Using WANdisco Subversion MultiSite

Revision History

REVISION	DATE
1.0	December 2008
2.0	February 2009
3.0	July 2009
4.0	September 2009

Contents

Contents, cont'd

1 Using the Admin Console

The Admin Console is a simple interface that allows you to monitor and perform administrative tasks for Subversion MultiSite.

You can run the Admin Console from any node. The login is `admin`. Passwords are the same for all nodes, and are user-defined during installation.

To access the Admin console, all you need is the IP address of any node and the WANdisco port number.

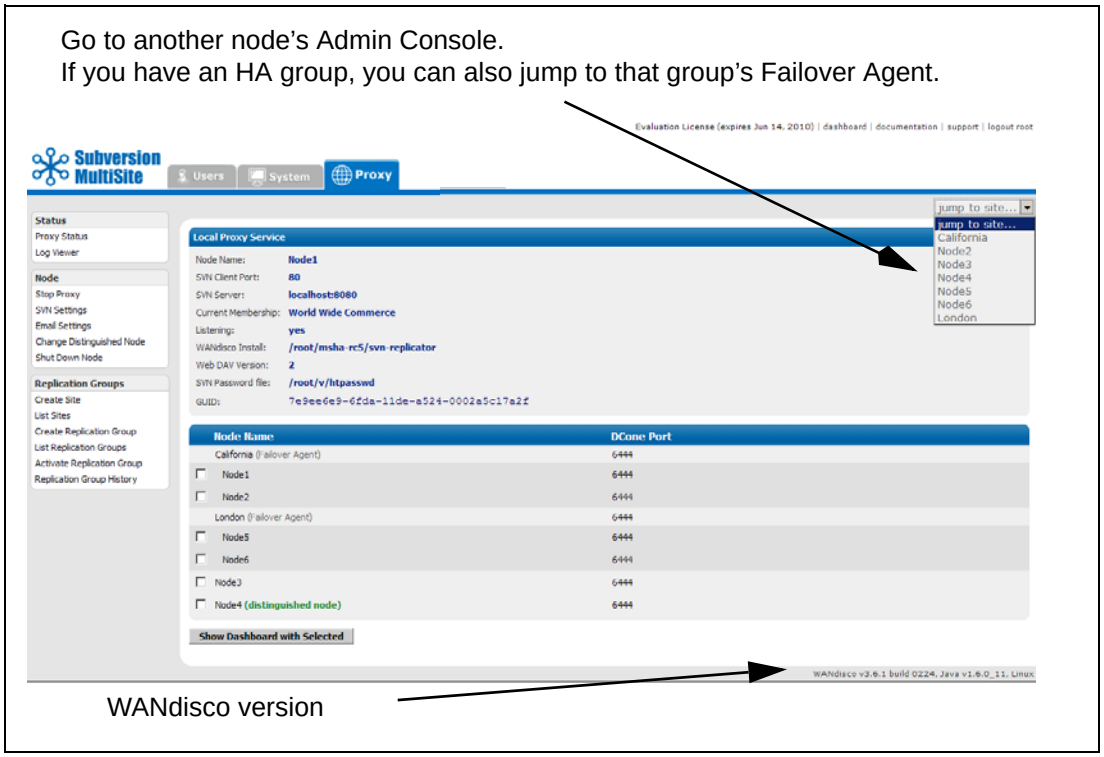
1.1 Starting the Admin Console

To start the Admin Console, in a browser's address bar, type

http://<IP address>:<replication port number>

The Admin Console's Home page appears.

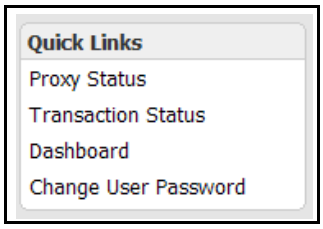
MultiSite's Admin Console has three or four tabs, depending on your WANdisco product. For Subversion MultiSite and High Availability, the tabs are Users, System and Proxy. The Access Control option has four tabs: Security, System, Proxy, and Reports.



1.1.1 Logging In

1.1.1.1 Quick Links

There are a few status commands available to a user who has not logged in: Proxy Status, Transaction Status, Dashboard, and Change User Password (see Having Subversion Users Change Their Passwords).



1.1.1.2 The admin Login

WANdisco's default login is `admin`, and the password is user-defined during installation. To change the login, see Changing WANdisco's admin Login. To change the password, see Changing the WANdisco Password. To recover a lost password, see Resetting or Recovering the Admin Console Password.

1.2 The Security Tab — for Access Control

This tab appears with:

- MultiSite and Access Control

NOTE:

> Password fields appear for users only if you chose to have WANdisco control the Subversion password file during installation. For DAV, WANdisco does not handle the user authentication.

Role Administration

Create Role	Create new roles and assign them privileges. Subversion permissions are: list, read, prewrite, write, delete, copy, admin. For a complete discussion of roles and permissions, see Managing Roles and Permissions.
List Roles	Display all roles: default and any you create. Privileges are also displayed. To delete a role, check any role's checkbox and click **Delete Selected**.

User Administration

Create User	Create any Subversion user.
Username	Enter in the Subversion user's username.
Password	Enter the user's password.
Confirm Password	Confirm the password.
First	Enter the user's first name.
Last	Enter the user's last name.
Email	Enter the users email address.
Default Role	
List Users	This command displays all users.
Import Users	You can import an existing list of users. The import file must be a comma delimited text file, of the format `userid,lastname,firstname,email`.
Change Admin Password	You can change the WANdisco Admin password *for this node only* with this command. See Changing the WANdisco Password in Procedures and Troubleshooting.

Group Administration

Create Group	
Name	Required field. You must name the group.
Description	Enter in a description for the group.
Client IP Pattern to Allow	Optional. You can allow certain IP patterns. Use regular expressions. If you do use this option, no other client IPs are allowed without specific ACLs.
Rule	
File / Dir Pattern	Browse to the file or directory pattern for this group, and specify either Allow or Deny. Use regular expressions.
add allow	identify any files and directories that this group has access to
add deny	identify any files and directories that this group does not have access to
Group Assignment	Assign the group as a sub-group, if desired.
Create Group	Select this command once you have defined a group.
List Group	This command shows all the groups. You can list all users in each group.
Assign Users	This command allows you to assign users to groups. If a user is already in a group, his or her name does not appear in the list of available users.
Remove Users	Use this command to remove users from a group.
Import Groups	You can import a list of existing groups. The import file must be a comma delimited text file, of the format `groupname,parent-name[,description]`. If there is no parent name, specify `null`.

ACL Administration

This menu item can be toggled off. See Toggling the ACL Display.

