bmcsoftware

BMC Track-It!

Administrator's Guide

Version 11

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC™

www.bmc.com

Legal Notices

Restricted rights legend

Numara Software, Inc.
2202 North West Shore Blvd. Suite 650
Tampa, FL 33607 USA
800 557 3031
Customer Support: 800 836 2326 (United States and Canada) or contact your local support center.

Table of Contents

Welcome to BMC Track-It! 11 Technician Client

Notes:

- For help with online help and printed documentation, see Online Help and Guides (PDFs).
- The topics in the online help are also available in the printed versions (PDF) on the Product Documentation section of our Support Web page

---

BMC Track-It! Technician Client is a fully-integrated help desk and asset management solution designed for small to medium-sized businesses. BMC Track-It! enables specialized technicians to apply best practices and proactive management techniques for delivering advanced Help Desk and Asset Management services to the organization. BMC Track-It! delivers the automation and integrated tools necessary to cost-effectively manage IT assets and deliver superior end-user support.

For more information, please see the BMC Track-It! Overview (PDF).

BMC Track-It! 11 Administrator's Guide

Getting Help, Support, and Training

User Assistance (Online Help and Guides)

Note: The topics in the online help are also available in the following printed versions (PDF) on the Product Documentation section of our Support Web page at http://support.numarasoftware.com/support/updates.asp?product=2&content=Documentation&version=11&Offering=2&lang=EN

Product Documentation (PDFs)

- BMC Track-It! Administrator's Guide
- BMC Track-It! Technician's Guide
- BMC Track-It! Self Service Guide (for end users)
- BMC Track-It! Web Technician's Guide
- BMC Track-It! Mobile Web Technician's Guide
- System Requirements
- FAQs
- BMC Track-It! Installation Guide
- BMC Track-It! Bar Code Installation Guide
- BMC Remote Control 9.5 User's Guide
- Evaluation Guide

Note: If you are in a location where an internet connection is unavailable, you can install the BMC Track-It! help files (FlashHelp) on a local IIS server. See Installing Offline Help.

Track-It's online help system uses WebHelp, a Web-based help format. When you access a help topic in the BMC Track-It! application, either from the Help menu or from Help buttons, the help topics are delivered from the BMC Track-It! Web server to your Web browser (such as Internet Explorer). BMC Track-It! Mobile Web uses a mobile WebHelp, specially formatted for mobile screens.
To Use the BMC Track-It! Online Help:

1. Press the **F1** key, or select **BMC Track-It! Help** from the **Help** menu on Track-It's main menu bar.
   The **Help** dialog displays.
2. Enter your search terms in the **Search for:** text box, then click the **Search** button.

   Track-It's search engine searches not only the online help topics, but the KnowledgeBase on the BMC Track-It! Support Web page.

   Help topics are comprised of:

   - Overviews
   - Workflows
   - Getting up and running checklists
   - Procedural steps

   KnowledgeBase articles consist of:

   - Troubleshooting
   - Technical information
   - Specific how-to information based on customer requests

- Online tutorials (videos)

The matching Help topics (indicated by a round, blue icon) and KnowledgeBase articles (displayed by a square white icon) display on the **Search Results** pane.

3. Select a Help topic or KnowledgeBase article from the list.

   - To view the entire online help (FlashHelp), drag the Help dialog to the left or right until you can see the FlashHelp dialog (indicated by a blue toolbar).
   - KnowledgeBase articles from our Support page at www.numarasoftware.com/support.asp.

Installing Off-line Help (Local Files on Your IIS Server)

If you are in a location where an internet connection is unavailable, you can install BMC Track-It!'s help files (FlashHelp) on a local IIS server. You will, however, need a Web browser (such as Internet Explorer) to view the FlashHelp. Follow the instructions in our Support article "Track-It! Web Help is Not Configured Correctly".

Note: To return to using the online help from the BMC Software Web site after following the directions in the article above, restore the backed-up copies of the files (TrackIt.Application.AddIn.xml and Master.cfg) and restart the Web services and the BMC Track-It! Service Management service.

Customer Support and Resources

For information on BMC Software Maintenance and Support, please see our Web page at www.numarasoftware.com/support.asp.

For customers who have purchased a maintenance and support plan, you can log in to your account at www.numarasoftware.com/support/MySupport.asp. From there you can:

- Submit a request (eSubmission)
- Submit an incident against a known problem
- Request an enhancement to the product
- View enhancements previously submitted
- View the status of your submitted incident numbers
- Sign up for Webinars (live online training) to get up and running with BMC Track-It!
- View your recent KnowledgeBase searches and recently-viewed articles
- View new product documentation
- Exchange files with the technical support department

Accessing the BMC Software Support Web Page

In order to access the KnowledgeBase articles, user guide PDFs, and other documents on our Support Web page, a Support profile is required. Our Support Web site can only be accessed by customers who have created a support profile. You will need at least one product serial number for a BMC Software product you own. If you do not know your product serial number, you can find it in Help > About in BMC Track-It!.

To set up your Support profile:

1. Go to http://support.numarasoftware.com/support/login.asp.
2. Enter your **user name** and **password**, or click the **"Create a Support Profile" l**ink to create a new profile.
3. After logging in, select the **Profile** tab.
4. Verify that the **"Yes, remember my account information"** option is enabled.

Maintaining Registration Support and Licenses

The **Support Center** in the Administration Console enables you to maintain your BMC Track-It! registration/contact information, support plan, and licenses. You can also automatically renew your support plan and request additional licenses directly from the **Support Center** window.

Note: Only the BMC Track-It! administrator has access to the Support Center.

To Access the Support Center:

1. From the main menu bar, select **Tools/Administration Console/Administration/ Support Center**.
2. Click the **Support Center** button. The **Home** tab displays.
3. Your BMC Track-It! version, support and update information is displayed and is read only (cannot be edited).

Maintaining Your Registration/Contact Information

When you update your contact information, we are automatically notified via the internet.

To Maintain Your Contact Information:

1. Click the **View Details** hyperlink on the **Home** tab, or click the **Registration** tab.
2. The Ship To, Bill To, Billing Contact, and Support Contact tabs display. This is the information we will use to contact you.
3. To update your contact information, enter the information in the fields for all four tabs. All fields are editable except the Company Name.
4. If your shipping and billing information is the same, click the Bill to the Same Address check box.
5. To add your company's logo, click the **Add Your Logo** hyperlink.
6. Your logo must be in either of the following formats: BMP, ICO, WMF.
7. Select the image file from the **Logo Image** dialog.
8. Click the **Save Changes** button.

Maintaining Your Support Plan Information

Your support plan information is displayed listing the plan, expiration date, telephone number and e-mail address of your account representative, Knowledgebase subscription, and number of upgrades.

To Renew Your Support Contract:

1. On the **Registration** tab, click the hyperlink **Click Here to Renew Your Support Contract Today**!
   This will launch your e-mail editor with pre-populated information addressed to our account representatives.
2. Send the e-mail and your renewal request will be automatically processed.

Maintaining Your License Information

To View Your License Information:

1. Click the **Licensing** tab, or click the **View** hyperlink in the **License** area on the **Home** tab.
   The Licensing tab displays. A detailed description displays for each of your licensed Features

and Modules. The Owned column displays your number of licenses. The In Use column displays the number of licenses currently in use.

To Request a Quote for Additional Licenses:

1. Click the hyperlink **Click Here to Request a Quote for Additional Licensing**.
   Your e-mail editor launches and an e-mail message is automatically created.
2. Send the e-mail and your request will be sent directly to your sales representative, who will contact you as soon as possible.

Checking for Updates (New BMC Track-It! Releases)

The Check for Updates service will automatically download new releases and notify the selected Administrator when they are available. The updates can be accessed and installed through the Support Center.

To Check for Updates:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Administration/Check for Updates**.
3. Click the **Enabled** checkbox.
4. Enter the number of days from the current date to check for updates in the **Frequency** field.
5. Select the **Technician** to notify if updates are available.
6. If you want a **Work Order to be automatically created when updates are available**, click the designed checkbox.

   The date the last update check was run displayed in the **Last Run:** field. The date the next update will be run displays in the **Next Run:** field.

7. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Training and Professional Services

In addition to the user assistance Online Help and Guides (PDFs) and Customer Support, the following resources are available to help you learn how to use BMC Track-It!:

Subscription Online Training
Please visit our Web site for information on BMC Software Training .

Classroom and On-site Training
Please visit our Web site for information on BMC Software Training .

Professional Services
Please visit our Web site for information on BMC Software Professional Services Consulting
.

Installing BMC Track-It! Technician Client and BMC Track-It! Web

BMC Track-It! Installation Guides

Please see the PDF versions of the BMC Track-It! Technician Client and BMC Track-It! Web (including Mobile Web and Self Service Web) installation guides.

Migrating Data

Migrating data is not required in order to upgrade to BMC Track-It! 11. The upgrade is an in-place upgrade. Please see the PDF version of the BMC Track-It! 11 Updating Guide

Configuring BMC Track-It!

Keyboard Shortcuts (Administrators)

Administrators can access the Administration Console by pressing the F9 key while in the BMC Track-It! main window.

Getting up and Running with Advanced BMC Track-It! Help Desk and Asset Management Configuration

Once you have configured the basic BMC Track-It! help desk and asset management settings (in the previous topic), you can set up any of the following *advanced features*.

Advanced Technician Access Features

- Technicians' access to Track-It! data by module, technician, department, location and drop-down fields, can be controlled, and sensitive report information can be secured (Security Policies)

Advanced Help Desk Features

- **E-mails** sent to your Help Desk can be **automatically converted to work orders** (E-mail Monitor)
- **Specific technicians can be assigned to work orders** based on requestor, department, and/or work order types (Skill Routing Policies)
- **Technicians and/or users can be notified** of **work order events and escalations** (E-mail Monitor, Escalations, and Event Policies)
- **Users can receive notification of their work order status** via e-mail (E-mail Monitor)
- **Service Level Agreements** can be maintained with SLA document attachments and SLAs can be automatically assigned to work orders (Service Level Agreements)
- Technicians can be given **permission to edit Descriptions and Resolutions** in work orders (Journaling)
- Work Order drop-down options are populated with **customized lookup table values** (such as work order Priorities, Types, Resolution Codes, etc.) and work orders can contain **customized user-defined lookup drop-down fields**
- Technicians can create **work order templates**
- **Work order due dates can be automatically calculated**, and **notifications** and **escalations** can be processed based on specified help desk **operating hours**
- **End users can submit their own service requests**, check the **status** of their requests, and **search solutions** (**Track-It! Self Service**)
- Users can reset their own passwords and unlock their accounts (with **Password Reset,**

Advanced Asset Management Features

- Auditing
    - **Full hardware/software audits** can be performed
    - **Macintosh computers can be audited** (with the Mac Audit add-on module for Track-It!
    - The Track-It! **Agent icon can be hidden from users' task bars** while their computers are being audited, and can prompt the user to provide information **during the audit process**

    - The scheduled **audit queue can be managed (stop, suspend, clear audits**, etc.)
    - Perform **audit merges**
- Software License Management
    - **Software license usage and compliance** can be managed (with the Software License Management module)
- Bar Code
    - **Assets can be tracked using bar codes** and a scanner (with the Track-It! Bar Code module available as an add-on to Track-It!).

Configuring Advanced Features

☑	TASK	MODULE/WINDOW	HELP TOPIC
SET UP ADVANCED HELP DESK FEATURES			
	1. Set up advanced Help Desk data (Lookup tables)		
	a. Customized Lookup fields	Tools/Administration Console/Lookup Tables/Help Desk/Lookup#1 (through Lookup #8)	Creating Customized Lookup Fields for Work Orders
	b. Work Order Description Activity Codes	Tools/Administration Console/Lookup Tables/Help Desk/Work Order Description Activity Codes	Creating Work Order Description Activity Codes
	c. Work Order Technician Note Activity Codes	Tools/Administration Console/Lookup Tables/Help Desk/Technician Note Activity Codes	Creating Work Order Technician Note Activity Codes
	d. Work Order Resolution Codes	Tools/Administration Console/Lookup Tables/Help Desk/Resolution Codes	Creating Work Order Resolution Codes
	2. Enable Technicians to Append Description and Resolution Notes in Work Orders	Tools/Administration Console/Configuration/Help Desk/Journaling	Enabling Technicians to Append Description and Resolution Notes in Work Orders (Journaling)
	3. Set up Technician Security Policies (Control Technicians' access to BMC Track-It! data)	Tools/Administration Console/Lookup Tables/Administration/Security Policies	Introduction to Security Policies
	4. Configure E-mail Monitor and work order notifications	Various: see help individual topics	E-mail Monitor and Work Order Notifications Overview
	5. Set up work order Skill Routing Policies	Tools/Administration Console/Lookup Tables/Help Desk/Skill Routing Policies	Setting up Skill Routing Policies
	6. Set up Service Level Agreements (SLAs)	Tools/Administration Console/Lookup Tables/Help Desk/Service Level Agreements	Setting up Service Level Agreements (SLAs)
	7. Create work order Templates	From Help Desk Module: New Work Order/ Template icon on toolbar/Select Template/New	Creating Work Order Templates
SET UP BMC Track-It! WEB APPLICATIONS FOR YOUR HELP DESK			
	8. Configure Self Service (optional add-on module for end users)	Tools/Administration Console/Administration/Self Service	Track-It Self Service Overview
	10. Configure Password Reset	Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility >Track-It! Password Reset Administrator dialog > User Interface tab	Getting up and Running with BMC Track-It! Password Reset

☑	TASK	MODULE/WINDOW	HELP TOPIC
SET UP ADVANCED ASSET MANAGEMENT FEATURES			
	11. Set up advanced Auditing features		
	a. Configure full hardware/software audit scans	Inventory/ Auditing/Scan Settings/Windows Scan Criteria/Full Hardware/Software Scan	Configuring Full Hardware/Software Audit Scans
	b. Configure Auditing to capture specific files and run commands	Tools/Administration Console/Configuration/Inventory/ Auditing/ File Captures	Configuring Auditing to Capture Specific Files and Run Commands
	c. Configure user interaction during audits (such as prompting the user to provide information during the audit process)	Tools/Administration Console/Configuration/Inventory/ Auditing/User Interaction	Configuring User Interaction for Audits
	d. Display or hide the BMC Track-It! Agent icon on users' computers during audits	Tools/Administration Console/Administration/Track-It! Agent	Displaying the BMC Track-It! Agent Icon on Users' Computers
	e. Manage the scheduled audit queue (stop, suspend, clear audits, etc.)	Tools/Administration Console/Configuration/Inventory/ Auditing/Queue	Managing the Scheduled Audit Queue
	f. Configure audit merges	Tools/Administration Console/Configuration/Inventory/ Merging/Performance and Schedule	Configuring Audit Merges
	g. Configure auditing for Macintosh computers	Tools/Administration Console/Configuration/Inventory/ Auditing/Macintosh Settings	Mac Audit Overview
	12. Set up the Software License Management Module	Tools/Administration Console/Lookup Tables/Software License Management	Software License Management Workflow (Administrator)
	13. Install the BMC Track-It! Bar Code Solution	See the PDF version of the BMC Track-It! Bar Code Installation Guide (Select the BMC Track-It! version, then select BMC Track-It! Bar Code Installation Guide.)	Installing the BMC Track-It! Bar Code Solution
CONFIGURING THE USER INTERFACE			
	14. Set BMC Track-It!'s default language	Tools/Administration Console/Administration/Language	Setting the Default Language
	15. Change field label text and require fields	Press the **CTRL+F2** in a field label	Changing Field Label Text and Requiring Fields

Configuring the User Interface

Setting the Default Language

BMC Track-It! can be configured to run in several different languages. The language you select will be the default language that each technician will use. Technicians can override this setting to suit their personal preferences.

To Set the Default Language:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Administration/ Language**.
3. Select the language from the drop-down list.
4. Click the **Apply** button to save your changes, and the **OK** button to close the window.

See also: Setting User Preferences (Language, Start-up Module, and Password)

Changing Field Label Text and Requiring Fields

You can change the text of field labels in BMC Track-It! to fit your organization's needs. For example, in the Library module, you might want to change the label "Serial #" to "ISBN #".

Notes:

- Some fields are used in other areas of the application, such as the "Location" field. If you make a change, for example, to this field in the Library module, it will also change the field label wherever it displays in the application.

To Change Field Label Text and Require Fields:

1. Click in the field label (such as the label's text box), then press the **CTRL+F2** keys.
2. On the **Field Options** dialog, enter the new text for the label in the **Label** field.
3. To require users to enter a value in the field for the label, click the **Required** check box.
4. To enter a default value that will automatically display in the field, enter it in the **Default Value** field.
5. To set a maximum length (in characters), enter a number in the **Maximum Length** field.
6. Click the **OK** button.

To Restore the Default Label Text:

1. Click in the label field (such as the label's text box), then press the **CTRL+F2** keys.
2. Click the **Restore Label** button on the **Field Options** dialog.
3. Click the **OK** button.

Customizing Toolbars and Creating Toolbar Buttons

Technicians can customize toolbars and create toolbar buttons for BMC Track-It! modules and detail windows (such as the Work Order and Asset detail windows). Administrators can also globally customize the Help Desk module and Work Order detail toolbars so that all Technicians can use specific toolbar buttons. Toolbar buttons can be associated with batch or executable files, as well as URLs. For example, you can link the button to the BMC Track-It! Technician's Guide (PDF) on our Support Web page.

To Show or Hide a Toolbar:

1. Select the module for the toolbar you want to customize.

2. Right click anywhere on the toolbar and select or deselect the toolbar's name (such as Standard, Search, or Global).

To Customize a Toolbar:

1. Select the toolbar you want to customize.
2. Right click anywhere on the toolbar and select **Customize**.
3. On the **Customize Toolbar** dialog, select an item from the **Available Toolbar Items** list, then click the **Add** button to place it in the **Current Toolbar Items** list.
4. Click the **Move Up** or **Move Down** buttons to move the toolbar buttons to the left or right on the toolbar.
5. To remove a toolbar item from the toolbar, select the item from the **Current Toolbar Items** list, then click the **Remove** button.
6. When you're finished customizing the toolbar, click the **Accept** button.

Note: You can only edit customized buttons (see below).

To Create a Toolbar Button:

1. Select the module for the toolbar you want to customize.
2. Right click anywhere on the toolbar and select **Customize**.
3. On the **Customize Toolbar** dialog, select a toolbar (**Standard** or **Global**), then click the **New** button.
   Notes: Only Technicians with BMC Track-It! Administrator rights can customize global toolbars. Also, the Help Desk and Work Order global toolbars are independent of each other. If you want to add the same customized button, you will need to add it separately for both toolbars.
4. On the **Customize Toolbar Button** dialog, enter a name for the toolbar button in the **Name** field.
5. Enter descriptive text for the toolbar button in the **Tooltip** field.
   This will be displayed when Technicians mouse over the button.
6. Click the checkbox below the Tooltip textbox to display the Tooltip text with the tooltip's icon.
7. Click the **Select** button under **Display Icon** to define the button's icon.
   Note: If you select an application in the next step, the associated icon will automatically display. If you don't select an application, select a file type of .ico (16 x 16 pixels) for best results.
8. Click the **Ellipses** (...) button next to the **Path** text box to enter a URL, file path, or to select an executable or batch file.
9. Optional: You can enter parameters in the **Parameters** text box, or click the **Add Parameter** button to select them.
   The list of parameters are BMC Track-It! database fields, and are available for the Inventory and Help Desk toolbars so that you can use them with batch or executable files.
10. Click the **Save** button on the **Customize Toolbar Button** dialog.
11. To edit the button, select it, then click the **Edit** button. When finished, click the **Accept** button on the **Customize Toolbar** dialog.
    The new buttons now display on the toolbar.

Basic Configuration - Help Desk

Setting up Basic Help Desk Data (Lookup Tables)

Defining Work Order Priorities

Note: You can define Work Order Priorities from the **Administration Console** or from a Work Order in the **Help Desk** module. See **To Define Work Order Priorities**, below.

In order to logically and effectively manage your help desk work orders, you need to establish a system of Work Order Priorities. These are a set of values your technicians use to rate the importance of one work order versus another. We've found that most organizations that implement BMC Track-It! as their help desk system use the following Work Order Priorities:

Suggested Work Order Priorities

Work Order Priorities	**Suggested Resolution Time**
1 -- Urgent	4 hours, override hours of operation
2 -- High	1 day
3 -- Medium	2 days
4 -- Low	4 days
5 -- Project	Varies, depending on scope of project
6 -- Self Service	Technician is responsible for assigning a priority

Notice the numbers preceding the Work Order Priorities. The purpose of these prefixes is to allow BMC Track-It! to display a **sorted** list of Work Order Priorities based on the degree of urgency (rather than alphabetically), which makes it quicker and easier for your technicians to locate and assign a code from the drop-down list. The Project code is useful for prioritizing network upgrades and maintenance procedures. The Self Service Work Order Priority is initially used to set all work orders that are received from end-users to the same priority level. Later, your technicians can adjust the priority of each work order, based on your help desk policies.

As a general rule, you should not create too many Work Order Priorities because they'll confuse your technicians. Having too few Work Order Priorities, on the other hand, will make your help desk less efficient. The Work Order Priorities that we've suggested here seem to work well for most organizations.

To Define Work Order Priorities:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Work Order Priorities, c**lick the **Add** button.
2. From a Work Order in the **Help Desk** module, click the **Add** button next to the **Priority** drop-down.
   The **Work Order Priority** dialog displays.
3. In the **Description** field, enter a name for the Work Order Priority.
4. Click the **Save** button.

Defining Work Order Statuses

Note: You can define Work Order Statuses from the **Administration Console** or from a Work Order in the **Help Desk** module.

Work Order Statuses are used to classify the state of a Work Order. In BMC Track-It!, there are two default statuses for Work Orders: Open and Closed. You can define your own statuses (such as Pending) to help you differentiate Work Orders.
To Define Work Order Statuses:
From the Administration Console

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Work Order Statuses**.
2. Click the **Add** button.

From a Work Order in the Help Desk Module

1. Click the **Add** button next to the **Status** drop-down.

   The **Work Order Priority** dialog displays.

2. Click the **Add** button.
3. Enter a name in the **Status Name** text box on the **Work Order Status** dialog.
4. Select Open or Closed from the **System Type** drop-down.
5. Click the **Save** button.

.

Defining Work Order Types, Subtypes, and Categories

You can set up Work Order Types to differentiate Work Orders so that they can be assigned to specific technicians, sort and filter Work Orders in the Help Desk grid, and to create reports. You can also add Subtypes and Categories to Work Order Types.
To Define Work Order Types, Subtypes, and Categories:

1. From the main menu bar, select **Tools > Administration Console > Lookup Tables > Help Desk > Work Order Types**.
2. Click the **Add** button
3. To add a top-level Type, select **Add Type**.
   This adds a Work Order Type to the top level of the hierarchical tree view.
4. To add a **Subtype** to the top-level type, select the top-level type, click the **Add** button, then select **Add Subtype**.
5. To add a **Category** to the Subtype, select the **Subtype**, click the **Add** button, then select **Add Category**.
6. Click the **Save** button.

To Print the List of Work Order Types:

1. Right click on the **Work Order Types** panel, then select **Print**.
   The report displays in the Crystal Reports XI viewer.
2. Click the **Print** button on the viewer.
3. Select options from the **Print dialog**, then click **OK**.
   The report prints directly to your printer.

Departments

Departments are used in the Inventory, Help Desk, and Training modules in order to group users. Administrators can grant technicians security privileges by Departments. Additionally, reports can also be generated based on departments.
To Set up a Department:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Departments**.
2. On the **Departments** panel, click the **Add** button.
3. On the Departments dialog, enter information in the following fields:
    - Department
    - Department Number
    - Head (Department Head's User Name)
    - Location
    - Phone
    - Fax
    - Comments
4. Click the **Save** button to close the dialog.
5. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Setting up Department Numbers

Department Numbers can be assigned to Departments, and the same Department Number can be used for multiple Departments if necessary.
To Set up Department Numbers:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Department Numbers**.
2. On the **Department Numbers** panel, click the **Add** button.
3. On the **Department Numbers** dialog, enter the number.
4. Click the **Save** button to close the dialog.
5. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Setting up Locations

Locations are used to identify the physical location that a person occupies (e.g., Third Floor, Tampa, etc.).
To Set up Locations:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Locations**
2. On the **Locations** panel, click the **Add** button.
3. On the **Locations** dialog, enter the **Location Description**.
4. Click the **Save** button to close the dialog.
5. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Importing Users and Technicians with the Directory Importer

Directory Importer Overview

If your company is currently using a directory service, BMC Track-It! provides a simple way to import the directory data into BMC Track-It!. Directory Importer has the following features:

- Directory Importer works with both Microsoft's Active Directory® (AD) and with LDAP-compliant directories
- Directory Importer will check your directory service for new users and add them to the BMC Track-It! database as Users and/or Technicians
- Directory Importer will check your directory service for changes and apply updates to imported Users and Technicians
- When configuring Directory Importer you can specify what type of BMC Track-It! license will be allocated to the imported Technicians and Users
- You can run Directory Importer as-needed or set it to run on a schedule

You can set up Directory Importer by completing the following tasks, explained in detail in the next topics:

1. *Set up User and Technician groups in your directory service*
   It is recommended that you create new Track-It! Users and Technicians groups in your directory service to facilitate the configuration of Directory Importer.
2. Open the BMC Track-It! Administration Console and specify your directory service
3. Select the Technician groups to import and what type of license to allocate (Named or Concurrent) for access to BMC Track-It! Technician Client and BMC Track-It! Web
4. Select the User groups to import and which groups will be allocated Self Service Web licenses
5. Edit Field Mappings between your directory service and the BMC Track-It! database (optional)
6. Manually run Directory Importer or set up a recurring schedule

Once Directory Importer is run, the individual Technicians and Users can be viewed and edited from the lookup tables (see Viewing and Editing Technician Accounts and Viewing and Editing User Properties, and Viewing the Directory Importer Log).

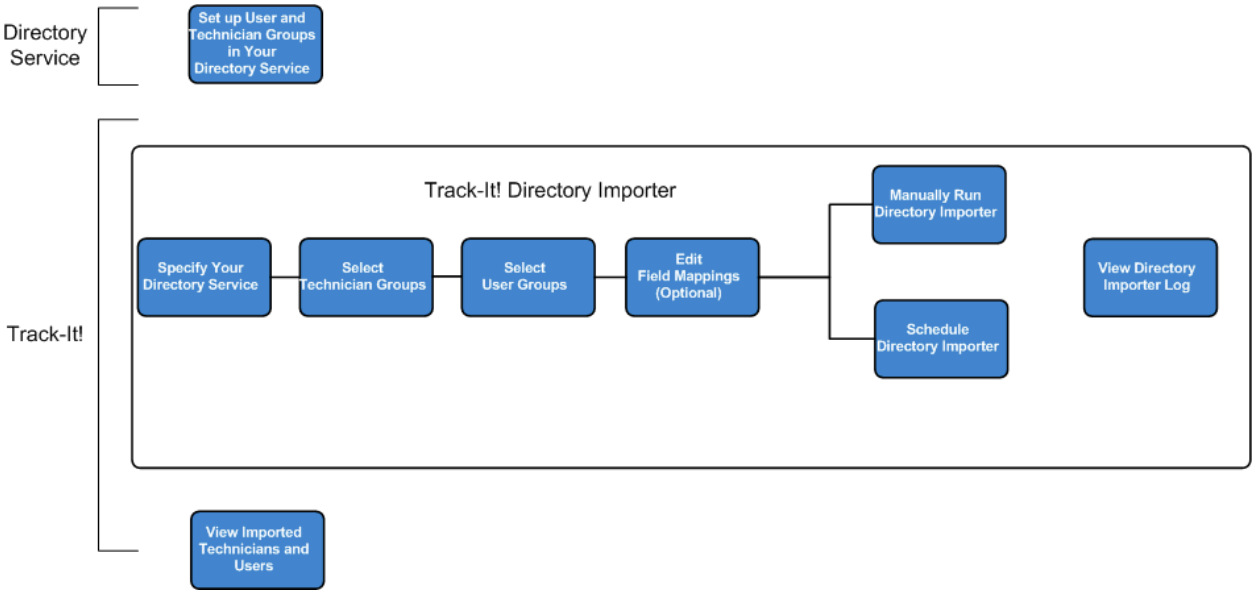
To Access the Directory Importer:

1. Select **Tools > Administration Console > Configuration > Administration > Directory Importer**.

Next Topic: Directory Importer Workflow

Directory Importer Workflow

The flowchart below represents the tasks in the topics for this chapter.



Next Topic: Specifying the Directory Service for Directory Importer

Configuring the Directory Importer

Specifying the Directory Service for Directory Importer

You can configure Directory Importer to use either a Microsoft Active Directory® or an LDAP-compliant directory.

Note: See our KnowledgeBase article on How to Configure Track-It! 9 Directory Importer to Import from More than One Directory or Directory.

To Specify the Directory Service for Directory Importer:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > Directory Importer > Directory Service**.
2. The **Microsoft Active Directory® service** option is enabled by default, and the domain name where the BMC Track-It! server is located displays. However, you can specify another domain name in the text box.
3. If you want to use **LDAP**:
    a. Select the **LDAP** server option.
    b. Enter the **path** for the LDAP server (e.g., LDAP://server:389).
    c. Click the **Refresh** button to view the list of Object Classes.
    d. Select or enter the **Object Class** (e.g., organizationalPerson) in the associated field.
4. If you don't want to use **anonymous access** for the directory service, deselect that option.
5. If you're using your credentials as opposed to anonymous access, enter your **User Name** and **Password** to log in to the directory service (domain name\user name). (You can click the **Browse** button to find your name).
6. Click the **Test Login** button to test your connection to the directory service.

7. Click the **Apply** button to save your changes.

Next Topic: Selecting Technician Groups from Your Directory Service

Selecting Technician Groups from Your Directory Service

You can import users and their information from your directory service and designate them as Technicians in BMC Track-It!. When selecting the Technician groups from your directory service, you can specify whether to allocate a **Named** or **Concurrent** Technician license, or skip license allocation and assign licenses via the Technicians lookup table at a later time. (A Technician license is required so that Technicians can log in to the **BMC Track-It! Technician Client** and **BMC Track-It! Web** applications.)

Once you select the Technician groups to import into BMC Track-It!, you can run the Directory Importer (see Scheduling and Manually Running the Directory Importer).

To Select Technician Groups from your Directory Service and Assign License Types:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > Directory Importer > Selection/Licensing > Technicians**.

   BMC Track-It! graphically displays the number of allocated (in use) and available **Named** Technician licenses and the number of allocated and owned **Concurrent** Technician licenses. Previously selected Technician groups display in the **Selected Groups** grid, as well as the types of licenses allocated to those groups.

2. Click the **Add** button on the **Technicians** panel.
3. Select the desired group of Technicians from the **Add Groups** dialog.

   You can also select individual Technicians, if desired.

4. Select **Named** or **Concurrent** license from the **Technician License Allocation** drop-down list, then click the **OK** button.
5. If you don't want to assign any licenses at this time, select the **"Skip"** option.

   Note: Directory Importer only sets the license during User and Technician creation; it does not change the license type of an existing User or Technician. You can assign or change Technicians' License Types later once the import is complete (see Viewing and Editing Technician Accounts).

6. Click the **OK** button on the **Add Groups** dialog, then click the **Apply** button on the **Technicians** panel of the **Administration Console**.

   Next, you'll need to run the Directory Importer to import the selected Technicians into BMC Track-It! (see Scheduling and Manually Running the Directory Importer).

Next Step: Scheduling and Manually Running the Directory Importer

Selecting User Groups from Your Directory Service

You can import users and their information from your directory service and designate them as Users in BMC Track-It!. When selecting the User groups from your directory service, you can specify whether to allocate a Self Service license, or skip license allocation for now and assign licenses via the Users lookup table at a later time.

Once you select the User groups to import into BMC Track-It!, you'll need to run the Directory Importer (see Scheduling and Manually Running the Directory Importer).

To Select User Groups from your Directory Service and Assign Self Service Licenses:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > Directory Importer > Selection/Licensing >Users**.
2. Click the **Add** button on the **Users** panel.
3. Select the desired group in your directory service from the **Add Groups** dialog.

   You can also select individual Users, if desired.

4. Select the **"Allocate a Self Service license..."** from the **Self-Service Allocation** drop-down list if you want the user group to be assigned a license to access Self Service Web.
5. If you don't want to assign any licenses at this time, select the **"Skip the allocation of licenses..."** option.

   You can assign Self Service licenses later once the import is complete (see Viewing and Editing User Properties).

6. Click the **OK** button on the **Add Groups** dialog, then click the **Apply** button on the **Users** panel of the **Administration Console**.

   Next, you'll need to run the Directory Importer to import the selected Users into BMC Track-It! (see Scheduling and Manually Running the Directory Importer).

To View the List of Users in a User Group:

1. Select the User group from the **Selected Groups** grid, then click the **Properties** button.

   The lists of child objects display (from your directory service). You can change the license allocation from here, if desired, to allocate a license or skip the allocation.

Next Step: Scheduling and Manually Running the Directory Importer

Editing Field Mapping for Directory Importer (Optional)

When Users and Technicians are imported with Directory Importer, the process uses specific attributes from your directory service that are mapped to BMC Track-It!'s Technician and User data.

You can use the default settings, or you can optionally specify the directory service attribute that you want to map to a BMC Track-It! User or Technician field (such as mapping the Microsoft Active Directory® "streetAddress" attribute to the "User Def. 1" Track It! field).

You can restore the default mapping at any time.

Notes:

- You may need to adjust the Field Mapping for the specific directory service selected on the Directory Service panel (see Specifying the Directory Service for Directory Importer).
- For LDAP, at least one Linking Field must be selected between BMC Track-It! and your directory service. For Microsoft Active Directory®, the Directory Importer will use the Security Identifier (SID) as the linking field.
- User Names

- When a new Technician or User is created, the password is blank by default.
- A Technician and User cannot share the same user name. If a Technician and a User are imported with the same user name, the Technician will keep that user name.
- If both the User name and Windows Account Name are imported, Self Service Web will first try to use the Windows Account Name to automatically log in.
- When a BMC Track-It! User is imported with a Windows Account Name and a Self Service license, the User can directly access Self Service Web using Windows authentication.

For advanced options, see Advanced Field Mapping (Directory Importer).

Field Mapping Limitations

Character String Length

- A field value may not exceed the size of the BMC Track-It! field to which it is mapped.
- A field value will be truncated to fit the mapped BMC Track-It! field.

Notes:
See the BMC Track-It! ERD (Entity Relationship Diagram) for column lengths.

To view the ERD:
1. Log in to your profile on our Support site at http://www.numarasoftware.com/support/Login.asp.
2. Click the **My Profile** link on the left.
3. Select the **Track-It!** tab, then click the **11 Data Model (PDF)** link under **Documents, Release Notes & What's New**.

To View and Edit Field Mapping for Directory Importer:
1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > Directory Importer > Field Mapping**.
2. To edit field mappings, select the field from the **Field Name** drop-down.
3. To use the field for **Users** or **Technicians**, click the associated check box (unless is it disabled).
4. Click the **Apply** button to save your changes.

To Restore Default Mapping:
1. Click the **Restore Default Mapping** button to return the mapping to its original state.

Related Topic: Advanced Field Mapping (Directory Importer)

Advanced Field Mapping (Directory Importer)

You can append static text to your directory fields so that they display in BMC Track-It! field values. Static text is text that remains constant and is not updated by Directory Importer. You can also combine static text with directory fields.

