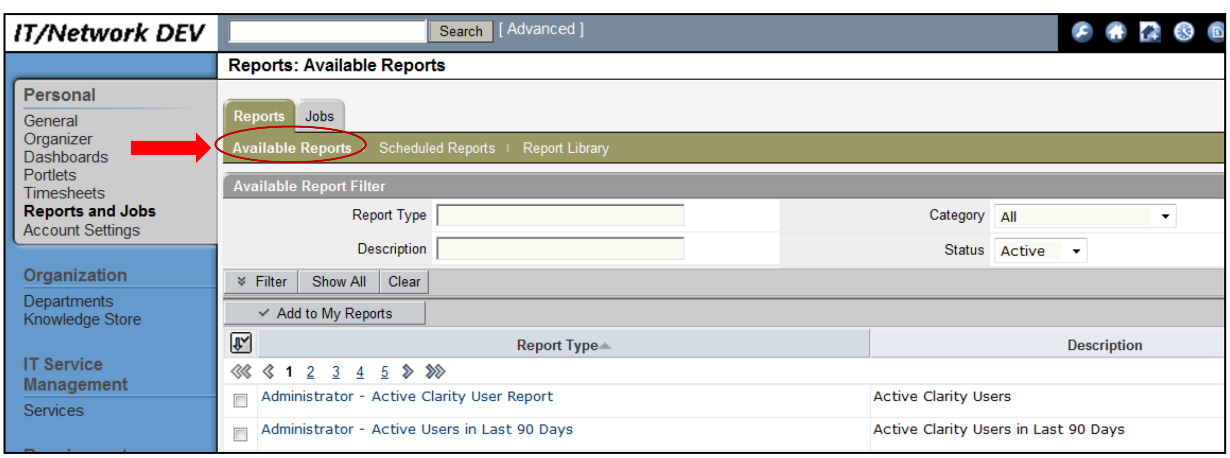
The **Available Reports** or **Available Jobs** pages list all reports or jobs to which a user or administrator has access. The report type is the user's view of the report or job definition. Each available report or job has one corresponding report or job definition and one report or job type. From this view, you can select a report or job type and set run criteria.

The **Scheduled Reports** or **Scheduled Jobs** pages list all scheduled run instances that a user or administrator has created. A single report can have many scheduled runs. You can manage scheduled runs from this view, including checking statuses and modifying schedules.

*Note: Refer to the "**Common Features and Personal Options User Guide**" for more information.*

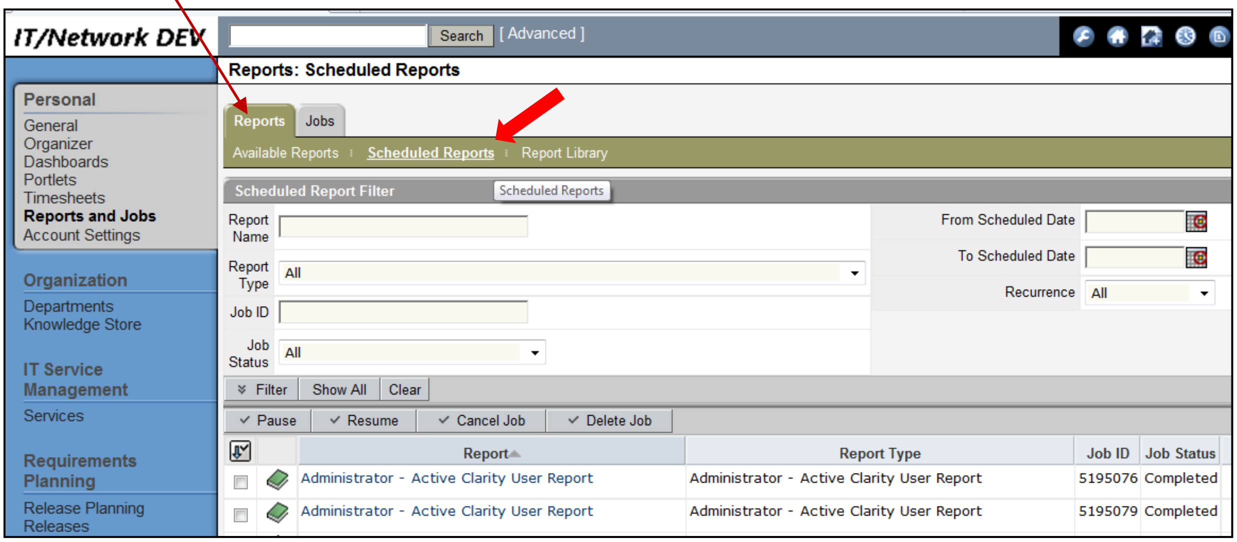
7.6.8.1 Viewing Available Reports

1. Click the **Reports** tab.
2. Click the **Available Reports** subtab and the **Reports: Available Reports** page displays all available reports that the user or administrator has permission to access.