For a complete discussion on ACLs, see About Access Control Lists.

Create ACL	Create an ACL with this command. Create more than one at a time, use List ACLs.
User / Group	Specify the user or group for this ACL.
Rule	Specify `allow` or `deny`.
Privilege	Identify a privilege for this ACL.
Operate On	Specify if this ACL operates on a single user or the group.
IP Pattern	Optional. You can identify an IP pattern for this ACL. If you do identify an IP pattern, all other IPs are excluded, unless you create an allow ACL for a specific IP address.
File / Dir Pattern	Identify the file or directory pattern for this ACL.
Create ACL	Select this command to create the ACL.
List ACLs	This command lists all existing ACLs. You can create, edit or delete ACLs with this command. Use this command when creating multiple ACLs.

1.3 The Users Tab

This tab appears with:

- MultiSite
- MultiSite and High Availability
- High Availabilty

User Administration

Create User	Create any Subversion user.
Username	Enter in the Subversion user's username.
Password	Enter the user's password.
Confirm Password	Confirm the password.
First	Enter the user's first name.
Last	Enter the user's last name.
Email	Enter the users email address.
Default Role	
List Users	This command displays all users.
Import Users	You can import an existing list of users. The import file must be a comma delimited text file, of the format `userid,lastname,firstname,email`.
Change Admin Password	You can change the WANdisco Admin password *for this node only* with this command. See Changing the WANdisco Password in *Procedures and Troubleshooting*.

1.4 The System Tab

This tab appears with:

- MultiSite
- MultiSite and High Availability
- MultiSite and Access Control
- High Availabilty

The System tab offers several commands and utilities for MultiSite.

1.4.1 Left Side Menu

System

Log Viewer	
SVNProxyServer-prefs.log	This node's main log file.
web proxy.log	A log from the installation.
Show Log	Click this to display a log in the Dashboard.
Transaction Status	You can search for a specific transaction.
Transaction Number	Enter in the transaction number.
Site Submitted From	Select the node where the transaction originated.
Show Status	Click this after entering the data in the above fields.
System Config	For Access Control.
Show ACLs?	Default is **Yes**. Check **Yes** or **No** to show ACLs. **Yes** causes the ACL Administration menu to display on the Security tab.
Display Sibling Groups?	Check **Yes** or **No** to display sibling groups. **No** is recommended.
Log Level	WANdisco uses one log, and the default level is **info**. The levels vary from **severe**, where you get only the most severe warnings, to **finest**, which logs every action.
Free Memory	This command frees the memory (GC stands for garbage collection) for the current node. The command occurs when you click on this menu selection. The display shows information on the command that was just performed.
max mem used by JVM	the maximum memory that JVM can use on the current node
free memory before GC	the amount of free memory before you ran this command
free memory after GC	the amount of free memory after you ran this command
memory freed	the total amount of memory freed at the command's completion
Dashboard	offers another way to get to the Dashboard. The Dashboard is discussed in detail in The Dashboard.
Backup	
Export Settings	This command allows you to export WANdisco settings, including all users, for later importation into a WANdisco product.
Import Settings	This command allows you to import WANdisco settings, including all users.

1.5 The Proxy Tab

This tab appears with:

- MultiSite
- MultiSite and High Availability
- MultiSite and Access Control
- High Availabilty

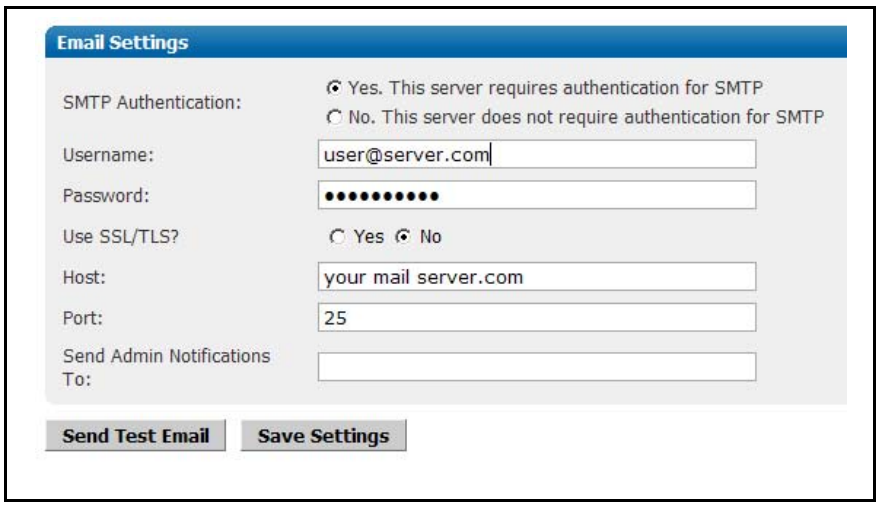
The Proxy tab by default lists the Proxy Status for this node.

1.5.1 Left Side Menu

Node

Proxy Status	This command displays the node's status in the tab's main area.
Node Name	Identifies this node.
Current Replication Group	Identifies the active replication group.
Replicated SVN Client Port	Identifies which port Subversion clients connect to WANdisco.
Listening	Identifies whether WANdisco is listening to clients on the SVN client port. For a complete explanation, see WANdisco is Listening in About Subversion MultiSite.
WANdisco Install	Displays where WANdisco is installed on this node.
GUID	Displays this node's Globally Unique Identifier.
Java Version	Displays this node's currently installed JAVA version.
Log Viewer	You can view the `SVNProxyServer-prefs.log` file in the Dashboard.

SVN Settings	The current values are displayed. You can edit them here.
Sharing the Server	Specify whether WANdisco and Subversion are on the same server.
Use Pre-Replication Hooks	The default is **No**. If you are using pre-replication hooks, specify **Yes**, and select the appropriate Subversion version. See Setting Up Hooks in *Procedures and Troubleshooting*.
Subversion Server Ver	If you use pre-replication hooks, specify which version of Subversion you have.
Suversion Server Port	The port WANdisco uses to communicate with Subversion.
SVN Executable	The fully qualified path to the svn executable. On many *nix machines you can run "which svn" to determine the path to the file. For example: `/usr/bin/svn`
	Replicate the location of the svn executable to all nodes
	Only set the location of the svn executable at this node
Save Settings	Save any changes.
Repository and DAV Location	This is the location DAV uses to browse the repository.
Edit	Edit the repository settings.
Check Consistency	Check repository consistency. See Checking Repository Consistency.
Schedule Consistency Check	You can schedule the check to run on a regular basis, hourly or daily.
Add Repository	Add another repository here. You are responsible for changing the Apache settings outside WANdisco. See Adding a Repository to a Replication Group.



