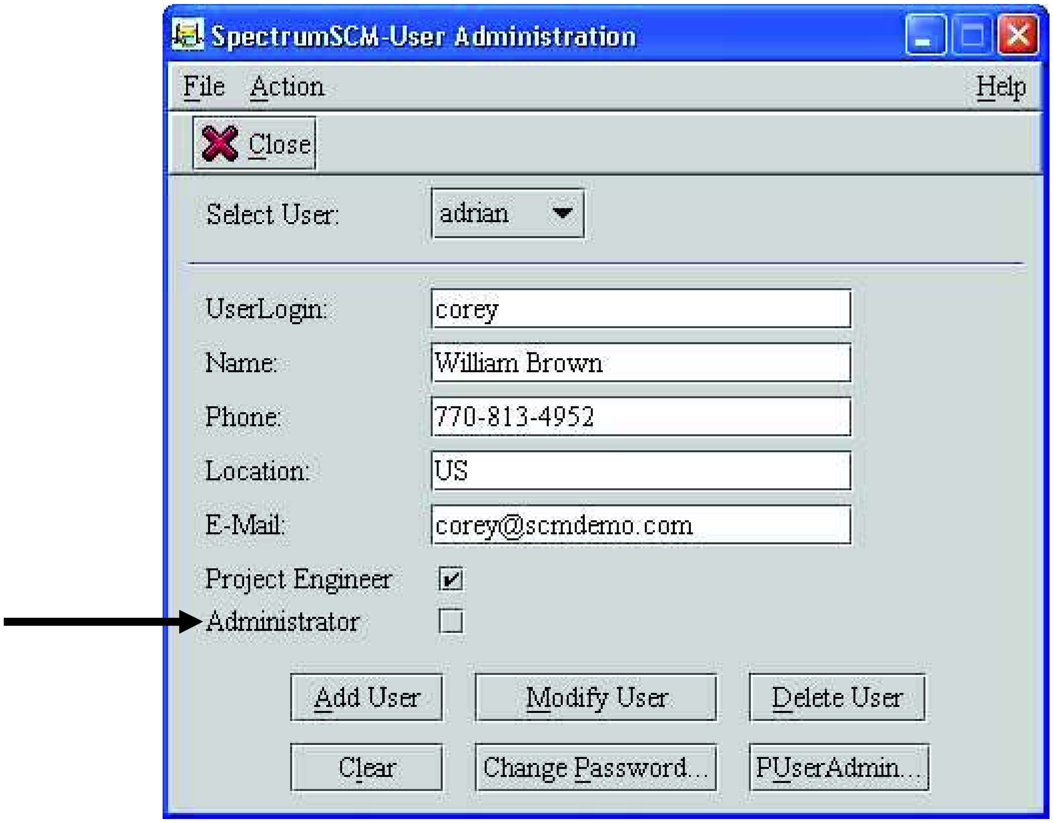
Chapter 12

12 SpectrumSCM Administrative Functions

This chapter covers the SpectrumSCM system administration functions and some project-level administration functions accessible via the Administration menu option on the Main Screen.

The **Administrator** is the root/all-powerful user of the SCM tool. The “scm” administrator account is automatically added to the tool at build time. This may be removed at a later time but at a minimum you must always have at least one SCM administrator in the SpectrumSCM system. When a user is added to the SpectrumSCM system, he or she can be assigned Administrator authority level via the User Administration screen. *See Chapter 5, User Management, for details.*



Select User: adrian

UserLogin: corey

Name: William Brown

Phone: 770-813-4952

Location: US

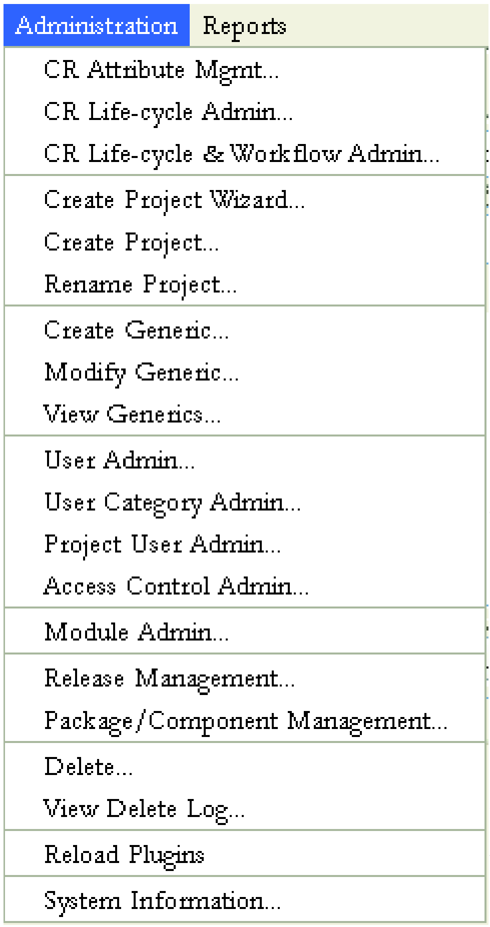
E-Mail: corey@scmdemo.com

Project Engineer ☑

Administrator □

12.1 SpectrumSCM Administration Menu

The Administration options are available via the Main Screen.