7.6.8.2 Viewing Scheduled Reports

1. Click the **Reports** tab.

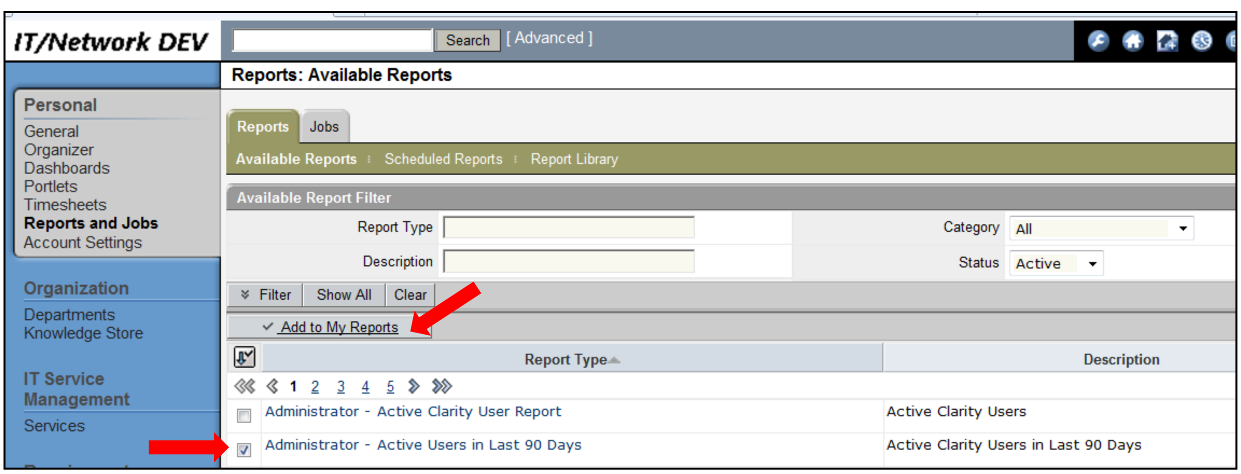


2. Click the **Scheduled Reports** subtab and the **Reports: Scheduled Reports** page displays all scheduled reports that the user or administrator has permission to access.

7.6.8.2.1 Add to My Reports Option

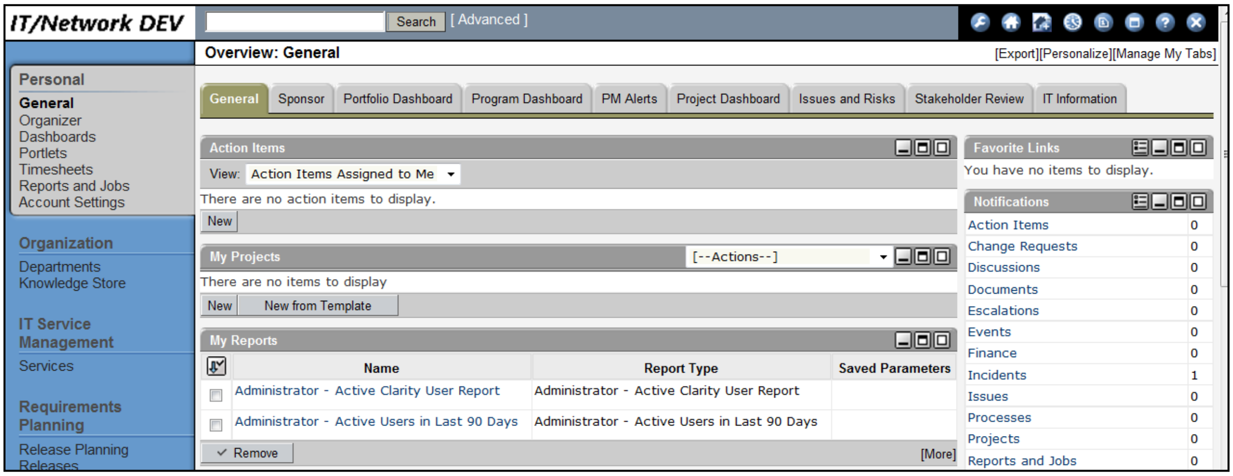
You can add selected reports to the **My Reports** section of your **Overview: General** page.