Email Settings

Set the email settings for the watchdog contact. You have to set the email in watchdog also. See About Watchdog Mode in *Procedures and Troubleshooting*.

SMTP Authentication	Select whether you need SMTP Authorization.
Username	For authentication, enter a valid username.
Password	For authentication, enter a valid password.
Use SSL/TLS?	Does your email server use SSL/TLS?
Host	Enter the email host.
Port	Enter the email port number.
Send Admin Notifications to:	Enter in the email address of the person to send email to.
Save Settings	Save any changes.
Send Test Email	Save any changes, and run an email test. Selecting this displays the test page, where you can see the test results.

Change Distinguished Node

Change the distinguished node immediately. Verify with Proxy Status.

If you have a distinguished node rotation schedule in place, the distinguished node is changed immediately, but then the schedule rotates to the next node at the scheduled time of rotation.

For information on the distinguished node, see the Replication Example in *About Subversion MultiSite*.

Current Distinguished Node	This names the current distinguished node.
New Distinguished Node	Select another node from the replication group.
Assign Selected Node	Click this after selecting another distinguished node.

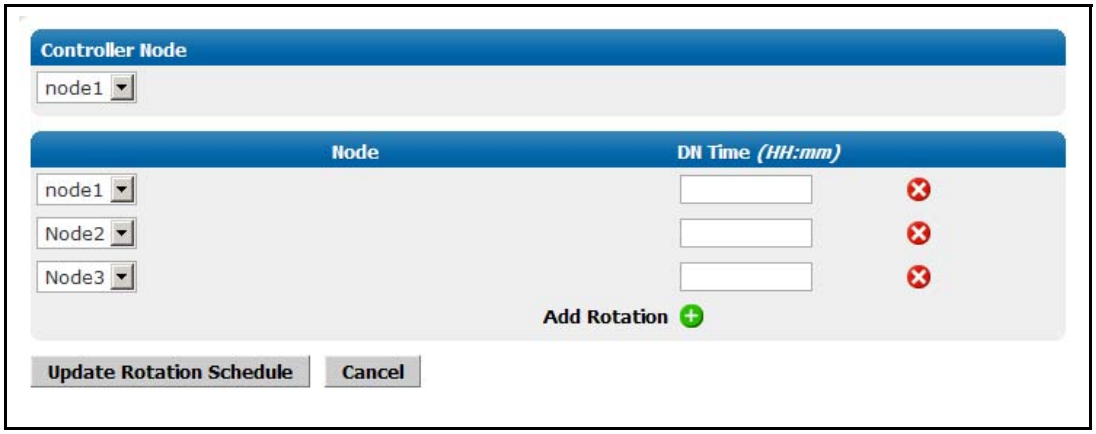
Distinguished Node Rotation

Specify a schedule to rotate the distinguished node. The schedule is based on the local time zone of one node — the **Controller Node**.

For at least one other node, select the time for that node to become the distinguished node, using the 24 hour clock syntax.

Save changes by clicking **Update Rotation Schedule**.

Note: If you use the **Change Distinguished Node** feature when you have a rotation schedule in place, the change occurs just until the next scheduled rotation.



Stop Proxy

Stop this proxy only

This stops WANdisco at this site. See Temporarily Disabling Subversion Access At Selected Sites.

If this node is part of an HA sub group, this option is not available. See Starting and Stopping HA Sub Group Nodes.

Synchronize Stop

Synchronized stop of all proxies
A synchronized stop stops WANdisco at all nodes, and replication is suspended. All nodes must be available for this to work. See Performing a Synchronized Stop in *Procedures and Troubleshooting*.

If this node is part of an HA sub group, this option is not available. See Starting and Stopping HA Sub Group Nodes.

Shut Down Node

This command shuts down WANdisco at this node. To restart it, go to `svn-replicator/bin` and type `perl svnreplicator`.

Replication

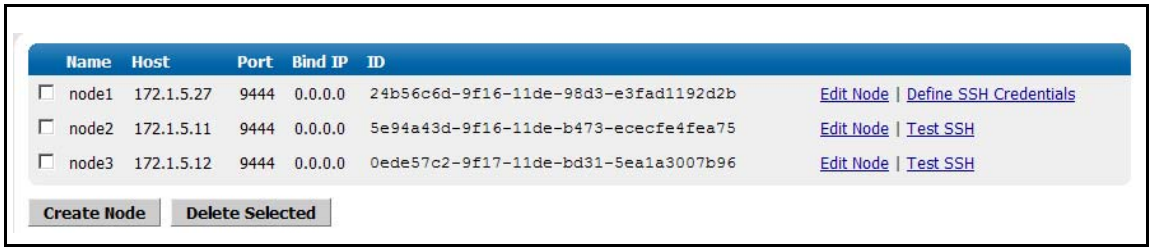
Nodes

Lists all the nodes you have defined in WANdisco. Any Failover Agents are noted. Note that nodes listed here may or may not be included in the current replication group. To see the current replciation group, go to **Proxy Status**.

Create Node

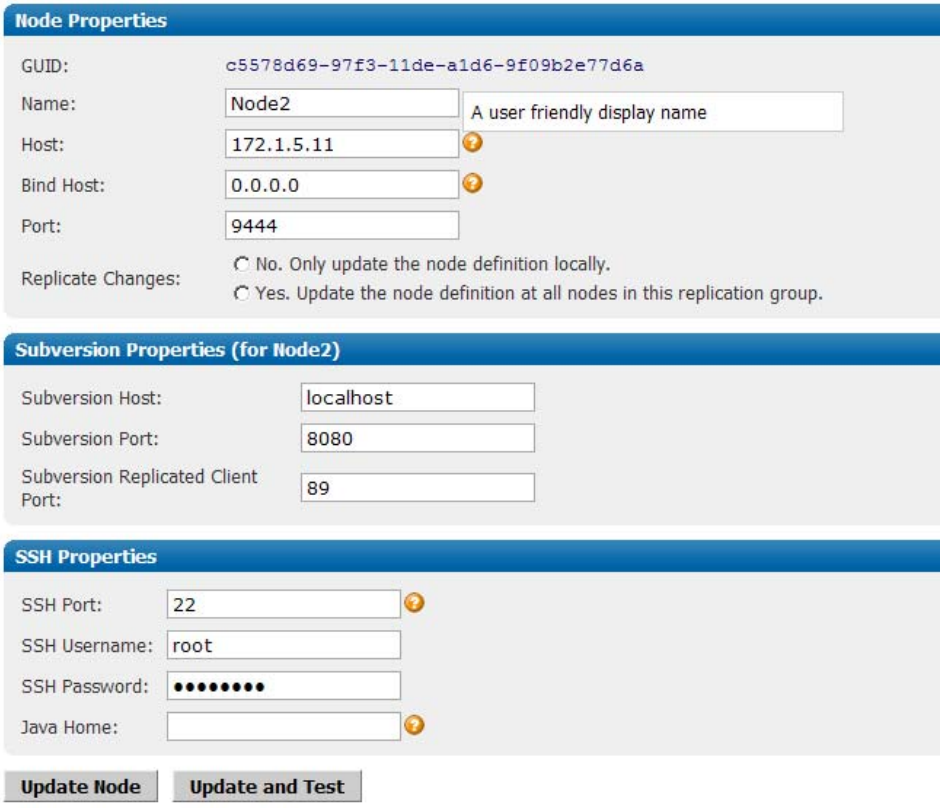
Create a node. Note that you need to notify WANdisco of any new IP address in order to receive an updated license key.