CR Attribute Mgmt - Manage the system-wide and project specific change request attributes.
CR Life-cycle Admin - Manage the life-cycle definitions and their assignment to projects.
CR Life-cycle & Workflow Admin – Manage the graphical workflow definitions and their assignment to projects.
Create Project Wizard – Add a new project using a wizard that runs through all the project creation steps
Create Project - Add a new project.
Create Generic - Add a new generic/branch to the current project.
Modify Generic - Modify a generic, specifically to manage its commonality lock i.e. whether developers are allowed to perform common edits.
View Generics – View the existing generics and their relative heirarchies.
User Admin - Maintain the system-wide user list. This includes names and contact information only.
User Category Admin - Maintain the set of user categories/roles.
Project User Admin. - Manage the Project-User relationship. I.e. manage which users are assigned to work on which projects and with what roles.
Access Control Admin – Define role based access permissions for generics, directories and files
Module Admin - Maintain your module definitions.
Release Management - Create and manage releases.
Package/Component Management – Create and manage packages and their components.
Delete - To delete an item (Project, Generic, Directory or File).
View Delete Log – View and possibly restore deleted items. Items that are marked as soft deleted can be retrieved. Hard deleted items cannot be restored.
Reload Plugins – Reload and restart user defined custom API plugins.
System Information – A "gas gauge" for the project repository. It shows you how much of the repository space is left. If System Repository Space is running low, contact Spectrum Software Support.

- CR Attribute Management is described in Chapter 7.
- CR Lifecycle Admin, Create Project, Create Project Wizard, Create Generic, and Modify Generic functions are used during project set-up and are described in Chapter 6, Process Management. Create Generic and Modify Generic are also used in Branching, which is described in Chapter 11, Branching, Merging and Re-common.
- User Admin, User Category Admin, Project-User Admin and Access Control Lists are used to control security and user access permissions. These are described in Chapter 5, User Management.
- Module Admin is a user level function that is used in managing source files and is described in Chapter 8.
- Release and Package Management functions are described in Chapter 9.
- Only Administrators and Project Engineers would generally have the ability to use the Delete function, however this is covered by the role based permissions and is configurable through the user category screen. File, Folder, Generic and Project deletion is described in Chapter 8 – Source File Management. CRs are deleted via the Change Request Assign/Modify screen described in Chapter 7.
- See Chapter 14 – API Concepts and Usage for more information on defining and using plugins.

12.2 Other Administrative Functions

The following functions can be executed from the command line or via the Windows START menu.

- **checkServer** - Check the status of the current SpectrumSCM server.
- **startServer –** Starts the SpectrumSCM server.
- **startServerAsService –** On Microsoft Windows platforms it might be desired to setup and run the SpectrumSCM server as a Windows service. Executing this script will install the Microsoft supplied ***AutoExNt*** service and set it to run automatically. If the server machine is restarted the SpectrumSCM server process will then restart automatically. See http://www.spectrumscm.com/FAQ.htm#_NTService for more details on this.
- **stopServer** - Stop the SpectrumSCM server. Note that this requires the user to input an administrator login and password for security reasons.
- **startUI –** Starts the SpectrumSCM graphical user interface client.
- **cloneActivation –** When the SpectrumSCM server is installed a control file is located in the users home directory and on Microsoft Windows platforms “Start” menu items will be inserted. If another user is requested to perform administration duties they would not have access to these control items. Simply executing the “cloneActivation” script (as that new user) will set up the appropriate control file and menu items.
- **uninstall –** used to uninstall all components of the server and UI. Do not use this when doing upgrades! It removes ALL components of SpectrumSCM, including all project databases.
- **uninstallUI –** removes the components of the SpectrumSCM user interface from a client machine.

To use the SpectrumSCM UI, the SpectrumSCM server must be up and the SpectrumSCM UI client on your machine must be started.

To check to see if the server is up:

In a WINDOWS environment
Start-> Programs -> SpectrumSCM UI ->CheckServer
In a UNIX or LINUX environment
change directory to the **<SpectrumSCM install>/bin** directory
execute the command **checkServer**

If the Server is running, you can start the SpectrumSCM UI
In a WINDOWS environment
Start-> Programs -> SpectrumSCM UI ->StartUI.
In a UNIX or LINUX environment
The UI can be started from the command line, nohup'ed, assuming you are running an X-server on the UNIX/Linux system. It can also be started from an xterm window.
change directory to the **<SpectrumSCM install>/bin** directory
execute the command **startUI**

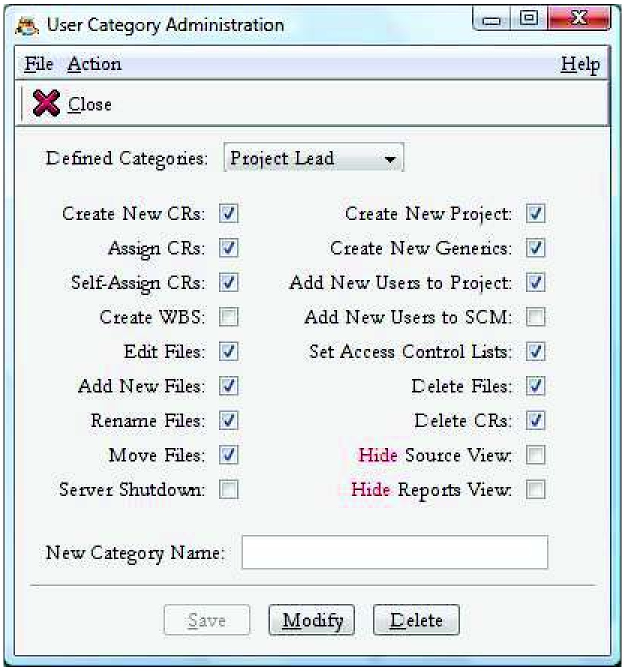
The UI is closed by exiting the graphical user interface (File / Exit) or by closing the SpectrumSCM UI window.