1. Select the checkbox next to the desired **Report Type**.



2. Click **Add to My Reports**.

The report that is added displays on your **Overview: General** page.



7.6.8.2.2 Scheduled Report Filter

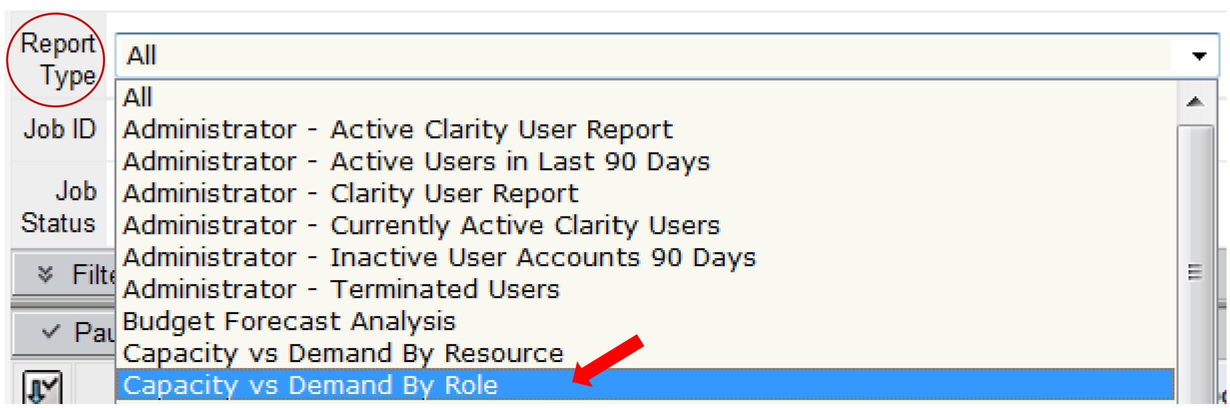
Enter search data in the field you want to filter on and and click **Filter**.

- **Report Name**

  Enter the name of the report you want to filter.

- **Report Type**

  Click the desired report type filter on the pull-down menu.

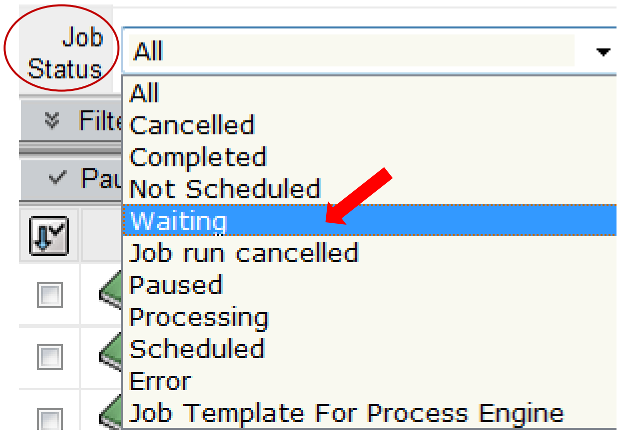


- **Job ID**

  Enter the ID of the job you want to filter.

- **Job Status**

  Click the desired job status filter on the pull-down menu.



- **From Scheduled Date**

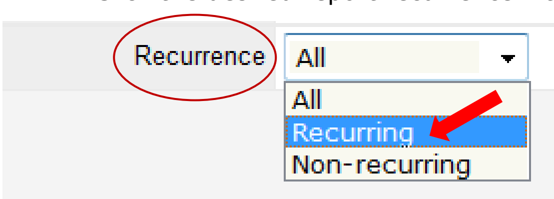
  Click the calendar icon to enter the beginning date of the filter range.

- **To Scheduled Date**

  Click the calendar icon to enter the ending date of the filter range.