Delete Selected You cannot delete a node belonging to an active replication group. Check the node you want to delete, and click **Delete Selected**.



To edit a node's properties, click on the node's name.

Node Properties

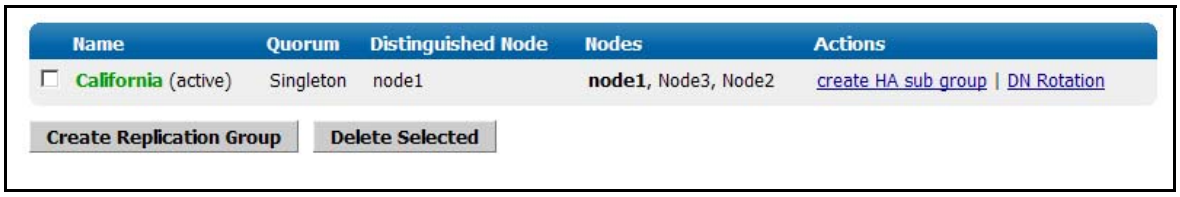


GUID	The WANdisco-assigned GUID is listed.
Name	The node's name is listed.
Host	The node's host is listed.
Bind Host	The node's bind host is listed.
Port	WANdisco's communication port is listed.

Replicate Changes	Select either **Yes** or **No** to replicate the change to the node's replication group.
Subversion Host	The Subversion host is listed.
Subversion Client Port	The node's Subversion client port is listed.
SSH Port	The node's SSH port is listed.
SSH Username	The SSH username is listed.
SSH Password	The SSH password is obscured.
Java Home	Usually, no path is present.
Update Node	Click this to save any changes.
Update and Test	Click this to test the SSH functionality and the check for Java Home for this node.
Replication Groups	All defined replication groups are listed. The currently active replication group is noted with *(active)*.

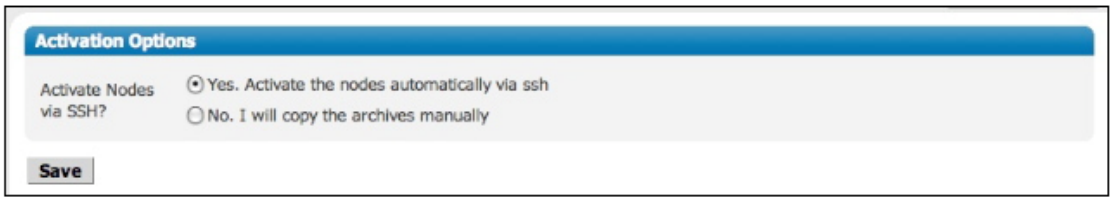
NOTE:

Only one replication group can be active at a time.

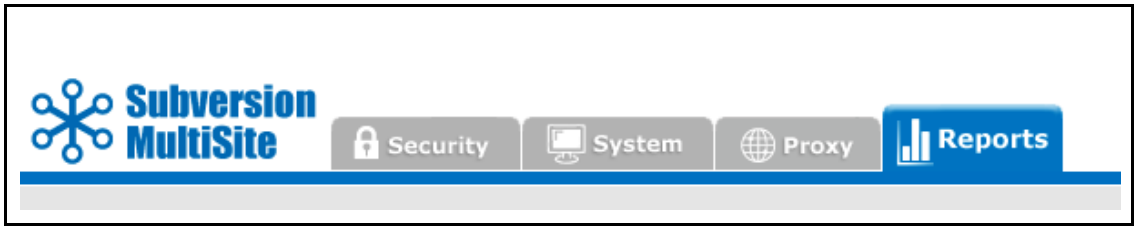


Create Replication Group	Create any new replication groups. See Creating a New Replication Group.
Delete Selected	Delete any non-active replication groups.
create HA sub group	For High Availability only. Create any HA sub groups. For information on setting up HA sub groups, refer to step 52 in Installation.
activate	Activate a replication group. For more information, see Activate the Replication Group in Installation.
Replication Group History	A table presents the current and any past active replication group activity.

Activation Options	Specify the desired option. Your selection here applies to all activations of any replication groups, until you change it.

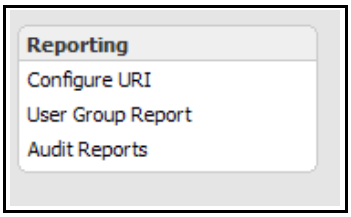


1.6 The Reports Tab — for Access Control



This tab appears with:

- MultiSite and Access Control



Reporting

Configure URI	Refer to About Audit Reports.
User Group Report	Generate these reports, and view them with Log Viewer in the System and Proxy tabs.
Audit Reports	Refer to Chapter About Audit Reports.