Static Text Limitations

- A static text value can contain any text character except open and closed brackets "[ ]" , and the plus sign "+". These are used to build the static text strings.
- Combinations of static text are also limited to the size of the BMC Track-It! field it is mapped to and will be truncated (see also Character_String_Length in the previous topic, Editing Field Mapping for Directory Importer (Optional)

To Append Static Text to a Field:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > Directory Importer > Field Mapping**.
2. In the **Field Name** text box, enter the static text between brackets, such as [text].

   To add spaces, include them between brackets, such as [ ].

3. Check the **Users** and/or **Technicians** check box.
4. Click the **Apply** button to save your changes.

Examples

Static Text Replacing Default Directory Field Values

In the example below, all of the BMC Track-It! Users are located in Tampa, FL, so the Administrator set up Field Mapping in BMC Track-It! and replaced the default Microsoft Active Directory® field "physicalDeliveryOfficeName" with the static text [Tampa, FL] Now the Location field for all Users in BMC Track-It! will show Tampa, FL.

BMC Track-It! Destination	**Directory Service Data Source**		**Mapping**	
Field Name		**Linking Field**	**Users**	**Technicians**
Location	[Tampa, FL]	☐	☑	☐

Static Text Combined with Default Directory Field Value

In the example below, the Administrator wanted the area code in addition to the telephone number to display in the Phone field of the Technicians' records in BMC Track-It!. The Administrator added the static text "813" to the default Microsoft directory field "telephoneNumber" so that it displays in BMC Track-It! as "813 227-5400".

BMC Track-It! Destination	**Directory Service Data Source**		**Mapping**	
Field Name		**Linking Field**	**Users**	**Technicians**
Comments	[813]+telephoneNumber	☐	☐	☑

Scheduling and Manually Running the Directory Importer

Once you've select the user groups from your directory service to import into BMC Track-It! as Users or Technicians, you'll need to run the Directory Importer, either manually or through scheduled imports.

You can schedule the Directory Importer to run once a day at a designated time or multiple times a day on a specified time interval (such as hourly).

To Run the Directory Importer:

1. To **schedule** the Directory Importer, select **Tools > Administration Console > Configuration > Administration > Directory Importer** from the main menu bar, then select **Automated Schedule**.
2. On the Automated Schedule panel, select one of the following options:

    - **Run the import process once a day...**, then enter a time, **OR**
    - **Run the import process based on this frequency** (the default is 1,440 minutes -- once per day)

4. To **manually** run the Directory Importer, click the **Import Now** button.
   The Directory Importer log displays details about the import process.

   Double click the "Info" event for the import process to view details such as the names and number of Technicians and Users that were imported.

Once the Directory Importer has been run:

- Any user attributes that have changed in your directory service (such as telephone number) will be automatically updated in BMC Track-It!
- New users added to your directory service will be automatically added to Track It!.
- If a Technician's or User's Microsoft network directory account is disabled and they were assigned a license, the license will automatically be revoked and made available for another Technician or User
- If the user is removed from the directory service, the corresponding Technician will still exist in BMC Track-It! and must be deleted in order to make the license available for other Technicians.

To View Imported Users and Technicians:

1. Click the **View all technicians** or **View all users** hyperlink.
   This will open the Technicians or Users lookup table. (See Viewing and Editing Technician Accounts).

See also: Viewing the Directory Importer Log

Viewing the Directory Importer Log

The Directory Importer Log displays the Date/Time, Event Type (Info, Status, or Error), and Summary of the Technicians and Users imported by Directory Importer. This includes the number of new and modified individual users that were imported, and any that failed to import.

To View, Print, or Export the Directory Importer Log:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > Directory Importer**.
2. Select **Automated Schedule**.
3. Double click the record (Error, Information, or Status) in the **Directory Importer Log** to view details.

The **Event Detail** dialog displays details for the Error, Information, or Status. For example, the "Info" event type with the summary "Import Process Completed for Directory Service" displays the number of Technicians and Users that were created, and existing Technicians and Users that were updated. The details display the user attributes that were either created or updated.

4. To copy the information, click the **Copy to Clipboard** button.
5. To print the information, see Printing Grid Contents.
6. To export the information, see Exporting Grid Contents
7. Click the **Close** button to return to the **Automated Schedule** panel.

To Purge the Directory Monitor Log Messages:

1. Click the **Purge Log** button.
2. Click the **Yes** button on the **Purge Confirmation** dialog.

   A message in the log will display the number of purged records.

Disabling Automatic Spell Checking for Work Order Notes

BMC Track-It! Administrators can disable automatic spell checking for Work Order notes. This can be done from the BMC Track-It! Server and will globally affect Technician Client installations.

Note: Once automatic spell checking is disabled, the F7 spell check feature will also be disabled. (See Spell Checking Work Order Notes in the Technician's Guide.)

To Disable Automatic Spell Checking:

1. Navigate to \\Program Files\BMC Software\Track-It!\Track-It! Services\ConfigurationData.
2. Open the BMC.TrackIt.Application.AddIn.xml configuration file in a text editor such as Notepad.
3. Locate the following code: <SpellCheckerEnabled>true</SpellCheckerEnabled>.
4. Change the SpellCheckerEnabled property to "false", then save and close the file.
5. Restart the BMC Track-It! Service Management service.
6. BMC Track-It! Technician Client will need to be closed and reopened to apply the change.

Now when a note is entered for a Work Order, the wavy red underlines will no longer display for misspelled words.

Setting Up Help Desk Operating Hours

The system uses Operating Hours to calculate due dates and to determine when Work Order notifications are sent.

To Setup Help Desk Operating Hours:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Help Desk/Operating Hours**.
2. Select the Start time from the **Start** drop-down list.
   The **Start** time denotes when your Help Desk opens for business. For a 24-hour work day, enter the following values: 12:01 AM through 11:59 PM. You can also use BMC Track-It! to help extend "working hours" if necessary. After-hours support means that your technicians are not in the office, but they can be reached by beeper or cell phone.
3. Select the End time from the **End** drop-down list.
   The **End** time denotes when your Help Desk closes for the day.
4. Click the check boxes next to the **days of the week** your Help Desk is open.
5. To enter holidays and other days when your Help Desk is scheduled to be closed, click the **Add** button.
   Note: You may have to enlarge the Administration Console window to see the **Add**, **Edit**, and **Delete** buttons.
6. On the **Configure Non-working Day** dialog, enter the **Date** and a **Description** of the day the Help Desk is closed (such as a specific holiday), then click the **OK** button.
7. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Distributing the BMC Track-It! Technician Client
(Configuration Wizard Step 2 of 3: Distributing Technician Client Applications)

BMC Track-It! Technicians can install the BMC Track-It! application by clicking on a link sent via e-mail from your Help Desk e-mail account.
To Distribute the BMC Track-It! Technician Client to Technicians:
(If you're using the **Configuration Wizard**, start with the screen: Step 2 of 3: Distribute Technician Client Applications.)

1. From the main menu bar, select **Tools/Administration Console/Administration/Distribute Technician Client.**

   The **Technician Client Click-Once** link is displayed.

2. Select the technician(s) from the **Available Technicians** list, then click the **Add** button. (You can select multiple technicians by holding the Shift or CTRL key as you select them). This places the technicians in the Technicians to Notify list.
3. Click the **Send E-mail** button.
4. On the **Enter E-mail Address** dialog, enter the e-mail address that was set up for your Help Desk e-mail account (e.g. help@yourcompany.com, then click the **OK** button.

   The selected Technicians will receive an e-mail with a link so that they can install the BMC Track-It! Technician Client.

Viewing, Editing, and Manually Adding Technicians

Viewing and Editing Technician Accounts

Once you have either imported Technician groups from your directory service using Directory Importer (see Selecting Technician Groups from Your Directory Service) or manually added Technician accounts (see Manually Adding Technician Accounts, you can edit them from the Technicians panel in the Administration Console. The following describes editing a Technician's contact and account information, including licenses. To edit Escalations, Notifications, or Security, see the links at the bottom of this topic.

To Edit Technician Accounts:

1. From the main menu bar, select **Tools > Administration Console > Lookup Tables > Administration > Technicians**.
   (From the **Help Desk** module, you can select **Technicians** from the **See Also** pane).

   The following Technician licensing information is displayed for the license types your organization owns:

   - The number of allocated (in use) and available **Named** Technician licenses is displayed. The number of allocated licenses are those that have been assigned to Technicians. Available licenses are also displayed.
   - The number of allocated and owned **Concurrent** Technician licenses is also displayed.

Assigning Technician Licences from the Grid List

1. To quickly assign a license or change the **License Type** for one or multiple Technicians at a time, select the **Technicians** in the grid, then right click and select **Technician Licensing**, then select the License Type (**Named**, **Concurrent**, or **None - No Access**).

   A **Results** log displays the new License Type, and notifies you if there were any problems assigning the license.

   Note: The currently logged in Technician will not be able to set their own license type to None (to prevent locking themselves out of the Technician Client).

Editing a Technician's Attributes

Attributes include Name, Title, Phone, Extension, Department, Department Number, and other custom fields.

Important Note: Field values in italics* (such as Department: *Accounting*) are managed by the Directory Importer and should not be directly modified in BMC Track-It!. Modifications to managed items should only occur in the directory service. The information can be entered, but when the Directory Importer is run and any of the Technician fields have changed, these values will be replaced by those existing in your directory service.

*The italics only display if you have a license for scheduled imports and the Automated Schedule is enabled in the Directory Importer (see Scheduling the Directory Importer in the Administrator's Guide.

1. Select the Technician and click the **Edit** button.
2. On the **General** tab of the **Technicians** dialog, edit the **Contact Information** for the Technician.

Editing a Technician's Account Information (Configuring Login Information)

This includes User Name, Password, Login using Windows authentication, Hourly Rate, License Type, and Account Status (Locked/Not in Use).

1. To allow the Technician to log in to BMC Track-It!, enter a **User Name** and **Password** in the **Account Information Section**.
2. To allow the Technician to log in using Windows authentication:
   a. Select the **User can log in using Windows authentication with the following account** check box.
   b. In the **Windows Account Name** field, enter the **domain name**, followed by a backslash (\), and the user's Windows username (for example, **DOMAIN1\mfranklin**).

      For detailed instructions on configuring Windows authentication, see our KnowledgeBase article: Windows authentication for technicians in Track-It! 11.
3. (*Optional*) If you are tracking expenses, enter the **Hourly Rate** for the technician in the designated field.
   The hourly rate entered will be used to automatically calculate charges in the Billing Information section of the Resolution tab for a Work Order.
4. Select the **License Type**, select a type (Named User, Concurrent, or None - No Access).
5. Click **Save**.

See the following for detailed instructions on editing a Technician's Account with the Escalation, Notification, and Security tabs on the Technician dialog:

Manually Adding Technician Accounts
Designating a Technician for Work Order Escalations
Setting the Technician's E-mail Address for Notifications
Creating Custom Security Policies

Manually Adding Technicians

The most efficient way to add Technicians to BMC Track-It! is by importing them as a group from your directory service with the Directory Importer. (See Selecting Technician Groups from Your Directory Service.) However, you can manually add a Technician, if desired.

To Manually Add a Technician:

1. From the main menu bar, select **Tools > Administration Console > Lookup Tables > Administration > Technicians**.
   (From the **Help Desk** module, select **Technicians** from the **See Also** pane).
2. Click the **Add** button.

Editing a Technician's Attributes

Attributes include Name, Title, Phone, Extension, Department, Department Number, and other custom fields.

Important Note: Field values in italics* (such as Department: *Accounting*) are managed by the Directory Importer and should not be directly modified in BMC Track-It!. Modifications to managed items should only occur in the directory service. The information can be entered, but when the Directory Importer is run and any of the Technician fields have changed, these values will be replaced by those existing in your directory service.

*The italics only display if you have a license for scheduled imports and the Automated Schedule is enabled in the Directory Importer (see Scheduling the Directory Importer in the Administrator's Guide.

1. Select the Technician and click the **Edit** button.
2. On the **General** tab of the **Technicians** dialog, edit the **Contact Information** for the Technician.

Editing a Technician's Account Information

This includes User Name, Password, Login using Windows authentication, Hourly Rate, License Type, and Account Status (Locked/Not in Use).

1. To allow the technician to log in to BMC Track-It!, enter a **User Name** and **Password** in the **Account Information** section.
2. To allow the Technician to log in using Windows authentication, see Configuring Windows Passthrough Authentication for Technicians.
3. (*Optional*) If you are tracking expenses, enter the **Hourly Rate** for the technician in the designated field.
   The hourly rate entered will be used to automatically calculate charges in the Billing Information section of the Resolution tab for a Work Order.
4. Select the type of license for the technician from the **License Type** drop-down (Named User, Concurrent, or None - No Access).

5. Click the **Save** button.

See the following for detailed instructions on editing a Technician's Account with the Escalation, Notification, and Security tabs on the Technician dialog:

Editing Technician Accounts
Designating a Technician for Work Order Escalations
Setting the Technician's E-mail Address for Notifications
Creating Custom Security Policies

Viewing, Editing, and Manually Adding Users

Viewing and Editing User Properties

Once you have either imported User groups from your directory service using Directory Importer or manually added Users, you can edit them from the Users panel in the Administration Console. The following describes editing a User's contact and account information including Self Service licensing, associating assets to a User, adding the User's photo; and viewing training information.
To Edit User Properties:

1. From the main menu bar, select **Tools > Administration Console > Lookup Tables > Administration > Users**.

Assigning Self Service Licenses

The most efficient way to assign Self Service licenses to Users is with the BMC Track-It! Directory Importer (see Selecting User Groups from Your Directory Service), where you can select to automatically assign Self Service licenses when new users are added to BMC Track-It!. However, you can also manually assign Self Service licenses to multiple users at a time from the Users lookup table or assign individual Users on the Users dialog.

Note: It is not necessary for Change Management Approvers to have a license to use BMC Track-It! Self Service; their BMC Track-It! Administrator only needs to provide them with a login user name.
To Assign Self Service Licenses to Multiple Users at a Time:

1. To quickly assign a **Self Service License** for one or several Users at a time, select the **Users** in the grid, then right click and select **Self Service Licensing**, then select **Include**.

   You can select **Exclude** to remove a Self Service License from a User.

   A **Results** log displays the license assignment and notifies you if there were any problems assigning the license.

To Grant Users Access to Self-Service Web and Configure Login Information:

1. Double click the **User's name** in the grid.
2. On the **Web Access** tab of the **Edit User** dialog, enter a **User Name** and **password** in the designated fields, or see Step 5 below to select an existing Windows account.
3. To disallow the user from changing passwords, select the **User cannot change password** checkbox.
4. If you are *not* using Windows Authentication, you can require the user to change the password at the next login. Select the **User must change password at next login** checkbox.

5. To enable the user to login with their existing Windows account, select the **User can login using Windows authentication with the following account** checkbox, then click the Ellipses (...) button next to the **Windows Account Name** field to open the **Select Account** window. Select the user name and click the **Add** button.

   For details, including how to configure pass through authentication, see our KnowledgeBase article: New Windows pass through authentication for Self Service users.
6. Click the **Access to Self-Service Web** check box (*not* required for Change Management Approvers: only a login User Name is required).
7. Click the **Save** button.

See also: Manually Adding Users

Editing a User's Attributes

Important Note: Field values in italics* (such as Department: *Accounting*) are managed by the Directory Importer and should not be directly modified in BMC Track-It!. Modifications to managed items should only occur in the directory service. The information can be entered, but when the Directory Importer is run and any of the User fields have changed, these values will be replaced by those existing in your directory service.

*The italics display if you have a license for scheduled imports and the Automated Schedule is enabled in the Directory Importer (see Scheduling and Manually Running the Directory Importer in the Administrator's Guide.

1. Select the User and click the **Edit** button.
2. On the **General** tab of the **Edit User** dialog, edit or enter the **Contact and Regional** information.
3. Click the **Save** button.

The User information (Full Name, Title, Phone, etc.) display in the grid on the Users panel.

Associating Assets with a User

To Associate an Asset with a User:
1. On the **Assets** tab, click the **Add** button.
2. The **Search** dialog displays. Enter the first four characters of the Asset Name or Asset ID in the Search for: field, then click the **Search** button.
3. Select the asset from the search results, then click the **Select** button.
4. Click the **Save** button.

Changing a User's Photo

To Change the User's Photo:
1. On the **Graphic** tab, click the Browse button to navigate to a file (such as .bmp or .jpg).
2. Click the **Save** button.

Viewing Training Information

You can view Training information (courses set up for individuals) on the Course History tab. See Tracking Training for Individuals in Your Organization in the Technician's Guide for details on Training.
To View Course Histories for an Individual:

1. Select the **Course History** tab
   The list of scheduled courses for the individual is displayed.
2. Double click a course to view details.

See also: Manually Adding Users

Manually Adding Users

The most efficient way to add Users to BMC Track-It! is by importing them as a group from your directory service with the Directory Importer. (See Selecting User Groups for Directory Importer) However, you can manually add a User including contact and Self Service licensing information.
To Manually Add Users:

1. From the main menu bar, select **Tools > Administration Console > Lookup Tables > Administration > Users**.
   (From the **Help Desk** module, select **Users** from the **See Also** pane).

2. Click the **Add** button.
3. On the **General** tab of the **Edit User** dialog, enter information in the following fields:

   Important Note: Field values in italics* (such as Department: *Accounting*) are managed by the Directory Importer and should not be directly modified in BMC Track-It!. Modifications to managed items should only occur in the directory service. The information can be entered, but when the Directory Importer is run and any of the User fields have changed, these values will be replaced by those existing in your directory service.

   *The italics display if you have a license for scheduled imports and the Automated Schedule is enabled in the Directory Importer (see Scheduling and Manually Running the Directory Importer in the Administrator's Guide.

4. To grant users to access to Self Service Web, see Viewing and Editing User Properties
5. Click the **Save** button.

Adding the User's Photo

To Add the User's Photo:

1. On the **Graphic** tab, click the Browse button to navigate to a file (such as .bmp or .jpg).
2. Click the **Save** button.

See also: Editing User Properties and Viewing and Editing User Properties

Advanced Configuration - Help Desk

Setting up Advanced Work Order Lookup Tables

Creating Customized Lookup Fields for Work Orders

Lookups are the eight customized fields that display on the **Classification and Schedule** tab for Work Orders.

To Create Customized Lookup Fields for Work Orders:

1. From Track-It!'s main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Lookup#1 (through Lookup #8).**
2. Click the **Add** button.
3. Enter a description in the **Name** text box on the **User Lookup** dialog, then click the **Save** button.

Creating Work Order Description Activity Codes

Work Order Description Activity Codes are used to categorize Work Order Descriptions.

To Create Work Order Description Activity Codes:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Work Order Description Activity Codes**.
2. Click the **Add** button.
3. Enter a description in the **Name** text box on the **Work Order Description Activity Code** dialog, then click the **Save** button.

Creating Technician Note Activity Codes

Technician Note Activity Codes are used to categorize Work Order Technician notes.

To Create a Technician Note Activity Code:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Technician Note Activity Codes**.
2. Click the **Add** button.
3. Enter a description in the **Name** text box on the **Technician Note Activity Code** dialog, then click the **Save** button.

Creating Resolution Codes

Resolution Codes are used to categorize Work Order Resolutions.

To Create a Resolution Code:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Resolution Codes**.

2. Click the **Add** button.
3. Enter a description in the **Name** text box on the **Resolution Code** dialog, then click the **Save** button.

Enabling Technicians to Append Description and Resolution Notes in Work Orders (Journaling)

Journaling enables you to control the changes Technicians make to the Description and Resolution notes in Work Orders. When Journaling is enabled, data can be appended, but not deleted. By default, the Journaling feature is enabled. When Journaling is disabled, users cannot edit Description or Resolution Notes.

To Enable Technicians to Append Description and Resolution Notes in Work Orders:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Help Desk/Journaling**.
2. To disable the Journaling feature, make sure the check box is not selected.
3. Set **New at top** or **New at bottom** to determine the order in which new entries are displayed when technicians add to Description and Resolution notes in Work Orders.
4. Click the **Apply** button to save your changes, and the **OK** button to close the window.

   Now Technicians will be able to edit Description and Resolution notes in Work Orders.

Note: If this option is changed for existing Work Orders, you may have to manually adjust the chronological order of current data entries.

Setting up Technician Security Policies

Security Policies Overview

Introduction to Security Policies

In BMC Track-It!, people are categorized into two main groups: technicians and users. BMC Track-It! technicians can include help desk technicians, help desk analysts, managers, purchasing agents, trainers, accountants, executives, and anyone else who is responsible for entering or analyzing data. The definition of technicians can be as narrow or as broad as the number of different types of people in your organization who are authorized to view, enter, and manipulate data through BMC Track-It!'s security model.

The term "users" refers to everyone else. Users are the people who use the assets listed in BMC Track-It!'s Inventory module. They are the people who call the help desk for support in the form of problems, requests, and questions. **Users are not granted BMC Track-It! security privileges**, because they don't have the ability to directly access any of the modules. Their access points are limited to verbal requests, e-mail requests, and the Self Service Web requests.

- **There are** two security policies (Default and Administrator) that are installed with the application. You can add additional security policies.

Next topic: BMC Track-It! Role-Based Security Model

BMC Track-It! Role-Based Security Model

BMC Track-It! implements a multilevel, role-based security model, built around modules, locations, departments, and assigned technicians. Security becomes increasingly restrictive when you assign module-based privileges, and can be tightened farther by removing permissions based on locations, departments, and assigned technicians.

There are two distinct aspects of BMC Track-It! security: what technicians can see (data) and what technicians can do (functionality). The ability to define roles provides granular access to data and functionality. A security template contains these permissions and controls the things technicians can see and do in the application. By modifying privileges in a security template, technicians will experience a more restricted list of items in drop-down lists and will be able to perform fewer operations. The extent to which these restrictions are implemented is fully customizable based on your requirements.

- There are two security policies (Default and Administrator) that are installed with the application. You can create additional security policies.
- Administrators can customize drop-down edit privileges.

Next topic: BMC Track-It! Technician Roles

BMC Track-It! Technician Roles

A role is a collection of **privileges** that are granted to BMC Track-It! technicians. Each role may have a unique set of characteristics, tailored specifically to meet the needs of the BMC Track-It! technicians who play that particular role in your organization.

There are two existing security policies (Default and Administrator) that are installed with the application. You can create additional security policies.

Example of BMC Track-It! Roles

> Suppose, for example, a BMC Track-It! administrator identifies two roles for BMC Track-It! technicians: one role is called **Executives** and the other is called **Purchasing Agents.** The administrator then creates BMC Track-It! **security policies** that correspond to each of these roles.
>
> The following month, Dave Miller is hired as the new CEO. He wants to be aware of everything that happens in his organization, but he only wants to be able to view **Inventory**, **Purchasing**, **Help Desk**, and **Library** information. Like many of the other executives, Dave doesn't want to risk accidentally deleting or changing any information, so he asks his BMC Track-It! administrator to give him limited access to the database. Having received similar requests from other executives in the past, the BMC Track-It! administrator simply adds Dave Miller's name to the Executives security policy that already exists.
>
> Tom Smith is a member of the Accounting department in Boston, and his job description requires him to assume a **Purchasing** Agents role. Cheryl Thomas' job description also includes the Purchasing Agents role, so the administrator assigns both Cheryl and Tom to the Purchasing Agents security policy, regardless of the fact that they are members of different departments. In this example, the department and location have no bearing on who is assigned to the Purchasing Agents policy. However, in other companies, the administrator may choose to exclude certain technicians from the Purchasing Agents role, depending on which department or location they belong to. For example, an administrator might grant Tom Smith full control of the **Purchasing** module because he is located in Boston (this location processes all purchase orders). Cheryl Thomas might only be granted permission to view the

contents of the Purchasing module because she is located in Tampa. It's important to remember that one technician can only be assigned to one security policy.

Role-Based Security Policies

There are two security policies available when BMC Track-It! is installed: *Default* and *Administrator*. Custom Security Policies can be created with BMC Track-It!. Both policies initially allow access and full control for every module and feature within the application. The Administrator can then assign access and permissions (Full Control, Add, View, Delete and Edit) for each module and then assign technicians to the default security policy.

Notes:

- Technicians can be assigned to only one security policy at a time.
- BMC Track-It! includes two security policies (Default and Administrator) that are installed with the application. You can create additional security policies.

The fundamental concept in a role-based security policy is that of a privilege. The following privileges are pre-defined on a system-wide basis during setup:

- Full Control (Add, View, Delete and Edit)
- View
- Edit
- Delete
- Add (only available on the module level)
- Access to Tools/Administration Console and Configuration Wizard
- Drop-down Edit (making restrictions by location, department, or assigned technician will affect what technicians will be able to do with their drop-down Edit privileges)

Security privileges can be assigned in the Technician's dialog or at the security policy level (Define Security Policies dialog, above).
Modifying Security Policies
If your privacy policy changes (in many organizations, it changes periodically), the access rules need to be changed in only one central place, making BMC Track-It! a cost-effective solution.

If the administrator modifies a security policy, such as removing Inventory privileges, this will cause the privileges to be changed for each technician that has been assigned to that particular policy.
Modifying Policies Example:
Suppose, for example, Frank is assigned to the Help Desk Technician policy, which grants permission to delete work orders. However, the help desk analyst doesn't want Frank to be able to delete work orders. As a result, the administrator either needs to modify the Help Desk Technician policy to prevent the ability to delete records, or create a custom security policy with these specific security rights, then add Frank to the new policy. Alternatively, the administrator could create a custom policy for Frank in the Technician's dialog.

Next topic: Administrative Security Policy

Administrative Security Policy

In addition to granting full control over all modules, the Admin security policy allows Track-It! administrators to:

- manage technician accounts
- add entries for data entry fields, which allows technicians to select items from drop-down lists (speeds data entry and improves the integrity of reports by forcing technicians to use standard terms)
- manage performance settings for each module
- define field options as default
- auto-populate specific fields
- make certain fields required
- setup auditing and scheduling parameters

Next topic: Default Security Policy

Default Security Policy

The BMC Track-It! Default security policy provides all BMC Track-It! technicians with full control privileges over every module, including administrative privileges. It is highly recommended that you remove administrative privileges from the Default policy before assigning it to any technicians.

There are two existing security policies (Default and Administrator) that are installed with the application. You can add additional security policies.

Next topic: Creating Custom Security Policies

Creating Custom Security Policies

Creating Custom Security Policies Overview

BMC Track-It! is installed with a Default Security Policy that allows everyone full control over every module and feature within the application. Keep in mind that this default policy is provided only as a convenience to get you started. In most cases, full control should only be given to a select group of BMC Track-It! technicians. New (custom) policies should be created and modified based on your technician groups' particular access requirements. After your security policies have been created, you can assign technicians to the appropriate groups. If more specific changes are required, you can create a custom security policy for each BMC Track-It! technician who doesn't fit into one of your predefined roles. Suppose, for example, your Help Desk Analyst needs to be able to view and edit information in the Inventory module, but not be able to add or delete information. Allowing full control to the Auditing and Graphs modules will allow an analyst to perform an audit and merge the audit data, while he or she is supporting a user on the phone and viewing graphs.

When setting up BMC Track-It! security policies, keep in mind that you're building templates that will be used to expedite the creation of accounts for other technicians with similar security settings. The following table lists sample privileges for selected roles. The roles and privileges that you choose to define may be different from those listed in the table, depending on the structure of your organization.

Important Notes:

- The default policy is only provided as a convenience. In most cases, full control should only be granted to a select group of BMC Track-It! technicians.

- If technicians are currently assigned to a particular security policy, that policy cannot be deleted.

BMC Track-It! Modules/Features versus Sample Privileges

	Sample Privileges for Selected Roles		
BMC Track-It! Module or Feature	**First-Tier Technician**	**Second-Tier Technician**	**Middle Manager**
Inventory	View	View, Edit, Add	Full Control
Purchasing	None	None	Full Control
Help Desk	Add	View, Edit, Add	Full Control
Training	View, Edit, Add	None	Full Control
Library	View, Edit, Add	None	Full Control
Reports	None	None	Full Control
Graphs	None	None	Full Control
Auditing	None	None	Full Control
Administration	None	None	None
drop-down Edit	Disabled	Enabled	Enabled

To Create a Custom Security Policy:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Security Policies**.
2. Click the **Add** button to add a new security policy.
3. In the **Define Security Dialog**, enter a **Policy Name**.
4. Enter a **Policy Description**.
5. Click the **Save** button, and continue with the next topic.

See the next topics on Assigning Technicians and Restricting Privileges by Module, Location, Department, and Assigned Technician.

Next topic: Restricting Privileges by Module

Assigning Technicians to Security Policies

Previous Topic: Creating Custom Security Policies

You can assign technicians to a Security Policy from the Security Policies panel or from the Technicians panel in the Administration Console.

To Assign a Technician to a Security Policy (Security Policies Panel):

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Security Policies**.
2. Double click to open the Security Policy, or select the policy, then click the **Select** button.
3. On the **Define Security Policy** dialog, click the **Assign Technicians** button.

4. On the **Assign Technicians to Policy** dialog, select a technician or group from the **Available Technicians** list, then click the **Add** button to add them to the **Policy Members** list.
5. Click the **OK** button.

To Assign a Technician to a Security Policy (Technicians Panel):

1. From the main menu bar, select **Tools//Administration Console/Lookup Tables/Administration/Security Policies**.
2. Double click to select the **Technician**, or click the **Select** button.
3. On the **Security** tab, select the **Security Policy** from the drop-down list.
4. See Restricting Privileges by Assigned Technician for detailed instructions on the next step.
5. Click the **Save** button.

Restricting Privileges by Module (Security Policies)

Previous Topic: Creating Custom Security Policies

Note: BMC Track-It! includes two security policies (Default and Administrator) that are installed with the application. You can create additional security policies.

Caution: Report row-level security is not implemented for the **Dashboard** module (graphs and pivot grids). If your Technicians have access to the Dashboard module, they will be able to view all System Dashboard graphs and pivot grids, as well as the two default Dashboard graphs (Overdue Work Orders and Work Order Activity This Month) on their **Home Page**. To set Dashboard security, see below.

At the highest level, BMC Track-It! allows you to restrict security privileges by module.
Example:

Suppose, for example, you decide to create a custom security policy called Help Desk Technician. In this policy, you want your technicians to be able to view existing work orders and also be able to make changes to their own work orders. So, you grant view and edit privileges to the Help Desk module.

If this were a new BMC Track-It! installation with no security restrictions in place, BMC Track-It! would grant your technicians view and edit privileges for all new work orders. However, for the purpose of this example, several work orders already exist in this database and a view-only permission was previously established by another restriction (e.g., location, department, or assigned technician) for Work Order #2. Consequently, BMC Track-It! will respect the view-only permission (most restrictive, in this case) that had been previously applied.
To Restrict Privileges by Module:
(Continued from Creating Custom Security Policies)

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Security Policies**.
2. Double click to open the Security Policy, or select the policy, then click the **Select** button.
3. To allow or deny privileges, select the **Modules** tab, then click the check box in the **Allow** column next to the module that you want to change.
4. Click the **Save** button.

Next topic: Restricting Privileges by Location

Restricting Privileges by Location (Security Policies)

Previous Topic: Restricting Privileges by Module

At the next level of granularity, BMC Track-It! allows you to restrict security privileges by location.
Note: BMC Track-It! includes two security policies (Default and Administrator) that are installed with the application. You can create additional security policies.
Example

Suppose, for example, you decide to create a custom security policy called Help Desk Technician. In this policy, you want your technicians to be able to view existing work orders and also be able to edit their own work orders. So, you grant view and edit privileges to the Help Desk module.

Over the next few weeks, though, Technician "A" continues to make unauthorized changes to work orders submitted by users from the Tucson office, despite several verbal warnings to stop. You can prevent Technician "A" from making any future changes by restricting him to view-only privileges for all work orders that are requested by users in the Tucson office.
To Restrict Privileges by Location:
(Continued from Restricting Privileges by Module)

1. From the main menu bar, select **Tools//Administration Console/Lookup Tables/Administration/Security Policies**.
2. Double click to open the Security Policy, or select the policy, then click the **Select** button.
3. On the **Locations** tab, right click next to the Location, then select one of the options: **Full Control, No Access, Read Only, or Can Edit.**
   You can also select the Location, then select an option from the **Change** button.
4. Click the **Save** button.

Next topic: Restricting Privileges by Department

Restricting Privileges by Department (Security Policies)

Previous Topic: Restricting Privileges by Location

At the next level of granularity, BMC Track-It! allows you to restrict security privileges by department.

Note: BMC Track-It! includes two security policies (Default and Administrator) that are installed with the application. You can create additional security policies.

Example

Suppose, for example, you decide to create a custom security policy called Help Desk Technician. In this policy, you want your technicians to be able to view existing work orders and also be able to edit their own work orders. So, you grant view and edit privileges to the Help Desk module.

Over the next few weeks, though, Technician "A" continues to make unauthorized changes to work orders submitted by users who are members of the Administration department, despite several verbal warnings to stop. You can prevent Technician "A" from making any future changes by restricting him to view-only privileges for all work orders that are requested by users in the Administration department.
To Restrict Privileges by Department:
(Continued from Restricting Privileges by Location)

1. From the main menu bar, select **Tools//Administration Console/Lookup Tables/Administration/Security Policies**.
2. Double click to open the Security Policy, or select the policy, then click the **Select** button.
3. On the **Departments** tab, right click next to the Department, then select one of the options: **Full Control, No Access, Read Only, or Can Edit.**
   You can also select the Department, then select an option from the **Change** button.
4. Click the **Save** button.

Next topic: Restricting Privileges by Assigned Technician

Restricting Privileges by Assigned Technician (Security Policies)

Previous Topic: Restricting Privileges by Department

In order to provide an additional level of granularity, the BMC Track-It! security model includes the concept of "Self". In an implicit manner, Self refers to the technicians who have been assigned to a particular **security policy** (i.e., on the **Assigned** tab of the Security Policies dialog). In other words, the **Assigned** tab controls what privileges technicians should have with regard to viewing, editing, and deleting information (e.g., work orders, purchase orders, etc.) that belong to other technicians assigned to that policy on the **Assigned** tab. Regardless of what the Administrator sets as the Technician's privileges on the **Assigned** tab, that technician will have full privileges to his or her own work orders.

Note: BMC Track-It! includes two security policies (Default and Administrator) that are installed with the application. You can create additional security policies.
Example
Suppose, for example, you want to create a security policy that allows technicians to access the **Help Desk** module in a view-only manner, but also allows them to have full control over work orders that have been assigned to them). This can be easily accomplished through the **Define Security Policies** dialog by granting view-only permission to the **Help Desk** module and No Access to all Technicians on the **Assigned** tab.

The concept of Self significantly reduces the amount of configuration that is required to setup and enforce your organization's security policies. At the lowest level of granularity, BMC Track-It! allows you to restrict security privileges by assigned technician. Suppose, for example, you decide to create a custom security policy called Help Desk Technician. In this policy, you want your technicians to be able to view existing work orders and also be able to edit their own work orders. So, you grant view and edit privileges to the **Help Desk** module and Read Only privileges to all Technicians on the Assigned tab.
To Restrict Privileges by Assigned Technician:
(Continued from Restricting Privileges by Department)

1. From the main menu bar, select **Tools//Administration Console/Lookup Tables/Administration/Security Policies**.
2. Double click to open the Security Policy, or select the policy, then click the **Edit** button.
3. On the **Assigned** tab, right click next to the Technician or group, then select one of the options: **Full Control, No Access, Read Only, or Can Edit.**
   You can also select the Technician or group, then select an option from the **Change** button.
4. Click the **Save** button.