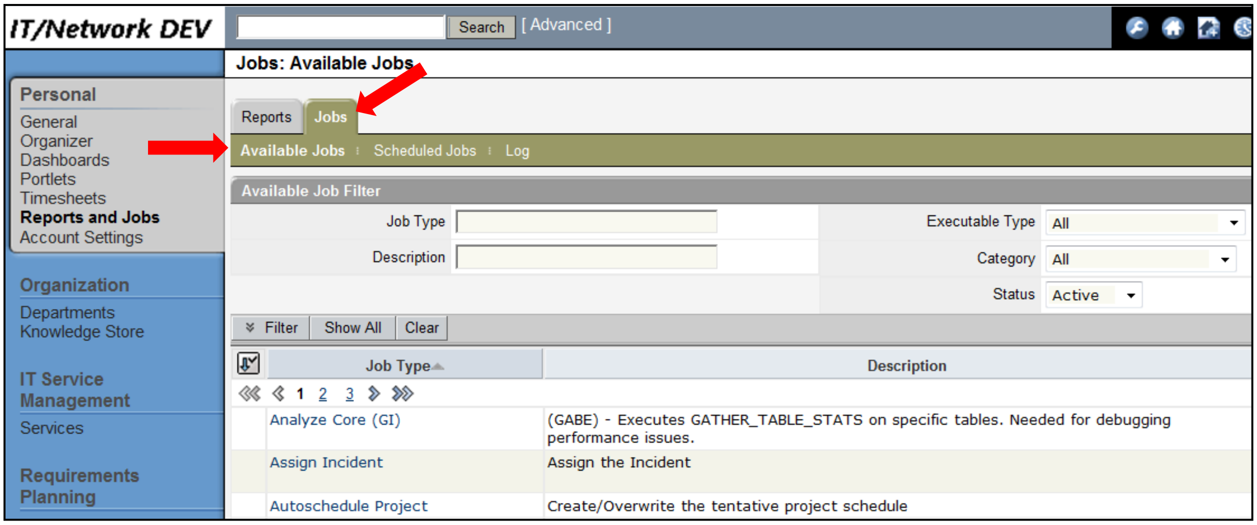
- **Recurrence**

  Click the desired report recurrence filter on the pull-down menu.



7.6.8.3 Viewing Available Jobs

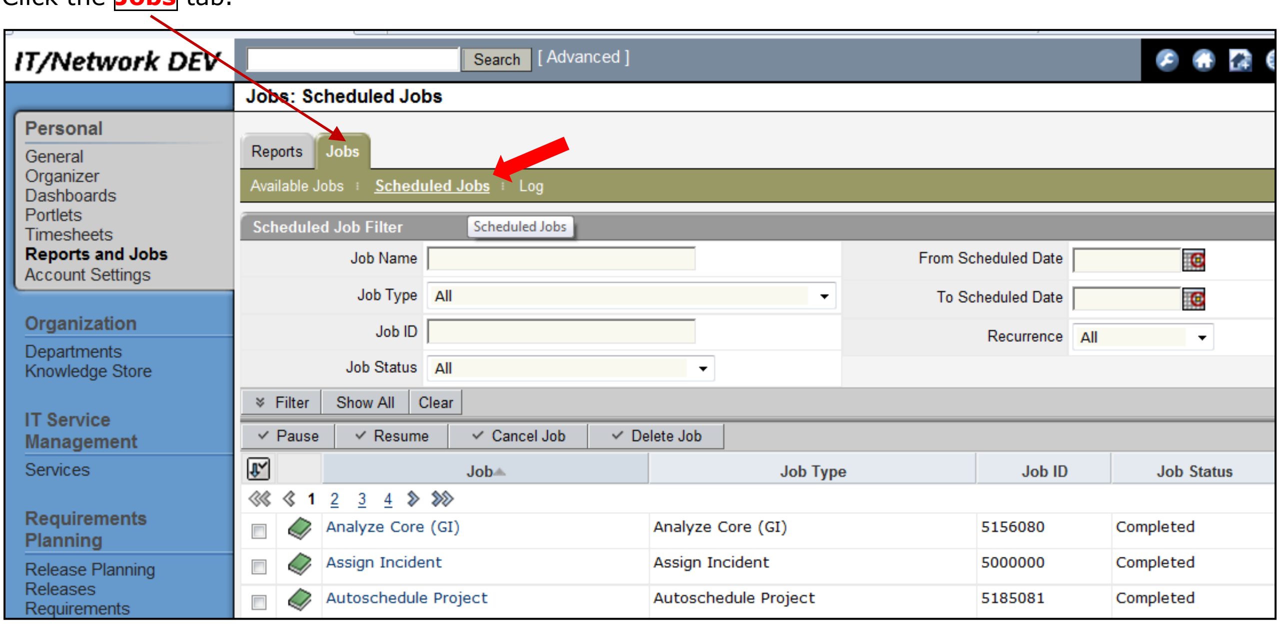
1. Click the **Jobs** tab.



2. Click the **Available Jobs** subtab and and the **Reports: Available Jobs** page displays all jobs that the user or administrator has permission to access.