1.7 Failover Agent Tabs

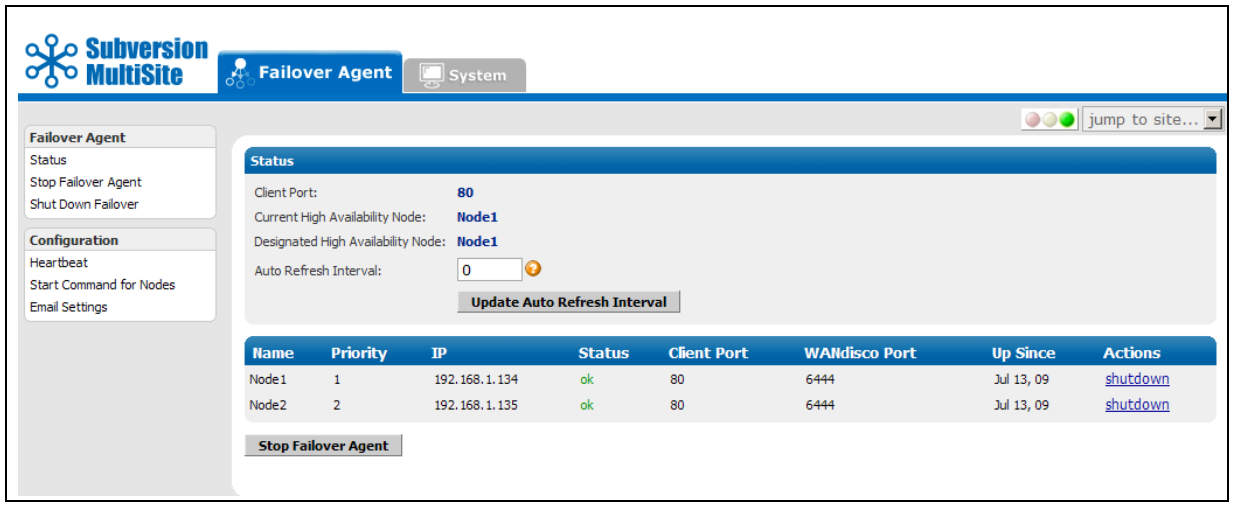
The Failover Agent's Admin Console has two tabs: The Failover Agent tab and the System tab. The Failover Agent tab displays only those nodes within its High Availability sub group.

1.7.1 Failover Agent Tab

The Failover Agent tab displays the status of other nodes in its HA sub group, gives information on the current active primary, and offers several commands in the left menu.

The status of the High Availability sub group displays in the upper right. One of three circles pulses, giving the current status: green signifies all nodes are up, yellow signifies at least one node is not responding, and red signifies that all nodes are not responding.

The Status section names the Current Active Primary (the node listening to the Subversion client through the Failover Agent) and the Designated Primary (priority level 1). These are the same node unless failover has occurred. The Auto Refresh Interval offers you the ability to automatically update the page. The default is 0.



1.7.1.1 Starting and Stopping HA Sub Group Nodes

This is where you start and stop the HA sub group nodes.

NOTE:

If you shut down the current node, you trigger a failover. Shutting down any other node in the HA sub group does not result in a failover.

A stand-alone High Availability sub group of three or more nodes has a majority response quorum. If you shut down a majority of nodes in your HA group, replication stops, and can only continue when a majority of the HA nodes are running.

Each node is listed by name, priority order, IP address, current status (**ok** and **not responding**), client port (in use only by the current active primary), replication port, date of last start up, and action (**shutdown** or **start**).

1.7.1.2 Left Side Menu

High Availability

Status	This command displays the HA sub group's status in the tab's main area.
Stop Failover Agent	This stops Subversion access to Subversion clients. You must confirm your action.
Shutdown Failover	This shuts down the Failover Agent. Restart the Failover Agent by typing `<product directory>/svn-failover/bin/failoveragent`.

Config

Heartbeat	For a complete discussion on the heartbeat, see Failover and the Heartbeat in *About Subversion MultiSite*.
Missing Heartbeat Count	The number of missing heartbeat responses the FA gets before marking a node as unavailable.
Interval	The time between queries from the FA to the nodes. You can specify a different number for each node.
Connection Timeout	The time to wait before assuming the query has failed. You can specify a different number for each node.
Save All	Save changes for all nodes.

Start Command	Enter in commands to start the sub group nodes.
SSH Command	Enter the absolute path for the SSH executable.

Start Command	Enter syntax to start the node. For Windows, in the Start Command field, enter
	`perl -x -S`
	`<pathname>\svn-replicator\bin\svnreplicator`
	
	For Unix, you can start the process in the background by appending the command. Enter the start command, then add:
	
	For csh/tcsh users:
	
	`</dev/null >&/dev/null &`
	
	For Bourne/Korn/BASH users:
	
	`</dev/null >/dev/null 2>&1 &`

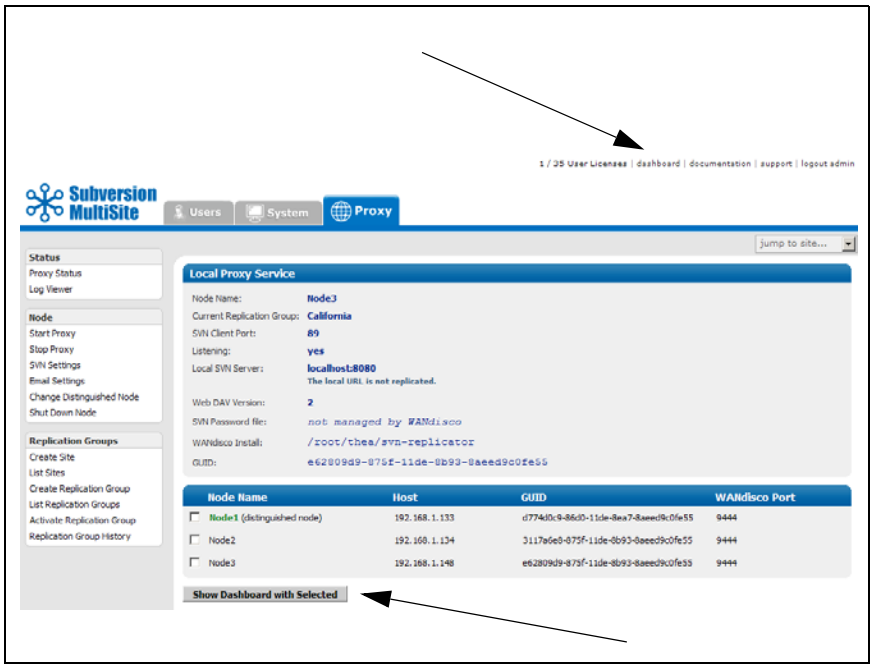
Save All	Save changes for all nodes.
Email Settings	The Failover Agent sends emails when: a) current active primary dies, and WANdisco receives a client request, triggering failover; b) priority 1 node comes back online; c) in a two node group, the second node dies, triggering backup exclusion protocol. See Email Settings on Proxy tab.
Primary	
Start Primary	This command only appears if the current acting primary is off. Start the current acting primary with this feature if you programmed the Start command on this tab. Otherwise, use the command line `<prod directory>/svn-replicator/bin/svnreplicator`