12.3 Who can execute Administrative functions

Access to the SpectrumSCM Administrative functions is limited and allowed by system and project level permissions.

As the default, when users are added to the SpectrumSCM system,

- Administrators have access to all functions.
- Project Engineers have access to most functions except User Admin. A project engineer at the system level is a project engineer across all projects in the system. Users can be granted Project Engineer permissions on a project-by-project basis through the Project-User Administration screen.
- Users would generally only have access only to Module Admin *(see Chapter 8, Module Admin for details)*



Defined Categories: Project Lead

Create New CRs: ☑
Assign CRs: ☑
Self-Assign CRs: ☑
Create WBS: □
Edit Files: ☑
Add New Files: ☑
Rename Files: ☑
Move Files: ☑
Server Shutdown: □

Create New Project: ☑
Create New Generics: ☑
Add New Users to Project: ☑
Add New Users to SCM: □
Set Access Control Lists: ☑
Delete Files: ☑
Delete CRs: ☑
Hide Source View: □
Hide Reports View: □

New Category Name:

NOTE: These defaults can be overridden by project-level category permissions when categories are set up on the **Category Administration** Screen.

Any user assigned to a role that allows "Create New Project" permissions will have access to the system wide functions involved in setting up a new project. These include the attribute management and life-cycle management screens.

Users who have the permission to "Create New Generics" will also have access to the Generic Engineer aligned functions of Release Management and Package Management.

Permission to "Add New Users to SCM" allows access to the User Admin screen/function. Permission to "Add New users to Project" provides access to the Project User Admin screen/function. Permission to "Delete Files" provides access to the Admin menu -> Delete function.

NOTE: Pay attention to how the System-level and project-level permissions interact. Define and assign project-level roles carefully, giving users only the permissions they require to complete their work assignments.
See Chapter 5 for details on User Management, including system and project level permissions.

12.4 SpectrumSCM Security Features

SpectrumSCM offers a variety of security features to protect the assets it manages. These features fall into two groups, access control and communications security.

12.4.1 Access Control

SpectrumSCM employs a traditional account-based access model. The SpectrumSCM administrator role is responsible for creating user accounts. These accounts are protected by a login/password pair, which must be provided when a user logs into the application. This is the default application security model, an open mode that is generally acceptable for use on a corporate intranet. Additional Access Control can be configured through the server configuration wizard (or by editing the file *SERVER INSTALL DIRECTORY*/SCM_VAR/etc/security/accessControl).

12.4.2 Communications Security / SSL

By default, SpectrumSCM operates in an open mode, which is generally acceptable for use on a corporate intranet. This mode is the most efficient and appropriate for a majority of installations. If it is necessary to use SpectrumSCM across an uncontrolled, non-secure network (such as the Internet), SpectrumSCM provides a means of using **SSL** (**S**ecure **S**ocket **L**ayer) to protect its communications, assuring that source files may be checked out, modified, and checked in securely. SpectrumSCM can be configured to protect its communications using **SSL**, a security standard developed by Netscape and approved by the Internet Engineering Task Force as a standard).

The administrator must obtain an SSL key and configure SpectrumSCM. The configuration file must be edited to use SSL. This is done through the server configuration wizard or by directly editing *SERVER INSTALL DIRECTORY/SCM_VAR*/etc/scm.properties. The last section of the file pertains to SSL. The **ssl.inuse** property should be set "true" and the other SSL properties, particularly the SSL keystore (where the SSL key is stored) and the password that protects it must be provided.

Once the server has been properly configured for SSL, the SpectrumSCM clients may connect by using the SSL option. The SSL can be turned on via the UI Configuration Wizard or by supplying **-ssl** on the command line.

NOTE: Secured communications is not accomplished without a price - overall responses will be slower due to additional encryption/decryption processing at both ends of the connection.

12.4.3 Location Control

SpectrumSCM provides an additional level of security based on the user's workstation hostname (or IP address). A user can be restricted to logging into the application from specific hosts. This feature is called **Location Control**; to enable it a "doAccess" line must appear in the accessControl file followed by "access" lines specifying allowed user/workstation combinations:

EXAMPLE SCRIPT

```
doAccess
      access  user1   workstation1
      access  user2   workstation2
etc.
```

The accessControl file is located in the following directory: <SERVER INSTALL DIRECTORY>\SCM_VAR\etc\security

NOTE: With location control turned on, users can only log into the SpectrumSCM system from specified workstations. Even valid users attempting to login from workstations other than those specified in the accessControl file will be denied, *even if they supply a valid password!*

12.4.4 Unauthenticated Commandline Access (Single Sign-On)

SpectrumSCM provides a UNIX-style command line interface for accessing many of its features, however as mentioned above the default security scheme would require a login and password for each server access. This may prove to be unnecessarily tedious when typing in a sequence of commands or incompatible for some activities (automated checking out of files by a nightly build script). This situation also comes up in the general world with people accessing many different IT systems and applications and has become known as **Single Sign-On**.