7.6.8.4 Viewing Scheduled Jobs

1. Click the **Jobs** tab.



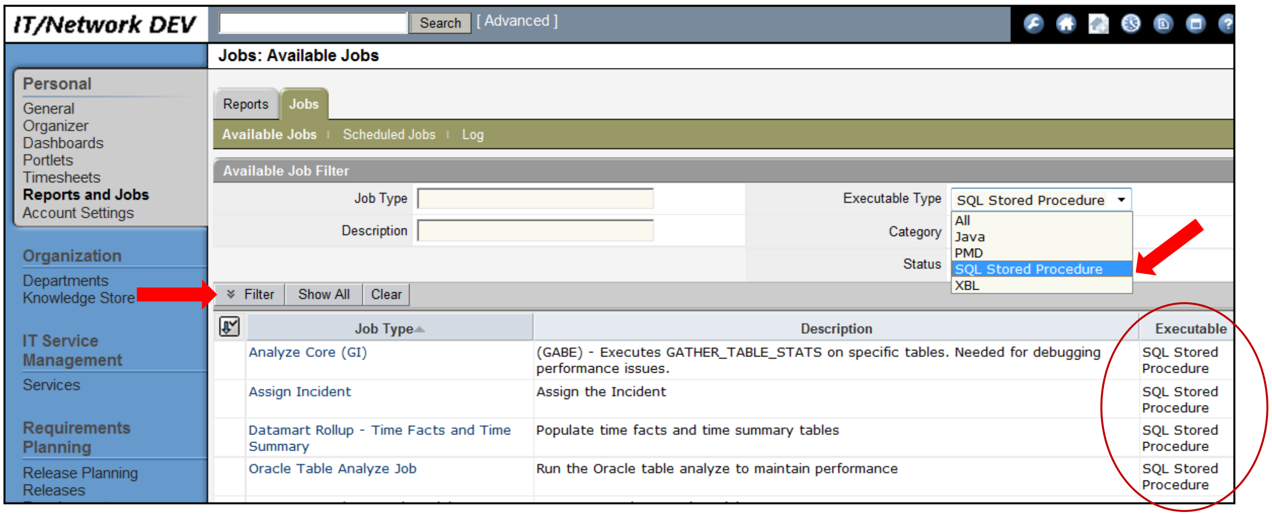
2. Click the **Scheduled Jobs** subtab and the **Jobs: Scheduled Jobs** page displays all scheduled jobs.

7.6.8.5 *Filtering Reports and Jobs*

You can enter the job or report type or description to filter for specific data. You can also select any of the following views from associated pull-down menus.