1.7.2 The System Tab

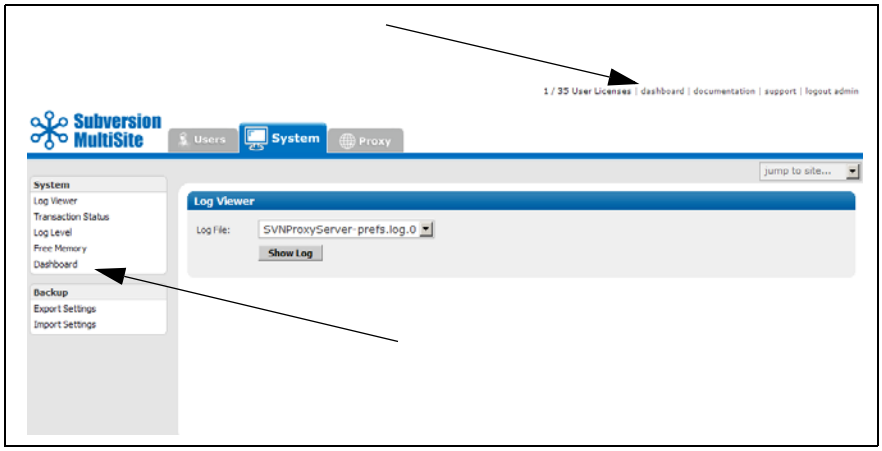
The commands on this tab are the same as on a node's System tab. See The Users Tab.

1.8 The Dashboard

There are two ways to get to the Dashboard from the Proxy tab.

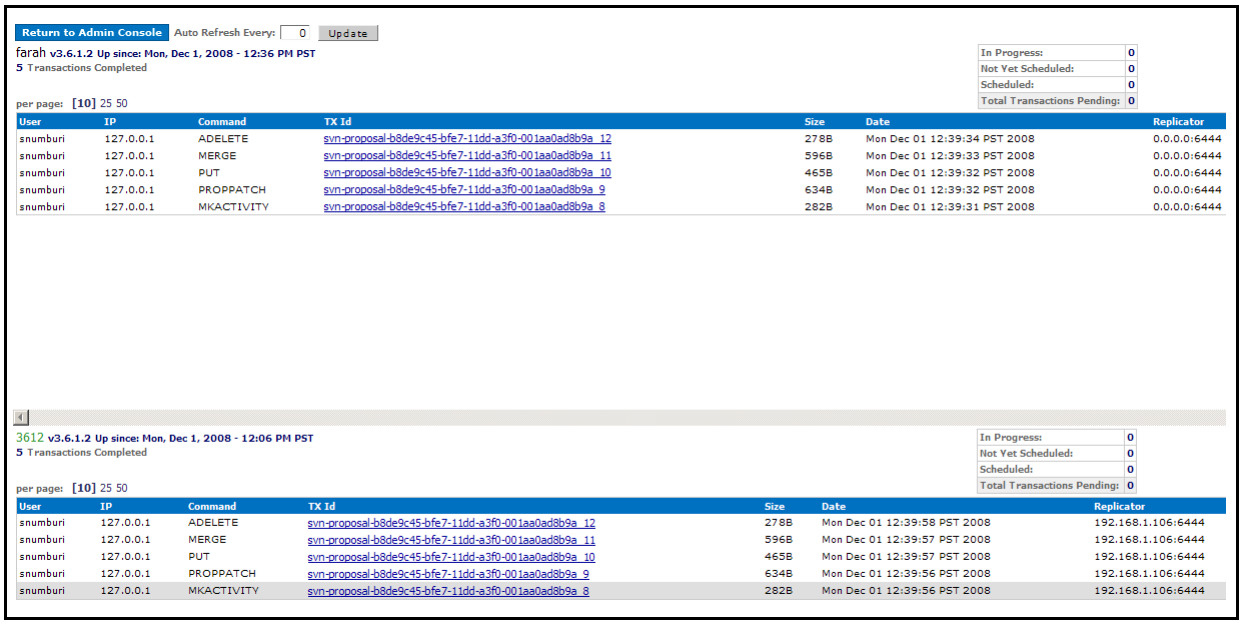


And there are two ways to get to the Dashboard from the System tab.



The Dashboard shows each node's transactions. As soon as MultiSite receives a Subversion transaction request, that transaction joins the replication group's queue. There is one queue for the replication group. Pending transactions are not displayed, but are counted in the **Total Transactions Pending** box in the upper right.

When MultiSite finishes processing a transaction, the transaction displays in the **TX Id** field. The **Replicator** field displays the node where the transaction originated. For example, 0.0.0.0:6444 means the local node originated the transaction, while another IP address identifies that node as the transaction's originator.



1.8.1 Pending Transactions

There are three statuses of replicated transactions before they are committed to Subversion.

- **Not Yet Scheduled** - these transactions are in the queue
- **Scheduled** - these transactions are approved by the quorum and are waiting to be executed
- **In Progress** - these transactions are in the process of being completed

The **Total Transactions Pending** lists the total number of transactions in all statuses.

1.8.2 Completed Transactions

Once a transaction is completed, the Dashboard lists it in the transaction list, and that transaction is no longer considered in the **In Progress** count. The completed transaction joins the count in the **Transaction Completed** display. This display keeps count of transactions since replication began.

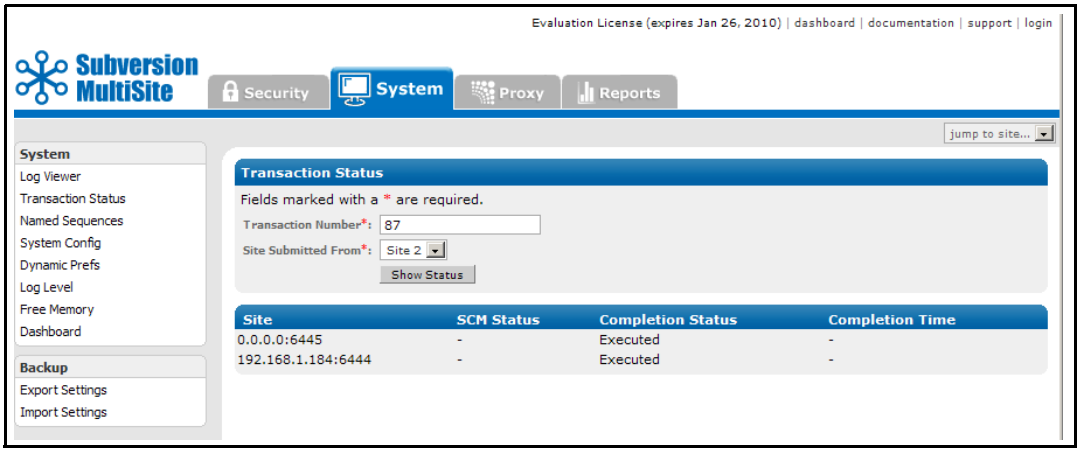
1.8.3 Refreshing the Dashboard Display

The Dashboard by default does not refresh. As MultiSite is completing many transactions, a display that refreshes often would be very confusing to read. While the order of completed transactions is the same at all nodes, the real time of when a transaction is posted may vary from node to node. To refresh the Dashboard, click **Update**. You can also set the Dashboard to refresh automatically by entering a number in seconds in the field.