SpectrumSCM provides a feature called **Unauthenticated Commandline Access** to *relax* security, to allow unauthenticated command line access by specific users at specific workstations. Administrators should exercise caution when configuring this feature, and use it sparingly, if at all, considering all security ramifications.

Basically what single **"sign-on/unauthenticated access"** does is move the access control responsibility to the operating system/work-station level. Once a user has successfully logged in to the operatingsystem/work-station, that login information is what is then used to access the individual applications such as SpectrumSCM.

To enable this feature a "doUnauth" line must appear in the accessControl file followed by "unauth" lines specifying allowed user/workstation combinations.

EXAMPLE SCRIPT

```
doUnauth
      unauth  user1   workstation1
      unauth  user2   workstation2
etc.
```

Users logging in to the UI or executing command line functions from their corresponding workstations as configured in the accessControl file will not be required to provide a password since that verification has already been performed by the operating system.

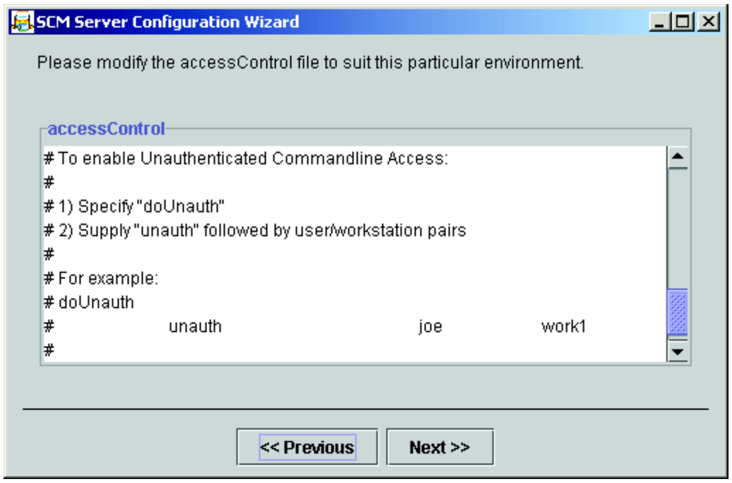
Administrators should exercise caution when configuring this feature, since if access to the workstation is not tightly controlled (ie access cards, screen locks etc) inappropriate accesses might occur.

The accessControl file (SERVER INSTALL DIRECTORY/ SCM_VAR/etc/security/accessControl) can be edited directly or via the Server Configuration Wizard.

To use the Command Line interface in a Windows environment, start the Command Prompt (cmd.exe) via Start / Programs/ Accessories / Command Prompt. In Unix or Linux, use the command line or an xterm window. Commands are executed from the <SCMUI install> bin directory:

```
        Unix or Linux example:         > cd   /home/user/scm/bin
        Windows example:               > cd   C:\home\user\scm\bin
```

See Chapter 13 for details on using Command Line Commands.

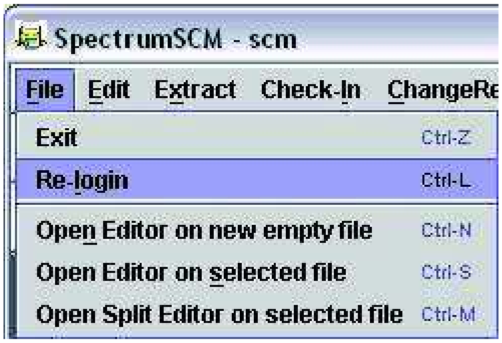


Please modify the accessControl file to suit this particular environment.

```
# To enable Unauthenticated Commandline Access:
#
# 1) Specify "doUnauth"
# 2) Supply "unauth" followed by user/workstation pairs
#
# For example:
# doUnauth
#               unauth                  joe             work1
#
```

NOTE/CAUTION!: Whereas Location Control tightens security, Unauthenticated Commandline Access could be viewed as relaxing security. In addition, Location Control takes precedence over Unauthenticated Commandline Access.

12.4.5 Automatic Login Control


SpectrumSCM - scm
File
Edit
Extract
Check-In
ChangeRe
Exit
Ctrl-Z
Re-login
Ctrl-L
Open Editor on new empty file
Ctrl-N
Open Editor on selected file
Ctrl-S
Open Split Editor on selected file
Ctrl-M

Setting up unauthenticated command line accounts also enables GUI automatic logins. Users that have an unauthenticated entry in the access control file will not need to enter a password into the initial GUI login screen. The system will automatically detect the user's login account from the operating system environment and attempt to use that information to automatically sign the user in the

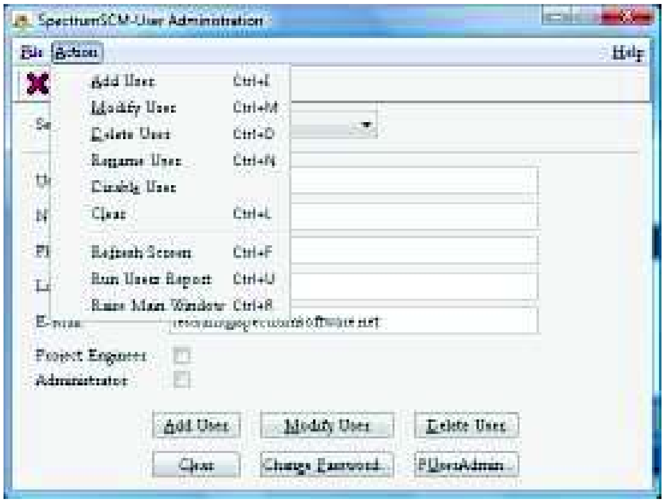
SpectrumSCM system. Failed automatic logins will present the user with the standard login/password screen for manual identification.