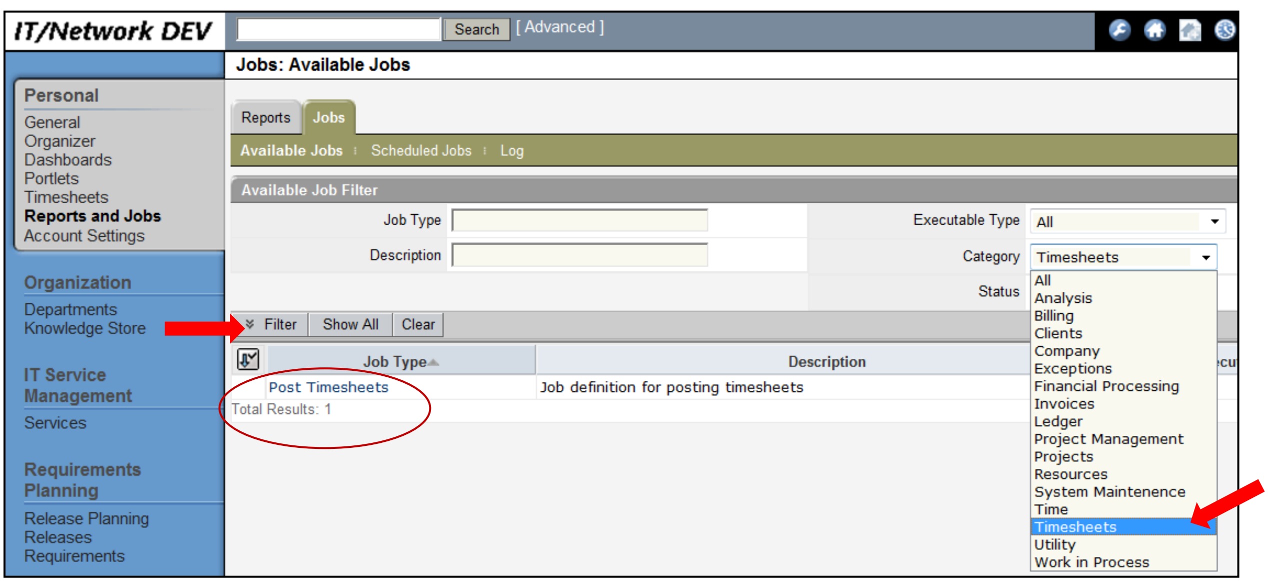
7.6.8.5.1 View by Executable Type

1. Click the down-arrow on the **Executable Type** multi-select box to display the menu.
2. Select the type of executable job you want to search for.
3. Click **Filter**.



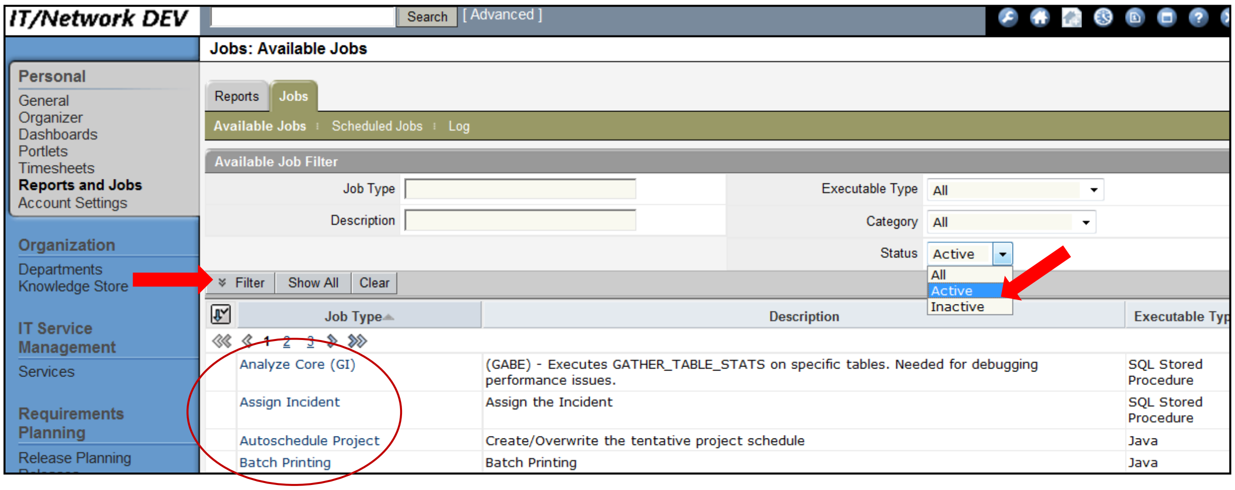
7.6.8.5.2 View by Category

1. Click the down-arrow on the **Category** multi-select box to display the menu.
2. Select the category you want to search for.
3. Click **Filter**.



7.6.8.5.3 View by Status

1. Click the down-arrow on the **Category** multi-select box to display the menu.
2. Select the category you want to search for.
3. Click **Filter**.



7.6.8.6 Viewing Report Library and Job Log

The **Report Library** page lists all generated reports that the user has access to view. The report instance is the output generated from a scheduled run. The **Job Log** page lists all jobs logs available for the user to view.

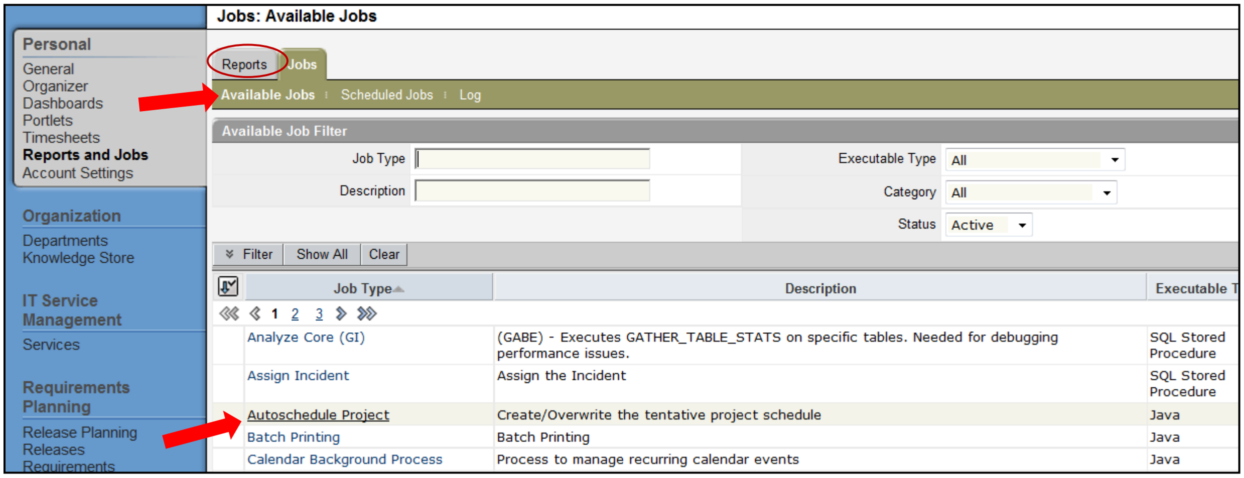
> ***Note:*** *You must set the job log option on the Job Definition page for the job log to generate.*