Next topic: Understanding Crystal Reports Security in BMC Track-It!

Understanding Crystal Reports Security in Track-It! (Security Policies)

Previous Topic: Restricting Privileges by Module

If you add new reports or customize existing reports, security will be automatically applied when those reports are viewed by Technicians within BMC Track-It!, based on the Security Policies set up by Module, Location, Department, and Assigned Technician.

Notes:

- There are two security policies (Default and Administrator) that are installed with the application. You can create additional security policies.
- You can set up data entry privileges for modules and customize drop-down edit privileges.

Example

Suppose you have a report that retrieves all open Work Orders. BMC Track-It! technicians will only be able to view the report details for those they are privileged to view (based on Module, Location, Department, and Assigned Technician). As another example, suppose you create a custom report by department. That report will display only the items that pertain to departments that the technician can see, based on department-level privileges.

To Allow Technicians to View Reports:

1. Follow the instructions in the previous topics on Restricting Privileges (by Module, Location, Department, and Assigned Technician).
2. Select the **Modules** tab, then click the check box in the **Allow** column next to **View Reports** in the **Reports** section.
3. Click the **Save** button.
   The Technicians will now be allowed to view reports, based on their privileges for the Security Policy.

Important Notes:

- **WARNING:** While The BMC Track-It! report security model provides adequate protection in typical business environments, it is the BMC Track-It! administrator's responsibility to determine if additional precautions are needed to ensure the security of your data.
- **Caution:** Report row-level security is not implemented for the **Dashboard** module (graphs and pivot grids). If your Technicians have access to the Dashboard module, they will be able to view all System Dashboard graphs and pivot grids, as well as the two default Dashboard graphs (Overdue Work Orders and Work Order Activity This Month) on their Home Page. To set Dashboard security, see Restricting Privileges by Module.
- If you create custom reports using Crystal Reports, keep in mind that you are working with a complete set of live data. Consequently, the person who is assigned to create the report should be authorized (by your organization) to view all of the raw data.
- If your organization creates and uses custom reports in BMC Track-It!, you should thoroughly test these reports using several technician accounts with various security settings before deploying them in your application. Make sure your data is displayed with the correct restrictions for each account.
- If you attempt to use dynamic SQL statements or stored procedures in your custom reports, all data that is received via those statements will be passed without security restrictions. BMC Track-It! will not parse these statements.
- The BMC Track-It! Business Rules File contains critical logic that determines how security is applied and managed within BMC Track-It! While technicians must have Read-Only permission to this file in order to run BMC Track-It!, they must not attempt to make any changes to this file. Modifying the contents of this file may result in sweeping (undesired) changes in your BMC Track-It! application and the implementation of its security restrictions.

E-mail Monitor (Work Order Creation, Event Policies, and Notifications)

E-mail Monitor and Work Order Notifications Overview

The BMC Track-It! E-mail Monitor is a group of services that enables the following automatic processes:

Inbound E-mails

- Converts E-mails to work orders
  - E-mails sent to your help desk mail account(s) are converted into work orders
  - BMC Track-It! includes E-mail Monitor Management (multiple E-mail Monitor Policies and E-mail Monitor Addresses).
    - BMC Track-It! includes one default E-mail Monitor Policy.
    - You can create multiple E-mail Monitor policies so that work orders are automatically created from e-mails sent to any of your Help Desk e-mail addresses depending on the request (such as per facility location, or type of help desk task).
  - Rules can be created to prevent certain messages from becoming work orders

Outbound E-mails

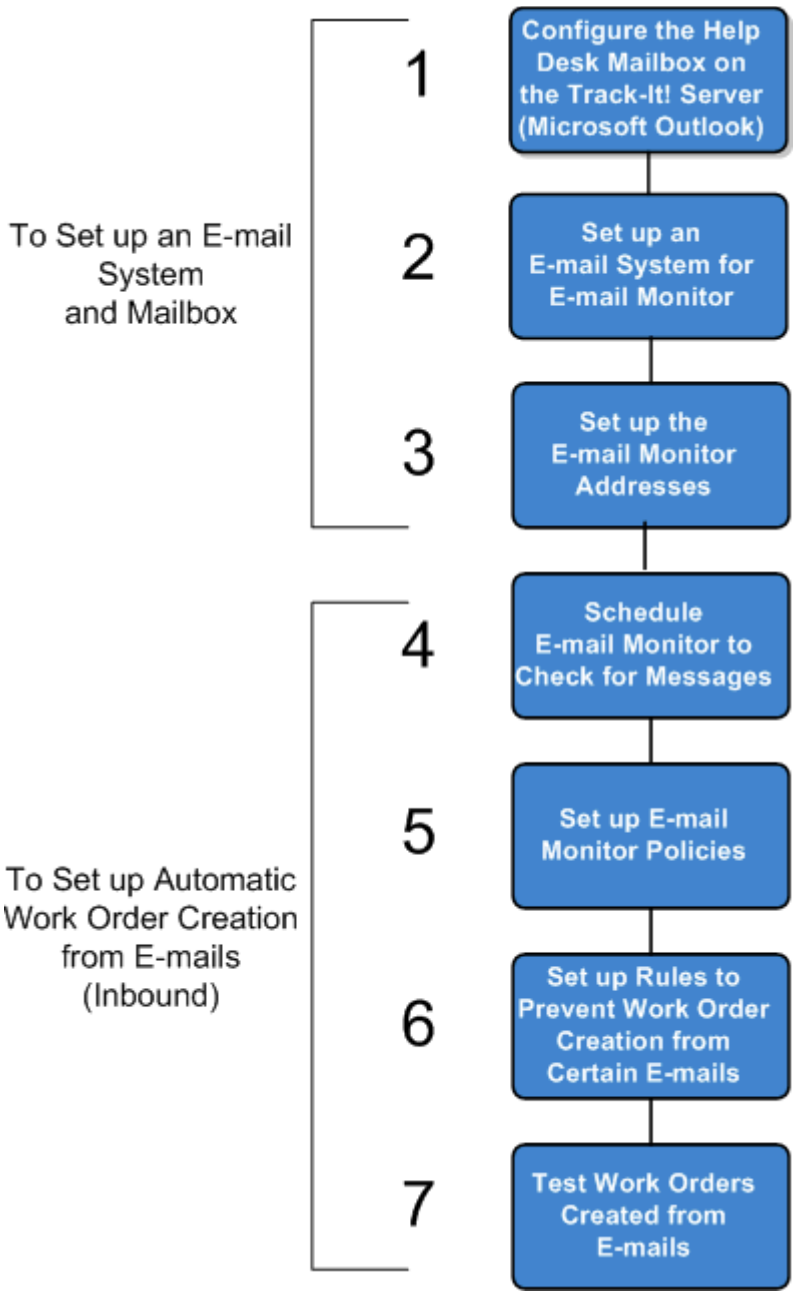
- E-mails users the status of their work orders
- Notifies technicians and/or users of work order events and escalations

To configure the E-mail Monitor, see the next topic, E-mail Monitor and Work Order Notifications Workflow (Steps 1-7) and E-mail Monitor and Work Order Notifications Workflow (Steps 8-16).

E-mail Monitor and Work Order Notifications Workflow (Steps 1-7)

Follow steps 1-16 below to configure the E-mail Monitor. (For a description of the E-mail Monitor, see the previous topic: E-mail Monitor Overview).

The flowchart below represents the tasks in the topics for this chapter.

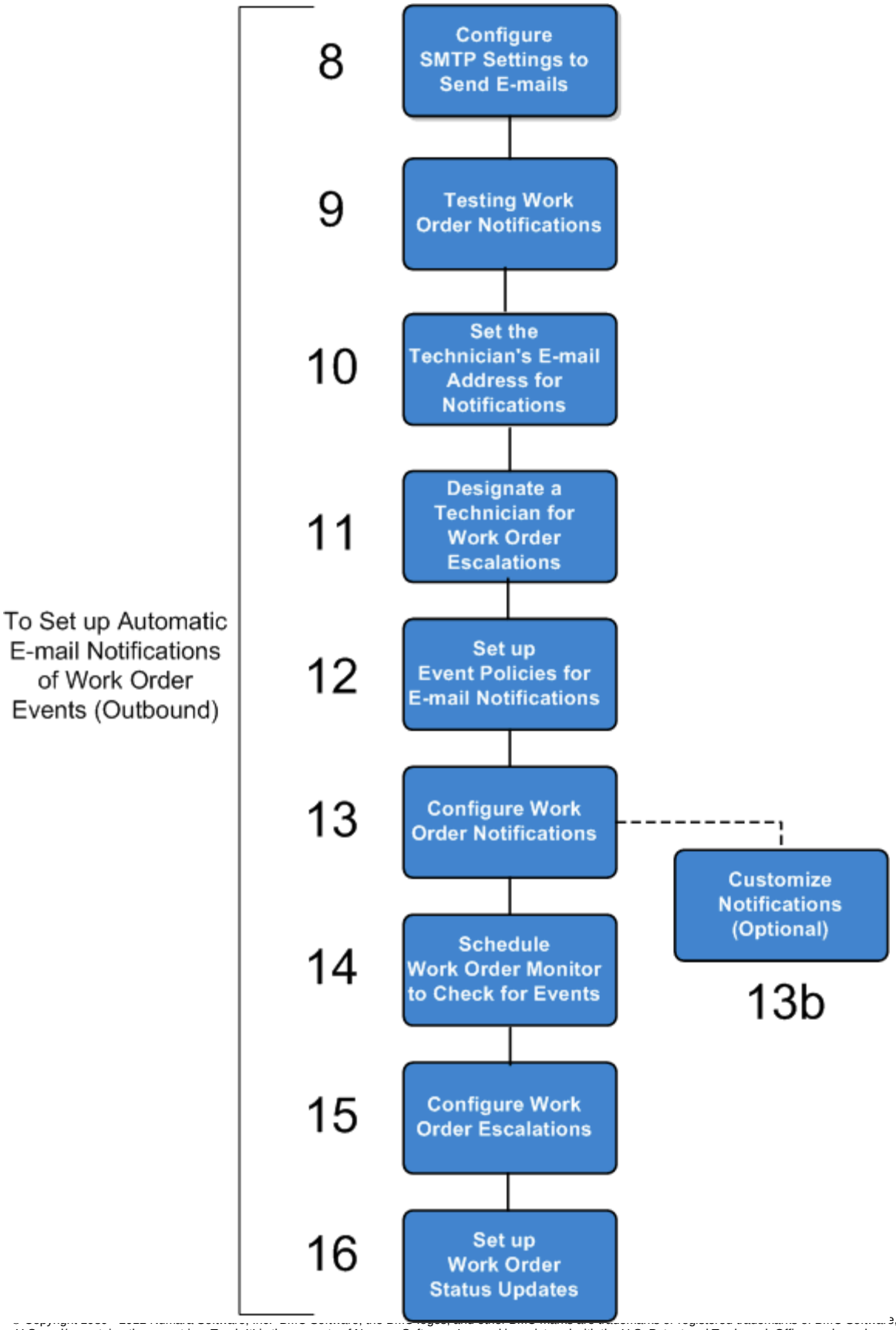


Next Topic: E-mail Monitor and Work Order Notifications Workflow (Steps 8-16)

E-mail Monitor and Work Order Notifications Workflow (Steps 8-16)

(Continued from E-mail Monitor and Work Order Notifications Workflow - Steps 1-7).

The flowchart below represents the tasks in the topics for this chapter.



Setting up the E-mail System and Mailbox

Step 1: Configuring the Help Desk Mailbox on the BMC Track-It! Server for Microsoft Outlook

The first step in setting up E-mail Monitor is to decide which type of e-mail system you want to use so that work orders can be automatically created from e-mails. This topic describes how to set up E-mail Monitor to work with MAPI (Microsoft Outlook). See below for other e-mail systems.

Using Other E-mail Systems

Microsoft Exchange (MAPI Clients Other than Outlook)
You can skip the steps below and go to Step 2: Setting up an E-mail System for E-mail Monitor.

POP3/SMTP
You can skip the steps below and go to Step 2: Setting up an E-mail System for E-mail Monitor.

Lotus Notes
You can skip the steps below and go to Step 2: Setting up an E-mail System for E-mail Monitor.
Novell GroupWise
Please see the Groupwise section in our KnowledgeBase article on How to Configure Track-It! 9 to Send and Receive Mail

IMPORTANT: Do not remote into the BMC Track-It! Server to complete these steps -- you will need a console-based connection.
Prerequisites Checklist
First, verify the following prerequisites on the server where BMC Track-It! is installed:

	1. Microsoft Exchange Server and the BMC Track-It! Server are on the same domain (or a two-way trust is established between them)
	2. Microsoft Outlook client is installed

To Configure Microsoft Outlook on the BMC Track-It! Server:

1. **Configure Microsoft Outlook for the Help Desk mailbox**

    a. Log on to the BMC Track-It! Server with the Help Desk account.
    b. If not already configured, set up the initial Outlook profile.
    c. Make sure Cached Mode is disabled in Outlook:

        i. In Microsoft Outlook, from the **Tools** menu, select **E-mail Accounts**.
        ii. In the **E-mail Accounts** dialog, under **E-mail**, make sure the radio button next to **View or change existing e-mail accounts** is selected, then click **Next**.
        iii. Select your **Microsoft Exchange Server** account, then click the **Change...** button.
        iv. To turn off Cached Exchange Mode, under Microsoft Exchange Server, clear the **Cached Exchange Mode** checkbox.
        v. Click the **Next** button, then click **OK** on the next dialog.
        vi. Click **Finish**.
        vii. Restart Outlook for the change to take effect.

    d. Note the Mail Profile Name
        (The profile name will be used to configure a MAPI e-mail system, explained in the next topic Step 2: Setting up an E-mail System for E-mail Monitor.

i. From the **BMC Track-It! Server**, access the Mail setup (**Start/Control Panel/Administrative Tools/Services**).
ii. Double click the **Mail** icon.
iii. On the **Mail Setup** dialog, click the **Show Profiles** button.
iv. Make a note of the profile name (such as Help Desk), then click the **Cancel** button.

Step 2: Setting up an E-mail System for E-mail Monitor (Administration Console)

(Configuration Wizard Step 1 of 3: Configure E-mail Settings)

You can set up E-mail Monitor to receive e-mail using MAPI, POP3/SMTP, Exchange, or Lotus Notes. MAPI is used for e-mail systems such as Outlook, Exchange and GroupWise. POP3/SMTP is used if you have an unattended server where it is not required to log in. If you don't have Microsoft Outlook, you can use the Exchange Server option described below to install a free MAPI compliant Exchange client.

Notes:

- The instructions below pertain to MAPI, POP3/SMTP, Exchange, and Lotus Notes. For Groupwise, please see our KnowledgeBase article on How to Configure Track-It! 9 to Send and Receive Mail
- Verify that Microsoft Exchange Server and the BMC Track-It! Server are on the same domain (or a two-way trust is established between them)

To Set up an E-mail System for E-mail Monitor:
(If you're using the **Configuration Wizard**, start with the screen: Step 1 of 3: Configure E-mail Settings)
MAPI

1. From the main menu bar, select **Tools/Administration Console/Configuration/ Help Desk/E-mail Monitor/Monitor Configuration.**
2. Select the **MAPI** option, then click the **Settings** button.
3. Specify the login credentials and associated profile that connects your MAPI client (such as Outlook) to your e-mail system.
4. Select the appropriate profile name, then click the **Save** button.
   This is the same profile name noted in the previous topic (Step 1: Configuring the Help Desk Mailbox on the BMC Track-It! Server for Microsoft Outlook) in Step 1d: Note the Mail Profile Name.
5. Click the **Apply** button on the **Monitor Configuration** panel to save your changes, or the **OK** button to close the window.

POP3/SMTP

(If you have an unattended server where it is not required to log in)

1. Select the **POP3/SMTP** option on the **Monitor Configuration** panel, then click the **Settings** button.
2. On the **Servers** tab, enter the name for the incoming mail server in the **Incoming Mail (POP3)** field.
3. Enter the account name that will grant BMC Track-It! access to your incoming mail server in the **Account Name** field.
4. Enter the password in the **Password** field, then reenter it in the **Confirm Password** field
5. Click the **Save** button on the **POP3/SMTP** dialog.
6. On the **Advanced** tab, the **Incoming Mail** displays default server port numbers and Server Timeouts. In most cases, POP3 uses port 110.
7. You can adjust the **Server Timeouts** in intervals from 30 seconds to five minutes.

If BMC Track-It! fails to connect to a mail server on its first attempt, the Server Timeouts tell BMC Track-It! how long to wait before making another attempt. The default value of 30 seconds is acceptable for most applications.

8. Click the **Apply** button on the **Monitor Configuration** panel to save your changes, or the **OK** button to close the window.

Exchange Server (MAPI Compliant Client)

1. Select the **Exchange Server** option, then click the **Settings** button.

   (If you haven't already installed a MAPI compliant Exchange client, click the "Learn more about configuring your connection" link under Current Configuration.
   This will open the BMC Track-It! support article with information on downloading and installing a free Exchange client.
2. Once the Exchange client is installed, on the BMC Track-It! server, navigate to **\\Program Files\Common Files\BMC Software\Track-It! Shared**.
3. Delete the file: **mapi32.dll**, since it is not compatible with the free Exchange client.
4. On the **Exchange Server** dialog in BMC Track-It!, enter the **Server Name**.
5. Enter the **Mailbox Name** (typically a user name).
   You can enter variations of the name (such as Joe Smith or jsmith) and BMC Track-It! will find the user name
7. Specify the login credentials (**User Name** and **Password**) to use when receiving e-mail messages sent to the mailbox. BMC Track-It! will prompt you to add the user as a local administrator if necessary.
8. To test the connection to the Mail Server, click the **Test Connection** button.

   BMC Track-It! will test the connection and display an Information dialog (successful or failed). If the test failed, a red icon will display next to the relevant field. Point to the icon for a tooltip describing the problem. If successful, BMC Track-It! will resolve the Exchange Server account information, which will display on the Monitor Configuration panel once saved.
9. Click the **Save** button to return to the **Monitor Configuration** panel.
10. Click the **Apply** button on the **Monitor Configuration** panel to save your changes, or the **OK** button to close the window.

Lotus Notes

1. Select the **Lotus Notes** option on the **Monitor Configuration** panel, then click the **Settings** button.
2. On the Lotus Notes dialog, enter the **Server Name**.
3. Specify the login credentials (**User Name** and **Password**) to use when receiving e-mail messages sent to the mailbox. BMC Track-It! will prompt you to add the user as a local administrator if necessary.
4. To test the connection to the Mail Server, click the **Test Connection** button.
5. Click the **Save** button to return to the **Monitor Configuration** panel.
6. Click the **Apply** button on the **Monitor Configuration** panel to save your changes, or the **OK** button to close the window.

Step 3: Setting up E-mail Monitor Addresses

You can set up multiple E-mail Monitor addresses for your Help Desk mailbox. When you set up E-mail Monitor Policies, work orders are automatically created from users' e-mails sent to the specific E-mail Monitor Policy's Help Desk e-mail address and assigned to the designated Technician. You can set up different Help Desk e-mail addresses depending on the request (such as per location or Work Order type). For example, two e-mail addresses can be set up to be forwarded to your Help Desk mailbox: one

for Tampa and one for New York. When a user in the Tampa office sends an e-mail to Tampa-HelpDesk@company.com, a Work Order is created based on matching criteria as set up for the E-mail Monitor Policy. (See also Setting up E-mail Monitor Policies).

To Set up E-mail Monitor Addresses:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/E-mail Monitor Addresses**.

   The **E-mail Monitor Address** dialog displays. You can also access this dialog from the ***E-mail Monitor Policy*** dialog in the **Administration Console**.

   a. From Track-It!'s main menu bar, select **Tools/Administration Console/Configuration/Help Desk/E-mail Monitor/E-mail Monitor Policies**.
   b. Click the **Add** button (+) next to the **E-mail Monitor Address** drop-down list.
   c. Follow the steps in #3, below.

2. Click the **Add** button to create a new E-mail Monitor Address.
3. Enter the e-mail address and display name in the **E-mail Monitor Address** dialog, then click the **Save** button.

   For example:

   2.

   - E-mail address: TampaHelpDesk@mycompany.com
   - Display name: Tampa Help Desk

Setting up Automatic Work Order Creation from E-mails (Inbound)

Step 4: Scheduling E-mail Monitor to Check for Messages

You can set up the E-mail Monitor to automatically check for e-mail messages sent to your help desk e-mail account (at specified time intervals). You can also manually check for e-mail messages with the **Check E-mail Now** button. The **E-mail Monitor Log** on this panel can be printed or exported to a file (.txt, .xls, or .html). The log can also be purged.

When all the steps to configure E-mail Monitor are complete (see E-mail Monitor Workflow), the e-mail messages will be converted into work orders.

Notes:

- For testing purposes, you can click the **Check E-mail Now** button, then click the **Refresh** button and view the information in the **E-mail Monitor Log** (see instructions below).

To Schedule E-mail Monitor to Check for Messages:

1. From the main menu bar, select **Tools/Administration Console/Configuration/ Help Desk/E-mail Monitor/Monitor Schedule.**
2. Click the **Enabled** check box to enable this feature.
3. Select the **Frequency** at which you want BMC Track-It! to check the Help Desk inbox for new messages from the **Time Interval** field.

   The recommended (default) interval is 15 minutes.
   You should carefully consider this time interval before you define it because your service level agreements (SLAs) may require that you define a shorter interval than expected.

4. Click the **Apply** button to save your changes, or the **OK** button to close the window.

To Check the E-mail Monitor Mailbox Now:

1. Click the **Check E-mail Now** button.

To View, Print, or Export the E-mail Monitor Log:

The **E-mail Monitor Log** displays the Date/Time, Event Type, and Summary of the mailbox check.

1. Double click the record (per row) in the **E-mail Monitor Log** to view details.
2. In the **Event Details** dialog, click the **Previous** or **Next** button to view each record.
3. To copy the information, click the **Copy to Clipboard** button.
4. To print the information, see Printing Grid Contents in the Technician's Guide.
5. To export the information, see Exporting Grid Contents Technician's Guide.
6. Click the **Close** button to return to the **Monitor Schedule** panel.

To Purge the E-mail Monitor Log Messages:

1. Click the **Purge Log** button.
2. Click the **Yes** button on the **Purge Confirmation** dialog.

   A message in the log will display the number of purged records.

Step 5: Setting up E-mail Monitor Policies

E-mail Monitor Policies enable work orders to be automatically created from e-mails sent to your Help Desk mailbox. When an e-mail is received, the criteria set up on the policy is matched with the E-mail Monitor Address (the address to which the request was sent), e-mail Subject, Requestor, Department, and/or Location. The Subject match can be based on text strings and .NET regular expressions, such as "`printer|copier|fax machine`". (Subject matches are made regardless of case sensitivity).

The Work Order is then created and populated with the Requestor's name and Work Order Summary (based on the Subject of the e-mail). The policy can also be set up to route the Work Order to an assigned Technician. A Work Order Template can be selected or created and applied to the policy so that Work Orders created from e-mails are already populated with specified field values (such as Work Order Type, Subtype, Category, Priority, etc.).

Notes:

- Make sure to complete the configuration steps in E-mail Monitor and Work Order Notifications Workflow (Steps 1-7) and E-mail Monitor and Work Order Notifications Workflow (Steps 8-16) to ensure that the Work Orders are created from e-mails and notifications are sent.
- There is one default E-mail Monitor Policy. You can edit the default E-mail Monitor Policy, except for the Matching Criteria. The default policy cannot be disabled or deleted.
- You can create multiple E-mail Monitor policies and multiple E-mail Monitor addresses so that work orders are automatically created from e-mails sent to any of your Help Desk e-mail addresses depending on the request (such as by location, or Work Order type).
- E-mail Monitor Policies have precedence over Skill Routing policies.
- The E-mail's subject will always override the Work Order template's summary.

Example of an E-mail Monitor Policy and a Work Order Created from an E-mail

Note: See To Set up an E-mail Monitor Policy for detailed instructions. To access the E-mail Monitor Policy dialog: From Track-It!'s main menu bar, select **Tools/Administration Console/Configuration/Help Desk/E-mail Monitor/E-mail Monitor Policies**.

In the following example, a Requestor located in Tampa sends an e-mail to the Tampa Help Desk's e-mail address requesting help with a printer. Based on the E-mail Monitor Policy's regular expression set up to

filter by the e-mail's Subject:
printer|copier|fax machine and the Requestor's Location (Tampa), the Work Order is created using the specified Work Order Template. The Work Order created from the policy's template is pre-populated with field values (such as Priority, Type, Subtype, and Category). The Work Order is then routed to the Assigned Technician, and the Requestor receives an automatic response with a Work Order number and a link to check the Work Order's status.

Note: If you want to print this page, please print in landscape to view the table below. In Internet Explorer, select File/Page Setup/Landscape, and then click the Print button.

E-mail Monitor Policy	**Incoming E-mail from Requestor**	**Work Order**	**Auto-response E-mail**
Matching Criteria **E-mail Monitor Address** TampaHelpDesk@mycompany.com **E-mail Subject** `printer|copier|fax machine` **Requestor** <Any> **Requestor Department** <Any> **Requestor Location** Tampa **Actions** **Set Technician Assigned to:** Albert Elliott **Apply Work Order Template:** **Template Name:** Printer toner (replace) **Priority:** 3 - Medium **Type:** Hardware **Subtype:** Peripherals **Category:** Printers	To: TampaHelpDesk@mycompany.com From: Joe.Smith@mycompany.com Subject: Could you please replace the toner in the printer? The toner is out on the printer. Could you please replace it? Thanks. Joseph Smith	**Summary:** Could you please replace the toner in the printer? **Requestor:** Joe Smith Work Order created based on Requestor's Location (Tampa) **Assigned Technician:** Albert Elliott **Priority:** 3 - Medium **Type**: Hardware **Subtype:** Peripherals **Category:** Printers	To: Joe.Smith@mycompany.com From: TampaHelpDesk@mycompany.com Subject: New Work Order 1234 has been created from your e-mail Your Work Order has been logged as Work Order number 1234. Please do not reply to this e-mail as it is an automated notification. If you wish to add information or check the status, use the links below.

Example of an E-mail Monitor Policy and a Work Order Created from an E-mail

To Set up an E-mail Monitor Policy:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Help Desk/E-mail Monitor/E-mail Monitor Policies**.
2. Click the **Add** button to create a new E-mail Monitor Policy.
3. On the **E-mail Monitor Policy** dialog, enter a name for the policy in the **Name** field.

Matching Criteria

You can set up an E-mail Monitor Policy to find matches in e-mails sent to the Help Desk for any of the following criteria:

- E-mail Monitor Address (the address to which the request was sent)
- E-mail Subject (will display as the Work Order's Summary)
- Requestor (the BMC Track-It! user name or the sender's e-mail address if the user name does not exist in BMC Track-It!).
- Requestor's Department (the Department set up on the User's profile in BMC Track-It!)
- Requestor's Location (the Department set up on the User's profile in BMC Track-It!)

To Set up Matching Criteria:

1. In the **Matching Criteria** section, select an **E-mail Monitor Address** from the drop-down list that you want to associate with this E-mail Monitor Policy.

   You can also add new e-mail addresses by clicking the **New** button (+) to access the **E-mail Monitor Address** dialog. (For more information, see Step 3: Setting up E-mail Monitor Addresses).

   Note: BMC Track-It! will match on the To: Address (the E-mail Monitor address). If your e-mail system causes the To: Address to change, BMC Track-It! will not find a match.

2. To match on the Subject of an e-mail, click the **Edit** button next to the **E-mail Subject** field, enter the text string or a .NET regular expression in the **Subject Regular Expression** dialog, then click the **OK** button.

   Example: "Urgent" will match all e-mail subjects containing the word "Urgent". (The match will be made regardless of case sensitivity).

   See the support article on our Web page for more regular expression examples: Regular Expressions in Track-It! 8.5 E-Mail Monitor Policies

3. To match on the Requestor (e-mail sender), select the Requestor from the **Requestor** drop-down list.
   - To edit the User, double click the **User Name**.
   - To add a User, click the **New (+)** button.
   - Click the **Ellipses (...)** button to find a User or create a new User.

   Note: If an individual sends an e-mail to the E-mail Monitor address, and a User Name associated with the e-mail address does not exist in BMC Track-It!, the sender's e-mail address will display on the Work Order.

4. To match on the Requestor's Department, select the Department from the **Requestor Department** drop-down list.
5. To match on the Requestor's Location, select the Location from the **Requestor Location** drop-down list.

Actions

Enabling Auto-responses to Requestor-submitted E-mails and Customizing the Template

The auto-response e-mail notification informs Requestors that their e-mail was received, and provides the Work Order number with a hyperlink to check the Work Order's status .
To Set up Auto-responses:

1. Click the **Send Auto-Response** checkbox in the **Actions** section.
2. To customize the default notification text that will display in the e-mail response, click the **Auto-Response Template...** button. See Step 13b: Customizing Notifications (Optional) for detailed instructions.

Assigning a Default Technician
To Assign a Default Technician for Work Orders Created from Help Desk E-mails:

1. Select the Technician from the **Set Technician Assigned to:** drop-down list.

   Important Note: E-mail Monitor Policies have precedence over Skill Routing policies.

Applying a Work Order Template

You can apply a Work Order template to the E-mail Monitor Policy so that Work Orders created from e-mails are already populated with specified field values (such as Work Order Type, Subtype, Category, Priority, etc.).

Note: The E-mail's subject will always override the Work Order template's summary.
To Apply a Work Order Template:

1. Select a template from the **Apply Work Order Template** drop-down list.

   (You can double-click a template name in the drop-down list to open it).

2. To create a new template:
   a. Click the **Ellipses (...)** button.
   b. Click the **New** button on the **Apply Template** dialog.
   c. For detailed instructions, see Creating Work Order Templates.
3. Complete the Work Order Template (as described in the topic Documenting the Issue in the Technician's Guide) and save it.
4. Close the **Apply Template** dialog, then select the template from the **Apply Work Order Template** drop-down list on the **E-mail Monitor Policy** dialog.

Enabling the E-mail Monitor Policy

When you create an E-mail Monitor Policy, it is automatically enabled by default, and the **Policy Enabled** checkbox is checked (at the bottom of the **E-mail Monitor Policy** dialog). You can un-check it if you are not ready to enable the Event Policy.

Using the E-mail Monitor Address for E-mail Notifications

This checkbox enables E-mail Monitor to use the e-mail address to which the request was sent (the E-mail Monitor address) for e-mail notifications to the requestor. For example, notifications will be sent from TampaHelpDesk@mycompany.com if the requestor's e-mail was sent to TampaHelpDesk@mycompany.com. If this checkbox is not checked, E-mail Monitor will use the system e-mail address for e-mail notifications (see Step 1: Configuring the Help Desk Mailbox on the BMC Track-It! Server for Microsoft Outlook).
To Use E-mail Monitor Address for E-mail Notifications:

1. Click the **Use E-mail Monitor Address for E-mail** checkbox.

When you have finished creating or editing the E-mail Monitor Policy, click the **Save** button.

Related Topic: To set up rules to prevent Work Orders from being created from e-mails sent to your Help Desk, see Step 6: Setting up Rules for Work Orders Generated from E-mails.

Step 6: Setting up Rules for Work Orders Generated from E-mails

You can set up rules for e-mails in order to enable E-mail Monitor to ignore certain types of e-mails (and prevent work orders from being created from them).

Note: To assign a default Technician for Work Orders created from e-mails, see Setting up E-mail Monitor Policies.

You can create multiple E-mail Monitor policies so that work orders are automatically created from e-mails sent to any of your Help Desk e-mail addresses depending on the request (such as per facility location, or type of help desk task).

Note: Once you set up the rules, the help desk mailbox will still receive the e-mails -- they just won't be converted to work orders.

Ignoring Certain Types of E-mails When Automatically Creating Work Orders

You can set up rules for senders as well as text in e-mails so that the E-mail Monitor will ignore these types of e-mails and not automatically create work orders from them.

Senders, Subject Line, and Message Body

Certain defaults to prevent work orders from being created are already set up in the E-mail Monitor for senders and subject lines. This includes if the sender is "Postmaster" or "Mail Delivery Subsystem" or if the subject line says "Undeliverable Mail, Re:, or Out of Office". You can add text such as "@yahoo.com" (without the quotes) as well, which will prevent work orders being created from any e-mails from the specific domain.

If a user sends a new e-mail regarding an existing work order, you can prevent a new work order from being created by setting rules for the body of the message.

To Set up Rules to Ignore E-mails and Prevent Work Orders from Being Created:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Help Desk/E-mail Monitor/Rules**.
2. On the **Rules for Senders**, **Rules for Subjects**, or **Rules for Body** tabs, enter the text to create the specific rule on a separate line.
   For example, if your auto response contains text such as "This is a system-generated message -- please do NOT reply":
2. Copy the message from your auto response in the **Rules for Body** text box.
3. Click the **Apply** button to save your changes, and the **OK** button to close the window.

This completes the process for Automatically Creating Work Orders from E-mails (Inbound). See the next topic on Step 7: Testing Work Orders Created from E-mails.

Step 7: Testing Work Orders Created from E-mails

To Test Work Orders Created from E-mails

1. Send an e-mail to your help desk e-mail account (as configured in Configuring the Help Desk Mailbox on the BMC Track-It! Server).
2. Click the **Check E-mail Now** button on the **Monitor Schedule** panel in the **Administration Console** (See Scheduling E-mail Monitor to Check for Messages).
3. Wait a minute, then refresh the Work Order grid in the Help Desk module (right click the grid and select **Refresh**, or press the **F5** key). See also Viewing Work Orders in the Technician's Guide).

   The Work Order created from the e-mail should display in the work Order grid.

Setting up Automatic E-mail Notifications of Work Order Events (Outbound)

Automatically Notifying Technicians and Users of Work Order Events (Overview)

You can set up the Work Order Monitor to automatically notify technicians and users when certain Work Order events occur, such as when a Work Order is Created, Modified, or Closed. Technicians and users can be notified automatically from BMC Track-It! via e-mail or text message (SMS). Follow the steps (8-16) in this chapter to set up notifications.

Notes:

- It is not necessary to set up inbound e-mail for work order notifications.
- Sent messages are not maintained, but the work order's Audit Trail tab will record that a message was sent (see Viewing the Work Order's Audit Trail in the Technician's Guide).
- You can also manually e-mail a Work Order directly from BMC Track-It! to the Technician. See E-mailing Work Order Details to Requestors and Technicians in the Technician's Guide).

Step 8: Configuring SMTP Settings for Sending E-mail

(Configuration Wizard Step 1 of 3 Configure E-mail Settings - SMTP Settings)

NOTE: Only SMTP (not MAPI) is used to send e-mail with the E-mail Monitor.
To Configure SMTP Settings for Sending E-mail:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Administration/E-mail Configuration/SMTP Configuration.**

   (This dialog can also be accessed from the **Configuration Wizard** (Step 1 of 3: Configure E-mail Settings, then click Next to the SMTP dialog).