Once logged in, the user can use the **re-login** control, located in the File Menu Pulldown to log into the system as a different user.

12.5 Renaming Users

New

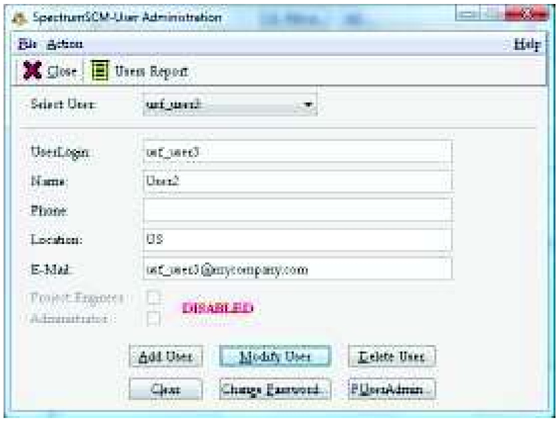
You can rename an existing user-id while maintaining full tracability of all the CRs that would transition from the old user-id to the new one.



12.6 Disabling Users

New

You can disable a user so that their full identification is maintained but yet they would not be able to login to the SpectrumSCM system. You can enable a later date if you choose do so as well. Additionally you can click on the **"Users Report"** tool bar icon. This report displays the roles of all users across all projects. You can see the "DISABLED" status of "usf_user3" used in the example below.



Select User: usf_user3

UserLogin: usf_user3

Name: User2

Phone:

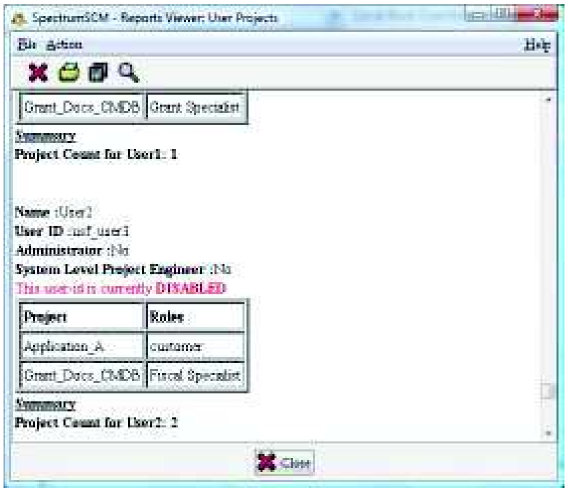
Location: US

E-Mail: usf_user3@mycompany.com

Project Engineer: □

Administrator: □

DISABLED



Grant_Docs_CMDB	Grant Specialist

Summary

Project Count for User1: 1

Name :User2

User ID :usf_user3

Administrator :No

System Level Project Engineer :No

This user-id is currently DISABLED

Project	**Roles**
Application_A	customer
Grant_Docs_CMDB	Fiscal Specialist

Summary

Project Count for User2: 2

12.7 Email Setup and Setting up email authentification

SpectrumSCM supports full e-mail notifications of Change Request creation and transitions. In fact by setting this up, **automatic email notifications happen** in real time for CR/Task creations, assignments, re-assignments, progressions, workflow transitions etc. You do not have to manually send an email when you create/assign/progress an incident or CR.

These emails are send to the person whom it is assigned and to all stake holders (based on the roles/workflow rules) instantaneously in real time. In addition the Task/CR shows up on the individuals CR list on the main SpectrumSCM screen when they log in as well.

The email notification feature can be configured at install time (you would have seen that screen during installation) or also at any time after installation as well.

STEPS:

So to set this up, stop your SpectrumSCM Server application. **(if it is up).**

The configuration information is available through the **Server Configuration Wizard.**

Since you have already installed the product, you can bring this screen up by going to **Start Programs->Server Configuration Wizard.**

Select the SCM_VAR entry that you see on the screen and hit the **<Edit>** button. This will bring up the **scm.properties** file.

This file holds all of the system configuration parameters

For using the email notification, in the scm.properties file under the MAIL section, uncomment the mail.smtphost line and set the **mail.smtp.host** parameter to your mailhost name or the appropriate smtp server name.

For using the **email authentification**,below the header which says "Authentication" uncomment the following as shown below. I have shown an example from one of my scm.properties file. You replace the appropriate values in the ones shown in red with your mail configuration details. Contact your Mail administrator to get these details.

```
#
# | Mail Mail Mail Mail Mail Mail Mail
# V
#
# Set this next line to the SMTP mail host for your
# organization. ex: smtp.mycompany.com
#
# mail.smtp.host mailhost
mail.smtp.host     smtpauth.earthlink.net
#
```

```
# Authentication ----------------------------------------
# If your smtp host requires authentication then
# you'll want to enable the following attributes:
#
mail.smtp.auth true
scm.smtp.auth.login johndoe@mindspring.com
#
# The SpectrumSCM server will use the login and password associated
# with the supplied login as the SMTP server login and password combo.
#
# Authentication ----------------------------------------
#
# The SCM mail "from" address. This is the address that all the
# mail will appear to have come from. Make sure to use a valid
# e-mail address here.
#
scm.from  johndoe@mycompany.com
```

****

After you make these entries in the properties file, restart the server.