When the scheduled report or job run recurs, an instance of the report or job log is generated for each recurrence. For example, if a scheduled report run is set to recur monthly, then an instance of that report is created each month.

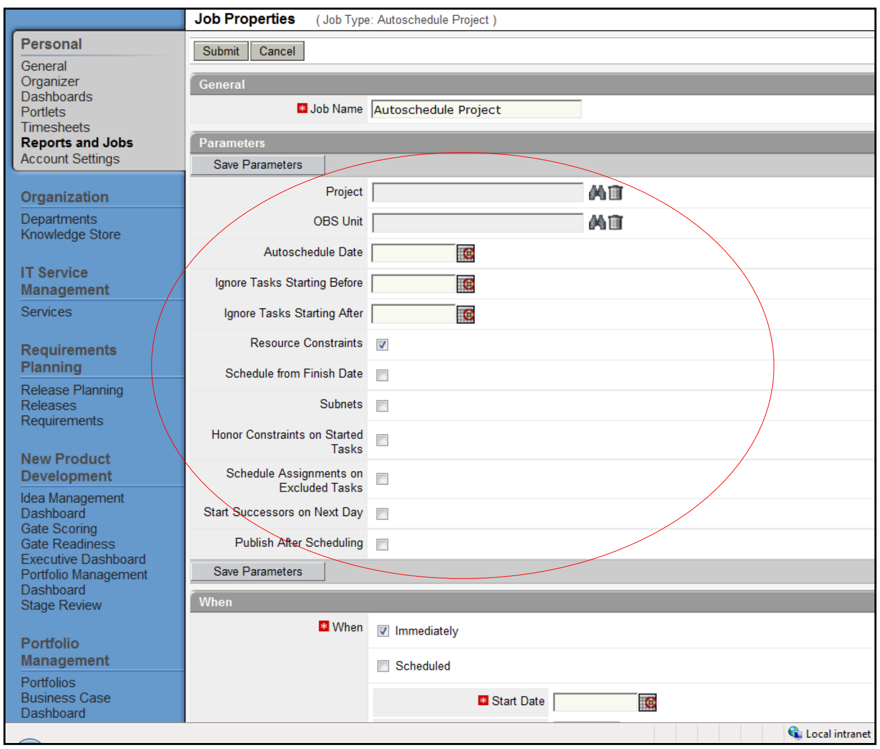
You can view reports that run immediately after they are generated. You also have the option to save and share reports and jobs with others. Job logs that run immediately or that are scheduled to run are stored in the job log upon completion.