2. Enter the **SMTP Host Name** (or IP Address) in the designated field (such as smtp.ourdomain.com).
3. Enter the **Port Number** in the designated field (the default SMTP port is 25).
   NOTE: Some anti-virus software automatically blocks port 25. (See our KnowledgeBase article: Notifications Not Sent from Track-It! if McAfee VirusScan is Installed).
4. If the server requires an encrypted connection (SSL), click the designated checkbox.

5. If the **SMTP requires authentication**, click the designated checkbox.
    a. Enter the **User Name** and **Password**.
    b. Then enter the password again in the **Confirm Password** field.
6. To test the SMTP settings, click the **Send Test E-mail** button.
7. In the **Enter E-mail Address** dialog, Enter the recipient's e-mail address, then click the **OK** button.
   A confirmation message will display if the message was sent. If not, an error message will display with relevant details.
8. Click the **Apply** button to save your changes, or the **OK** button to close the window.

To Specify the "From Address" for E-mail Notifications:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Administration/E-mail Configuration/From Address.**
2. Enter the e-mail address (such as "Administrator@TheCompanyDomain.com") in the **From Address** field.
3. Enter the display name (such as "BMC Track-It! Server" in the From Address **Display Name** field.
4. Click the **Apply** button to save your changes, or the **OK** button to close the window.

Step 9: Testing Work Order Notifications

When setting up Work Order notifications to send to users and/or technicians, you can test to see that e-mails are properly sent. This can be accomplished from the Distribute Technician Client panel on the Administration Console. (This will send a test e-mail with installation instructions for the Technician Client).

To Test Work Order Notifications:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Administration/Distribute Technician Client.**
2. Select the technician(s) from the **Available Technicians** list, then click the **Add** button.
   (You can select multiple technicians by holding the Shift or CTRL key as you select them). This places the technicians in the Technicians to Notify list.
3. Click the **Send E-mail** button.
4. On the **Enter E-mail Address** dialog (if displayed), enter the e-mail address that was set up for your Help Desk e-mail account (e.g. help@yourcompany.com), then click the **OK** button.
5. Click the **Apply** button to save your changes, or the **OK** button to close the window.

   When you click Send E-mail, it will fail immediately if the SMTP information is incorrect. If that is the case, adjust the settings in Step 8: Configuring SMTP Settings for Sending E-mail until you can successfully send a "Technician Client Click-Once" E-mail.

Step 10: Setting the Technician's E-mail Address for Notifications

You can notify technicians via e-mail or text message (SMS). When configured, the Directory Importer will import the Technicians' e-mail addresses. However, you can change the e-mail address on the Notifications tab of the Technician dialog.

Note: If you manually change the Technician's e-mail address, it will be overwritten each time the Directory Importer is run.

To Set the Technician's E-mail Address for Notifications:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Technicians**.
2. Double click to select the **Technician**, or click the **Select** button.
3. On the **Notification** tab, enter the Technician's **e-mail address** (if not already populated using the Directory Importer) in the **E-mail** section.
4. Enter the Technician's SMS e-mail address in the **Text Message (SMS)** section.
   (Contact your mobile service provider for the correct format, since this varies by provider).
5. To enter a maximum message length for text messages, enter a value in the **Maximum Message Length** field (in characters, such as 50).
6. Click the **Save** button.

Related Topics:
E-mailing Work Order Details to Requestors and Technicians
Step 13: Configuring Work Order Notifications
Directory Importer Overview

Step 11: Designating a Technician for Work Order Escalations

When setting up a Technician's properties, you can designate another Technician to be assigned a Work Order if the assigned Technician has not resolved it by the due date. Typically you would escalate the Work Order to a lead Technician or manager.

You can also set up BMC Track-It! to automatically notify the "Escalate to" Technician, via e-mail, when specific events occur during a Work Order's life cycle. See Step 15: Configuring Work Order Escalations.

To Designate a Technician for Work Order Escalations:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Administration/Technicians**.
2. Double click to select the **Technician**, or click the **Select** button.
3. On the **Escalation** tab of the **Technicians** dialog, select the Technician to whom the overdue work order should be escalated from the **Escalation** drop-down.
4. Click the **Save** button.

Related Topics: Step 15: Configuring Work Order Escalations

Step 12: Setting up Work Order Event Policies

Note: To customize **Work Order Notification Templates**, see Step 13b: Customizing Notifications (Optional). (Event Policies must be set up and enabled for notifications to be sent -- see E-mail Monitor and Work Order Notifications Workflow (Steps 8-16).

You can set up Work Order Event Policies so that when a Work Order is created, BMC Track-It! matches the Work Order with criteria set up on the policies (such as Priority) to determine the Work Order's Due Date and Expected Completion Date. You can set up policies based on the following additional criteria:

- Requestor
- Department
- Location

- Type
- Subtype
- Category
- Priority

The Event Policy can also be set up to automatically notify Requestors, Assigned Technicians, and/or the "Escalate to" Technician when certain events occur with Work Orders matching those criteria. For example, a Work Order with a specific Type (such as Network) can be set up so that the Assigned Technician is notified when the Work Order is created, and escalated to a lead technician if the work is not closed within a specified amount of time. See Step 15: Configuring Work Order Escalations.

Important: You will need to set up at least one Event Policy and at least one Notification so that notifications are automatically sent. Set up a basic event policy so that when a new work order is created, a notification is sent to the Assigned Technician. (See the next topic, Step 13: Configuring Work Order Notifications.)

Notes:

- To automatically assign particular Technicians or Technician groups to Work Orders, see Setting up Skill Routing Policies

To Set up an Event Policy:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Event Policies**.
2. Click the **Add** button to create a new Event Policy.
3. On the **Event Policy dialog**, enter a name for the policy in the **Name** field.
4. Select a **Service Level Agreement** from the drop-down list (if you have an SLA contract). (See also Setting up Service Level Agreements (SLAs).

Setting Matching Criteria

To Set Matching Criteria:

1. In the **Matching Criteria** section, select options from the following drop-down lists:

    - Requestor
    - Department
    - Location
    - Type
    - Subtype
    - Category
    - Priority

Creating Work Order Templates Based on the Event Policy:

To Create a Work Order Template:

1. To create a new Work Order Template based on the Event Policy, click the **Create Template** button. For detailed instructions, see Creating Work Order Templates.

Setting Notification Actions

To Set Notification Actions:

1. To set the Event Policy's **Due Date**, in the **Actions** section, enter or select the number of Days, Hours, and Minutes in the designated fields.

    This is the date and time a work order with these criteria is due from the moment the Work Order is created.

2. To set the **Expected Completion Date**, enter or select the number of Days, Hours, and Minutes in the designated fields.

   This is the date and time a work order with these criteria is expected to be completed from the moment the Work Order is created.

3. To set a reminder alarm that the Due Date is approaching, enter or select the number of Days, Hours, and Minutes in the **Set Due Date Approaching Alarm** fields.
   Once notifications are configured, a notification will be sent at the designated time. See Step 13: Configuring Work Order Notifications.

4. To set a reminder alarm that the Expected Completion Date is approaching, enter or select the number of Days, Hours, and Minutes in the **Set Expected Completion Date Approaching Alarm** fields.

   Once notifications are configured, a notification will be sent at the designated time. See Step 13: Configuring Work Order Notifications.

5. To **Override Operating Hours** on all dates and times above, click the indicated check box above "Set Due Date".

   Note: The due date and time will be calculated differently if Override Operating Hours is selected.

   For example:

   - Overriding Operating Hours: If the due date on the Event Policy is set to 1 hour, and the event (create work order) occurs at 10:00 PM, and working hours are 9:00 AM to 5:00 PM, and override operating hours is selected, the notification gets sent at creation time (10p), and the work order is due at 11:00 PM. (Notifications are sent regardless of an operating hours override).

   - Not Overriding Operating Hours: For the above scenario, if you don't override operating hours, the work order isn't due until 10:00 AM the next day. The notification still gets sent when the work order is created (10:00 PM).

6. By default, the Event **Policy Enabled** checkbox is selected. You can de-select it if you are not ready to start the Event Policy and send notifications.
7. If desired, you can continue to the next steps now, or you can click the **Save** button now to save your changes.
8. The new policy displays on the **Event Policies** panel of the Administration Console.
9. Click the **Edit** button to edit the Event Policy. **Make sure to complete the next steps in:** Step 13: Configuring Work Order Notifications

Step 13: Configuring Work Order Notifications

Work Order Notification templates are used by Work Order Monitor to automatically notify Requestors via e-mail or Assigned Technicians via e-mail or text message (SMS). The templates are also used to notify the "Escalate to" Technician when certain events occur with Work Orders. For example, if there is an Event Policy set up to notify the Assigned Technician when a Work Order is created for a Network issue, e-mail or text message notifications will be sent with the default text of the notifications that you select. You can customize the e-mail text with work order labels and fields that display in the subject and body of the e-mail or text message (see Step 13b: Customizing Notifications (Optional).

Notes:

- After creating Work Order Notification Templates, Work Order Event Policies must be set up and enabled for notifications to be sent (see Step 12: Setting up Work Order Event Policies).
    - **Important: At least one Event Policy and at least one Notification must be set up so that notifications are automatically sent**.
- You can test your e-mail notification formatting once you've configured the E-mail Monitor to send e-mail notifications (see Step 9: Testing E-mails Sent from E-mail Monitor).

Work Order Notifications can be sent for each of the Work Order events below to Requestors, Assigned Technicians, and/or the "Escalate to" Technician:

- New Work Order (Users template only)
- Work Order Assigned to a Technician
- Work Order modified by someone other than the assigned Technician
- Work Order's status is changed
- Work Order's expected completion date approaching
- Work Order's expected completion date overdue
- Work Order's due date approaching
- Work Order overdue
- Work Order closed
- Manual Notification
- Auto-response to requestor-submitted e-mails (Users template only)

Configuring Work Order Notifications

Notifications can be sent to the Requestor, Assigned Technician, and/or "Escalate to" Technician throughout various events in the life cycle of a Work Order (New, Modified, Closed, etc.).

Note: The "Escalate to" Technician must be set up in order for Work Order notifications to be sent to them. See Step 11: Designating a Technician for Work Order Escalations and Step 15: Configuring Work Order Escalations.

To Configure Work Order Notifications:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Event Policies**.

   Note: You can also access the Work Order Notification Templates from the following location; however, Work Order Event Policies must be set up and enabled for notifications to be sent: **Tools/Administration Console/Configuration/Help Desk/Work Order Events/Work Order Notification Templates**.

2. Select the **Event Policy** from the **Event Policies** panel in the **Administration Console**.
3. Click the **Configure Notifications** button on the **Event Policy** dialog.
4. Select the tab for the individual(s) to receive the notification(s): Requestor, Assigned Technician, or "Escalate to" Technician.
5. Select the checkbox next to the events for which you want to send notifications (such as Work Order Assigned to a Technician or Work Order's Due Date Approaching).
6. Click **OK** to return to the **Event Policy** dialog.

   Once you select the notifications in the steps above, and a Work Order event occurs that meets the specified criteria in the Event Policy, Requestors and/or Technicians will receive the notifications by e-mail or SMS, whichever are set up for the particular Technician on the Technicians dialog. If you selected the Work Order Assigned to a Technician event, when a new work order is created, the assigned technician will receive a notification. If a work order is

reassigned to a different technician, the new assigned technician will receive a Work Order Assigned to a Technician notification.

Note: The Assigned Technician will not receive an e-mail for actions they perform on their own Work Orders.

Related Topic:

Step 13b: Customizing Notifications (Optional).

Step 13b: Customizing Notifications (Optional)

You can customize the default notification text in templates that will display in e-mail notifications. You can also configure notifications to include hyperlinks and attachments, and send text messages (SMS). This includes the following templates:

- Work Order notifications (Event Policies)
- E-mail Monitor Policies notifications

(Labels and fields template-specific).

Notes:

- For Password Reset notifications, see Creating E-Mail Templates for Password Reset Notifications.

Example: Customized Work Order Notification Template and E-mail Message

Customized Work Order Notifications Template

The following customized e-mail notification will be sent to Technicians to notify them that a new work order has been created and assigned to them (on the text in the Subject and Body will display in the e-mail):

E-mail Subject:
New Work Order {ID}, {SUMMARY}
E-mail Body:
Work Order {LABEL ID}: {ID} has been added to your queue:
{LABEL:EXPECTEDCOMPLETIONDATE}: {EXPECTEDCOMPLETIONDATE}

Customized Work Order Notifications Template

The e-mail will display as follows:

From: HelpDesk@YourCompany.com
To: TechnicianName@YourCompany.com
cc:
Subject: Assigned Work Order 12345

Work Order ID: 12345 has been added to your queue:

Expected Completion date: 10/11/08

E-mail Created from Customized Work Order Notification Template

To Customize Notifications:

1. Navigate to the template you want to customize:
   - Work Order Notification templates
     - Tools/Administration Console/Configuration/Help Desk/Work Order Events/Work Order Notification Templates.
   - E-mail Monitor Policies auto-response template
     - Tools/Administration Console/Configuration/Help Desk/E-mail Monitor/E-mail Monitor Policies (select the policy, then click the Auto-Response Template button).

2. Customizing Message Contents:

   a. To **delete** a label and/or field in the Subject or Body text boxes:
      i. Select the text and press the **Delete** key.

      The default template displays some of the available labels and fields in the **Subject** and **Body** text box. (You can delete, edit, and add them as described in the steps below).

      In this example, we will delete the first paragraph in the Body:

      "{REQUESTOR} ({LABEL:CALLBACKNUMBER}: {CALLBACKNUMBER} and {LABEL:REQUESTOREMAIL}: {REQUESTOREMAIL}), has submitted a work order for the following issue, {SUMMARY}."

   b. Enter any **customized text and spaces** in the Subject or Body text boxes.
      - You can **cut and paste** the fields and labels to arrange them, and enter any additional customized text you'd like to display in the message.

   c. To add **hyperlinks to URLs** (such as http://www.numarasoftware.com):

      i. Type the URL in the text box.

The hyperlinks will automatically display in the text box and the notifications.

Hyperlink Protocol Examples:

http://www.test.com
https://www.test.com
www.test.com
ftp://ftp.test.com
ftp.test.com
mailto:user@domain.com
user@domain.com
news://news.domain.com
file://c:/temp

d. To **add** a label and/or field:
   i. Place your cursor in the location of the **Subject** or **Body** text box where you want to insert the label and/or field.

      Note: If you don't select a specific location for the label and/or field, they will display at the bottom of the text box.

   ii. Click the **Insert Field** button.
   iii. Select a field from the list in the **Insert Work Order Field** dialog, or select a **Category,** such as "General (Header)", then select a field, such as "ID").

      Note: Fields with multiple lines of text (such as those in Description fields) cannot be used in the Subject of an e-mail, so they will not be available for selection.

   iv. To **insert the field label and value**, click the check box at the bottom of the **Insert Work Order Field** dialog.

      In this example, the field label and value "{LABEL:ID}: {ID}" was inserted, and the text will display: " Work Order ID {ID} has been added to your queue:"

      You can select multiple fields by holding the Ctrl key while selecting them. Hold the Shift key to select multiple fields in sequential order.

         Note: Labels and fields are automatically formatted with braces around the text such as these: **{**LABEL:ID**}**: **{**ID**}**. If you rearrange the text, make sure to keep the braces intact.

   v. Click the **Close** button when you are finished selecting fields and labels.

3. To **include work order attachments** to the e-mail messages, click the designated check box at the bottom of the **Work Order Template** panel (below the **Body** text box).
4. To send notifications via **text message (SMS):**
   a. Click the checkbox under **Text Message (SMS)**.
      (A text message will be sent to the assigned Technician each time an e-mail notification is sent).
   b. To customize the text message, place your cursor in the SMS message text box, and follow the steps in Customizing Message Contents (2b), above.
5. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Make sure you've finished all the steps in the relevant notifications type to make sure your notifications are sent. When these steps are complete, you can test your notification formatting. (See Step 9: Testing E-mails Sent from E-mail Monitor).

Step 14: Scheduling Work Order Monitor to Automatically Check for Events

You can configure the Work Order Event Monitor to automatically check for Work Order Events at specific time intervals so that work order notifications can be sent.
To Schedule Work Order Monitor to Automatically Check for Events and Send Notifications:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Help Desk/Work Order Events/Scheduling**.
2. Click the **Enabled** check box to enable this feature.
3. Select the frequency at which you want to check for events from the Time Interval field (in minutes).
4. Click the **Apply** button to save your changes, or the **OK** button to close the window.

Step 15: Configuring Work Order Escalations

You can set up Event Policies so that the "Escalate to" Technician is automatically notified, via e-mail, when any of the events below occur during a Work Order's life cycle:

- Work Order's expected completion date approaching (notifications sent at the time specified on the Event Policy)
- Work Order's expected completion date overdue
- Work Order's due date approaching (notifications sent at the time specified on the Event Policy)
- Work Order overdue

Note: The "Escalate to" Technician must be set up on the Technician dialog. See Step 11: Designating a Technician for Work Order Escalations.
To Configure Work Order Escalations:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Event Policies**.
2. Select the Event Policy, then click the **Edit** button.
3. Click the **Configure Escalations** button.
4. Select the events for which you want to notify the "Escalate to" Technician (see the bulleted list above), then click the **OK** button.

   Note: The Due Date Approaching Alarm and the Expected Completion Date Approaching Alarm must be set up on the Event Policy in order to configure these for escalations. See

Step 16: Setting up Work Order Status Updates

Work Order Status Updates are auto-response messages that BMC Track-It! can send to users when they send e-mails requesting the status of a Work Order. You can specify the information to include in the auto-response e-mail (from the fields below), as well as a hyperlink users can click to receive the

auto-response e-mail and a hyperlink to append Work Order. Hyperlinks will be included for status inquiries and for appending new information to an existing Work Order.
To Set up Work Order Status Updates:

1. From the main menu bar, select **Tools/Administration Console/Configuration/ Help Desk/E-mail Monitor/Work Order Status Updates.**
2. Select the **Include hyperlinks** checkbox if you want users to be able to click to receive the auto-response e-mail and a hyperlink to append Work Order.
3. Select the Work Order database **fields** that you want to include in the message from the **Available content** list, then click the **Add** button to add them to the **Selected content** list.
4. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Configuring E-mail and SMS Templates for Work Orders

The default text for e-mails and text messages you can send from Work Orders is based on the Manual Notification template. You can change the template text directly from the **Send Technician E-mail Message** or **Send Requestor E-mail Message** dialog without having to go to the Administration Console.

Note: Only BMC Track-It! Administrators can modify the e-mail and SMS templates.

To Configure the E-mail Template:

1. From the **Help Desk** module Work Order grid, right click on any Work Order and select **E-mail Requestor** or **E-mail Technician** (the templates are different for each type of recipient.)
2. Alternatively, from the **Work Order** detail window, click the **E-mail Requestor** icon or select **E-mail** from the **E-mail Technician** icon on the toolbar.
3. On the **Send Technician E-mail Message** or **Send Requestor E-mail Message** dialog, click the **Template** button.

   This opens the **Manual Notification** (template) dialog. Changes you make to the template will affect the content of all messages sent to recipients from the Work Order. (See Customizing Notifications for detailed instructions.)
4. After you've made the changes, click the **Save** button on the **Manual Notification** dialog.

To Configure the text message (SMS) Template:

1. From the **Help Desk** module Work Order grid, right click on any Work Order and select **E-mail Technician**, then select **Text Message (SMS).**
2. Alternatively, from the **Work Order** detail window, select **Text Message (SMS)** from the **E-mail Technician** icon on the toolbar.
3. On the **Send Text Message (SMS)** dialog, click the **Template** button.

   This opens the **Manual Notification** (template) dialog. Changes you make to the template will affect the content of all text messages sent to Technicians from the Work Order. (See Customizing Notifications for detailed instructions.)
4. After you've made the changes, click the **Save** button on the **Manual Notification** dialog.

Setting up Skill Routing Policies

A Skill Routing Policy is used to assign a specific Technician to Work Orders based on matching criteria. When you set up a Skill Routing Policy and a Work Order is created that matches the criteria set up on the policy, the Technician assigned to the policy will automatically be assigned to the Work Order.

The system matches the criteria selected on the Work Order based on the order listed below:

- Requestor
- Department
- Location
- Type
- Subtype
- Category
- Priority

Skill Routing Policies Example

Skill Routing Policy Description		Matching Criteria					Assigned Technician or Technician Group
		Requestor	Department	Type	Subtype	Category	
1	All Networking requests from Executive department to Network Group		Executive	Networking			Network Group
2	All Desktop Hardware requests from Marketing department to John Smith		Marketing	Desktop	Hardware		John Smith (Desktop Hardware Tech)
3	All Desktop Applications requests to Desktop Applications Group			Desktop	Applications		Desktop Applications Group
4	All Requests from the CEO for Desktop Applications (presentations) to Mary Brown	CEO		Desktop	Applications	Presentations	Mary Brown (Desktop Applications Lead)

Notes:

- If desired, the Assigned Technician on a Work Order with a Skills Routing Policy can be changed.
- E-mail Monitor Policies take precedence over Skill Routing Policies.
- If you need to set up a Work Order policy based on events or priorities, see Setting up Event Policies.

To Set up a Skill Routing Policy:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Skill Routing Policies.**
2. Click the **Add** button to create a new **Skill Routing** Policy.
3. On the **Skill Routing Policy** dialog, enter a name for the policy in the **Name** field.
4. In the **Matching Criteria** section, select options from the following drop-down lists (matching will occur based on the order listed below):

- Requestor
- Department
- *Location
- Type
- Subtype
- Category
- *Priority

5. In the **Actions** section, select the T**echnician** to assign to the policy.
6. By default, the **Policy Enabled** checkbox is selected. You can de-select it if you are not ready to start the Skill Routing Policy.
7. Click the **Save** button on the **Skill Routing Policy** dialog.
   The new policy displays on the Skill Routing Policies panel of the Administration Console.

   When new Work Orders are created with your selected criteria, they will be assigned to the Technician you designated. See also Assigning Technicians to a Work Order.

Setting up Service Level Agreements (SLAs)

A Service Level Agreement is typically a contract between two parties (IT and another) to provide a minimal level of support, including prioritization, response time, and resolution commitment. The Service Level Agreement panel in the **Administration Console** enables you to name the SLA and attach an actual SLA document, such as a contract.

Notes:

- The SLA has no functionality in the system (other than storing the SLA document) until you associate the SLA with an Event Policy.

To Set up a Service Level Agreement:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Service Level Agreements**.
2. Click the **Add** button to create a new **Service Level Agreement**.
3. On the **Service Level Agreement** dialog, enter a name for the SLA in the **Name** field.
4. Enter any desired **Comments** in the designated text box.
5. To attach a file of the actual contract for the SLA, click the **Add** button, then navigate to the file from the **Open Attachment** dialog. Select the file, then click the **Open** button.
   The file displays in the **Attachments** section of the **Service Level Agreement** dialog.
6. To set up an Event Policy for the SLA, click the **Add** button in the **Event Policies** section.
7. When you are finished setting up the SLA, click the **Save** button on the **Service Level Agreement** dialog.

   The new SLA displays on the **Service Level Agreement** panel of the **Administration Console**. The **Classification and Schedule** tab of Work Orders associated with an SLA displays the SLA Name, the associated Event Policy Name, and Due Date.

See Also: Setting up Event Policies and Scheduling Due Dates and Deadlines in the Technician's Guide.

Creating Work Order Templates

You can create work order templates so that technicians can save data entry time when documenting recurrent issues. For example, technicians can select work order templates with pre-populated information for resetting user passwords, replacing network components, restoring lost data, and other

types of issues that may commonly occur within your organization. Work Order Templates can also contain Assignments. (See Adding Assignments to Work Orders.)

You can create Work Order Templates from the **Help Desk** module or from the Administration Console. You can also create them based on an Event Policy in the **Event Policies** panel in the **Administration Console**. (See Setting up Work Order Event Policies).

Certain fields are unavailable while you are creating the template so that they can be selected when creating new work orders from them. These are:

- Asset
- Call Back Number
- Date Completed
- Department Number
- Expected Completion Date
- Technician Assigned

To Create a Work Order Template from the Help Desk Module:

1. Select **New Work Order** from the **Tasks** pane in the **Help Desk** module.
2. Select **Template** from the **Actions** menu on the **Work Order** window tool bar, then click **Select Template**.
3. Click the **New** button on the **Apply Template** dialog box.
4. Complete the Work Order form as described in the topic Documenting the Issue in the Technician's Guide.

To Create a Work Order Template from the Administration Console:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Work Order Templates.**
2. Click the **Add** button on the **Work Order Templates** panel.
3. Complete the Work Order form as described in the topic Documenting the Issue in the Technician's Guide.

To Create a Work Order Template from an Event Policy (Administration Console):

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Help Desk/Event Policies.**
2. Select the Event Policy and click the **Add** (or **Edit** button for existing Event Policies).
3. Click the **Create Template** button.
4. Complete the Work Order form as described in the topic Documenting the Issue in the Technician's Guide.

See also: Creating a Work Order from a Template in the Technician's Guide.

Customizing Reports and Print Output

You can customize BMC Track-It! reports with Crystal Reports XI once you have exported them. (See Importing and Exporting Reports in the Technician's Guide.).

The default reports for individual work orders, assets, purchase orders, solutions, and software titles can also be customized. (These reports are accessed when Technicians click the Print button in BMC Track-It! for the selected records in a module's grid, such as a work order in the Help Desk module). Customizing reports might be useful for adding your organization's logo or selecting which database fields display. BMC Track-It! Administrators can replace the default reports with customized reports via the Print Output panels for each area in the Administration Console.

To Replace a Default Report with a Customized Report:

1. From the main menu bar, select **Tools/Administration Console/Configuration**, then select the desired module (Help Desk, Solutions, Inventory, Purchasing, or Software License Management).
2. Select **Print Output**.
3. Click the **Export Report** button on the **Print Output** panel.
4. On the **Save As** dialog, navigate to the drive or folder where you want to save the report, then click the **Save** button on the dialog.
5. Open the report (.rpt) in **Crystal Reports** and customize it as desired, then save it.
6. On the **Print Output** panel in BMC Track-It!, click the **Import Report** button.
7. On the **Open** dialog, navigate to the report, then click the **Open** button.
8. Click the **OK** button on the **Print Output** panel to save your changes and close the **Administration Console**.

Technicians will now be able to view the customized report when they print the individual records per module, such as work orders in the Help Desk module.

To Restore a Default Report:

Repeat Step 1 above, then click the **Restore Default Report** on the **Print Output** panel.

Self Service

BMC Track-It Self Service Overview

BMC Track-It! Self Service is a Web-based application that enables your end users to submit their own Work Orders and check the status of their requests. Users can attach files, such as screenshots, to Work Orders.

Users can also search for internal BMC Track-It! Solutions.

Users can audit their computers and change their passwords.

Change Management approvers can also approve Requests for Change with Self Service.

Note: Online help is available once users log in to Self Service. The topics in the online help are also available in the BMC Track-It! Self Service Guide (PDF) on the Product Documentation section of our Support Web page

See Also: BMC Track-It! Installation Guides, Configuring Self Service, and Change Management Overview

Configuring Self Service

You can configure Self Service Web to control the way users are allowed to submit Work Orders to your Help Desk, and to audit their own computers.

To Configure Self Service Web:

1. From the main menu bar, select **Tools/Administration Console/Administration/Self Service**.
2. Select an option from the Login Options (When a user attempts to log into Self Service) drop-down list:
    - Grant access and prompt the user to create a password for future logins, OR
    - Deny access for new users -- don't allow users to automatically create a new user ID and password.

3. Click the checkboxes to select options in the **Work Order Creation Options** section:
    - Allow Self Service users to complete their own Work Orders. (See Closing and Canceling Your Own Work Orders in the Self Service Guide.)
    - Allow Self Service users to attach files to their Work Orders (See Adding a New Work Order in the Self Service Guide.)
    - Allow Self Service users to view attachments to Solutions. (See Adding and Maintaining Work Order Solutions in the Technician's Guide.)
4. To enable or disable end users to audit their own computers, select an option from the Audits from Self Service drop-down list:
    - Enable the link for users and allow them to run audits
    - Hide the link from users. Don't allow them to run audits.
5. Click the **Apply** button to save your changes, and the **OK** button to close the window.

See the next topic, Viewing and Editing User Properties, for information on assigning Self Service licenses to users.

Viewing and Editing User Properties

Once you have either imported User groups from your directory service using Directory Importer or manually added Users, you can edit them from the Users panel in the Administration Console. The following describes editing a User's contact and account information including Self Service licensing, associating assets to a User, adding the User's photo; and viewing training information.
To Edit User Properties:

1. From the main menu bar, select **Tools > Administration Console > Lookup Tables > Administration > Users**.

Assigning Self Service Licenses

The most efficient way to assign Self Service licenses to Users is with the BMC Track-It! Directory Importer (see Selecting User Groups from Your Directory Service), where you can select to automatically assign Self Service licenses when new users are added to BMC Track-It!. However, you can also manually assign Self Service licenses to multiple users at a time from the Users lookup table or assign individual Users on the Users dialog.

Note: It is not necessary for Change Management Approvers to have a license to use BMC Track-It! Self Service; their BMC Track-It! Administrator only needs to provide them with a login user name.
To Assign Self Service Licenses to Multiple Users at a Time:

1. To quickly assign a **Self Service License** for one or several Users at a time, select the **Users** in the grid, then right click and select **Self Service Licensing**, then select **Include**.

    You can select **Exclude** to remove a Self Service License from a User.

    A **Results** log displays the license assignment and notifies you if there were any problems assigning the license.

To Grant Users Access to Self-Service Web and Configure Login Information:

1. Double click the **User's name** in the grid.
2. On the **Web Access** tab of the **Edit User** dialog, enter a **User Name** and **password** in the designated fields, or see Step 5 below to select an existing Windows account.

3. To disallow the user from changing passwords, select the **User cannot change password** checkbox.
4. If you are *not* using Windows Authentication, you can require the user to change the password at the next login. Select the **User must change password at next login** checkbox.
5. To enable the user to login with their existing Windows account, select the **User can login using Windows authentication with the following account** checkbox, then click the Ellipses (...) button next to the **Windows Account Name** field to open the **Select Account** window. Select the user name and click the **Add** button.

   For details, including how to configure pass through authentication, see our KnowledgeBase article: New Windows pass through authentication for Self Service users.
6. Click the **Access to Self-Service Web** check box (*not* required for Change Management Approvers: only a login User Name is required).
7. Click the **Save** button.

See also: Manually Adding Users

Editing a User's Attributes

Important Note: Field values in italics* (such as Department: *Accounting*) are managed by the Directory Importer and should not be directly modified in BMC Track-It!. Modifications to managed items should only occur in the directory service. The information can be entered, but when the Directory Importer is run and any of the User fields have changed, these values will be replaced by those existing in your directory service.

*The italics display if you have a license for scheduled imports and the Automated Schedule is enabled in the Directory Importer (see Scheduling and Manually Running the Directory Importer in the Administrator's Guide.

1. Select the User and click the **Edit** button.
2. On the **General** tab of the **Edit User** dialog, edit or enter the **Contact and Regional** information.
3. Click the **Save** button.

The User information (Full Name, Title, Phone, etc.) display in the grid on the Users panel.

Associating Assets with a User

To Associate an Asset with a User:

1. On the **Assets** tab, click the **Add** button.
2. The **Search** dialog displays. Enter the first four characters of the Asset Name or Asset ID in the Search for: field, then click the **Search** button.
3. Select the asset from the search results, then click the **Select** button.
4. Click the **Save** button.

Changing a User's Photo

To Change the User's Photo:

1. On the **Graphic** tab, click the Browse button to navigate to a file (such as .bmp or .jpg).
2. Click the **Save** button.

Viewing Training Information

You can view Training information (courses set up for individuals) on the Course History tab. See Tracking Training for Individuals in Your Organization in the Technician's Guide for details on Training.
To View Course Histories for an Individual:

1. Select the **Course History** tab
   The list of scheduled courses for the individual is displayed.
2. Double click a course to view details.

See also: Manually Adding Users

Configuring Password Reset

Password Reset Overview

BMC Track-It! Password Reset provides users with a Password Reset Assistant Web page that enables them to securely reset forgotten network passwords and unlock their accounts without assistance from the help desk or IT staff. With the optional Password Reset Kiosk, users can access the Password Reset Assistant from their own computers instead of a co-worker's.

Once configured, users access the BMC Track-It! Password Reset Assistant Web page by clicking the URL link you provide them (usually on your organization's intranet) from:

- Their own computer using their network account
- A coworker's computer using their own network account
- Any computer using a Password Reset kiosk account (optional)

Prerequisites

In order to set up BMC Track-It! Password Reset, you should be familiar with the following terms and concepts.

- Microsoft Internet Information Services and SSL (in Configuring the Password Reset Web Site and Testing the Certificate)
- For the Password Reset Kiosk version (optional):
  - Creating a user in your Windows Active Directory (in Setting up the Kiosk Selfhelp Account, Policy, and Privileges)
  - Creating security policies and permissions and using the SYSVOL shared directory on your network (in Copying the KioskBrowser.exe File to the SYSVOL Shared Directory)
  - Login scripts (optional -- in Customizing the Password Reset Users' Kiosk Login Screen)
  - Microsoft Management Console (in Setting up the Kiosk Selfhelp Account, Policy, and Privileges)
- For troubleshooting, TCP ports and ASPNET user account (in Troubleshooting Password Reset (TCP, ASPNET)

Next Topic: Password Reset Security and Strength Policies

Password Reset Security and Strength Policies

Password Reset Security

BMC Track-It! Password Reset takes advantage of the following security protocols:

- Microsoft Security Support Provider Interface (SSPI) is used to obtain integrated security services for authentication, message integrity, message privacy, and secure quality of service.
- Secure Socket Layer (SSL) is used to provide secure data communications through encryption and decryption.
- Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is used to encrypt and decrypt user page requests, as well as the pages that are returned.
- HTTPS and SSL support the use of X.509 digital certificates from the server so that, if necessary, a user can authenticate the sender.

Password Strength Policies

BMC Track-It! Password Reset enforces the various password policies offered by the operating system with these caveats:

- Password Reset does not allow a user to reset their password if the "Minimum Password Age" policy is set to a value other than 0 days.
- The "Enforce Password History" policy is not fully enforced for password resets done through the Assistant. It will allow them to re-use passwords more quickly than when the password is changed through the operating system. One way to accommodate this would be to double the number of passwords remembered.
- To help users know what your password complexity requirements are, describe them in the Admin Utility's "Security Policy Description" entry box. This description will then be visible to the user when they are prompted to enter their new password.
- If a user's choice for a new password does not meet the requirements of the password policy that is currently in force in your organization, the application will return an error message indicting that an *invalid password format* has been entered.

Next Topic: Getting up and Running with BMC Track-It! Password Reset

Configuring Password Reset

Getting up and Running with BMC Track-It! Password Reset

The following is a list of tasks necessary to configure the Password Reset Assistant and the optional Password Kiosk. Once you've completed these steps, your users will be able to register on the Password Reset Assistant Web page. After you've granted them permissions (see step 2 below), they will be able to use the Password Reset Assistant.
Prerequisites
In order to set up BMC Track-It! Password Reset, you should be familiar with the following terms and concepts.