Then you need to do one more step. You need to create a user_id and password in SpectrumSCM as well. So in the above example, the created user id is johndoe@mindspring.com and it had the password in the SpectrumSCM database its corresponding mail password. Ask your Mail administrator for the appropriate id and password.

Please refer to **Sec 3.4 of Chapter 3 SpectrumSCM Server and UI Configuration** in the User Guide (available at www.spectrumscm.com) for more details on the **scm.properties** file entries.

12.8 Backing up the SpectrumSCM data

Regular backups are recommended. The SpectrumSCM data (all the information about users, projects, everything else) is stored on the server in the directory specified at installation time, for example, **<SSCM_INSTALL_DIR>\SCM_VAR**. In addition, any project databases created in other directories would also need to be backed up.

Archiving these files regularly using any third-party backup mechanism is appropriate. If you do not remember where these directories are, you can pull up the *create project* menu item and select the project database directory's combo box, this will display all the directories that you are currently using.

It is recommended that the SCM server be properly shutdown and halted before the backup to guarantee that the data is stable. However, in general, running the backup at a quiet time (overnight) is perfectly adequate and does not require a server shutdown.

12.9 Setting Quick-start Tutorial under local environment

Included with the SpectrumSCM product is a quick-start tutorial. This is available via the SpectrumSCM Main Screen **HELP** menu option. As supplied, this will connect to the SpectrumSCM web site to get the most up-to-date information. If for some reason you prefer to have the tutorial information installed locally, it is provided on the installation CD, in the **tutorial** sub-directory. The tutorial is in HTML format for easy viewing with any standard browser.
Uncomment this line in the scm.properties file to allow Internet access to the tutorial.

scm.tutorial http://www.spectrumscm.com/Tutorial/scmstart.htm

To set up for a locally installed tutorial, replace the default entry for scm.tutorial in the scm.properties file. Use the Server Configuration Wizard or directly edit the scm.properties file and comment out the internet access and uncomment the local access, entering the path as described:

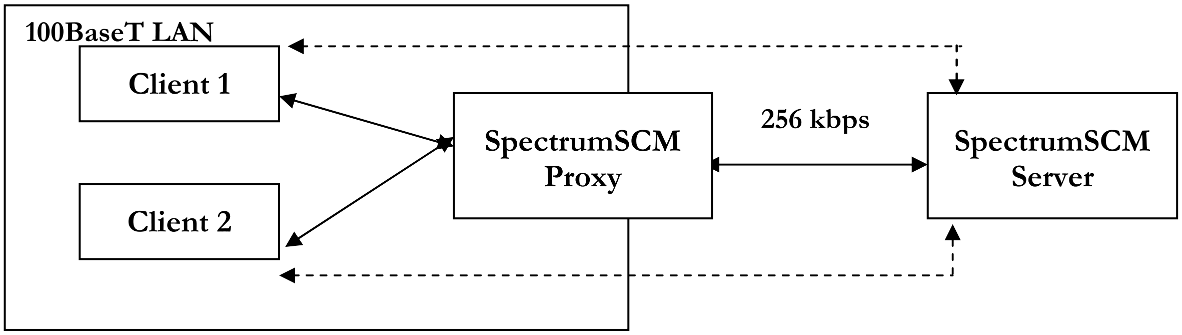
```
# The SCM Tutorial is accessed across the web by default.
# If access to the public network is not available, the
# tutorial path can be redirected to a local resource
# like in the following example for Windows:
#
# scm.tutorial  file:/C:/SCM_INSTALL_DIR/help/Tutorial/scmstart.htm
#
# or like this for Unix platforms:
#
# scm.tutorial  file:/SCM_INSTALL_DIR/help/Tutorial/scmstart.htm
#
# You do not have to use reverse slashes on the Windows platform.
# The tutorial materials are available on the SpectrumSCM installation
CD_ROM.
# Copy the entire Tutorial directory off of the CD_ROM to some location
# on a local or shared network drive, like in the examples above.
#
```

(See Chapter 3,SpectrumSCM Server and UI Configuration for more information on editing the scm.properties file.)

12.10 SpectrumSCM Proxy

The SpectrumSCM Proxy provides enhanced performance for distributed development teams in bandwidth constrained network topologies. The proxy acts as a bridge between the SpectrumSCM client and server and builds a local cache for frequently checked out revisions of e-Assets that are under source control. Files checked out by a client are used to serve similar requests from other clients, thus improving overall response time for check-outs and extracts. The proxy not only provides a better user experience for remote teams but also reduces the network traffic across the WAN and the load on the remote SpectrumSCM server. Load sharing can be achieved by using multiple proxies for different projects in SpectrumSCM. As opposed to multi-repository solutions for distributed development, the proxy uses a single repository model and thus removes the administrative overhead involved with maintenance and synchronization of multiple repositories. Also, the single repository architecture provides for a more reliable mechanism for version control activities while allowing the user to take full advantage of the integrated change management, process management and other advanced features in SpectrumSCM. The proxy updates its cache transparently as and when users check-out and check-in files and thus does not depend on the server to "push" updated information into its cache.