7.6.9 Run or Schedule Jobs to Run

1. On the **Jobs: Available Jobs** page, click the **Available Jobs** subtab.



2. Click the **Job Type** link for the job you want to run or schedule to run and the **Job Properties** page displays.

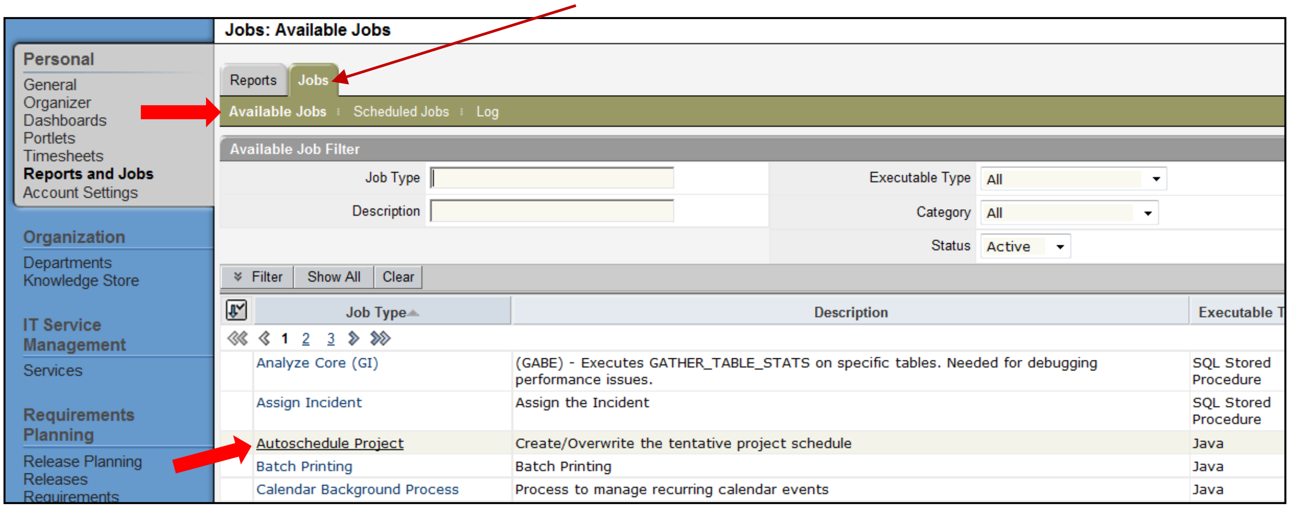


3. Define the job's run properties as needed and submit your changes to run the job immediately or at its scheduled time.

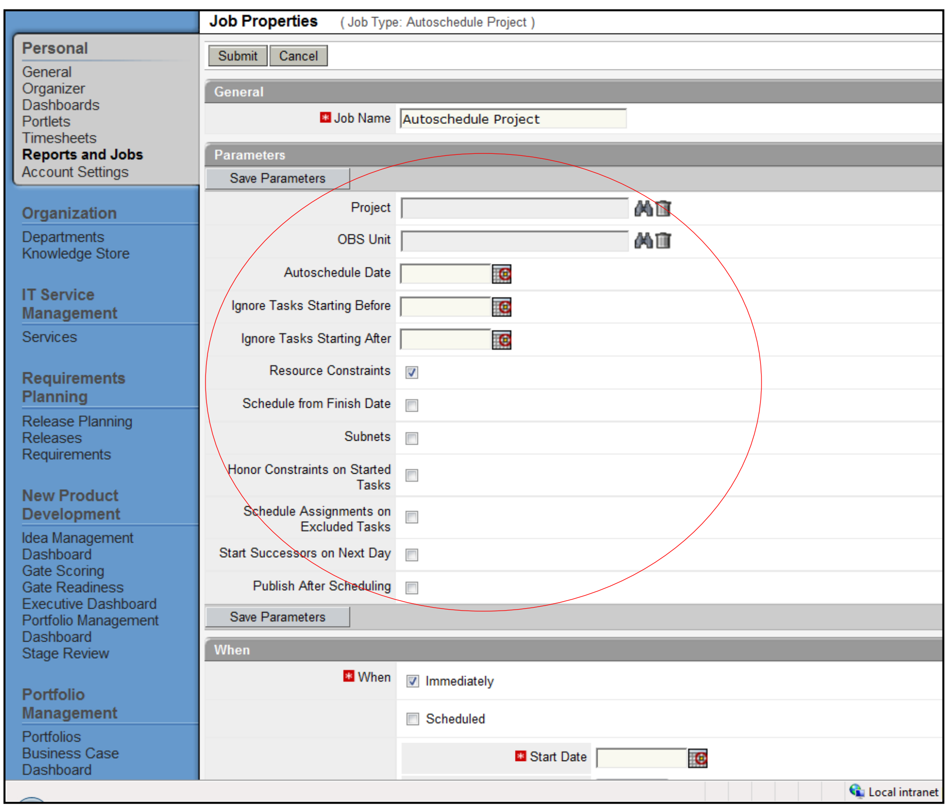
> ***Note:*** *For information on entering data on the Job Properties page, refer to* ***"Section 7.6.10 Edit Report Definition Properties"*** *below.*

7.6.10 Run or Schedule Reports to Run

2. On the **Jobs: Available Jobs** page, click the **Jobs** tab and the **Available Jobs** subtab.



3. Click the **Job Type** link for the job you want to run or schedule to run and the **Job Properties** page displays.



4. Define the job's run properties as needed and submit your changes to run the job immediately or at its scheduled time.