1.8.4 Transaction Status

To see details on a transaction's status, click on the transaction in the **Tx Id** column.

That transaction appears in the Transaction Status page (on the System tab). You can see information about that transaction.



2 Managing Users

This chapter provides information on setting up users for MultiSite. You can create users, delete users, and search users by several criteria. You should be familiar with the Admin Console, described in Using the Admin Console.

If you have an existing LDAP or NIS database, you can integrate it with WANdisco. WANdisco offers a free, unsupported plug-in. See the *LDAP Plug-in* document at http://www.wandisco.com/php/products_documentation.php.

The document contains a download link for the plug-in.

2.1 Is WANdisco Controlling the Password File?

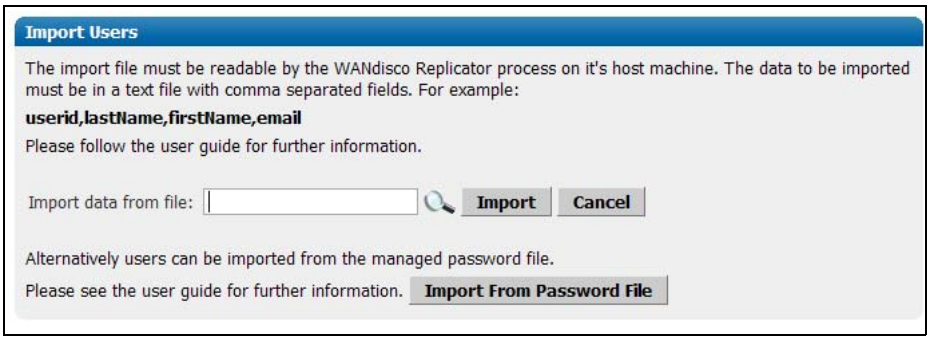
Upon WANdisco installation, if you selected to have WANdisco control the Subversion password file, any user you enter in WANdisco can use Subversion.

If WANdisco is not managing the Subversion password file, and a user is entered in WANdisco but has not been registered in Subversion, and he or she tries to access Subversion, they would see an `Access Denied` error message in their client.

You can check if WANdisco is managing the password file by going to the Proxy tab, clicking **SVN Settings**, and clicking Edit on the repository listed. If the Manage Password box is checked, WANdisco is managing the password file.

If you selected the wrong choice during installation, you can still have WANdisco manage the password file. Check the Manage Password file checkbox, browse to the password file, and click **Update**.

2.2 Creating or Importing Users



NOTE:

> For Access Control, all users must have a role. Use either a WANdisco supplied role, or create your own. See Managing Roles and Permissions in Managing Users.

If WANdisco is managing the password file, use the import tool, up to the license limit. If the user exists in the Subversion password file, and you also import that user into WANdisco, the entry is not overwritten. If the user is imported, but does not exist in the password file, the password is set to their email address.

If WANdisco is not managing the password file, WANdisco lazily creates any new user, up to the license limit, once Subversion authenticates them. You can also use the **Import Users** command.

For Multisite with AccessControl, you must specify a role for each user. Roles are discussed in About Roles and Groups for Access Control. Use a CSV file to import many users. The file has the format `userid,lastName,firstName,role,email[,group1[,group2...groupN]]`. If WANdisco is managing the password file, and the user exists in the password file, the entry is not overwritten. If WANdisco is managing the password file and the user does not exist in the password file, the user's password is set to his or her email address.

To add a new user, click on **Create User** in the Security tab. Specify a (Subversion) username.

Enter the password, and the user's names. The email address is optional.

2.3 Deleting Users

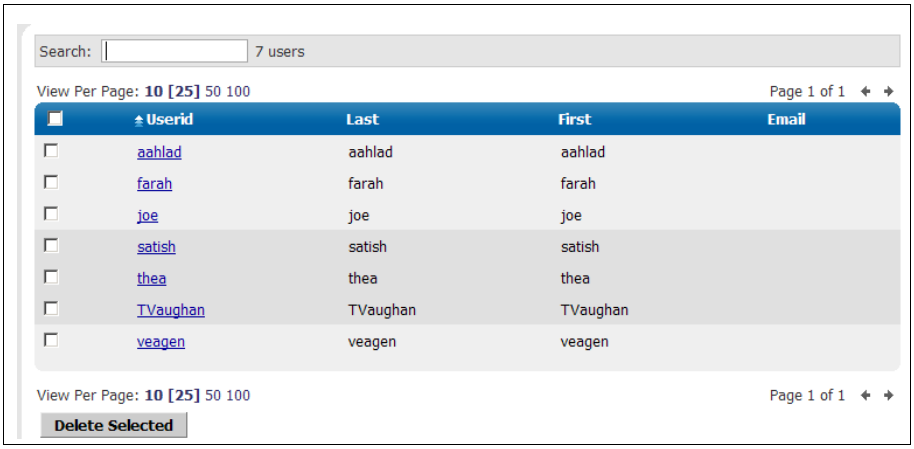
To remove users, click **List Users**. Select the users you want to delete with the checkbox on the left and click **Delete Selected**.

2.4 Listing and Searching for Users

To get a list of all the registered users, click on the **List Users** command. The User List page shows all users by default. The page size is set to show 25 users per page, but you can change that by selecting **View Per Page** on top of the user list. Arrows at the right corner allow you to scroll to the next or previous page.

Use the **Search** box to find users. Begin typing a user's first or last name, and an incremental search starts. Return to the full list by clearing the **Search** box.

All the columns in the user list are enabled for sorting. Clicking on the column header lets you sort in ascending or descending order. The sortable columns include: Userid, last name, first name, and email.



You can click on the user id hyper link to edit the user. You can also delete as many users as you like. Delete all users by checking the checkbox in the table header, and then click the **Delete Selected** button.

2.5 Importing Users

You can import an existing list of users with the **Import Users** command. The import file must be a comma delimited text file, of the format `userid,lastname,firstname,email`.