- Microsoft Internet Information Services and SSL (in Configuring the Password Reset Web Site and Testing the Certificate)
- For the Password Reset Kiosk version (optional):
    - Creating a user in your Windows Active Directory (in Setting up the Kiosk Selfhelp Account, Policy, and Privileges)
    - Creating security policies and permissions and using the SYSVOL shared directory on your network (in Copying the KioskBrowser.exe File to the SYSVOL Shared Directory)
    - Login scripts (optional -- in Customizing the Password Reset Users' Kiosk Login Screen)

- Microsoft Management Console (in Setting up the Kiosk Selfhelp Account, Policy, and Privileges)
- For troubleshooting, TCP ports and ASPNET user account (in Troubleshooting Password Reset (TCP, ASPNET)

To Access the Password Reset Administrator Console:

1. Click **Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility.**

To Configure Password Reset:

TASK	MODULE/WINDOW	HELP TOPIC
Configure Password Reset with the Password Reset Administration Console		
1. Customize the Password Reset Web page	Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility > Track-It! Password Reset Administrator dialog > User Interface tab	Customizing the Password Reset Web Page
2. Grant or deny permissions to end users	Track-It! Password Reset Administrator dialog/ Permissions tab	Granting/Denying Permissions
3. Define challenge questions	Track-It! Password Reset Administrator dialog/ Questions tab	Defining Challenge Questions
4. Enable automatic work order creation	BMC Track-It! Password Reset Administrator dialog/ Template tab	Enabling Automatic Work Order Creation and Creating Work Order Templates
5. Create Password Reset work order templates	BMC Track-It! Password Reset Administrator dialog/ Template tab	Enabling Automatic Work Order Creation and Creating Work Order Templates
6. Create e-mail templates for Password Reset notifications to users	BMC Track-It! Password Reset Administrator dialog/ E-mail tab	Creating E-Mail Templates for Password Reset Notifications
Configuring and Testing Your Password Reset Web Site		

7. Configure Password Reset Web site	Start/ Programs/Administrative Tools/Internet Information Services	Configuring the Password Reset Web Site and Testing the Certificate
8. Test the certificate	http://localhost/TIWEB/PasswordReset	Configuring the Password Reset Web Site and Testing the Certificate
Test the Password Reset Assistant as a User		
9. Test the Password Reset Assistant as a User	BMC Track-It! Password Reset Administrator dialog/	Testing the BMC Track-It! Password Reset Assistant as a User
Advertise the Password Reset Assistant to Users		
10. Create an e-mail announcement to advertise Password Reset to users	E-mail client	Creating an E-Mail Announcement to Advertise Password Reset to Users
11. Add an announcement in BMC Track-It! to advertise the Password Reset Assistant	Start/All Programs/BMC Track-It!	Creating announcements
Implement a Password Reset Kiosk Account (Optional)		
12. Copy the KioskBrowser.exe File to the SYSVOL share directory	C:\Program Files\BMC Software\Track-It!\Track-It! Web\Password Reset\bin	Copying the KioskBrowser.exe File to the SYSVOL Shared Directory
13. Set up the Kiosk Selfhelp Account, Policy, and Privileges	Windows Active Directory	Setting up the Kiosk Selfhelp Account, Policy, and Privileges
14. Customize the Password Reset Users' Login Screen	See topic for logon scripts	Customizing the Password Reset Users' Kiosk Login Screen

Next Topic: Customizing the Password Reset Web Page

Customizing the Password Reset Web Page

You can customize the information displayed on the Password Reset Assistant Web page with your organization's name and contact information, such as your help desk URL, special instructions, and a description of your security policy, in the event that users need additional assistance.
To Access the Password Reset Administrator Console:

1. Click **Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility.**

To Customize the Password Reset Web Page:

1. Select the **User Interface** tab on the **BMC Track-It! Password Reset Administrator** dialog.
2. Enter the **Title** that you want to appear at the top of the page.
3. Enter your help desk's URL and contact instructions.
4. Enter information on how to reset using Password reset in the Reset Help text box.
5. Enter a description of your organization's security policy.
6. Click the **Apply** button.

Next Topic: Granting/Denying Permissions

Granting/Denying Permissions

You can determine which users will have permission to reset their password or unlock their account. You can also determine the number of times a day users can use Password Reset to reset their password.

Once you notify users of how to access the Password Reset Assistant Web page, and they complete the registration information, their user names will display on the Permissions screen of the Password Reset Administration Console. (See Advertising the Password Reset Assistant to Users.) When you have finished setting up Password Reset and/or the optional Password Reset Kiosk, return to this topic and complete the steps below.

To Access the Password Reset Administrator Console:

1. Click **Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility**

To Add/Remove Users from the Permission List:

1. Select the **Permissions** tab in **BMC Track-It! Password Reset Administrator** dialog.
2. Select the **User Name** that you want to **Add** or **Remove**.
3. Click the **Right-Arrow** or **Left-Arrow** button to move the selected user to the desired list.
4. Click the **Apply** button.

Next Topic: Defining Challenge Questions

Defining Challenge Questions

Challenge questions are used as an alternative means of authenticating users before they can reset their own accounts or replace forgotten passwords with new ones. You can use the default challenge

questions supplied with Password Reset, edit existing questions, or you can create an unlimited number of your own customized questions. You can also determine the number of questions users are required to answer.

You should consider using questions that will make it easy for your users to remember the answers. The following are examples of default and customized questions:

Default Questions

- What's your favorite color?
- What's your mother's maiden name?
- What's your pet's name?

Customized Challenge Questions

- What was your first pet's name?
- What are the last four digits of your social security number?

Editing Existing Challenge Questions

Note: If any users have already registered their accounts with BMC Track-It! Password Reset, and you edit an existing question, users can still use their previously registered answers. For example, if you changed the question: "What's your pet's name?" to "What *was* your *first* pet's name?", users can respond with the initial answer they gave during registration.

To Access the Password Reset Administrator Console:

1. Click **Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility.**

To Edit Existing Questions:

1. Select the **Questions** tab in **BMC Track-It! Password Reset Administrator** dialog.
2. Select the question and press the **F2** key.
3. Edit the question, then click the **OK** button on the **Edit Question** dialog, then click the **Apply** button.

Adding New Challenge Questions

You can add an unlimited number of new challenge questions. Challenge question answers are not case-sensitive.

Important Note: Once a question is created, it cannot be deleted.

To Add a New Challenge Question:

1. Click the **Create a Custom Question** button.
2. Enter your question in the text box of the **Create Question** dialog, then click the **OK** button, then click the **Apply** button.

After you've edited or created your questions, make sure to make them available to users by adding them to the Web page (see below).

Determining the Number of Questions Users Are Required to Answer

You can ask your users to choose and answer either all or up to two challenge questions from the list of available questions.

To Determine the Number of Required Questions:

1. Select either the **All** radio button or select a number (1 or 2) from the drop-down on the second radio button, then click the **Apply** button.

Adding the Challenge Questions to the Password Assistant Web Page

To Add the Challenge Questions to the User Interface (Web Page):

1. Select the question from the list on the left, then click the **Right-Arrow** button to move the selected questions to the list on the right.
2. If desired, use the **Up-Arrow** or **Down-Arrow** button to position the selected question in the list, then click the **Apply** button.

Now when users attempt to edit their Password Reset accounts or reset their passwords, they will be required to enter answers to the challenge questions.

Next Topic: Enabling Automatic Work Order Creation and Creating Work Order Templates

Enabling Automatic Work Order Creation and Creating Work Order Templates

Note: This information applies to the Password Reset add-on module. To create work order templates for BMC Track-It!, see Creating Work Order Templates.

Automatic Work Order Creation for Password Reset Attempts
You can configure BMC Track-It! Password Reset to automatically generate work orders in BMC Track-It! to track all user attempts for the following:

- Successful or Unsuccessful attempts:
  - Password Reset
  - Account Unlock
- Password Reset Misuse

With this configuration, work orders are automatically created, then closed if the user is successful in registering his or her account or resetting the password. If the user is unable to successfully complete any of these processes, the work order will be assigned to a technician and routed through your help desk based on the priority level that you define.

Note: BMC Track-It! Monitor can be configured to automatically send an e-mail notification to the requestor, indicating that a work order has been generated and a technician has been assigned to help resolve the issue. (See E-mail Monitor and Work Order Notifications Overview).
Work Order Templates for Password Reset Events
You can configure Password Reset work order templates so that when automatic work orders are created, the user's name, user's domain name, and user's login name are automatically displayed in the work order. The following default strings can be used in your work order templates, which will be substituted by the actual user information when the work order is created.

	Work Order Template Strings for User Information	
User Information Strings	**Description**	**Used in Work Order's:**
%UserName%	Name of the user from the BMC Track-It! database	Requestor field, Description field
%LoginDomain%	Domain name for the user account	Description field
%LoginUserName%	Login name for the user account	Description field

You can use the default text as displayed on the Work Order Template screen, or you can use the strings with your own text.
Example

For example, you want the Description field for all password-related work orders that are submitted by Tom Jackson to read:

> Tom Jackson needs the password to be reset for the following domain and account: Marketing\TJackson

To accomplish this, you would enter the following substitution string into the Description field of the password reset work order template:

> **%UserName%** needs the password to be reset for the following domain and account: **%LoginDomain%\%LoginUserName%**

To Access the Password Reset Administrator Console:

1. Click **Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility.**

To Configure Work Order Templates for Password Reset Events

1. Select the **Work Order Template** tab in **BMC Track-It! Password Reset Administrator** dialog.
2. Select an option from the **Outcome of User Operation** drop-down list (such as Unsuccessful Password Reset).
3. Select the **Submit Work Order for this Operation** checkbox.
4. Enter the text or select an option from the following fields:
    - Default Requestor

      Important Note: If the User Name is not in your database, Password Reset will populate the Requestor field (%UserName%) with the name: "PasswordReset".
    - Assigned Technician
    - Priority

    - Hours
    - Summary
    - Description
    - Resolution
    - Work Order Type
        - Type
        - Subtype
        - Category
5. Click the **Apply** button.

Next Topic: Creating E-Mail Templates for Password Reset Notifications

Creating E-Mail Templates for Password Reset Notifications

You can configure BMC Track-It! Password Reset to send e-mail notifications to users for specific events that occur when they use the Password Reset Assistant.

- Successful or Unsuccessful attempts:
    - Password Reset
    - Unlock Account
- User Registration
- Update User Registration

Once you've configured Password Reset to send notifications, and users register using the Password Reset Assistant (see Testing the BMC Track-It! Password Reset Assistant as a User), whenever they use the Assistant, they will receive an automatic e-mail when any of the above events occur.

When BMC Track-It! Password Reset generates an e-mail notification to users, it can automatically customize the text and user information that appears in the Body field of each e-mail. You can use the default text for a different message for each of the four possible events, or you can create your own. You can use the user information strings listed below to automatically include user-specific information in each new e-mail notification. This information includes the user's name, user's domain name, and user's login name.

	E-mail Notification Strings	
User Information Strings	**Description**	**Used in E-mail's:**
%UserName%	Name of the user from the BMC Track-It! database	Body field
%LoginDomain%	Domain name for the user account	Body field
%LoginUserName%	Login name for the user account	Body field

Example
For example, if you want the body of your e-mail notification to read:

> Dear **Mary Wilson**,
>
> Your password for your **Sales\MWilson** network account has been successfully reset.
>
> Thank you for using the Password Reset Assistant.

To accomplish this, you would enter the following substitution string into the Body field of the e-mail template:

> Dear **%UserName%**,
>
> Your password for your **%LoginDomain%\%LoginUserName%** network account has been successfully reset. Thank you for using the Password Reset Assistant.

To Access the Password Reset Administrator Console:

1. Click **Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility.**

To Create E-mail Templates for Password Reset Notifications:

1. Select the **E-mail** tab in **BMC Track-It! Password Reset Administrator** dialog.
2. Select the e-mail type from the **Active E-mail Server Type** radio buttons (Exchange/MAPI or SMTP).
3. Enter the **server** information.
4. Enter the user name for the mailbox.
5. Enter the **mailbox password**.
6. Enter the **name** that you want to display as the Password Reset administrator in the **From:** field (such as "Help Desk").
7. Enter the **e-mail address** that you want to display as the Password Reset administrator in the **E-mail:** field (such as "HelpDesk@your-company.com")
8. Select an option from the **Message Content for:** drop-down list (such as Successful Password Reset).
9. Click the **Send Message** checkbox.
10. Enter the subject appropriate for the option selected # 8 above in the **Subject:** field.
11. Enter a message appropriate for the option selected # 8 above in the **Body:** field.
12. Click the **Apply** button.

To Test E-mail Notifications:

1. Click the **Send Test E-mail to Self** button.
2. Enter an e-mail address (such as your own) in the **E-mail Test** dialog.

   A message will display to confirm whether or not the message was sent successfully.

Next Topic: Configuring the Password Reset Web Site and Testing the Certificate

Testing Your BMC Track-It! Password Reset Configuration

Configuring the Password Reset Web Site and Testing the Certificate

To Configure the Password Reset Web Site:

1. Open the **Microsoft Internet Information Services** from **Start/ Programs/Administrative Tools/Internet Information Services**.
2. Double-click the server name so that you see all the Web sites.
3. Expand the **Default Web Site**, then expand **tiweb**.
4. Right-click the **PasswordReset** Web site where you want to install the certificate, and then click **Properties**.
5. On the **Directory Security** tab, under **Secure Communications**, note that you now have three available options. To set the Web site to require secure connections, click **Edit**. The **Secure Communications** dialog box appears.
6. Select **Require Secure Channel (SSL)**, and then click **OK**.
7. Click **Apply** and then **OK** to close the **Properties** dialog.

To Test the Certificate:

1. Locate the site and verify that it works:
    a. Access the site through http by typing **http://localhost/tiweb/PasswordReset** in the browser.
    b. If you receive an error message such as: "HTTP 403.4 - Forbidden: SSL required":
        - Try to access the same Web page with a secured connection (https) by typing **https://localhost/TIWEB/PasswordReset** in the browser.
        - If you receive a security message that states that the certificate is not from a trusted root certification authority, click **Yes** to continue to the Web page.
    c. If you receive the following error message: "Server Error in '/TIWEB/PasswordReset' Application", see our KnowledgeBase article "Server Error in '/PasswordReset' Application" Error Page Appears When Launching Password Reset"

If you can view the Web page, you have successfully installed your certificate.

Next Topic: Testing the BMC Track-It! Password Reset Assistant as a User

Testing the BMC Track-It! Password Reset Assistant as a User

Before you deploy BMC Track-It! Password Reset throughout your organization, you should thoroughly test your configuration settings using a "test" user account. The following are instructions to test your Password Reset configuration by:

- Creating a test network user account in Password Reset
- Registering the test user account in Password Reset
- Updating the test user account in Password Reset
- Resetting a user Password

To Access the Password Reset Administrator Console:

1. Click **Start > All Programs > BMC Track-It! > BMC Password Reset > Password Reset Administration Utility.**

To Test Your BMC Track-It! Password Reset Configuration:

1. Create a typical network user account that you can use for testing.
2. Select the **Start Here** tab in the **BMC Track-It! Password Reset Administrator** dialog.
3. Click the **Password Reset Start Page** test link at the bottom of the page.

Note: If a "Page cannot be found" error is displayed in your browser, see our Support KnowledgeBase article: "Password Reset Start Page" Link Doesn't Work in the Password Reset Administration Utility

The **Password Reset Administration Start Page** is displayed, which allows you to access all of the links to register an account, unlock an account, reset a password, and update a registration from one convenient location.

Registering as a User in Password Reset

Notes:

- This Web page will NOT be visible to your network users. It is intended to be used by the administrator for testing purposes only.

- If you receive the following error message: "Server Error in '/TIWEB/PasswordReset' Application", see our KnowledgeBase article

1. Click the **Registration** link to begin the registration process and display the **Registration** Web page.
2. Click the **Register** button to continue. The next **Registration** Web page appears.
3. Enter the name of your Login Domain.
4. Enter your Username and Password.
5. Click the **Continue** button to continue. The next **Registration** Web page appears.
6. Enter your **E-Mail Address**.
7. Select a unique **Challenge Question** from each of the dropdown lists.
8. Enter your **Answer** twice for each of the questions.
9. Click the **Register** button to register your account using the selected challenge questions. The **Registration Completed Successfully** Web page appears.
10. Click the **Exit** button to exit the registration process.

    Your test user account is now registered and able to utilize the BMC Track-It! Password Reset Assistant.

Updating Password Reset Registration as a User

From time to time, users may want to update their password reset registration information. Users may choose to do this for security reasons, or perhaps they just want to select a new set of challenge questions whose answers are easier to remember. The process for updating a registration is similar to the initial registration process.

When a currently logged-in user revisits the BMC Track-It! Password Reset Assistant Web page, the challenge questions with masked answers (for security purposes) are displayed. The user's challenge question answers are masked to prevent coworkers from viewing this personal information.

Resetting a Password as a User

Once a user account has been registered, it's easy to reset the password for that account without having to call the help desk for assistance. To reset the password on your test user account, you must return to the Password Reset Administration Start Page, which allows you to access all of the links to register an account, unlock an account, reset a password, and update a registration from one convenient location.

Important: When choosing a password, make sure to comply with your company's password policy. If your new password does not meet the requirements of the policy that is currently in force, the application will return an error message indicating that you have entered an *invalid password format*.

1. Select the **Start Here** tab in the **BMC Track-It! Password Reset Administrator**.
2. Click the **Password Reset Start Page** test link at the bottom of the page in order to return to the **Welcome to the Password Reset Administration Start Page**:

3. Click the **Unlock Account and Reset Password** link to reset the password for your test user account.

   The **Account Reset Assistant** Web page displays.

4. Enter the name of your **Login Domain**.
5. Enter your **Username**.
6. Click the **Continue** button to continue.

   The **Account Unlock** Web page displays.

7. Enter your **Answer** for each of the questions.
8. Click the **Continue** button to authenticate your account based on the answers that you entered for each of the challenge questions.

   If you answered the challenge questions correctly, the next **Account Unlock** Web page appears.

9. Enter and confirm a new **Password** for your account.
10. Click the **Continue** button to continue.

    The last **Account Unlock** Web page displays.

11. Click the **Exit** button to exit the password reset process.

    Note: If you are running the Password Reset Kiosk (**`KioskBrowser.exe`**), the system will automatically log you out of the SELFHELP account. (See Implementing a Password Reset Kiosk Account (Selfhelp).

12. Try logging into your workstation using your test user account and new password.

Next Topic: Advertising the Password Reset Assistant to Users

Advertising the Password Reset Assistant to Users

Advertising the Password Reset Assistant to Users

Once a BMC Track-It! Password Reset has been installed on your network and configured, you should advertise the availability of the application and its benefits. Below are a few suggestions for advertising the Password Reset Assistant:

- Notify users by e-mail (best method)
  (See Creating an E-Mail Announcement to Advertise Password Reset to Users)
- Add an announcement in BMC Track-It! Self Service
  (See Creating announcements in the Technician's guide)
- Add instructions to your help desk's voice mail system
  (directing users to log in to the Password Reset Assistant Web page)
- Advertise the Password Reset Assistant on-site
  (on mouse pads, quick reference cards, employee handbooks, etc.)

Next Topic: Creating an E-Mail Announcement to Advertise Password Reset to Users

Creating an E-Mail Announcement to Advertise Password Reset to Users

Users should be notified of the deployment of BMC Track-It! Password Reset before and after it happens. They should be informed of what BMC Track-It! Password Reset is, why it's being deployed, how it will benefit users, and how users can register their accounts in order to utilize this service. If your organization has a large number of users, the best method for informing users about BMC Track-It! Password Reset is via e-mail (see the example below):

Example E-mail Announcement

From: Your Company's Help Desk
To: Everyone
Subject: How to Reset Your Own Passwords

To accommodate the growing needs of our organization, **[Your Company's Help Desk]** is activating a password management system on our network. This system will help you manage your own passwords in the following ways:

- If you forget your password, you will be able to reset it yourself without calling the help desk.
- If you get locked out of your account, you will be able to reset it yourself without calling the help desk.
- If you want to change your password reset registration information, you will be able to change it yourself without calling the help desk.

Please take a few moments to register with the password reset system now by:

1. Clicking on the following link: http://localhost/PasswordReset/ResetPassword.htm
2. Selecting and answering challenge questions from the drop-down lists.

That's all there is to it! After registering, if you forget or disable your Windows password, you can log into the Password Reset Web page using a coworker's computer to change your own password and/or reset your own account.

Thank you!
[Your Company's Help Desk]

See also: Creating announcements in the Technician's Guide.

Implementing a Password Reset Kiosk Account (Optional)

Implementing a Password Reset Kiosk Account (Selfhelp)

If your organization adheres to stringent security policies, you can set up an optional Password Reset Kiosk version of the Password Reset Assistant so that users can access the Password Reset Assistant on their own computers instead of having to use a coworker's computer.

The Password Reset Kiosk (**`KioskBrowser.exe`**) is a locked-down, alternate shell version of Internet Explorer. It uses a limited-privilege network account called Selfhelp. The login is a publicly-shared domain account with a public password. When users forget their passwords and are locked out, the Password Reset Kiosk browser displays on their computer screen automatically. Since only the BMC Track-It! Password Reset Web page displays, they are prevented from exiting the Password Reset Web page and accessing any other applications or their desktop. None of the Internet Explorer buttons, links, or other controls will display, and users cannot access any other Web pages.

WARNING: A Password Reset Kiosk account can provide users with added convenience, but it may also increase your network security risks if not implemented correctly.

Prerequisites
In order to set up The Password Reset Kiosk account, you should be familiar with the following terms and concepts.

- Creating a user in your Windows Active Directory (in Setting up the Kiosk Selfhelp Account, Policy, and Privileges)
- Creating security policies and permissions and using the SYSVOL shared directory on your network (in Copying the KioskBrowser.exe File to the SYSVOL Shared Directory)
- Login scripts (optional -- in Customizing the Password Reset Users' Kiosk Login Screen)
- Microsoft Management Console (in Setting up the Kiosk Selfhelp Account, Policy, and Privileges)

Next Topic: Copying the KioskBrowser.exe File to the SYSVOL Shared Directory

Copying the KioskBrowser.exe File to the SYSVOL Shared Directory

SYSVOL (System Volume) is a shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain. You'll need to copy the KioskBrowser.exe file into SYSVOL.

By default, the KioskBrowser.exe file can be found in the following directory: `C:\Program Files\BMC Software\Track-It!Web\Password Reset\bin.`
To Copy the KioskBrowser.exe File to the SYSVOL Shared Directory:

1. Copy the **KioskBrowser.exe** file from the **Bin** folder of the installed directory to the **SYSVOL** share on your network.

   This will allow network users to access an alternate shell version of Internet Explorer (KioskBrowser.exe). Although this custom browser purposely lacks most of the features and

functions of Internet Explorer, it still utilizes a control that requires Internet Explorer be installed on all workstations that may need access to the password reset kiosk account.

Note: In the event a user tries to log on using CTRL+ALT+DELETE, the following buttons are disabled:

- Lock Computer
- Task Manager
- Shut Down
- Change Password

The user can only Log Off or Cancel out of the menu and return to the Password Reset Assistant.

Next Topic: Setting up the Kiosk Selfhelp Account, Policy, and Privileges

Setting up the Kiosk SELFHELP Account, Policy, and Privileges

The SELFHELP user account is a limited-privilege account that users can log into in order to access the Password Reset Assistant via our alternate shell version of Internet Explorer (**`KioskBrowser.exe`**). Since most of Internet Explorer's functionality is not available in Kiosk Browser by design, there are very few settings that need to be manually configured in order to lock down the SELFHELP account.

Important: If you're running a Windows NT server with NT and/or 2000 clients, refer to the section below on *Windows NT/2000 Workstations on an NT Domain* for instructions on how to lockdown the SELFHELP account.

For Windows Server 2003 or Server 2008 with Active Directory

The following instructions replace steps A-E in “For Windows 2000 Servers with Active Directory”, below.

1. Open **Active Directory Users and Computers**.
2. Create an **Organizational Unit** to contain the **Password Reset kiosk user**.
3. Create the **Password Reset kiosk user** in the Organizational Unit created in Step 2.
4. Click **Start** > **Run**, type **MMC**, then click the **OK** button.

   (Alternatively, you can open the Server Manager and start with Step 7).
5. Click **File** > **Add/Remove Snap-in**.
6. Select the “**Group Policy Managemen**t” snap in, and click **OK**. (This can also be accessed from the Features section in Server Management.)
7. In the **Server Manager**, locate the **Organizational Unit** created in step 2 , then right click this Organizational Unit and select “**Create a GPO in this domain, and Link it here**”.
8. Right click the **newly created policy**, and click **Edit**.
9. On the **Group Policy Management Editor**, expand **User Configuration**, then **Policies**, then **Administrative Templates: Policy definitions**, then **Control Panel**, then **Display.** Disable the “**screen saver**” option.
10. Expand **User Configuration**, then **Policies**, then **Administrative Templates: Policy definitions**, then **System**. Enable “**Prevent access to registry editing tools**.”
11. Expand **User Configuration**, then **Policies**, then **Administrative Templates: Policy definitions**, then **System**.
12. Enable **custom user interface**, then enter the UNC path to the EXE, e.g., \\<servername>\netlogon\kioskbrowser.exe /url=http://ServerName/TIWEB/PasswordReset.
13. Expand **Computer Configuration**, then **Policies**, then **Administrative Templates: Policy definitions**, then **Windows Components**, then **AutoPlay Policies.** Enable the **turn off AutoPlay policy**, then select **All Drives**.

14. Expand **User Configuration**, then **Policies**, then **Administrative Templates: Policy definitions**, then **System**, then **Ctrl+Alt+Del Options**. Enable the "**Remove Change Password**", "**Remove Lock Computer**" and "**Remove Task Manager**"options.

For Windows 2000 (or Higher) Servers with Active Directory

Follow the instructions below on:

A. Creating the SELFHELP user account
B. Creating the SELFHELP group policy
C. Adding the SELFHELP user to the profile
D. Restricting the SELFHELP's user privileges
E. Preventing the SELFHELP user from mounting unprotected shares (optional extra security measure)
F. Applying the security policy to the SELFHELP user
G. Test the SELFHELP user login

A. To Create the SELFHELP User Account:

1. Log into the domain as Administrator.
2. Open **Active Directory Users and Computers**.
3. Create a **new user** called **SELFHELP**.
4. Clear the **password** fields.

   You may have to set your password strength rules to require a minimum length of 0 before you can clear the password fields.

5. Select the following checkboxes:
   - **User cannot change password**
   - **Password never expires**
6. Clear the following checkboxes:
   - **User must change password at next login**
   - **Account disabled**
7. Close **Active Directory Users and Computers**.

B. To Create the SELFHELP Group Policy:

1. On the domain controller, open the **Microsoft Management Console** (**Start/Run** from the Windows taskbar, type **mmc** in the text box, and press the **Enter** key).
2. Select **Console/Add/Remove Snap-in…** from the main menu bar.
3. Click the **Add…** button to view the available snap-ins and add a **Group Policy** snap-in.
4. Click the **Browse** button.
5. Select the **Domain/OU** tab.
6. Click the **New Policy** button (i.e., person icon) to create a new policy.
7. Name the group policy **SELFHELP POLICY**.
8. Select **SELFHELP POLICY** as the group policy for this snap-in.

C. To Add the SELFHELP User to This Profile:

1. Right-click on the new policy and select **Properties**.
2. Select the **Security** tab.
3. Click the **Add…** button and select the **SELFHELP** user that you defined earlier.
4. Under the **Permissions** for the SELFHELP user, select the following checkbox under the **Allow** column:
   - **Apply Group Policy**
5. Verify that the **Apply Group Policy** checkbox is disabled for all other users and groups.

D. To Restrict the SELFHELP User's Privileges:

1. Expand the tree under the **SELFHELP\User Configuration\Administrative Templates**.
2. Browse to **Control Panel\Display** and disable the following option: **Activate Screen Saver**.
3. Browse to **System** and enable the following options:
   - **Disable registry editing tools**
   - **Disable Autoplay**
     (Make sure to set the "**Disable Autoplay** on:" value to **All drives**)
   - **Custom user interface**
4. In the **Interface** file name box, type the full path (UNC name of the domain controller with the SYSVOL share) to Kiosk Browser (KioskBrowser.exe) on the domain controller.

   Make sure to include the URL switch. For example, type:

   \\<servername>\sysvol\kioskbrowser.exe /url=http://localhost/

5. Browse to following folder: **\System\Ctrl+Alt+Del Options** and disable the following:

   - Logoff
   - Task Manager
   - Lock Computer
   - Change Password

E. To Prevent the SELFHELP User from Mounting Unprotected Shares (Optional Extra Security Measure):
IMPORTANT: It is possible for end-users to **abuse** the SELFHELP account on Windows 2000/Active Directory by mounting unprotected share using the following command: "net use \\<servername>\sysvol /user:SELFHELP ".

However, you can configure a domain-wide policy that prevents the SELFHELP user from mounting shares on workstations and servers, but still allow it to mount the SYSVOL share on the domain controller that is used to apply the SELFHELP account.

To do this, you must:

- Create a policy that denies the SELFHELP user access to all network shares.
- Remove the SELFHELP user from that policy and give it only the privileges that it requires (i.e., access to the SYSVOL share).

The following procedure allows you to protect shares on Windows 2000 (or higher) workstations and servers that are otherwise open to user who are part of the Everyone group.

1. On the domain controller, select **Start/Settings/Control Panel/ Administrative Tools** from the Windows taskbar.
2. In the **Domain Security Policy** window, select **Windows Settings/Security Settings/Local Policies/User Rights Assignment**.
3. Double-click on **Deny access to this computer from the network** to open the **Security Policy Setting** dialog box.
4. Enable the **Define these policy settings** checkbox.
5. Click the **Add** button.
6. Select the **SELFHELP user** and click the **OK** button.

The SELFHELP user should now be prevented from mounting any network shares. You can verify this by checking that the SELFHELP user is listed under the **Computer Setting** column.

1. In the **Domain Security Policy** window, select **Windows Settings/ Security Settings/Local Policies/User Rights Assignment**.
2. Double-click again on **Deny access to this computer from the network** to open the **Security Policy Setting** dialog box.
3. Enable the **Define these policy settings** checkbox.
4. Make sure that **SELFHELP user** is ***not*** in the list.
5. Click the **OK** button.

At this point, you should have overridden the policy that was set in the steps above. Effectively, you have accomplished two tasks:

- You prevented the SELFHELP user from mounting any shares on user workstations, while
- Still allowing that user to access the SYSVOL share where Kiosk Browser is located.

You can verify this by making sure that the Computer Setting column is empty.

IMPORTANT: It may take some time for your policy changes to propagate to all of the servers and workstations on your network. You can expedite this process by typing the following at a command prompt: **secedit /refreshpolicy user_policy secedit /refreshpolicy machine_policy**. If you experience problems with this policy, make sure that your Windows 2000 workstations are using the Windows 2000 Domain Controller as their primary DNS server.

F. To Apply the Security Policy to the SELFHELP User:

1. After setting the group policy object (GPO) in **Microsoft Management Console (MMC)**, select **Console/Save** from the main menu bar to save this group policy.
2. This group policy should now be in effect every time the SELFHELP user logs into the domain.

G. Test the SELFHELP User Login

1. Login as the SELFHELP user to test the configuration.

   You should not be able to do anything other than access the BMC Track-It! Password Reset Assistant in the Kiosk Browser.

For Windows NT/2000 Workstations on an NT Domain

Follow the instructions below on:

A. Creating the SELFHELP user account
B. Updating or Creating the SELFHELP Policy File
C. Adding the SELFHELP user to the profile
D. Restricting the SELFHELP user's privileges
E. Applying the security policy to the SELFHELP user
F. Test the SELFHELP user login

A. To Create the SELFHELP User Account:

1. Log into the domain as **Administrator**.
2. Open **User Manager for Domains**.
3. Create a new **user** called **SELFHELP**.

4. Clear the **password** fields.
5. Select the following checkboxes:
    - **User cannot change password**
    - **Password never expires**
6. Clear the following checkboxes:
    - **User must change password at next login**
    - **Account disabled**
8. Click **Groups**, and then add the user to the **Domain Users** group and click the **OK** button.
9. Click **Account**, and then make sure that this account is setup as a **Global Account** in the **Account Type** frame. Click the **OK** button and then click the **Add** button.
10. If **User Manager for Domains** prompts you to enter a server, click the **Cancel** button.
11. Close **User Manager for Domains**.

B. To **Update** or **Create** the **SELFHELP Policy File**:

1. Open the **System Policy Editor**.

   If you can't locate it, search for the **poledit.exe** file on the Windows NT Server operating system **CD-ROM**.

2. On the **primary domain controller** (PDC), locate the **ntconfig.pol** file.

   It's usually located in the **\Winnt\System32\Repl\Export\Scripts** folder, if you have Directory Replication enabled. If you do not have Directory Replication enabled, search for the file in the **\Winnt\System32\Repl\Import\Scripts** folder.

3. If the **ntconfig.pol** policy file exists, open it via the **System Policy Editor**.

   If the file does not exist, select **File/New Policy** from the main menu to create a new policy file.

4. Select the **Default User** icon and press the **Delete** button.
5. Select the **Default Computer** icon and press the **Delete** button.

C. To Add the SELFHELP User to This Profile:

1. Select **Edit/Add User** from the **main menu**.
2. Select the **SELFHELP user** that you defined earlier and click the **Add** button.
3. Click the **OK** button.

D. To Restrict the SELFHELP User's Privileges:

1. Double-click the **SELFHELP User** icon in the main **System Policy Editor** window to open the user's properties.
2. Browse to **Control Panel\Shell\Restrictions** and select the following checkbox:
    - **Disable Shut Down command**
3. Browse to **System\Restrictions\Disable Registry** and select the following checkbox:
    - Disable registry editing tools
4. Browse to **Windows NT Shell\Custom user interface\Custom Shell** and select the following checkbox:
    - **Custom user interface**
5. In the text field for the default shell, type the full **NetBIOS path to Kiosk Browser** (KioskBrowser.exe) on the primary domain controller.

   Make sure to include the URL switch. For example, type: For example, type:

\\<servername>\netlogon\kioskbrowser.exe /url=http://localhost/PasswordReset/ResetPassword.htm

6. Browse to **Windows NT Shell\Restrictions** and clear the following checkbox:
   - **Only use approved shell extensions**
7. Browse to **Windows NT System** and select the following checkboxes:
   - **Disable Task Manager**
   - **Disable Lock Workstation**
   - **Disable Change Password**
8. Click the **OK** button to close the SELFHELP user's **policy properties** window.

E. To Apply the Security Policy to the SELFHELP User:

1. In the **System Policy Editor**, select **File/Save** from the **main menu**, and save the policy as **ntconfig.pol** in the **Windows NT NETLOGON** share. This can usually be found in the following folder on the **PDC: C:\Winnt\System32\Repl\Export\Scripts**.

   - If you do not have **Windows NT Directory Replication** enabled or configured, save the policy file directly to the **NETLOGON** share. This can usually be found in the following folder on the **PDC: C:\Winnt\System32\Repl\Import\Scripts**.

   - If you do not have a **NETLOGON** share on your **Windows NT PDC**, you must create one in the **folder shown above. Make sure to setup the permissions such that** Everyone has Read-Only access. Make sure to save the policy file as **ntconfig.pol** to the **NETLOGON** share.

F. Test the SELFHELP User Login

1. Login as the SELFHELP user to test the configuration.

   You should not be able to do anything other than access the BMC Track-It! Password Reset Assistant in the Kiosk Browser.