If the SpectrumSCM server is in a remote location and the available bandwidth between the local and remote ends is small, SpectrumSCM (like any other system) exhibits considerable lag for operations that require a file to be transferred across the wire. The proxy tries to address this issue by maintaining a "Local Cache" which reduces the number of file transfer operations across the WAN. Here is an example scenario:



Assume that the Clients C1 and C2 are on a 100BaseT LAN and the SpectrumSCM server is in a remote location, accessible through a 256 kbps WAN pipe (W). In the absence of the Proxy, the clients directly interact with the server and all file transfer operations happen over W. This can be slow and inefficient considering the fact that the bandwidth is small. In such situations, whenever the client C1 downloads a file from the server, other clients who need the same file can make use of the file downloaded by C1. Assuming that the file contents have not changed, the clients can bypass the server and get the file from within the LAN, which makes the operation extremely fast. Retrieving the file from within the LAN also reduces the network traffic across the WAN and the load on the remote SpectrumSCM server. Thus files downloaded from the server can be used to serve similar requests from different clients, provided that the file contents have not changed. This is the function of the SpectrumSCM Proxy.

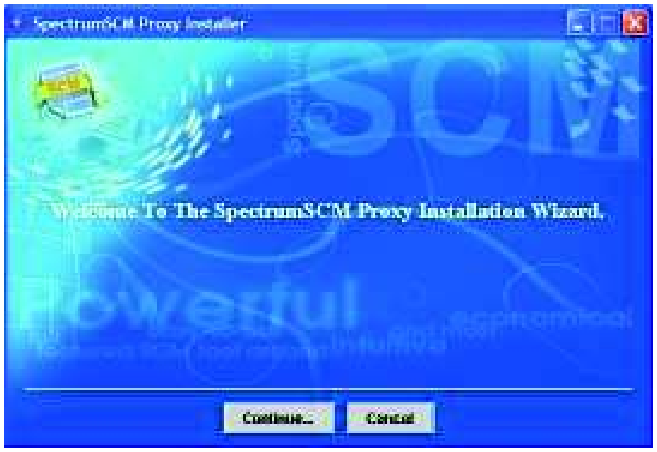
In a proxy based configuration, whenever a client needs a file from the server, it routes the request through the SpectrumSCM Proxy. The proxy checks its cache to see if it has the file that is being requested. If it determines that the file being requested and the cached copy are the same, it serves the request without downloading the file from the server. Thus the file is retrieved locally. If it is a miss, it downloads the file from the server, passes it on to the client and caches it for future use. Over a period of time, the number of hits will surpass the number of misses making checkout operations considerably faster. The SpectrumSCM Proxy also receives checkin triggers from the clients and updates its cache when users check-in files. The proxy not only caches the head revision, but also stores previous versions of a file and thus provides fast response times during release extracts and extraction of files by version/CRs.

Installation

You need to install the SpectrumSCM client or server before you can install the proxy. Instructions for installing the server/client are available on our website at **www.spectrumscm.com.** To install the SpectrumSCM Proxy, download the **ProxyInstaller.jar** file to a machine with a SpectrumSCM client/server installation. On Windows systems, you can double-click the jar file to launch the installation wizard. On UNIX systems, open a terminal window and run :

java -jar ProxyInstaller.jar

Follow the on-screen instructions to complete the installation. The proxy scripts and libraries will be installed under the SpectrumSCM install directory



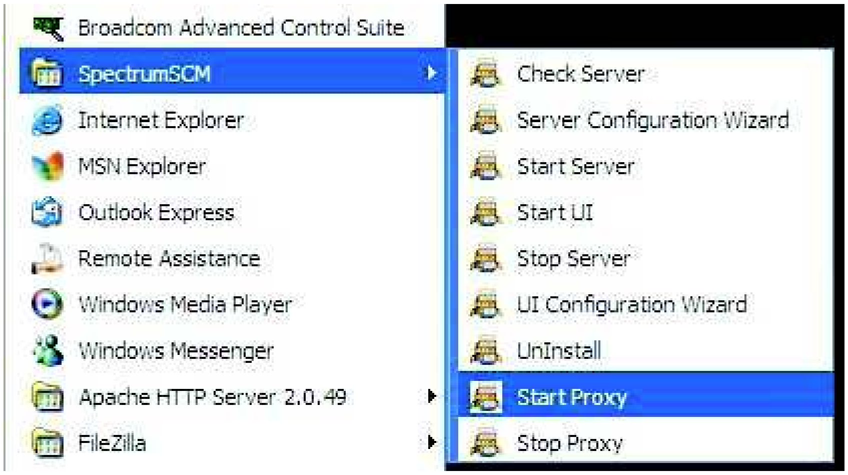
Welcome To The SpectrumSCM Proxy Installation Wizard.

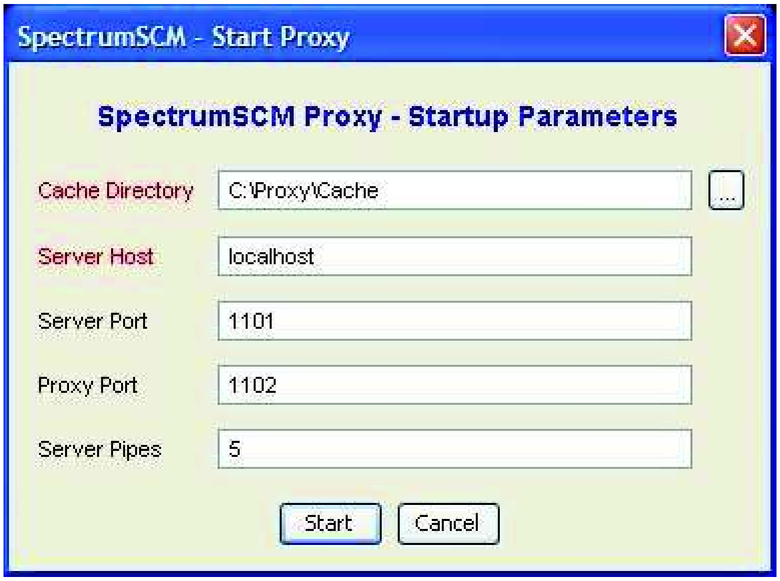
Starting the SpectrumSCM Proxy

The SpectrumSCM Proxy can be started using the GUI or command line modes. Users can specify the directory to use for the proxy cache. The proxy log files are maintained under <specified cache dir>/logs directory

Windows

Go to the SpectrumSCM menu under the Windows Start menu and choose the Start Proxy menu item or open a command prompt window and go to the <SpectrumSCM Install>/bin directory. Use the startProxy.bat script.





SpectrumSCM - Start Proxy

SpectrumSCM Proxy - Startup Parameters

Cache Directory: C:\Proxy\Cache

Server Host: localhost

Server Port: 1101

Proxy Port: 1102

Server Pipes: 5

Unix/Linux/Solaris

Open a terminal window and go to the <SpectrumSCM Install>/bin directory and execute the startProxy script

The Proxy startup program uses the following arguments:

-cache	Cache Directory for the Proxy	REQUIRED PARAMETER
-port	Listen Port for the Proxy	Defaults to 1102
-serverhost	SpectrumSCM Server IP	Defaults to localhost
-serverport	SpectrumSCM Server Transport Port	Defaults to 1101
-serverpipes	Max no. of connections b/w proxy & server	Defaults to 5
-gui	Start in GUI mode (overrides other options)	

Stopping the SpectrumSCM Proxy

Windows

Go to the SpectrumSCM menu under the Start menu and choose the Start Proxy menu item or open a command prompt window and go to the <SpectrumSCM Install>/bin directory. Use the stopProxy.bat script

Unix/Linux/Solaris

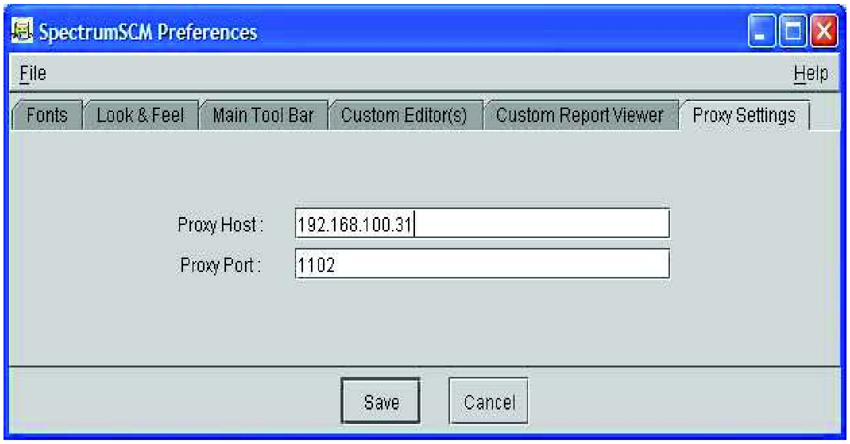
Open a terminal window and go to the <SpectrumSCM Install>/bin directory and execute the stopProxy script

The proxy shutdown program uses the following arguments:

-host	Proxy IP Address	Defaults to localhost
-port	Listen Port for the Proxy	Defaults to 1102
-gui	Start in GUI mode (overrides other options)	

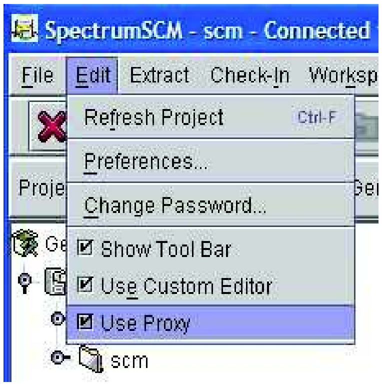
How to Use the SpectrumSCM Proxy

Start the SpectrumSCM client and choose the Edit-->Preferences menu item. Choose the Proxy Settings panel and specify the Proxy IP and Port Number. Save your settings and check the "Use Proxy" option under the Edit menu to route checkout requests through the proxy. Uncheck the option to communicate directly with the SpectrumSCM server.



Proxy Host : 192.168.100.31

Proxy Port : 1102


SpectrumSCM - scm - Connected
File
Edit
Extract
Check-In
Worksp
Refresh Project Ctrl-F
Preferences...
Change Password...
☑ Show Tool Bar
☑ Use Custom Editor
☑ Use Proxy
scm