Next Topic: Customizing the Password Reset Users' Kiosk Login Screen

Customizing the Password Reset Kiosk Users' Login Screen

You can advertise the presence of the SELFHELP account by including instructions on how to access this account on each user's login screen. For example, a user will see the following prompt at logon:

```
LogonPrompt"="If you forgot your password or your account is locked,
please logon with the username SELFHELP and no password.;
```

This process can be automated through a simple batch file or login script that can be deployed to all of the workstations on your network.

Automating Workstation Login Screen Changes via a Login Script
The login script can be as simple as a batch file that resides on each domain controller. When a user logs in, this file will run and execute whatever commands it contains. The following command file, for example, can be pushed down to all of the workstations on your network to automatically customize your users' login screens to include a message that explains how to log into the SELFHELP account.

WARNING: Do NOT make any other changes to the Windows system registry unless you're qualified to do so. Making incorrect changes to the registry can affect the proper operation of the operating system.

Listing for `LogonPrompt.cmd` file

```
@regedit /s C:\Program Files\BMC Software\Track-It!Web\Password
Reset\Samples\LogonPrompt.reg
```

The path to the **`LogonPrompt.reg`** file may vary, depending on where you installed the BMC Track-It! Password Reset application. The following Registry file, located in the **Samples** folder in the BMC Track-It! Password Reset directory, is called and executed by the LogonPrompt.cmd file:

Listing for `LogonPrompt.reg` file

Note: The following does not apply to Windows Vista:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]

"LogonPrompt"= "If you forgot your password or your account is
locked, please logon with the username SELFHELP and no password.;
```

For Windows NT/2000 Workstations on an NT Domain

In order to begin using the LogonPrompt.cmd file:

1. Every domain controller that may run this command file (i.e., that your users may log into) must contain a copy of the file in the **NETLOGON** share. This shared directory is actually the **C:\WINNT\System32\Repl\Import\Scripts** directory. You can copy the files there manually, or you can set up replication using the NT replication service. However, the most reliable approach is to manually copy the files to all of your domain controllers. You may want to create another batch file for the purpose of copying the login script to all of the servers after making changes.

2. Configure each user to run the command file. This is done through **User Manager**.
    a. Double-click on a group of users in **User Manager** to bring up the **Group Properties** page, and then click the **Profile** button.
    b. In the **Login Script Name** field enter the name of the command file that you created (e.g., **LogonPrompt.cmd**).

    Keep in mind is that you can use this feature to test subsequent versions of your file if/when you need to make changes. If you're adding a new section to the script, for example, give the updated file a different name, and pick a handful of users to test the new file by entering the new name in the field mentioned above. Once you are certain that the new file will work, you can replace the original with the new one.

Next Topic: Viewing Password Reset Attempts via Crystal Reports

Viewing Password Reset Attempts via Crystal Reports

BMC Track-It! Password Reset includes a Crystal Report that you can use to view all of your users' password reset attempts by department. By default, the **`PRbyDept.rpt`** file is located in:

```
C:\Program Files\BMC Software\Track-It! Web\Password
Reset\reports\PRbyDept.rpt
```

Next Topic: Troubleshooting Password Reset (TCP, ASPNET)

Troubleshooting Password Reset

In most environments, BMC Track-It! Password Reset installs and runs without experiencing any problems. However, due to the wide variety of network architectures and components in use today, conflicts may occur.

Manually Assigning a TCP Port

The BMC Track-It! Password Reset Account Management Service handles all of the password reset requests submitted by users. When a client machine requests a TCP connection to your BMC Track-It! Password Reset server, it needs to know which port to use for that connection. For example, if your Web browser was connecting to Microsoft's Web site, it would specify to Microsoft's server that it wishes to connect to port 80. If your e-mail software was sending mail for you, it would specify that it was connecting to port 25 on your mail server.

Since each Internet service has a unique port number that clients must specify when they want to use that service, BMC Track-It! Password Reset must determine which ports are free and which ones are in use before assigning a TCP Port Number for the BMC Track-It! Password Reset Account Management Service. In most cases, BMC Track-It! Password Reset will automatically select an available port for you (i.e., no configuration is needed). However, if necessary, you can manually change the port number by editing the **`port="9001"`** entries in **both** of the following files:

```
C:\Program Files\BMC Software\Track-It! Web\Password Reset\Account
Management Service \AccountManagementService.exe.config

C:\Program Files\BMC Software\Track-It! Web\Password
Reset\WebApplication\Web.config
```

Bypassing the ASPNET User Account

An important part of many Web applications is the ability to identify users and control access to resources. The act of determining the identity of the requesting entity is known as authentication. Generally, the user must present credentials, such as a name/password pair in order to be authenticated. Once an authenticated identity is available, it must be determined whether that identity can access a given resource. This process is known as authorization. ASP.NET works in conjunction with IIS to provide applications with authentication and authorization services.

By default, BMC Track-It! Password Reset runs under the same security context as ASP.NET. In other words, ASP.NET runs with a limited access account (the local machine account, which is called "localmachinename\ASPNET") in order to provide a more secure networking environment. The ASPNET user account only has access to the files needed by ASP.NET, which includes read access to the installation and application directories and read/write access to the temp directory. There are two primary reasons why you might want to use something other than the ASPNET user account:

- Your organization's IT policy requires you to run BMC Track-It! Password Reset under another network account
- BMC Track-It! Password Reset is running slow on your network

Bypassing ASPNET Due to IT Policies

If your organization's IT policy requires you to run BMC Track-It! Password Reset under another network account, you can change this behavior by selecting the checkbox and entering the username and password for a different user. The only condition is that the user you choose must be authorized to use the Account Management Service (this can be accomplished by editing the configuration file for the account).

Tips for Setting Up a New User Account

If you choose to run BMC Track-It! Password Reset under a custom user account, you should consider the following security guidelines:

- Avoid using the SYSTEM account.
- Avoid granting the new account the **Act as part of the operating system** privilege.
- Grant only the minimum set of required privileges and permissions.
- Use a strong password to protect the account. Strong passwords should include at least seven characters, and use a mixture of uppercase and lowercase letters, numbers, and other characters such as *, ?, or $.
- Clear the **User must change password at next logon** option.
- Select the **Password never expires** option.

Bypassing ASPNET to Improve Performance

Unless you're running .NET Server, there's only one worker process shared among all ASP.NET applications that are installed on the same machine. Since this can slow down your applications under certain conditions, BMC Track-It! Password Reset allows you to specify a different user account in order to avoid possible performance issues. By specifying a different user account, you can host multiple Web applications, each of them using their own SQL Server database, with integrated security on the same machine.

Configuring Scheduled Work Orders

Scheduled Work Orders Overview

Administrators can configure BMC Track-It! to automatically create and assign Scheduled Work Orders for routine maintenance tasks. For example, you can set up Scheduled Work Orders for repetitive tasks such as routine services, preventative maintenance, and back-ups.

See the next topics: Creating Work Order Schedules and Configuring Automated Schedules for Scheduled Work Orders.

Creating Work Order Schedules

The following describes how to create a Work Order Schedule that the Work Order Schedule Monitor will use to create Work Orders.

Note: Dates and times on the **Work Order Schedule** dialog are shown in your BMC Track-It! server's current time zone. The name of the time zone and the time difference between the time zone and the Coordinated Universal Time are shown at the top of the dialog, e.g., (UTC-04:00) Eastern Daylight Time.

To Create a Work Order Schedule:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Help Desk > Scheduled Work Orders > Work Order Schedules**.
2. Click the **Add** button.
3. On the **Work Order Schedule - New** dialog, select a template from the **Work Order Template** drop-down list.
   If Work Order Templates were previously created in Lookup Tables > Help Desk, they will display here. If no Work Order Templates display, see below **To Create a Work Order Template for the Scheduled Work Order.**
4. Select the start date for the Work Orders to be created from the **Date of First Occurrence** drop-down list.
5. Select **Use Skill Routing Policies to assign a Technician**, or select a specific Technician to assign the Work Orders to.
6. Select the Work Order Schedule recurrence pattern (**Hourly, Daily, Weekly**, or **Monthly**).
   a. Hourly
      i. Enter the start time for the Work Orders to be created in the **Start** field.
      ii. Enter the frequency for the Work Orders to be created in the **Run Every** field.
      iii. Enter the end time in the **End** field.
      Notes:
      - You can enter a Start time greater than the End time (for example, from 5:00 p.m. to 8:00 a.m.)
      - If, for any reason, the Work Order Schedule Monitor is stopped and started later, the Work Order Schedules will not be created for the time the Work Order Schedule Monitor was not running. Only the last Work Order for the current date will be created. After that, the Work Orders will be created on the minute of the Start time. For example: If the Start time is 12:30 AM and the Work Order Schedule Monitor was started at 12:45 AM, the Work Order will be created at 12:45 AM; and the next one will be created at 1:30 PM (not 1:45 AM) if the frequency was set at 1 hour.
      - If the Schedule is set to run on the 29th, 30th, or 31st day of the month and the month has fewer days, the Work Order will be created on the last day of the month.
7. Select one of the following options:
   a. **"Only create a Work Order after previously created Work Orders are completed"**, **OR**
   b. **"Use Operating Hours when calculating time intervals"**. (This is disabled for Monthly recurrence patterns.)
   (For more information, see Setting up Help Desk Operating Hours.)
8. Click the **Save** button to close the **Work Order Schedule** dialog.

To Disable the Work Order Schedule:

1. Uncheck the **Schedule Enabled** checkbox.

To Create a Work Order Template for the Scheduled Work Order:

1. Click the **Ellipses** button (...) next to the **Work Order Template** drop-down list.
2. On the **Work Order Templates** dialog, click the **New** button.
3. Complete the **Work Order Template - New** form as described in the topic "Documenting the Issue" in the Technician's Guide.
4. Click the **Save** and **Close** button on the **Work Order Template - New** form.

The Work Order Schedule Monitor is configured by default to automatically check the schedules every minute to determine whether new Work Orders should be created.

To View the Work Order Schedule Monitor Configuration:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Help Desk/Scheduled Work Orders/Automated Schedule**.

   By default, the Work Order Schedules are checked every minute. For the Work Order Schedule Monitor to work correctly, it is not recommended to change any of the settings on the Automated Schedule panel.

To Disable Schedule Checks:

1. Click the **"Do not automatically monitor Work Order schedules"** radio button.

To Manually Run the Schedule Check:

1. Click the **Check Now** button.
   The **Work Order Schedule Monitor Log** displays the information in the grid (see below).

To View, Print, or Export the Work Order Schedule Monitor Log:

The **Work Order Schedule Monitor Log** on the Automated Schedule panel displays the Date/Time, Event Type, and Summary of the schedule check. For example, this will display "Work Order [number] was created based on schedule [ID of the Work Order Schedule]."

1. Double click the record (per row) in the **Work Order Schedule Monitor Log** to view details.
2. In the **Event Detail** dialog, click the **Previous** or **Next** button to view each record.
3. To copy the information, click the **Copy to Clipboard** button.
4. To print the information, see Printing Grid Contents in the Technician's Guide.
5. To export the information, see Exporting Grid Contents Technician's Guide.
6. Click the **Close** button to return to the **Monitor Schedule** panel.

To Purge the Work Order Schedule Monitor Log Messages:

1. Click the **Purge Log** button.
2. Click the **Yes** button on the **Purge Confirmation** dialog.

   A message in the log will display the number of purged records.

Basic Configuration - Asset Management (Inventory)

Setting up Basic Inventory Data (Lookup Tables)

Creating Asset Types

In the Inventory module, Asset Types display in the inventory grid, along with their associate icon. You can create your own Asset Types as well.

To Create Asset Types:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Inventory/Asset Types**.
2. Select an **Asset Type** or **subtype**, then click the **Add** button.
3. On the **Asset Type** dialog, the Asset Type and/or subtype you are creating the Asset Type under are displayed.
4. Enter a **name** for the Asset Type in the indicated text box.
5. To select a display icon, either click the **Load Default** button to select the default icon, or click the **Select** button to select an icon image (.ico format).
6. Click the **Save** button on the **Asset Type** dialog.

Setting up Product Types

Product types are used to group components into categories such as software, hardware, supplies, furniture, etc. Product Types are used to create items in the **Master Items** list for use in **Inventory** and **Purchasing**.

Note: Supplies is a special Product Type that is handled different from all other product types. If you receive an item of the Supplies type, that item will ***not*** be sent to **Unassigned Equipment** in the **Inventory** module. The reason for this is to avoid a scenario such as ordering 500 boxes of staples, and having each box of staples appear as a separate entry in **Unassigned Equipment**. See also Storing Items in the Unassigned Equipment List and Transferring Items to and from the Unassigned Equipment List in the Technician's Guide.

To Set up Product Types:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Base Data/Inventory/Product Types**.
   You can also access the **Product Types** list from the **Tasks** pane in the **Purchasing** module.
3. On the **Product Types** panel of the **Administration Console**, click the **Add** button.
4. On the **Product Type** dialog, enter a name for the Product Type (such as Software or Hardware).
5. Click the **Save** button.
   The new Product Type displays in the grid on the **Product Types** panel.
6. Click the **Apply** button to save your changes, and the **OK** button to close the **Administration Console**.

To Delete a Product Type:

1. Select the Product Type from the **Product Types** panel of the **Administration Console**, then click the **Delete** button.
2. Click Yes when the confirmation dialog displays.
   The Product Type is removed from the grid on the **Product Types** panel.

Creating the Master Items Catalog for Purchasing, Inventory, and Library

Master Item List

The Master Items list is a "catalog" of Items you can create to list items you may be purchasing and/or adding to inventory. This list saves time with data entry. The list is similar to a catalog or product list. The items in the list are not actual purchases or inventory until you choose to add them to purchase orders or as Tracked Items in the Inventory module. The list can include virtually any type of Item -- from hardware to software or any other type of asset. In BMC Track-It!, an Item is the smallest increment of anything you would want to purchase and/or track in inventory. Examples of Items are: hardware such as CPUs, monitors, and keyboards; software, and non-PC assets such as DVD players. When you create an Item, you can include such information as Product, Manufacturer, Type (such as Desktop, Laptop, or Software), Vendor, Price, Warranty and Maintenance information, and more.

Items

There are several types of Items in BMC Track-It!:

- Items in the Master Item List

        - Not yet part of inventory -- similar to a catalog of Items to be purchased or placed into inventory
        - Manually added to the Master Item List by the BMC Track-It! Administrator
    - Items purchased (Purchasing Module)
    - Items placed into inventory (Inventory Module) by
        - being automatically detected along with its associated asset via the audit process
        - receiving purchase order Items
        - associating them to an Asset
        - storing them in the Unassigned Equipment list
            - Unassigned Equipment is an Asset used as a container to hold Items in inventory not yet associated to a particular asset

Assets and Items

Items are typically associated with an Asset, such as a computer or workstation, so that they can be tracked in the system. During the auditing process, BMC Track-It! places the Items in the Tracked Items list for the associated Asset (such as a computer and its peripherals). You can transfer items between assets and the Unassigned Equipment list. You can also promote an item to an asset so that it can be tracked (for items that wouldn't ordinarily be found during the audit process, such as those not connected to a network.

Creating Items in the Master Item List

You can access the **Master Item** list from:

- **the Administration Console**
- an individual asset in the **Inventory** module
- a purchase order in the **Purchasing** module (and from the **See Also** link in the **Tasks** pane)
- a library item in the Library module (and from the **See Also** link in the **Tasks** pane)
- a software title in the Software module (and from the **See Also** link in the **Tasks** pane)

To Create an Item in the Master Item List from the Administration Console:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Lookup Tables/ Inventory/Master Items**.
3. On the **Master Items** panel, click the **Add** button.
   The **Master Item** dialog displays.
4. Enter a description for the Item in the **Product Description** field (required).
5. Select or enter a category for the Item from the **Product Type** drop-down list (required).
   To add a Product Type if it is not listed, click the **Add** button next to the **Product Type** drop-down arrow.

   The following are optional:
   - Manufacturer
   - Part Number
   - Vendor
   - Warranty
   - Support
   - Price
   - Maintenance Vendor
   - Contact Person
   - Comments
6. If you have a license for the **Software License Management** module, you can associate a Software Item with an item in the **Master Items** list on the **Software** tab. (See Associating Software Titles with Master Items in the Technician's Guide.)
7. Click the **Apply** button to save your changes, and the **OK** button to close the window.

To Create an Item in the Master Item List from an Asset in the Inventory Module:

1. If the **Inventory** module is not already open, select **Inventory** from the **Navigation Pane**.
2. In the **Inventory** grid, double-click any Asset.
3. Select the **Tracked Items** tab on the left pane, then click the **Add** button.
4. Click the **New** button on the **Master Item Listing** dialog.
   The **Master Item** dialog displays.
5. Enter a description for the Item in the **Product Description** field (required).
6. Follow steps 4-5 above.
7. Click the **Save** button.

Deleting Items from the Master Item List

You can delete items from the Master Item list via the **Administration Console**.
To Delete an Item from the Master Item List (Administration Console):

1. Follow the steps above to access the **Master Item List** from the **Administration Console**.
2. Select the item and click the **Delete** button.
3. Click **Yes** when the confirmation message displays.

See also: Viewing Information in Grids in the Technician's Guide.

Next topic: Storing Items in the Unassigned Equipment Asset

Defining Networks

Networks are used to specify additional information about an asset so that technicians can quickly troubleshoot a problem.
To Create Asset Types:

1. From the main menu bar, select **Tools/Administration Console/Lookup Tables/Inventory/Networks**.
2. Click the **Add** button.
3. On the **Network** dialog, enter the name of the Network in the indicated text box.
4. Click the **Save** button.

Configuring Asset Discovery

Getting up and Running with Discovering Assets

Use the checklist below to configure asset discovery and manage discovered assets.

☑	TASK	MODULE/WINDOW	HELP TOPIC
	A. Configure Discovery Scan Criteria		
	Configure BMC Track-It! to Discover Devices by Windows Network Domains	Tools/Administration Console/ Configuration/Inventory/Network Discovery/Network Domains	Configuring Network Discovery
	B. Schedule Asset Discoveries		
	Schedule asset Discoveries	Tools/Administration Console/Configuration/Inventory/Network Discovery/Automated Schedule	Scheduling Asset Discoveries
	C. Manually Discover Assets		
	Manually discover assets (if not scheduled)	Inventory module/Tools/ Manage Discovered Assets	Manually Discovering Assets
	D. Manage Discovered Assets		
	Manage Discovered Assets	Tools/Manage Discovered Assets	Managing and Reconciling Discovered Assets

Configuring Network Discovery

(Configuration Wizard Step 3 of 3: Discover Network Assets)

You can set up the Network Discovery process to use specific scan criteria to detect any asset on your network. You can specify one or a combination of domains, IP addresses, organizational units, and/or SNMP communities. BMC Track-It! can be configured to scan the network at specified time intervals (such as every 30 minutes).

Once you've finished the configuring BMC Track-It!, you can view the discovered assets from the **Discovered Assets** link on Track-It's home page. This will display the discovered assets on the **Managed Discovered Assets** window.

To Discover Devices by Windows Network Domains:

(If you're using the **Configuration Wizard**, start with the screen: Step 3 of 3: Discover Network Assets.)

Scanning by Windows Network Domains will discover computers and printers.

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/Network Discovery/Network Domains**.
2. Click the **Add** button to select your Windows domains.
   The **Select Network Domains** dialog displays. You can select any number of domains. Press and hold the **Ctrl** key while you select the domains. If you're selecting domains in a continuous list, press and hold the **Shift** key while selecting them. Select domains one at a time if they have different logon credentials.
3. Enter the domain's administrator account **User Name** in the indicated field (domain name/user ID).
4. Enter the account's **password**, then enter the password again in the **Confirm Password** field.
5. Click the **OK** button.
   The selected domains display.
6. To remove domains, select the domain(s) and click the **Remove** button.
7. Click the **Apply** button to save your changes, and the **OK** button to close the window.

To Discover Devices by IP Addresses:

Scanning the network by IP addresses discovers computers and printers as well as switches, routers, hubs, and other networked devices that have an IP address.

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/Network Discovery/IP Addresses/SNMP Options**.
2. Click the **Add** button under I**P Addresses** to select IP addresses.
3. The **Specify IP Addresses & SNMP Options** dialog displays.
4. Enter a single IP address in the **Specific IP Address** field, or enter a range of IP addresses in the **Starting** and **Ending IP Address Range** fields.
5. Click the **OK** button.
6. To remove IP addresses, select the IP address(es) and click the **Remove** button.
7. Click the **Apply** button to save your changes, and the **OK** button to close the window.

To Discover Devices by SNMP Communities:

If you have defined your scan by IP addresses, you can also scan by SNMP communities. SNMP communities are groups of managed devices and network management systems within the same domain.

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/Network Discovery/IP Addresses/SNMP Options**.
2. Click the **Add** button under **SNMP Community Names** to specify SNMP Communities.
3. On the **Specify SNMP Communities** dialog, enter the **SNMP Community** name or select the **Default** name, then click **OK**.
4. Click the **Apply** button to save your changes, and the **OK** button to close the window.

To Discover Devices by Windows Active Directory Organizational Units:

If your windows environment uses active directories, you can scan by organizational units, which are container objects used within domains.

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/Network Discovery/Organizational Units**.
2. Click the **Add** button to select Organizational Units.

3. On the **Select Organizational Units** dialog, select one or multiple units and click **OK**.
4. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Scheduling Asset Discoveries

Scheduling Asset Discoveries and Notifying Technicians

You can schedule the Asset Discovery process to run at specified time intervals. You can also configure notifications settings so that technicians will be notified of new asset discoveries.

To Schedule Asset Discovery:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/Network Discovery/Automated Schedule**.
2. Click the **Enable Scheduled Asset Discovery** checkbox.
3. To change the time interval, select the minutes from the up and down arrows in the **Scan Time Interval** field, or enter the time in whole minutes.
4. Click the **Apply** button.

To Configure Notification Settings:

1. Select the technician from the **Technician to notify when new assets are discovered** drop-down list.
2. If you want a Work Order to be automatically created when new assets are discovered, click the **Create Work Order...** checkbox.
3. Click the **Apply** button to save your changes, and the **OK** button to close the window.

See also: Manually Discovering Assets in the Technician's Guide.

Configuring Basic Auditing Settings

Configuring the Audit Process Workflow

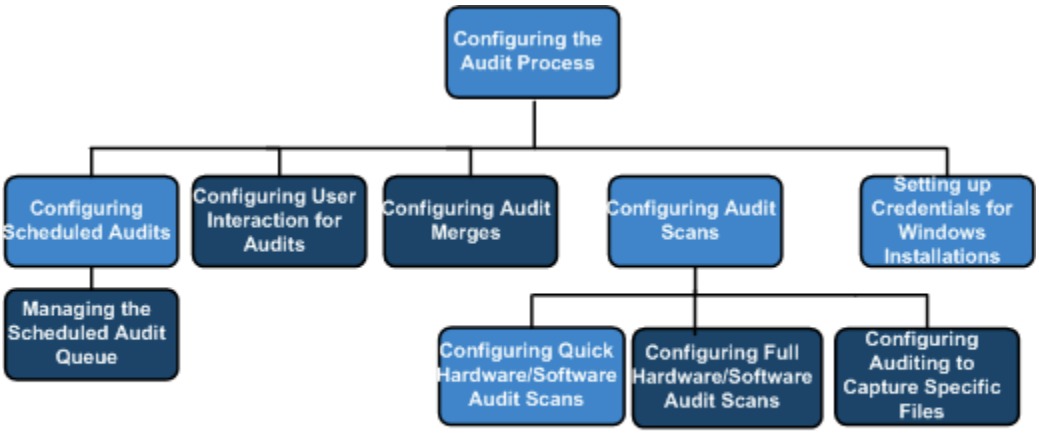
To configure basic auditing settings, see Setting up Auditing in Getting up and Running with Basic BMC Track-It! Help Desk and Asset Management Configuration. Basic settings are also described in the flowchart below (light blue boxes).

To configure advanced auditing settings, see Setting up Advanced Auditing Features in Getting up and Running with Advanced BMC Track-It! Help Desk and Asset Management Configuration.

The flowchart below represents the tasks in the following topics.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

Configuring Windows Audits

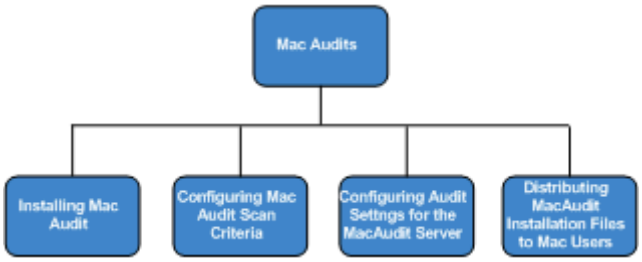


Basic

Advanced

Configuring Mac Audits

In addition to the configuration topics above, see the topics below for configuring audits for Macintosh computers.



Configuring When Users Can Manually Run Audits

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

The Track-It! Audit application, audit.exe, can be run manually on the target computer you want to audit. (The audit.exe application is located in the Track-It! Server folder and is shared through the *Trackit share* created during installation on the server.) On the **Manual Audit Restrictions** panel, you can configure when users can manually run audits to only run once a day, on specific days of the week, on a specific day of the month, or on a specific date.

This setting only affects manually-executed audits run directly with the Audit.exe application or when running the Audit.exe from a login script. (Administrators who use the login script method of auditing can use these scheduling options to control when audits are run so they do not have to continually modify their login script). To configure the Track-It! Server to automatically run audits using the Track-It! Server services rather than a login script, see Configuring Scheduled Audits.

To Configure When Users Can Manually Run Audits:

1. From BMC Track-It!'s main menu bar, select **Tools > Administration Console**, then select **Configuration > Inventory > Auditing > Manual Audit Restrictions**.
2. Select any of the following options:
    a. To limit the number of times the audit can be manually run to once each day, select the designated check box.
    b. Select the check boxes for the specific days of the week.
    c. Select or enter the specific day of the month for the audit to run.
    d. Select or enter the specific date for the audit to run.
    (You can select a date from the calendar or enter a date in the field, for example, 12/31/2013)
3. Click **Apply** to save your changes.

Configuring Scheduled Audits (Date/Time)

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

You can configure the Track-It! Server to automatically run audits using the Track-It! Server services rather than a login script by using Scheduled Audits. Scheduled Audits can be configured to run on specific days of the week, a specific day of the month, or on a specific date. In this case, the Track-It! server will keep track of the schedule and automatically contact the computer systems on your network and audit them based on the schedule you specify.

Note: You can exclude a specific computer from Scheduled Audits by right-clicking it in the Inventory module grid and clearing the “Include In Scheduled Audit Operations” check box. For detailed information, see Including and Excluding Computers from Scheduled Audits in the Technician's Guide.

To Configure Scheduled Audits:

1. From BMC Track-It!'s main menu bar, select **Tools > Administration Console**, then select **Configuration > Inventory> Auditing > Scheduled Audits**.
2. Select the **specific days of the week**, **specific day of the month** or **specific date** to run the audits.
3. Click the **Apply** button to save your changes, and the **OK** button to close the window.

See also: Viewing Software Audit Results and Viewing Hardware Audit Results in the Technician's Guide.

Configuring Audit Scans Overview

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

There are three types of scans to audit the network: Hardware Only, Quick scans and Full scans.

- **Hardware Only Scans**

  Captures only hardware such as monitors, keyboards, and CPUs.

- **Quick Hardware/Software Audit Scans**

  Captures hardware, as well as software from the workstation's main program locations, including: Start and Program menus, desktop, and key sections of the registry.

- **Full Hardware/Software Audit Scans**

  Captures all software, and can also be configured to capture files by specific file types and drives.

You can configure audit scan criteria on the **Windows Scan Criteria** window in the **Administration Console**. For detailed instructions, see the topics on Configuring Quick Hardware/Software Audit Scans, Configuring Full Hardware/Software Audit Scans, and Configuring Auditing to Capture Specific Files and Run Commands.

Configuring Quick Hardware/Software Scans

The Quick Scan captures hardware, as well as software from the workstation's main program locations, including: Start and Program menus, desktop, and key sections of the registry.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

To Configure Quick Scans:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Inventory/ Auditing/Scan Settings/Windows Scan Criteria**.
   The Quick Hardware/Software Scan is selected by default.
3. Select **Unidentified** from the **Quick Scan Software Destination** drop-down list.
   These are the installed software files on a computer (such as executable ".exe" files). See Viewing Software Audit Results in the Technician's Guide.
4. Select **Unidentified** from the **Installed Program Destination** drop-down list.
   These are the actual software programs, such as Microsoft Office Professional. See Viewing Software Audit Results in the Technician's Guide.

Note: We recommend leaving the designations for installed files and programs as Unidentified; however, they can be changed. (For an explanation of the different approval states, see Changing the Audited Software Approval Status in the Technician's Guide).

5. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Configuring Full Scans

Setting up Credentials for Windows Installations

The application requires a set of administrative credentials for use during software installations, such as the audit.exe, which is the executable file that runs audits in BMC Track-It!. These credentials will be used when installing files, setting up services, etc. The credentials you enter must have domain administrator privileges.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

To Enter Setup Credentials for Windows Installations:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Auditing/Setup Credentials**.
2. Enter your **User Name** in the designated field (e.g. DOMAIN\Username) or search for it from the **Browse** button.
3. Enter your **password**.
4. To test your credentials, click the **Test Login** button.
5. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Advanced Configuration - Asset Management (Inventory)

Advanced Auditing Configuration

Configuring the Audit Process Workflow

To configure basic auditing settings, see Setting up Auditing in Getting up and Running with Basic BMC Track-It! Help Desk and Asset Management Configuration. Basic settings are also described in the flowchart below (light blue boxes).

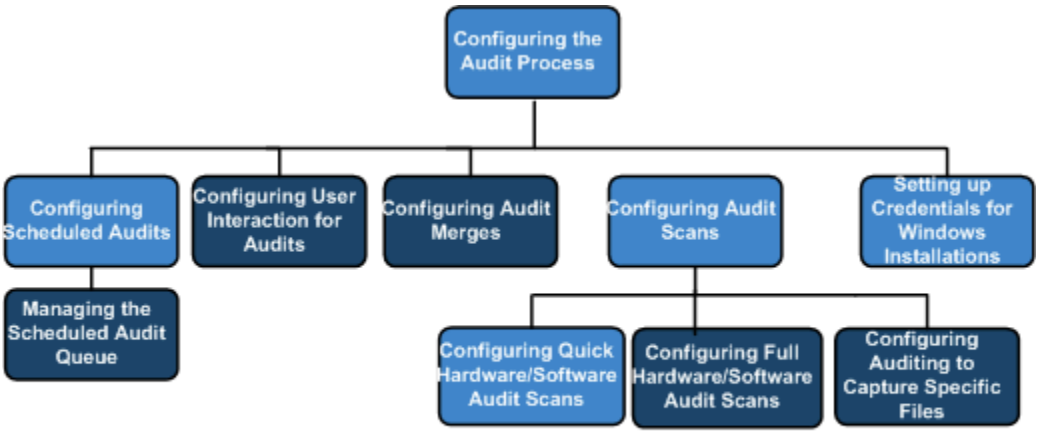
To configure advanced auditing settings, see Setting up Advanced Auditing Features in Getting up and Running with Advanced BMC Track-It! Help Desk and Asset Management Configuration.

The flowchart below represents the tasks in the following topics.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will

continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

Configuring Windows Audits

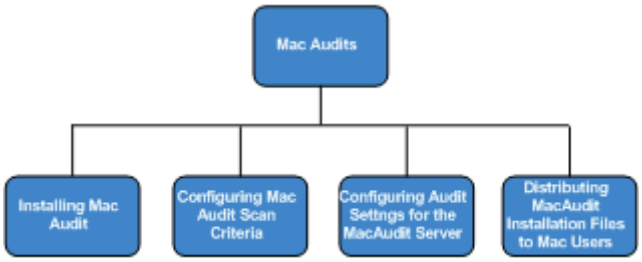


Basic

Advanced

Configuring Mac Audits

In addition to the configuration topics above, see the topics below for configuring audits for Macintosh computers.



Configuring User Interaction for Audits with the audit.exe Application

You can configure BMC Track-It! to interact with the user during the audit process using the audit.exe application in several different ways. You can also prompt the user to provide information during the audit process. This can save you time since you would otherwise have to manually associate assets with users after you've run the asset discovery process (see Associating an Asset with a User in the Technician's Guide).

For more information about the audit.exe application, see Running the audit.exe Application and Merging Audit Results in the BMC Track-It! Technician's guide.

Audit Modes

There are several audit modes you can configure.

- **Normal Interactive** launches audit.exe with a visible window. The user must select Next to continue with the audit.

- **Minimized Non-Interactive** launches audit.exe visibly, but the window is minimized to the taskbar. This requires no user interaction to complete the audit.

- **Hidden Non-Interactive** runs the audit.exe in the background. It is not visible at all to the user and requires no user interaction to complete the audit.

- **Visible Non-Interactive** runs the audit.exe similarly to the Normal mode, but requires no user interaction to complete the audit.

Prompting Options

Administrators can also configure prompting options so that the user is prompted for additional information during the audit process.

- **Always Prompt**: Users will always be prompted for information (previously entered information can be edited).

- **Prompt Once**: Users will be prompted for information only during the initial audit. You can also select to never prompt the user for information.

To Configure User Interaction and Prompting Options:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Auditing/User Interaction**.
2. Select the **Audit Mode** as previously described from the drop-down list.
3. Select the **Prompting** option from the drop-down list.
4. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Configuring Full Hardware/Software Audit Scans

The Full Scan captures all software, and can also be configured to capture files by specific file types and drives.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

To Configure Full Scans:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Inventory/ Auditing/Scan Settings/Windows Scan Criteria**.
3. Select **Full Hardware/Software Scan**.
   By default, the full scan includes executables and .com files. You can also set up the audit to scan for additional file types.
4. To add or change **file types**, click the **Ellipses** (...) button next to **Look for these types of software when scanning**.
5. On the **Configure File Types** dialog:
   a. Click the **Add** button to add a file type.

b. On the **Add File Type** dialog, enter the new file type in the text box (such as .avi), then click the **OK** button.
The new file type is added to the list on the **Configure File Types** dialog

You can also scan by specific drives. The C drive will be scanned by default.

6. To add more drives, enter the drive letters without spaces or commas (such as CDE).
7. Select **Unidentified** from the **Installed Program Destination** drop-down list.
These are the actual software programs, such as Microsoft Office Professional. See Viewing Software Audit Results in the Technician's Guide.

Note: We recommend leaving the designations for installed files and programs as Unidentified; however, they can be changed. (For an explanation of the different approval states, see Changing the Audited Software Approval Status in the Technician's Guide.)

8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Configuring Auditing to Capture Specific Files and Run Commands

In addition to capturing files during Quick and Full Scans, you can configure the auditing process to capture up to 10 specific files (Windows as well as Macintosh).

You can also set up BMC Track-It! to run executable (.exe) commands by preceding the commands with an exclamation mark (!). For example, the command: ;! mem/C; captures the DOS memory settings of the machine.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

To Capture Specific Files:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Inventory/ Auditing/ File Captures**.
3. Click the **Enable file captures** checkbox.
The **File Capture Timeou**t defaults to 30 seconds. However, you can change it from the up and down arrows.
4. Enter the path and file name in the designated files for each file (**File #1** through **File #10**).
5. For Macintosh files, prefix the file name with "MAC" (e.g. MAC:/etc/passwd).
6. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Displaying the BMC Track-It! Agent Icon on Users' Computers

You can set up BMC Track-It! to hide or display an icon on the user's taskbar when BMC Track-It! Agent is running during auditing.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8x, and 9 Audit Merge Process"

To Display or Hide the BMC Track-It! Agent Icon on Users' Computers:

1. From the main menu bar, select **Tools/Administration Console/Administration/Track-It! Agent**.
2. Click the checkbox to enable the icon to display on the users' computers, or deselect the checkbox to hide the icon.
3. Click the **Apply** button to save your changes, and the **OK** button to close the window.

See Also: Configuring User Interaction for Audits

Managing the Scheduled Audit Queue

Once computers have been scheduled for audits, they are displayed on the **Queue** panel in the **Administration Console**. This displays the Asset Name, Status, Schedule Date and Time, Asset ID, User Name, and Audit Completed Date and Time. The **Queue History** tab displays the computers that were audited prior to the currently scheduled audits.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

Note: You can exclude specific computers from scheduled audits. (Computers must be selected in the Inventory grid before the scheduled audit is run.) See Including and Excluding Computers from Scheduled Audits in the Technician's Guide.

To Access the Queue Management Window:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Auditing/Queue**.

To Stop Scheduled Audits:

You can clear the **Current Queue**, which will stop the auditing process of the scheduled computers.

1. Click the **Clear** button on the **Current Queue** tab.
2. Click **Apply** to save your changes and click **OK** to close the window.

To Suspend Scheduled Audits:

If you need to suspend scheduled audits (e.g. if your network is down, etc.), you can suspend the audits until you're ready to resume them.

1. Uncheck the **Process Audit Queue** checkbox.
2. When you're ready to resume the audits, check the **Process Audit Queue** checkbox.

To Clear the Queue History:

1. Click the **Clear** button on the **Queue History** tab.
2. Click **Apply** to save your changes and click **OK** to close the window.

To Stop the Grids from Refreshing So You Can Sort and Filter Records:

If there are several records in the grids, it may be helpful to sort and filter the records. In order to do this, you'll need to stop the grids from refreshing as the audits are processing.

1. Uncheck the **Automatic Refresh of Grid Display** checkbox.

Related Topics:

Configuring Scheduled Audits

Configuring Audit Merges

The BMC Track-It! Merge feature inserts data collected through the Audit into Inventory.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

Note: BMC Track-It! automatically merges audit results when you set up scheduled audits or audit workstations on demand.

Performance

When audits are merged you can control how much CPU time is allocated to the merge process.
To Specify the Maximum CPU utilization to Apply During Audit Merge:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Merging/Performance**.
2. Enter a value (such as 25) representing the percentage of CPU usage during audit merge in the indicated field.
3. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Schedule

This setting specifies how often the audit data is merged into your inventory.
To Enable the Automatic Merge Process and Specify the Time Between Merges:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Merging/Schedule**.
2. Click the **Enable** checkbox.
3. Enter the **time between merges** (in minutes) in the designated field.
4. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Merging Audit Data

To Merge Audit Data:

1. On the Schedule panel, click the **Merge Now** button.

Note: BMC Track-It! automatically merges audit results when you set up scheduled audits or audit workstations on demand.

See also: Running the audit.exe application and merging audit results in the Technician's Guide.

Configuring the Asset Monitor Schedule

Note: For the Asset Monitor Schedule to work correctly, it is *not* recommended that you change any of the settings on the Automated Schedule panel.

The Asset Monitor is used by the system to perform various operations in the Inventory module, such as the purging audit history.

The Asset Monitor Schedule is configured by default to automatically run every 15 minutes to purge audit history.

In addition to configuring the Asset Schedule Monitor, Administrators can also manually run the Asset Monitor Schedule from the Automated Schedule panel. This is useful for testing configurations.

To configure the Asset Monitor Schedule

1. From BMC Track-It!'s main menu bar, select **Tools > Administration Console**, then select **Configuration > Inventory > Asset Monitor > Automated Schedule**.
2. To prevent the Asset Monitor Schedule from running, select **Disable the Asset Monitor**.
3. Click **Apply** to save your changes.
4. To manually run the Asset Monitor Schedule, click **Check Now**.

The **Asset Monitor Schedule Log** displays status, errors, and other information in the grid (see below).

Asset Monitor Schedule Log

The **Asset Monitor Schedule Log** displays the Date/Time, Event Type, and Summary of the Asset Monitor Schedule checks. For example, this will display "Audit History Purge Completed."

To print grid contents:
See Printing Grid Contents in the Technician's Guide.

To export grid contents:
See Exporting Grid Contents Technician's Guide.

To view log details:
1. Double click the record (per row) in the **Asset Monitor Schedule Log**.
2. In the **Event Detail** dialog, click the **Previous** or **Next** button to view each record.
3. To copy the information, click the **Copy to Clipboard** button.

To purge the Asset Monitor Schedule Log messages:
1. Click the **Purge Log** button.
2. Click the **Yes** button on the **Purge Confirmation** dialog.

   A message in the log will display the number of purged records.

Mac Audits

Mac Audit Overview

Mac Audit enables technicians to audit Macintosh computers (Mac OS 8.1 through 10.2 and higher). With Mac Audit, you can audit Macintosh computers on demand and run scheduled audits as you can with other BMC Track-It! auditing features.

Caution: Before performing any audits on computers created from a Ghost image (cloned), follow the instructions below to remove the file with the GUID that is used by the merge process. If the file is not removed and multiple machines have the same file, the audits will continuously merge into a single record in Inventory.

To prepare a Mac OS X machine for replication/ghosting:
Open the terminal and issue the following two commands exactly as they appear. Do not replace the forward slashes with back slashes or the quotes with double quotes.
- sudo /Library/StartupItems/TrackItMacAudit/TrackItMacAudit stop
- sudo rm '/Library/Application Support/Track-It!/Mac Audit/Workstation Info'

Notes:
- Mac Audit is an add-on to BMC Track-It!, and if purchased, it is automatically installed on the server when you install BMC Track-It!.

Important Notes:
- For **Mac OS 9 through 10.1**, please follow the installation instructions in the KnowledgeBase article on our support web page: How to Install MacAudit to Audit OS 8.x, 9.x and OS X Machines

- For **OS Mac OS 10.2 and higher**, please follow the installation instructions in the topic: Installing Mac Audit (Mac OS 10.2 and Higher).
- With Mac Audit, you can audit Macintosh computers connected on your network, but you won't be able to audit standalone workstations.

Next Topic: Installing Mac Audit (Mac OS 10.2 and Higher)

Installing Mac Audit (Mac OS 10.2 and Higher)

Mac Audit is an add-on to BMC Track-It! and if purchased, is automatically installed on the server when you install BMC Track-It!. Once Mac Audit is installed, you'll need to configure Mac Audit settings from the **Administration Console**. You'll also need to ensure that the necessary files are installed on your users' Macintosh computers that are connected to the network. Please see the Mac Audit Overview topic for important information.

Caution: Before performing any audits on computers created from a Ghost image (cloned), follow the instructions below to remove the file with the GUID that is used by the merge process. If the file is not removed and multiple machines have the same file, the audits will continuously merge into a single record in Inventory.

To prepare a Mac OS X machine for replication/ghosting:
Open the terminal and issue the following two commands exactly as they appear. Do not replace the forward slashes with back slashes or the quotes with double quotes.

- sudo /Library/StartupItems/TrackItMacAudit/TrackItMacAudit stop
- sudo rm '/Library/Application Support/Track-It!/Mac Audit/Workstation Info'

Important Note: For **Mac OS 9 through 10.1**, please follow the installation instructions in the

KnowledgeBase article on our support web page: BMC Track-It! Mac Audit Installation Quick Start Guide.

Steps to Install Mac Audit on Users' Macintosh Computers
The BMC Track-It! Mac Audit installation process is composed of the three steps outlined below. Follow the hyperlinks for detailed instructions.

1. Configuring the Mac Audit server and Mac Audit scan criteria
   - Configuring the Mac Audit server will determine how the Macintosh clients will communicate with the server to deliver audit results. It will also enable the clients to get configuration updates.
   - You can configure Mac Audit to scan for specific file types and file extensions. You can also designate a specific technician who will have the security privilege to capture files.
2. Distributing Mac Audit Installation Files to Mac Users
   - You can instantly create Mac Audit installation package files from the Administration Console, then have BMC Track-It! e-mail the files directory from your computer.
3. Installing Mac Audit Files on Macintosh Computers
   - Users can install the Mac Audit installation files on their own computers.

Next Step:
Configuring the Mac Audit Server

Distributing Mac Audit Installation Files to Mac Users

You can distribute the Mac Audit installation files to Macintosh users by saving the installation package to a shared network drive or you can have BMC Track-It! e-mail the files directory from your computer

Caution: Before performing any audits on computers created from a Ghost image (cloned), follow the instructions below to remove the file with the GUID that is used by the merge process. If the file is not removed and multiple machines have the same file, the audits will continuously merge into a single record in Inventory.

To prepare a Mac OS X machine for replication/ghosting:
Open the terminal and issue the following two commands exactly as they appear. Do not replace the forward slashes with back slashes or the quotes with double quotes.

- sudo /Library/StartupItems/TrackItMacAudit/TrackItMacAudit stop
- sudo rm '/Library/Application Support/Track-It!/Mac Audit/Workstation Info'

Important Note: The following instructions apply to Mac OS 10.2 and higher. For **Mac OS 8.1 through 10.2**, please follow the installation instructions in the topic: Installing Mac Audit.

Note: BMC Track-It! Mac Audit is available as an add-on to BMC Track-It!.
To Distribute Mac Audit Installation Files to Mac Users:
The following steps describe how to create the Mac Audit installation files and so that you can distribute them from a shared network folder. To e-mail the files, skip to item C, below.
A. Create the Installation Package Files

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Auditing/Macintosh Settings/Install Packages**.
2. Enter a user name and password under **Administrative Credentials for Macintosh Installs** (optional).
3. You can leave the default user name and password, which are the Administrative Credentials (the Mac Root Password) that were set up when BMC Track-It! was installed by your organization's administrator. However, you can enter a new user name and password which is what your end users will enter when installing the Mac Audit installation files on their Macintosh computers.
4. Click the **Create Installation Package** hyperlink.
5. The **Save As** dialog displays.
6. Navigate to where you want to save the files in the **Save In** drop-down list (such as a shared folder on the network).
7. Enter a name for the file in the **File Name** field. (You can use any name).
8. Leave the **Save as Type** drop-down as shown in the default.
9. Click the **Save** button.
   A zipped folder of the installation files is created and saved in the specified location in your file directory.

B. Distribute the Installation Package Files to the Mac Users

1. Give instructions to your Macintosh users on how to access the shared network folder.
   Alternatively, you can e-mail the files to the Mac users. You do not have to create the installation files -- just follow the instructions on e-mailing the files below.

C. E-mail the Files to the Mac Users

1. Click the **E-mail Installation Package** hyperlink on the **Install Packages** panel of the **Administration Console**.
2. Your E-mail application opens with the file attached.
3. Include in your e-mail message that the user needs to install the files on their Macintosh and to refer to the online help topic: Installing Mac Audit Files on Macintosh Computers.

Next Topic: Installing Mac Audit Files on Macintosh Computers

Configuring Audit Settings for the Mac Audit Server

These settings determine how the Macintosh clients communicate with the server to deliver audit results and get configuration updates. The Audit Server listens for results from Mac Audit Clients.

Note: BMC Track-It! Mac Audit is available as an add-on to BMC Track-It!.

Caution: Before performing any audits on computers created from a Ghost image (cloned), follow the instructions below to remove the file with the GUID that is used by the merge process. If the file is not removed and multiple machines have the same file, the audits will continuously merge into a single record in Inventory.

To prepare a Mac OS X machine for replication/ghosting, open the terminal and issue the following two commands EXACTLY AS THEY APPEAR. Do not replace the forward slashes with back slashes or the quotes with double quotes.

- sudo /Library/StartupItems/TrackItMacAudit/TrackItMacAudit stop
- sudo rm '/Library/Application Support/Track-It!/Mac Audit/Workstation Info'

To Configure Audit Settings for the Mac Audit Server:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Auditing/Macintosh Settings/Audit Settings**.
2. The **Server Type** defaults to **TCP: Audit Server**, but you can change it to SMB: Microsoft Networking or AFP Appletalk File Sharing from the drop-down list.
3. If you selected **SMB: Microsoft Networking** or **AFP Appletalk File Sharing**, enter the **Share User** and **Password**.
   The Share Name defaults to the share name set up during the installation of BMC Track-It!.
4. If you selected **SMB: Microsoft Networking**, the **IMTP_IP_Port** automatically displays.
5. The **Server Name/IP Address** defaults to the server name or IP address of the computer where Mac Audit is installed.
6. The **Audit Client Listen Port** automatically displays.
7. Click the **Enable Audit Server** checkbox.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

See also: Configuring Mac Audit Scan Criteria.

Configuring Mac Audit Scan Criteria

You can configure Mac Audit to scan for specific file types and file extensions. You can also designate a specific technician who will have the security privilege to capture files.

Caution: Before performing any audits on computers created from a Ghost image (cloned), follow the instructions below to remove the file with the GUID that is used by the merge process. If the file is not removed and multiple machines have the same file, the audits will continuously merge into a single record in Inventory.

To prepare a Mac OS X machine for replication/ghosting:
Open the terminal and issue the following two commands exactly as they appear. Do not replace the forward slashes with back slashes or the quotes with double quotes.

- sudo /Library/StartupItems/TrackItMacAudit/TrackItMacAudit stop
- sudo rm '/Library/Application Support/Track-It!/Mac Audit/Workstation Info'

Note: BMC Track-It! Mac Audit is available as an add-on to BMC Track-It!.
To Configure Mac Audit Scan Criteria:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/ Auditing/Macintosh Settings**.
2. Enter the user name in the **File Capture User** field for the technician who will have the security privilege to capture files.
3. Enter the folder name of the folder to scan for files in the **Scan only in this folder field**.
4. Enter the file types to scan in the **Look for these types of files when scanning** field. You can enter multiple file types separated by a semi-colon.
5. Enter the file extensions to scan in the **Look for files with these extensions when scanning** field.
6. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Distributing Mac Audit Installation Files to Mac Users

Uninstalling BMC Track-It! Agent

BMC Track-It! Agent is a client-side application that allows technicians to audit computers, either on demand or through scheduled audits. Agent is installed on clients' computers when an audit is run. If necessary, BMC Track-It! Agent can be uninstalled from Add/Remove Programs in the Windows Control Panel.

Software License Management

Software License Management Module Overview

The Software License Management module enables you to manage software license usage and compliance within your organization.

Note: The Software license Management module integrates with the Inventory, Help Desk, and Purchasing modules, and requires initial configuration.

Integration with the Inventory Module

During the audit process, the Inventory and Software license Management modules are automatically updated with any software and files found on networked computers.

Once computers are audited, the following information, as well as additional detailed information, is displayed in the Software License Management module:

- Software Title
- Description
- Versions
- Publisher
- licenses
  - Number of
    - Licenses Owned
    - Licenses Used
    - Active or Retired Licenses
    - Fully or Partially Assigned Licenses
  - Details on
    - Licensed or Unlicensed Usage (software title installed per Computer)
    - Upgraded and Renewed Licenses
  - Individual License Details
    - e.g. serial numbers, activation keys, and expiration dates

Note: Lookup Tables must be set up in the Administration Console for the above information to display.

Integration with the Help Desk Module

BMC Track-It! can also automatically create Work Orders when software license conditions change. This includes unauthorized installations, license expiration, pending expirations, over-utilizations licenses, and other conditions. Track-It Administrators can set up the work order generation in the Administration Console (see Generating Work Orders When Software License Conditions Change in the Administrator's Guide).

Integration with the Purchasing Module

When purchase orders for software are created and entered in the Purchasing module, BMC Track-It! automatically populates the Software License Management module with the names and number of licenses purchased.

Next Topic: Software License Management Workflow (Administrator's Guide) or Software License Management Workflow (Technician's Guide)

Software License Management Workflow (Administrator)

The following steps outline the process flow for using the setting up and using the Software License Management module.

1. Set up Lookup Tables in the Administration Console (Software, Help Desk, and Purchasing)

a. Software

- Software Publishers
- License Sources
- License Types
- Work Order Generation for License Condition Changes

b. Help Desk

This enables you to set up work orders for licensing notification.

- Work Order Types, Sub-types, and Categories
- Work Order Priorities
- User-defined Lookup #1 and #2

c. Purchasing

- Master Items
- Product Types
- Associate the Software Title to a Master Item

2. Set up Work Order Notification Options in the Administration Console (Help Desk)

- Automatically Notifying Technicians and Users of Work Order Events

Track-It Technicians can then perform the following tasks:

3. Create the Software Title

- Create the software title in the Software License Management module.

4. Associate the Software Title with an Item on the Master Items List

- The association automatically creates licenses for the software title when you purchase and receive the software item and record the details in the **Purchasing** module.

5. Discover IT Assets

- We recommend that you first discover your assets using Track-It's Asset Discovery process. Once the assets are discovered, workstation information is automatically sent to inventory, including software programs and files.

6. Audit the Network

After discovering your assets, you'll need to audit the workstations to update the software files and programs information. You can audit assets via Audit on Demand, Scheduled Audits and Auditing Standalone Workstations.

1.

- Audit on Demand and Scheduled Audits automatically merge and update the inventory information. If you audit standalone workstations, you'll need to manually merge the information so that your inventory information is updated.
- If you are not using Scheduled Audits, you should audit your workstations on a regular basis to ensure that you have the most updated information.

7. Assign Licenses to a Computer

- The Assets tab of the Software Title window displays a list of all of the computers with the installed software. You can select the appropriate software license from the list (from information entered when the software title was created, such as the serial number).

8. Other Licensing Tasks

Once a software title is licenses, you can perform the following licensing tasks:

- Revoke licenses (remove the license from the computer)
- Retire licenses
- Upgrade licenses
- Renew licenses

9. View Software License Reports

You can view and print the following Software reports:

1.
   - Expiring License Details
   - License History for Title
   - Software Title Details
   - Software Title Summary
   - Unauthorized Titles by Asset ID

Generating Work Orders When Software License Conditions Change

Generating Work Orders When Software License Conditions Change (Overview)

You can configure BMC Track-It! to automatically generate work orders when software license conditions change. These changes include:

- Asset License Revoked (license removed from an asset)
- Asset Unauthorized (license is not valid for the asset)
- License Deleted
- License Expired
- License Expiration Pending
- License Retired
- License Usage Critical Level (more licenses are needed)
- Under Licensed Title (over utilized licenses)

The work order will contain your configuration information. Click on the links above for detailed instructions.

Note: Make sure you have already set up the following Help Desk Lookup Tables and configuration options (also in the Administration Console):

- Work Order Types, Sub-types, and Categories
- Work Order Priorities
- User-defined Lookup #1 and #2
- Automatically Notifying Technicians and Users of Work Order Events

Next Topic: Generating Work Orders When a Software License is Removed from an Asset

Generating Work Orders When a Software License is Removed from an Asset (Revoked Licenses)

You can set up BMC Track-It! to notify your technicians, via work orders, when an authorized user (such as an administrator or technician) has removed a software license from an asset (such as a computer).

To Set Up Work Order Generation When a Software License is Removed from an Asset:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **Asset License Revoked**.
4. Click the **Enable Work Order Generation** checkbox.
5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).
6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Generating Work Orders When a Software License Has Been Unauthorized

Generating Work Orders When a Software License Has Been Unauthorized

You can set up BMC Track-It! to notify your technicians, via work orders, when an authorized user (such as an administrator or technician) has unauthorized a software title.

To Set Up Work Order Generation Generating Work Orders When a Software License Has Been Unauthorized:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **Asset Unauthorized**.
4. Click the **Enable Work Order Generation** checkbox.
5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).
6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Generating Work Orders When a Software License Has Been Deleted

Generating Work Orders When a Software License Has Been Deleted

You can set up BMC Track-It! to notify your technicians, via work orders, when an authorized user (such as an administrator or technician) has deleted a software title.
To Set Up Work Order Generation When a Software Title Has Been Deleted:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **License Deleted**.
4. Click the **Enable Work Order Generation** checkbox.
5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).
6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Generating Work Orders When Licenses Have Expired

Generating Work Orders When Licenses Have Expired

You can set up BMC Track-It! to notify your technicians, via work orders, when a software license has expired.
To Set Up Work Order Generation When a Software License Has Expired:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **License Expired**.
4. Click the **Enable Work Order Generation** checkbox.
5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).
6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Generating Work Orders When Licenses Are Expiring

Generating Work Orders When Licenses Are Expiring

You can set up BMC Track-It! to notify your technicians, via work orders, when a software license is expiring.
To Set Up Work Order Generation When Software Licenses Are Expiring:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **License Expiration Pending**.
4. Click the **Enable Work Order Generation** checkbox.
5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).

6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Generating Work Orders When Licenses Have Been Retired

Generating Work Orders When Licenses Have Been Retired

You can set up BMC Track-It! to notify your technicians, via work orders, when a software license has been retired.

To Set Up Work Order Generation When a Software License Has Been Retired:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **License Retired**.
4. Click the **Enable Work Order Generation** checkbox.
5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).
6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Generating Work Orders When Licenses Used Are at a Critical Level

Generating Work Orders When Licenses Used Are at a Critical Level

You can set up BMC Track-It! to notify your technicians, via work orders, when software licenses reach a critical level (more licenses are needed). For example, when there are 45 licenses used, and five available out of 50 owned, a work order will automatically be created.

To Set Up Work Order Generation When Licenses Used Are at a Critical Level:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **License Usage Critical Level**.
4. Click the **Enable Work Order Generation** checkbox.
5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).
6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Next Topic: Generating Work Orders When Licenses Are Over Utilized (Under Licensed)

Generating Work Orders When Licenses Are Over Utilized (Under Licensed)

You can set up BMC Track-It! to notify your technicians, via work orders, when software licenses are over utilized (under licensed).

To Set Up Work Order Generation When Software Licenses are Over Utilized:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management**.
3. Select **Under Licensed Title**.
4. Click the **Enable Work Order Generation** checkbox.

5. Enter the information in the designated text boxes that you would like to display on the work order (**Summary, Type, Subtype, Category, Priority, Lookup #1 and #2**).
6. Select the technician who will be assigned the work order from the **Technician Assigned** drop-down list.
7. Enter a description in the **Description** text box.
8. Click the **Apply** button to save your changes, and the **OK** button to close the window.

Setting up Software License Management Lookup Tables

Setting Up Software License Types

Software License Types are used in the Software License Management module to identify software titles as OEM, Enterprise, Site, or any user-defined description. Identifying the license as Bound to Asset means the license can only be associated to the specific asset. License Types are set up in the Lookup Tables section of the Administration Console.

To View License Types:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management** from the **Lookup Tables** section.
3. Select **License Types**.
   The list of License Types displays. To view more information, right click on the grid header, and select **Customize**. See also Creating User-defined Views in the Technician's Guide.

To Add License Types:

1. Click the **Add** button.
2. On the **License Types** dialog, enter a description for the License Type, then click the **OK** button.
   The name displays in the **License Types** grid.
3. To indicate that the license can only be associated to the specific asset, click the **Bound to Asset** check box. (If this column does not display, see #3 in To View License Types, above.
4. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **License Types** window.

To Edit License Types:

1. Select the License Type from the **License Types** grid, then click the **Edit** button.
2. Make the necessary changes.
3. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **License Types** window.

To Delete License Types:

1. Select the License Type from the **License Types** grid, then click the **Delete** button.
2. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **License Types** window.

Setting Up Software License Sources

License Sources are used in the Software License Management module to enter user-defined information about a software license (such as OEM or Vendor).

To View License Sources

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management** from the **Lookup Tables** section.
3. Select **License Sources**.
   The list of **License Sources** displays. To view more information, right click on the grid header, and select **Customize**. See also Creating User-defined Views in the Technician's Guide.

To Add License Sources:

1. Click the **Add** button.
2. On the **License Sources** dialog, enter a description for the License Source, then click the **OK** button.
   The name displays in the **License Sources** grid.
3. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **License Sources** window.

To Edit License Sources :

1. Select the License Source from the **License Sources** grid, then click the **Edit** button.
2. Make the necessary changes.
3. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **License Sources** window.

To Delete License Sources:

1. Select the License Source from the **License Sources** grid, then click the **Delete** button.
2. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **License Sources** window.

Setting Up Software Publishers

Software publishers are used in the Software License Management module to identify the company that develops and markets the software you are tracking. Publishers are set up in the Lookup Tables section of the Administration Console. The Publishers will display as an option when you are creating new software titles in the Software License Management module, and as a column in the Software grid.

To View Publishers:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Software License Management** from the **Lookup Tables** section.
3. Select **Publishers**.
   The list of Publishers displays. To view more information, right click on the grid header, and select **Customize**. See also Creating User-defined Views in the Technician's Guide.

To Add Publishers:

1. Click the **Add** button.
2. On the **Publisher** dialog, enter the software publisher's name, then click the **OK** button.
   The name displays in the Publishers grid.
3. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **Publishers** window.

To Edit Publishers:

1. Select the publisher from the **Publishers** grid, then click the **Edit** button.
2. Make the necessary changes.
3. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **Publishers** window.

To Delete Publishers:

1. Select the publisher from the **Publishers** grid, then click the **Delete** button.
2. Click the **Apply** button to save the changes, or click the **OK** button to save the changes and close the **Publishers** window.

Installing the Track-It! Bar Code Solution

Please see the PDF version of the BMC Track-It! Bar Code Installation Guide (Select the BMC Track-It! version, then select BMC Track-It! Bar Code Installation Guide.)

For more information, see Getting Started with Bar Coding in the Technician's Guide.

Setting up Purchasing

Setting up Shipping and Billing Information for Purchase Orders

You can set up default shipping and billing information for purchase orders. This information will display for each new purchase order that is created. You can, however, change the information for specific purchase orders, and include additional shipping information (such as delivery instructions).

To Set up Shipping and Billing Information for Purchase Orders:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Purchasing/Bill to/Ship to**.
3. Enter the contact information for there person who will be receiving the items in the **Ship to:** section.
4. Enter the contact information for there person who will be handling payments in the **Bill to:** section.
5. Click the **Apply** button to save your changes, and the **OK** button to close the **Administration Console**.

Now the shipping and billing information will automatically display on the **Shipping and Billing** tab on each new Purchase Order.

Enabling Automatic Generation of Purchase Order Numbers

The Purchasing module can be configured to automatically generate sequential numbers for each new Purchase Order.

To Enable Automatic Generation of Purchase Order Numbers:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Purchasing/Numbering**.
3. Click the checkbox to **enable automatic incrementing of Purchase Order numbers**.
4. Click the **Apply** button to save your changes, and the **OK** button to close the **Administration Console**.

Now, for each new Purchase Order, Track-It! will automatically generate the Purchase Order number. (You can change the number on the Purchase Order if necessary).

Setting up Sales Tax for Purchase Orders

You can configure a default sales tax rate to be applied to Purchase Orders, and whether or not tax is calculated on Shipping charges.

To Set up Sales Tax for Purchase Orders:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.

2. In the **Administration Console**, select **Purchasing/Sales Tax**.
   You can also access the Sales Tax panel from the **See Also** link in the **Tasks** pane of the **Purchasing** module.
3. Enter the sales tax in the **Tax Rate** field (e.g., .065 or .07).
4. Click the checkbox **Enable tax calculations on shipping charges** if necessary.
   The settings will take effect for any new Purchase Orders.
5. Click the **Apply** button to save your changes, and the **OK** button to close the **Administration Console**.

Now, when a new Purchase Order is created and items are added, the Sales Tax will be automatically calculated and displayed on the **Items** tab of the **Purchase Order** window.

Setting Up Vendors for Purchasing and Inventory

You can set up vendor information for use in the Purchasing and Inventory modules. This includes details such as Company Name, Contact Person, Payment terms, and contact information (address, e-mail, Web site, and telephone and fax numbers). You can also add comments for additional information.
To Setup Vendor Information:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Lookup Tables/Administration/Vendors**.
   You can also access the **Vendors** panel from the **See Also** link in the **Tasks** pane of the **Purchasing** module.
3. On the Vendors pane of the **Administration Console** enter the information in the following fields:

   - Company Name
   - Contact Person
   - Title
   - Default Payment Terms
   - E-mail Address
   - Web site
   - Address
   - Telephone Number
   - Fax Number
   - Comments

4. When you are finished, click the **Save** button.
   The vendor displays on the Vendors pane.

To Delete a Vendor:

1. Select the Vendor from the **Vendor** panel of the **Administration Console**, then click the **Delete** button.
2. Click Yes when the confirmation dialog displays.

   The Vendor is removed from the grid on the **Vendor** panel.

Setting up Courses for the Training Module

In order to track users' training in the **Training** module, you'll need to set up each course (within your organization or externally provided).

Note: Before you set up a course, make sure that **Locations** and instructors (as **Technicians**) are set up in Lookup Tables in the **Administration Console**.
To Set up a Course for the Training Module:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Lookup Tables/ Training/Courses**.
3. On the **Courses** panel, click the **Add** button.
   The **Course** dialog displays.
4. Enter a name for the course in the **Name** field (required).
5. Select the location where the course is offered from the Location drop-down list.
6. Enter the type of training in the **Type** text box (such as the subject area -- for example, BMC Track-It! Certified Technician.
7. Select the course instructor from the **Instructor** drop-down list.
   BMC Track-It! uses the Technicians list for instructors.
8. Enter the cost of the course in the **Course Fee** text box.
9. Enter the telephone number for the course provider or contact in the **Phone** field.
10. Enter the telephone number extension if applicable in the **Extension** field.
11. Enter the fax number in the **Fax** field.
12. Enter the day and time the class meets in the **Schedule** field (such as Monday 5-8p or MWF 5-8p).
13. Enter the date the course begins in the **Date** field.
    This displays a calendar so you can select the date.
14. Enter the contact person's name in the **Contact Person** field.
15. Enter any desired comments in the Comments field.
16. Click the **Save** button.
    The course information displays on the **Courses** panel of the **Administration Console**. You can edit or delete courses from the **Edit** and **Delete** buttons.
17. Click the **Apply** button to save your changes, and the **OK** button to close the **Administration Console**.

Configuring Change Management

Change Management Overview

Track-It!'s Change Management module provides an automated process to track and manage Requests for Change in your organization. When a Work Order is created that matches the criteria defined in a Change Management Policy it creates an associated Request for Change that is automatically placed into the approval process. Requests for Change are managed by the Work Order's Assigned Technician in the BMC Track-It! Technician Client. Approvers who have been assigned to the Request for Change communicate and vote through BMC Track-It! Web. Automatic notifications can be set up so that Approvers and Technicians are notified about specific events in the Request for Change's lifecycle.

Change Management Roles

The individuals involved in the Change Management process are:

BMC Track-It! Administrator

The BMC Track-It! Administrator sets up Change Management Policies, automatic e-mail notifications, and permissions for Technicians and Approvers.

Track-It! Technicians
The Technician can manage the Request for Change from either the Change Management module or from the Change Management tab on the Work Order.

Approvers
Approvers are the change management team members who vote to accept or reject Requests for Change. They can view information and comments, communicate, and vote on a Request for Change using BMC Track-It! Web. (A Request for Change is considered approved when all Approvers have approved, based on the number of approvals required.)

Note: It is not necessary for Approvers to have a license to use BMC Track-It! Self Service; their BMC Track-It! Administrator only needs to provide them with a login user name.

Configuring Change Management Workflow

The flowchart below represents the BMC Track-It! Administrator's tasks in the topics for this chapter.

Step 1: Setting up Change Management Policies

Change Management Policies define the approval process so that when Work Orders are created that match specific criteria, they enter into the Change Management process. Administrators can set up policies so that Approvers can either sequentially or simultaneously vote on Requests for Change. A due date can be set up for the voting process. The number of approvals required before a Request for Change is approved can also be specified.
To Set up a Change Management Policy:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Change Management > Change Management Policies**.
2. Click the **Add** button to create a new Change Management Policy.
3. Enter a name for the policy, for example, "Software Upgrade", in the **Policy Name** field of the **Change Management Policy** dialog.
4. To specify the order in which Approvers can vote, select "Sequential" or "Simultaneous" from the **Policy Type** drop-down list.
    a. Select **Sequential** if you want the Request for Change to be reviewed by one Approver at a time, in the order specified on the Change Management Policy.
    When automatic notifications are configured, a notification will not be sent to the next Approver until the previous Approver has approved the RFC.

b. Select **Simultaneous** if you want the RFC to be reviewed and decisions made by all Approvers at the same time. The approval process stops as soon as any single Approver rejects the RFC.

5. To set up the criteria that will cause a Work Order to enter the approval process, select the check boxes next to the Work Order fields under **Matching Criteria**, then select a value from the drop-down lists.
   - Each policy must have at least one matching criteria selected.
   - Change Management Policies must have unique matching criteria.
   - Once a Work Order enters the approval process under a Change Management Policy, it cannot be associated with any other Change Management Policy
   - The following fields can be set up as matching criteria (matching will occur based on the order listed below):
     - Requestor
     - Department
     - Location
     - Type
     - Subtype
     - Category
     - Priority

   You can add new values by any fields displaying the Add button (+).
6. If you want RFCs to have a due date by which a final decision needs to be made by Approvers, in the **Actions** section, enter or select the number of **Days** and/or **Hours** in the designated fields. This will calculate the date and time a decision is due from the moment the Work Order enters the Change Management process.
7. To **Override Operating Hours** for the Decision Due Date above, click the indicated check box. **Note:** if Override Operating Hours is selected, the decision due date and time will be calculated differently. See also: Setting up Help Desk Operating Hours.
8. To provide instructions for Approvers, enter the information in the **Instructions** text box.
9. Select the Approvers from the **Users** drop-down list, then click the **Add Approver** button. If you want to add a new User to the system, click the **Add** button (+) next to the **Users** field. Make sure to assign the User a Login name or select the option that they can log in using Windows authentication (see Viewing and Editing User Properties).
10. To specify the number of approvals required before a Request for Change is approved, enter or select a number in the **Number of Approvals Required** field.
11. Ensure the **Policy Enabled** check box is checked, then click the **Save** button.

Step 2: Configuring Notifications for Change Management Events

You can set up e-mail and text message notifications so that Approvers and assigned Technicians are automatically notified when specific events occur throughout the Change Management lifecycle. For example, a Change Management Policy can be set up so that Approvers are notified when a new Request for Change is created and when a decision is overdue. You can also customize the content of the notifications (see Step 13b: Customizing Notifications in the E-mail Monitor chapter).

Notifications will not be sent after a final decision has been made or a Request for Change has been canceled, except for the "Request for Change canceled" notification for Approvers and the "Request for Change final decision" notification to Approvers and/or Assigned Technicians.

To Configure Change Management Notifications:

1. From the main menu bar, select Tools **> Administration Console > Configuration > Change Management > Change Management Policies**.
2. Select the **Change Management Policy** in the grid, and then click the **Edit** button.
3. Click the **Configure Notifications** button on the **Change Management Policy** dialog.
4. On the **Configure Notifications** dialog, select the **Approvers** or **Assigned Technician** tab.

5. By default, all notifications are selected, but you can click the check boxes to deselect them if desired.
6. Click the **OK** button to return to the **Change Management Policy** dialog.

To Schedule BMC Track-It! to Send Notifications for Change Management Events
In order for BMC Track-It! to automatically send notifications for Change Management events, you'll need to enable the feature and set the frequency at which events are checked by the BMC Track-It! Server.

Note: Make sure SMTP is configured (See Step 8: Configuring SMTP Settings for Sending E-mail).
To Schedule BMC Track-It! to Send Notifications for Change Management Events:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Change Management > Scheduling**.
2. Ensure the **Enabled** check box is checked.
3. Select the frequency at which you want BMC Track-It! to check Change Management events and send notifications from the **Time Interval** field.
4. Click the **Apply** button to save your changes, or the **OK** button to close the window.

To Manually Process Change Management Events:

1. Click the **Process Now** button.

Step 3: Allowing Technicians Access to the Change Management Module

In order for Track-It! Technicians to view the Change Management module, create Requests for Change, and change Approvers on a Request for Change, the BMC Track-It! Administrator must grant permission on the Technician's security policy.
To Allow Technicians Access to the Change Management Module

1. From the main menu bar, select T**ools > Administration Console > Lookup Tables > Security Policies**.
2. Double click to open the Security Policy you want to modify in the grid. See "Creating Custom Security Policies"
3. In the **Change Management** section on the **Modules** tab of the **Define Security Policy Techs** dialog, select the checkboxes for the permissions that you want to grant:
   - **View Requests for Change**
     This allows Technicians to view the Change Management module in BMC Track-It! If they do not have permissions for this module, they will still have access to the Change Management tab on their assigned Work Orders.
   - **Reassign Approver**
     This allows Technicians to change Approvers on the Request for Change. (See Managing Requests for Change in the Technician's guide).
4. In the **Help Desk** section on the **Modules** tab, ensure the **Add Work Orders** checkbox is selected.
5. Click the **Save** button on the **Define Security Policy Techs** dialog.
6. Click the **Apply** button to save your changes, and the **OK** button to close the **Security Policies** panel in the **Administration Console**.

See also the Change Management chapters in the Technician's guide and the Self Service guide (for Approvers).

Reports

Customizing Reports and Print Output

You can customize BMC Track-It! reports with Crystal Reports XI once you have exported them. (See Importing and Exporting Reports in the Technician's Guide.).

The default reports for individual work orders, assets, purchase orders, solutions, and software titles can also be customized. (These reports are accessed when Technicians click the Print button in BMC Track-It! for the selected records in a module's grid, such as a work order in the Help Desk module).

Customizing reports might be useful for adding your organization's logo or selecting which database fields display. BMC Track-It! Administrators can replace the default reports with customized reports via the Print Output panels for each area in the Administration Console.
To Replace a Default Report with a Customized Report:

1. From the main menu bar, select **Tools/Administration Console/Configuration**, then select the desired module (Help Desk, Solutions, Inventory, Purchasing, or Software License Management).
2. Select **Print Output**.
3. Click the **Export Report** button on the **Print Output** panel.
4. On the **Save As** dialog, navigate to the drive or folder where you want to save the report, then click the **Save** button on the dialog.
5. Open the report (.rpt) in **Crystal Reports** and customize it as desired, then save it.
6. On the **Print Output** panel in BMC Track-It!, click the **Import Report** button.
7. On the **Open** dialog, navigate to the report, then click the **Open** button.
8. Click the **OK** button on the **Print Output** panel to save your changes and close the **Administration Console**.

Technicians will now be able to view the customized report when they print the individual records per module, such as work orders in the Help Desk module.

To Restore a Default Report:
Repeat Step 1 above, then click the **Restore Default Report** on the **Print Output** panel.

Scheduled Reports

Scheduled Reports Overview

Administrators can configure BMC Track-It! to schedule and automatically run reports and e-mail them to specified users. When scheduling a report, Administrators specify the report name, date and time to send the report, the email recipients, and whether or not to use Operating Hours.

Examples

- You might want to schedule the Open Work Order Aging report to automatically send to IT leads every week.
- You might want to schedule a custom report that you've created in Crystal Reports and imported into BMC Track-It!, such as the Completed Work Orders by Month report filtered by the current month.

You can schedule built-in reports for those that do not require input parameters, for example, the Open Work Order Aging or Open SLA Violations reports.

For more information on customizing reports using Crystal Reports, see Customizing Reports. For more information on BMC Track-It! report descriptions and on downloading and installing Crystal Reports to create and edit reports, see the BMC Track-It! Reports Descriptions PDF on our Support Web site.

See the next topics to configure Scheduled Reports:

1. Scheduling Reports
2. Configuring the Report Schedule Monitor to Check Report Schedules

Scheduling Reports

For an overview of this feature, see Scheduled Reports Overview.

To schedule a report:

1. From BMC Track-It!'s main menu bar, select **Tools > Administration Console**, then select **Configuration > Reports > Scheduled Reports > Reports Schedules**.
2. Click the **Add** button.
3. On the **Report Schedule - New** dialog, under **Selected Report**, select a report from the **Report Name** list.

   Note: As noted in the Scheduled Reports Overview, not all reports in the list can be scheduled. If you select a report that cannot be scheduled, the following message displays: "Selected report requires input parameters and therefore cannot be scheduled."
4. In the **Scheduled Effective Date** section, select the start date for the report to be run from the **Date of First Occurrence** list.

   (You can select a date from the calendar or enter a date in the field, for example, 12/31/2013)

   Note: Dates and times on the **Report Schedule** dialog box are shown in your BMC Track-It! server's current time zone. The name of the time zone and the time difference between the time zone and the Coordinated Universal Time are shown at the top of the dialog. For example, this would display as "(UTC-04:00) Eastern Daylight Time".
5. In the **Delivery Options** section, enter the e-mail address of the report recipient in the **To:** field. (You can enter multiple e-mail addresses separated by semi-colons.)
6. Enter the subject of the email in the **Subject** field.
   (You can also click the **More** button to display the **Delivery Options** dialog where you can add more recipients using Cc, Bcc; and text for the email message.

7. In the **Recurrence Pattern** section, select one of the following:

Options	Descriptions
Hourly	To run and email the report every hour: a. Select **Hourly**. b. In the **Start** field, select or enter the start time to run the report. c. In the **Run Every** field, select or enter the frequency at which the report is run (in hours). For example, • Enter 1 to run the report every hour • Enter 8 to run the report every eight hours c. In the **End** field, select or enter the a time to stop running the report. For example, • Enter 7:59 PM to stop running the report at that time. **Notes:** • You can enter a Start time greater than the End time. For example, to run the report overnight o from 5:00 PM to 8:00 AM • If, for any reason, the Report Schedule Monitor is stopped and started later, the next occurrence of the Report will be generated.
Daily	To run and email the report every day, or in a regular interval less than a week: a. Select **Daily**. b. In the **Time** field, select or enter the time to run the report. c. In the **Run Every** field, select or enter the frequency at which the report is run (in days). For example, o Enter 2 to run the report every other day. o Enter 3 to run the report every three days.
Weekly	To run and email the report on a particular day or days of every week or regular week interval: a. Select **Weekly**. b. Select the day or days to run the report. For example, o Select Friday to run the report every Friday. o Select Tuesday and Thursday to run the report on each of those days.
Monthly	To run and email the report on a particular day of every month or regular month interval: a. Select **Monthly**. b. In the **Time** field, select or enter the time to run the report. c. In the Run on Day field, select the day to run the report. For example, o Select 1 to run the report on the first day of every month. **Note:** If the report is set to run on the 29th, 30th, or 31st day of the month and the month has fewer days, the report will be generated on the last day of the month.

8. (Optional) Select the Use **Operating Hours when calculating time intervals** check box. (This option is dimmed for monthly recurrence patterns. For more information, see Setting up Help Desk Operating Hours.)
9. Click **Save**.

To edit a scheduled report:

1. On the **Report Schedules** panel, select the Report Schedule, then click **Edit**.
2. On the **Report Schedule** dialog, make the necessary changes, then click **Save**.

To prevent the Report Schedule Monitor from running and emailing a report

1. Clear the **Schedule Enabled** check box.

To delete a Report Schedule

1. Close the **Report Schedule** dialog.
2. On the **Report Schedules** panel, select the Report Schedule, then click **Delete**.

Configuring the Report Schedule Monitor to Check Report Schedules

For an overview of this feature, see Scheduled Reports Overview.

Note: For the Report Schedule Monitor to work correctly, it is *not* recommended that you change any of the settings on the Automated Schedule panel.

The Report Schedule Monitor is configured by default to automatically check the Report Schedules every minute to determine whether new reports should be run and emailed to the specified users. Administrators can, however, make configuration changes as necessary.

In addition to configuring the Report Schedule Monitor, Administrators can also manually run the Report Schedule Monitor from the Automated Schedule panel. This is useful for testing configurations.

Before you begin

1. Schedule a report.
2. Make sure SMTP is configured (See Configuring SMTP Settings for Sending E-mail).

To configure the Report Schedule Monitor

1. From BMC Track-It!'s main menu bar, select **Tools > Administration Console**, then select **Configuration > Reports > Scheduled Reports > Automated Schedule**.
2. To prevent the Report Schedule Monitor from running and emailing reports, select **Do not automatically monitor report schedules**.
3. Click **Apply** to save your changes.
4. To manually run the Report Schedule Monitor and email reports (based on the settings on the Report Schedules), click **Check Now**.

The **Report Schedule Monitor Log** displays status, errors, and other information in the grid (see below).

Report Schedule Monitor Log

The **Report Schedule Monitor Log** displays the Date/Time, Event Type, and Summary of the Report Schedule checks. For example, this will display "Report [name] was created based on schedule [ID of the Report Schedule]."

To print grid contents:
See Printing Grid Contents in the Technician's Guide.

To export grid contents:
See Exporting Grid Contents Technician's Guide.

To view log details:
1. Double click the record (per row) in the **Report Schedule Monitor Log**.
2. In the **Event Detail** dialog, click the **Previous** or **Next** button to view each record.
3. To copy the information, click the **Copy to Clipboard** button.

To purge the Report Schedule Monitor Log messages:
1. Click the **Purge Log** button.
2. Click the **Yes** button on the **Purge Confirmation** dialog.

   A message in the log will display the number of purged records.

Implementing ITIL Processes Using BMC Track-It!

Implementing ITIL Processes Using BMC Track-It! (Overview)

Note: ITIL is a suggested best practice framework. The following instructions are recommended guidelines only. Each customer implementation may vary depending on ITIL® interpretation and your organization's requirements.

You can configure Track-It's Help Desk module and use the Change Management module to support the IT Infrastructure Library (ITIL) incident, problem, and change management processes. This involves a few simple configuration changes in the Help Desk module and following a particular workflow between the Help Desk and Change Management modules. You can also use the Request Types defined below to create custom reports.

ITIL Definitions and Examples
ITIL provides guidance about creating and operating a Service Desk to provide efficient communication between the user community and the IT provider. The job of the Service Desk is to provide effective Incident, Problem, and Change management.

Service Request
A Service Request is a request from a User for information, advice, a standard change, or for access to an IT service. Service Requests are usually handled by a Service Desk, and do not require a Request for Change (RFC) to be submitted. Service Requests do not involve any failure in the IT Infrastructure. The objective of request fulfillment is to assist with general information and to provide a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists.

Translation: The Level 1 team handles these issues because they can be closed quickly and do not affect many customers.

Examples: Requests for information, “how to” questions, and recurring requests for standard services.

Incident

An incident is an unplanned interruption of an IT service or a reduction in quality of an IT service. The objective of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. This ensures that the best possible levels of service quality and availability are maintained.

Translation: The Level 1 team handles these issues because they can be closed quickly and do not affect many customers.
Examples: Cannot send or receive e-mail, cannot access internet, or printer won't print.

Problem

A Problem is an unknown cause of one or more incidents. The objective of Problem Management is to prevent problems and resulting incidents from happening, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

Translation: These are incidents that Level 1 support cannot handle or may be affecting many customers. (These are generally referred to as Problems before the cause is known, and Known Errors once the cause is determined.)
Examples: Exchange server has crashed, network drive is down, or printer is damaged.

Request for Change

A Request for Change is a formal communication seeking an alteration to one or more configuration items. The objective of the Change Management process is to ensure that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner.

Translation: All IT-related changes that may affect one or many customers are tracked with Change Management.
Examples: Adding memory to a computer, purchasing a new server, or installing the latest Windows operating system on computers.

Next Topic: Configuring BMC Track-It! for ITIL Processes

Configuring BMC Track-It! for ITIL Processes

The following describes how to configure the Help Desk module to support ITIL processes. Follow the instructions in the Configuring Change Management Workflow topic so that the Incident or Problems enter the Change Management process where necessary.

Step 1: Set up Work Order Types

If you've already set up Work Order Types, you can use the existing Types, Subtypes, and Categories or create new classifications. For more information on Work Order Types, see Classifying the Work Order Issue in the Technician’s Guide.

Step 2: Set up Work Order Notifications

Set up Work Order Notifications so that Technicians are automatically notified when a Work Order event occurs.

Step 3: Set up Skill Routing Policies

Skill Routing Policies allow you to assign specific Technicians to Work Orders based on their skill sets, which correspond to matching criteria on the Work Order fields.

Step 4: Set up Request Types

The following instructions describe how to set up a Work Order so that you can use a custom lookup table to classify types of requests (service request, incident, problem, and known error).

To Create a Customized Lookup Field for Request Types:

1. From the main menu bar, select **Tools > Administration Console > Lookup Tables > Help Desk**.
2. Select one of the **Lookup Tables** (Lookup#1 through #8).
3. Click the **Add** button.
4. In the **Name** text box on the **User Lookup** dialog, enter "Incident", then click the **Save** button.
5. Repeat the steps above to enter the values "Problem" and “Service Request”.

To Change the Work Order's Field Label to "Request Type" and Set the Default to "Service Request":

1. Open a Work Order.
2. Click in the **Lookup Table** field that you set up above, then press the **CTRL+F2** keys.
3. On the **Field Options** dialog, enter the "Request Type" in the **Label** field.
4. To use "Service Request" as the default value that will automatically display in the field, enter it in the **Default Value** field.
5. Click the **OK** button.

Now when a Work Order is created, the default Request Type will be set to Service Request

Step 5: Customize the Help Desk Grid View to Display the Request Type

This will enable you to quickly view the lists of Work Orders by Request Type.

To Customize the Help Desk Grid View to Display Request Type:

Note: You may need to exit re-start the BMC Track-It! Technician client to ensure your change to the Look Up field has been saved.

1. Right click anywhere on the grid, then select **Customize**.
2. In the **Customize Grid** dialog (**Columns** pane), select the Request Type, then click the **Add** button.

Next topic: ITIL Incident, Problem, and Change Workflow in BMC Track-It!

ITIL Incident, Problem, and Change Workflow in BMC Track-It!

After the Help Desk and Change Management modules are configured to support ITIL processes, follow the example workflow below.

In this example, Incidents relating to e-mail access will be created. Ultimately, it is determined that the Exchange Server needs a critical software update and is affecting many customers. A Problem and Request for Change will be created to resolve the issue.

Step 1: Create Work Orders and Classify Requests as Incidents

A Technician creates an Incident for a User’s request indicating they are having trouble with their e-mail. Similar Incidents have also been created by other Technicians.

1. Create and populate the Work Order. Select the **Classification Type**, **Subtype** and **Category**.
2. Select the **Request Type** "Incident".
3. Save the Work Order.

Step 2: Create a New Work Order or Copy the Work Order and Define It as a Problem

Several e-mail related Incidents have now been created. It has been determined that the e-mail Incident is affecting multiple users and cannot be resolved quickly. The incident will now become a Problem and enter the Problem Management process.

1. Create a new Work Order or copy one of the Incident Work Orders.
2. Change the **Subtype** and/or **Category** as appropriate.
3. Change the **Request Type** to Problem.
4. Save the Work Order.

Step 3: Assign Incident Work Order(s) to Problem Work Order

In order to keep track of who is affected by the Problem and to ensure they are notified when the problem is resolved, Incidents should be associated to the Problem. When the Problem is closed, the assigned Incident Work Orders will also close.

1. Make sure the Help Desk grid view is customized to show the **Request Type** column to easily determine which items are incidents.
2. On the Help Desk grid, select the Incident Work Order and assign it to the Problem Work Order.

Step 4: Root Cause Requires Problem Work Order to Enter Change Management Process
The problem team determines that the Exchange Server needs a critical software update to resolve the e-mail Incident. The Problem is classified to reflect the needed software update which causes it to automatically enter the Change Management process.

1. Change the **Subtype** and/or **Category** as appropriate after the root cause is determined.
2. If a Change Management policy is set up causing the Problem Work Order to automatically enter the Change Management process, a message will display. Click **OK**.
3. To view details, click the **Change Management** tab on the Work Order.

Step 5: Final Decision on Request for Change Notification Received
Once the Request for Change has been approved, the Problem team can resolve the issue and the Problem Work Order can be closed. This will notify all users who created Incidents.

1. Enter the resolution and any other information you want to add to the Problem Work Order.
2. Because there are Assignments, when you attempt to change the Work Order's status to Closed, a message will display. Click **Yes** to close the parent Work Order and Assignments.

Administrative Tools

Maintaining Registration Support and Licenses

The **Support Center** in the Administration Console enables you to maintain your BMC Track-It! registration/contact information, support plan, and licenses. You can also automatically renew your support plan and request additional licenses directly from the **Support Center** window.

Note: Only the BMC Track-It! administrator has access to the Support Center.
To Access the Support Center:

1. From the main menu bar, select **Tools/Administration Console/Administration/ Support Center**.
2. Click the **Support Center** button. The **Home** tab displays.
3. Your BMC Track-It! version, support and update information is displayed and is read only (cannot be edited).

Maintaining Your Registration/Contact Information

When you update your contact information, we are automatically notified via the internet.
To Maintain Your Contact Information:

1. Click the **View Details** hyperlink on the **Home** tab, or click the **Registration** tab.
2. The Ship To, Bill To, Billing Contact, and Support Contact tabs display. This is the information we will use to contact you.
3. To update your contact information, enter the information in the fields for all four tabs. All fields are editable except the Company Name.
4. If your shipping and billing information is the same, click the Bill to the Same Address check box.
5. To add your company's logo, click the **Add Your Logo** hyperlink.
6. Your logo must be in either of the following formats: BMP, ICO, WMF.
7. Select the image file from the **Logo Image** dialog.

8. Click the **Save Changes** button.

Maintaining Your Support Plan Information

Your support plan information is displayed listing the plan, expiration date, telephone number and e-mail address of your account representative, Knowledgebase subscription, and number of upgrades.

To Renew Your Support Contract:

1. On the **Registration** tab, click the hyperlink **Click Here to Renew Your Support Contract Today**!
   This will launch your e-mail editor with pre-populated information addressed to our account representatives.
2. Send the e-mail and your renewal request will be automatically processed.

Maintaining Your License Information

To View Your License Information:

1. Click the **Licensing** tab, or click the **View** hyperlink in the **License** area on the **Home** tab.
   The Licensing tab displays. A detailed description displays for each of your licensed Features and Modules. The Owned column displays your number of licenses. The In Use column displays the number of licenses currently in use.

To Request a Quote for Additional Licenses:

1. Click the hyperlink **Click Here to Request a Quote for Additional Licensing**.
   Your e-mail editor launches and an e-mail message is automatically created.
2. Send the e-mail and your request will be sent directly to your sales representative, who will contact you as soon as possible.

Distributing the BMC Track-It! Technician Client

(Configuration Wizard Step 2 of 3: Distributing Technician Client Applications)

BMC Track-It! Technicians can install the BMC Track-It! application by clicking on a link sent via e-mail from your Help Desk e-mail account.

To Distribute the BMC Track-It! Technician Client to Technicians:

(If you're using the **Configuration Wizard**, start with the screen: Step 2 of 3: Distribute Technician Client Applications.)

1. From the main menu bar, select **Tools/Administration Console/Administration/Distribute Technician Client.**

   The **Technician Client Click-Once** link is displayed.

2. Select the technician(s) from the **Available Technicians** list, then click the **Add** button.
   (You can select multiple technicians by holding the Shift or CTRL key as you select them). This places the technicians in the Technicians to Notify list.
3. Click the **Send E-mail** button.
4. On the **Enter E-mail Address** dialog, enter the e-mail address that was set up for your Help Desk e-mail account (e.g. help@yourcompany.com, then click the **OK** button.

   The selected Technicians will receive an e-mail with a link so that they can install the BMC Track-It! Technician Client.

Managing the Scheduled Audit Queue

Once computers have been scheduled for audits, they are displayed on the **Queue** panel in the **Administration Console**. This displays the Asset Name, Status, Schedule Date and Time, Asset ID,

User Name, and Audit Completed Date and Time. The **Queue History** tab displays the computers that were audited prior to the currently scheduled audits.

Caution: Before performing any audits on computers created from a Ghost image (cloned), be sure to remove the Trackitaudit.id file from the root of the C:, if it exists. (The file is hidden on the root of C: by default). If the file is not removed and multiple machines have the same Trackitaudit.id file, the audits will continuously merge into a single record in Inventory. For details, see our KnowledgeBase article "Track-It! 6.x, 7, 8.x, and 9 Audit Merge Process"

Note: You can exclude specific computers from scheduled audits. (Computers must be selected in the Inventory grid before the scheduled audit is run.) See Including and Excluding Computers from Scheduled Audits in the Technician's Guide.

To Access the Queue Management Window:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Inventory/Auditing/Queue**.

To Stop Scheduled Audits:

You can clear the **Current Queue**, which will stop the auditing process of the scheduled computers.

1. Click the **Clear** button on the **Current Queue** tab.
2. Click **Apply** to save your changes and click **OK** to close the window.

To Suspend Scheduled Audits:

If you need to suspend scheduled audits (e.g. if your network is down, etc.), you can suspend the audits until you're ready to resume them.

1. Uncheck the **Process Audit Queue** checkbox.
2. When you're ready to resume the audits, check the **Process Audit Queue** checkbox.

To Clear the Queue History:

1. Click the **Clear** button on the **Queue History** tab.
2. Click **Apply** to save your changes and click **OK** to close the window.

To Stop the Grids from Refreshing So You Can Sort and Filter Records:

If there are several records in the grids, it may be helpful to sort and filter the records. In order to do this, you'll need to stop the grids from refreshing as the audits are processing.

1. Uncheck the **Automatic Refresh of Grid Display** checkbox.

Related Topics:

Configuring Scheduled Audits

Viewing the Help Desk Audit Trail for Work Order Changes

BMC Track-It! automatically tracks and displays technician and system activity for a Work Order so you can monitor changes through its lifecycle. You can view the Audit Trail for all Work Orders in the Administration Console, or individual Work Orders from the Help Desk module (see Viewing the Work Order's Audit Trail in the Technician's Guide).

To View the Help Desk Audit Trail:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Audit Trail/Help Desk**.
3. Double click to view a particular Work Order's Audit Trail.

Viewing the Inventory Audit trail for Asset Changes

BMC Track-It! automatically tracks and displays Technician and system activity for an Asset so you can monitor changes through its life cycle. You can view the Audit Trail for all Assets in the Administration Console, which displays all created and deleted assets. You can view an individual Asset's Audit Trail from here, or from the Inventory module (see Viewing an Asset's Audit Trail in the Technician's Guide).
To View the Inventory Audit Trail:

1. Select **Administration Console** from the **Tools** menu on the main menu bar.
2. In the **Administration Console**, select **Audit Trail/Inventory**.
3. Double click to view a particular Asset's Audit Trail.

Changing Your Database Password

Warning: If you must change the BMC Track-It! Administrator's database password, it is recommended that you do so at a time when there are no users logged on to BMC Track-It!. Changing the database password will cause all connected clients and all connected services to immediately lose connection to the database server. By accepting this warning you understand that you will be logged off immediately after changing the password and all BMC Track-It! Services will have to be restarted after this change.
To Change Your Database Password:

1. Make sure that all users have logged off the BMC Track-It! application.
2. From the main menu bar, select **Tools/Administration Console/Administration/Change Database Password.**
3. Click the checkbox next to the **Warning** message.
4. Enter the **new password** in the designated textbox, and then enter it again in the **Confirm Password** textbox.
5. Click the **Apply** button to save your changes, and the **OK** button to close the window.
6. BMC Track-It! will close and you will need to restart the services (see below).

To Restart BMC Track-It! Services:

1. Run the Microsoft Management Console (MMC).
2. Restart all BMC Track-It! services:
    - "BMC Track-It! 9 Account Management Service" or ""BMC Track-It! 8.0 Account Management Service"
    - "BMC Track-It! Service Management"

3. If you are running BMC Track-It! Web components, restart them (listed below) as well as Internet Information Services (IIS) and all World Wide Web Services.

    BMC Track-It! Web components:

    - BMC Track-It! Self-Service
    - BMC Track-It! Web
    - Password Reset

You and other users can now log on to BMC Track-It!.

Monitoring and Maintaining System Health

System Health Overview

You can monitor and maintain the BMC Track-It! system health to keep the system running as efficiently as possible. The System Health Monitor managed from the **Administration Console**, notifies you which database activities are in need of maintenance (database index fragmentation, backup, and transaction log backup). It also notifies you when there are potentially invalid assets. (See descriptions below in

Monitored System Health Items.) Work Orders are automatically generated when a monitored item requires maintenance. The System Health Monitor can be scheduled to run automatically and can also be manually run .

Note: The System Health Monitor supports SQL databases only.

Monitored System Health Items

The following types of system health items are monitored:

- *Database Index Fragmentation*
  As data changes in the Track-It! database, indexes can become fragmented which can decrease overall performance. The System Health Monitor will provide a warning when the database index fragmentation goes above a configurable level.

  Instructions on reindexing the database are provided in the KnowledgeBase article: Database ReIndex.

- *Database Recoverability*
  - If the Track-It! database is not backed up on a regular basis, you will not be able to recover the system to an earlier state, if needed. The System Health Monitor will provide a warning when the database has not been backed up in a configurable amount of days.

  - A large transaction log could lead to poor performance and should be backed up on a regular basis. The System Health Monitor will provide a warning when the transaction log has not been backed up in a configurable amount of days.

  Instructions on backing up the database and transaction log are provided in the KnowledgeBase article: Database Backup.

- *Potentially Invalid Assets*
  Invalid Assets are assets where the audit/merge process has been compromised by the existence of a hidden file (TrackItAudit.id) on multiple PCs that were imaged from a PC that had been audited by Track-It!.

  Over time, these assets may be very slow to open and can cause the merge's performance to suffer.

  Instructions on removing invalid assets are provided in the KnowledgeBase article: Invalid Assets.

Next topic: Monitoring and Maintaining System Health

Monitoring and Maintaining System Health

You can monitor the BMC Track-It! System Health on the **Monitored Items** panel in the **System Health Monitor** in the **Administration Console**. See also System Health Overview.

To Monitor the BMC Track-It! System Health:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Administration/System Health Monitor/Monitored Items**.
2. Ensure that the **Enabled** checkbox is checked for each type of monitored item.

   Note: Although not recommended, you can disable an item from being monitored by deselecting

the **Enabled** checkbox.

The **Monitored Items** panel displays which items require action (indicated by "Yes" or "No"). Colors in the grid can be *customized*.

See Highlighting_Records_with_Conditional_Formatting in Creating User-defined Grid Views (BMC Track-It! Technician's Guide).

3. If action is required, click the **Description** link for the monitored item.

   This will open the KnowledgeBase article on our Web site with instructions on how to correct the issue. The articles also provide information on configuring the threshold the System Health Monitor will use to produce the warnings (for example, "Time since last database backup: 7 days").

4. Follow the instructions in the KnowledgeBase article.

   The next time the System Health Monitor is run, the **Monitored Items** panel will display the new status (such as "Database Backup Is Current"). The **System health Monitor Log** on the **Automated Schedule** panel will also display the new status.

Next topic: Configuring the System Health Monitor to Automatically Generate Work Orders

Configuring the System Health Monitor to Automatically Generate Work Orders

By default, the BMC Track-It! System Health Monitor generates a Work Order whenever a monitored system health item needs attention (such as database reindexing). Although not automatically assigned, you can assign a default Technician to System Health Work Orders.

The System Health Work Orders display in the Help Desk grid with the Work Order ID and the Summary from the System Health Monitor Log. By customizing the grid view, you can also see which Work Orders were created by the System Health Monitor by adding the "Opened by" column. See also Viewing and Finding Work Orders.

We recommend that you allow Work Orders to be automatically generated. If not, you'll need to remember to check the System Health Monitor in the Administration Console on a regular basis.

Example: Work Order Generated by the System Health Monitor

The Work Order description below is an example of the details provided, including the monitored item type, specific message, and link to the KnowledgeBase article with steps to correct the issue.

Notes

10/28/2009 3:19:19 PM by SystemHealthMonitor-WIN2003

The following monitored item is in need of attention:
Database Recoverability

The last monitor observation was:
Database Backup Is Out Of Date

A complete description of this monitored item and the steps required for corrective action can be found here:

http://support.numarasoftware.com/support/view_article.asp?ArticleID=4523

Work Order Notes: Description of Work Order Generated by the System Health Monitor

To Schedule the System Health Monitor to Generate Work Orders:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > System Health Monitor > Work Order Generation**.
2. Ensure the **Always create a work Order...** check box is checked.
3. To assign a default technician for System Health Work Orders, select a Technician from the **Technician** drop-down list.
4. Click the **Apply** button to save your changes, or the **OK** button to close the window.

Next topic: Scheduling the System Health Monitor

Scheduling the System Health Monitor

You can schedule the System Health Monitor to automatically check BMC Track-It! system health and display the status on the System Health Monitor Log at specific time intervals. Although the system check should only take a few seconds or less than a minute, it is recommended that you schedule the monitor to run during low periods of activity (the default is 12:00 a.m.). You can also manually run the system health check.

To Schedule the System Health Monitor:

1. From the main menu bar, select **Tools/Administration Console/Configuration/Administration/System Health Monitor**.
2. By default, the system health check will be run once a day at 12:00 a.m.
   It is recommended that you allow the System Health Monitor to check system health at least once a day. However, you can change this setting from the associated radio button.
   If preferred, you can schedule the system health check based on a time interval (for example, every 60 minutes).
3. Click the **Apply** button to save your changes.

   See Viewing the System Health Monitor Log for details about the System Health check results.

To Manually Check the System Health:

1. Click the **Check Now** button.

Next topic: Viewing the System Health Monitor Log

Viewing the System Health Monitor Log

The System Health Monitor Log on the **Automated Schedule** panel in the **Administration Console** displays details about BMC Track-It! system health and related events. The log can be printed or exported to a file (.txt, .xls, or .html). The log can also be purged.

The following are some of the messages displayed by the System Health Monitor Log:

Monitor Messages

Monitor Cycle

- Monitor cycle requested by user
- Monitor cycle started
- Monitor cycle completed

Database

- Database backup is current
- Database backup is out of date
- Index health satisfactory
- Index health unsatisfactory
- Status details (database reindex and database backup)

Invalid Assets

- Asset Health Satisfactory
- Asset Health Unsatisfactory
- Status details

Work Order

- Work order generated for monitored item

To View, Print, or Export the System Health Monitor Log:

1. From the main menu bar, select **Tools > Administration Console > Configuration > Administration > Automated Schedule**.

   The System Health Monitor Log displays the Date/Time, Event Type (Info, Status, or Error), and Summary of system health and related events.

2. To view details, double click the record in the **System Health Monitor Log**.

   The **Event Detail** dialog displays details for the Error, Information, or Status. For example, "Database backup is out of date" displays details such as the time since the last database and transaction log backup and configuration settings.

   Refer to **Monitored Items** panel in the **Administration Console** for the **Monitored Item** type (such as Database Recoverability) and a link to the KnowledgeBase article on how to correct the issue. See also Monitored System Health Items.

3. To copy the information, click the **Copy to Clipboard** button.

4. To print the information, see Printing Grid Contents.
5. To export the information, see Exporting Grid Contents
6. Click the **Close** button to return to the **Automated Schedule** panel.

To Purge the System Health Monitor Log Messages:

1. Click the **Purge Log** button.
2. Click the **Yes** button on the **Purge Confirmation** dialog.

   A message in the log will display with the number of purged records.

BMC Track-It! 11 Web

BMC Track-It! Web Overview

BMC Track-It! Web enables Technicians to access BMC Track-It! via the Web so that you can troubleshoot and solve IT issues while not at your desk. When you're back at your desk, you can manage any of the Work Orders, Inventory, and Solutions you created or edited in BMC Track-It! Web from the BMC Track-It! Technician Client.

The following modules are available in BMC Track-It! Web:

- **Help Desk**
- **Solutions**
- **Inventory**
- **Purchasing**
- **Library**
- **Change Management**

Note: Online help is available once you log in to BMC Track-It! Web (and is separate from the BMC Track-It! Technician Client online help). The topics in the online help are also available in the BMC Track-It! Web Technician's Guide (PDF) on the Product Documentation section of our Support Web page

To Access BMC Track-It! Web:

1. Go to the URL provided by your BMC Track-It! Administrator (typically `http://servername/TrackItWeb/` where "servername" is the name of the server).
2. Enter your user name and password and click the **Login** button.

   The **BMC Track-It! Web** home page displays.

BMC Track-It! 11 Mobile Web

BMC Track-It! Mobile Web Overview

BMC Track-It! Mobile Web enables you to access BMC Track-It! via mobile devices such as Android and iPhone smartphones. You can troubleshoot and solve IT issues while not at your desk. When you're back, you can manage any of the Work Orders you created or edited in BMC Track-It! Mobile Web from the BMC Track-It! Technician Client or BMC Track-It! Web.

Technicians can perform the following tasks in the Help Desk and Solutions modules from their mobile devices:

Home Screen

View Announcements

Help Desk

- View work orders
- Search for work orders by keyword and work order number
- Create work orders
- Edit work orders (including quick edits using preset fields
- Copy work orders
- Delete work orders
- Manage work order assignments
- View work order attachments
- View change management information
- Email conversation management (messages and responses are captured in the Work Order)

Solutions

- View Solutions

Inventory

- Create, modify, copy, and delete assets
- Audit assets
- Retire assets
- Email the requestor associated with an asset

Online help is available once you log in to BMC Track-It! Mobile Web on your mobile device. The topics in the mobile WebHelp are also available in the BMC Track-It! Mobile Web Technician's Guide (PDF) on the Product Documentation section of our Support Web page
A video tutorial of BMC Track-It! Mobile Web is available from the mobile Webhelp, and on our Web site.

To Access BMC Track-It! Mobile Web:

1. On your mobile device, go to the URL provided by your BMC Track-It! Administrator (typically `http://servername/TrackItWeb/` where "servername" is the name of the server).
2. Enter your user name and password, then tap the **Login** button.

   The **Work Order lists** display.

Note: If you would prefer to use the BMC Track-It! Web application from your mobile device, click the **View Full Site** link on the BMC Track-It! Mobile Web login screen.

See Also: Video Tutorial

Using BMC Track-It! Mobile Web (Video Tutorial)

This video tutorial will show you how to use BMC Track-It! Mobile Web.

iPhone/iPad (Quicktime .mov)

Android (.swf)

BMC Track-It! 11 Self Service

BMC Track-It Self Service Overview

BMC Track-It! Self Service is a Web-based application that enables your end users to submit their own Work Orders and check the status of their requests. Users can attach files, such as screenshots, to Work Orders.

Users can also search for internal BMC Track-It! Solutions.

Users can audit their computers and change their passwords.

Change Management approvers can also approve Requests for Change with Self Service.

Note: Online help is available once users log in to Self Service. The topics in the online help are also available in the BMC Track-It! Self Service Guide (PDF) on the Product Documentation section of our Support Web page

See Also: BMC Track-It! Installation Guides, Configuring Self Service, and Change Management Overview

Index