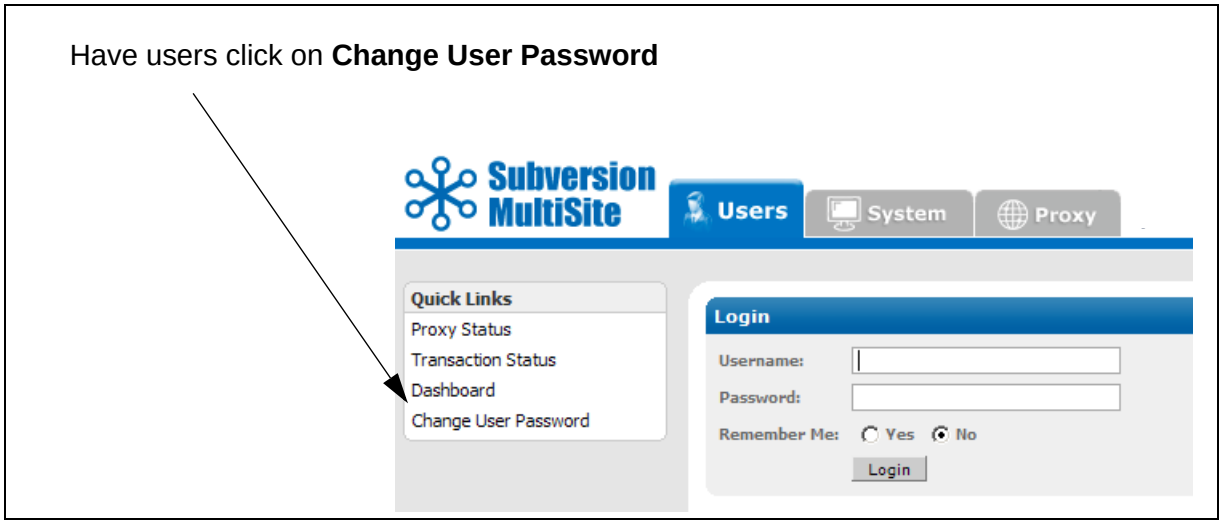
If WANdisco is controlling the Subversion password file, user passwords are changed to user email addresses upon importation. WANdisco recommends notifying users to change their Subversion password, as described in the next section.

2.5.1 Having Subversion Users Change Their Passwords

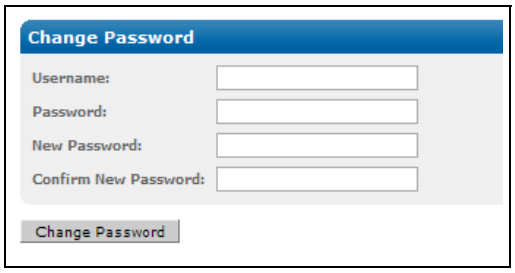
Use this only for users imported with the Import Users command. Importation changes users passwords to email addresses. Users can change Subversion passwords in WANdisco without logging in to WANdisco. Have the users go to:

```
http://localhost:6444/
```

The Admin Console appears. Have the users click on **Change User Password**.



The Change Password box appears. Users can enter their Subversion username, and their password (which is now their email address). Have them enter a new password and confirm it, then click **Change Password**. The users have successfully changed their passwords.



3 About Roles and Groups for Access Control

This chapter provides information on setting up users, roles and groups for Access Control. Most customers find that managing users' roles and groups offer enough access control. However, you can further refine Access Control with specific Access Control Lists, discussed in About Access Control Lists.

Please see also Access Control — Using the AuthZ Module in Recommended Deployment Practices.

Access Control initially does not allow any user access to any resource. By default, all users are denied. This is essential for security: it closes the window of vulnerability that would allow everyone full access between the time WANdisco is first installed and the time it takes an administrator to create access rules. In order to grant access, the administrator has to explicitly create roles, groups (which define resources) and users.

You should be familiar with the Admin Console, described in Using the Admin Console.

Resources assigned to subgroups are given to users who are members of parent groups because the users are automatically members of the subgroup. So, membership goes down the tree and inheritance, as a result, goes up.

3.1 Managing Roles and Permissions

Access Control's roles are based on Subversion permissions. The default roles are:

- list
- read
- prewrite
- write
- delete
- copy
- admin

The following table offers a mapping of actual Subversion commands to the minimum permission needed to execute them.

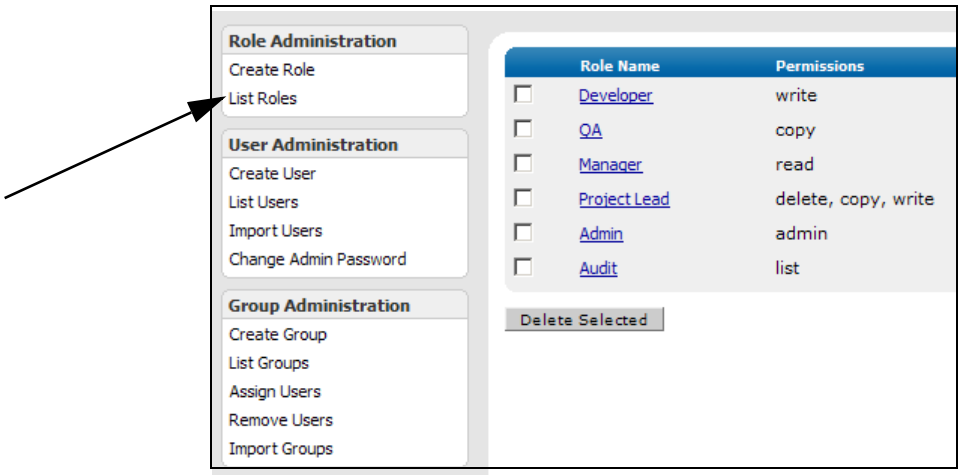
Subversion Command	Permission Required		Subversion Command	Permission Required
info	List		revert	Read
log	List		annotate	Read
ls	List		propget	Read
status	Read		proplist	Read
cat	Read		commit	Write
diff	Read		import	Write
checkout	Read		add	Write
cleanup	Read		lock	Write
update	Read		unlock	Write
revert	Read		copy	copy

Access Control comes with a few default roles with existing permissions. You can modify these roles as you wish. You can also create new roles. The permissions are inherited, meaning if a role has the write privilege, it also has the list and read permissions as well.

The roles work with groups, which you defined as files or directories. So the roles are applied within the groups (the defined files or directories).

Default Role	Privileges - Inherited Hierarchy
Audit	list
Manager	list, read
Developer	list, read, write
QA	list, read, copy
Project Lead	list, read, delete, copy, write
Admin	list, read, delete, copy, write

The **List Roles** command, under Role Administration, shows all roles: the default roles and any you have created. The permissions for the roles are also listed.



NOTE:

Admin serves as a permission, a role and a group. The Admin privilege has no constraints on it whatsoever. An admin has full permission to everything in the repository. It is designed to be used for a System Administrator.

If you assign a user the Admin role, or give a user Admin privileges, or put a user in the Admin group, that user has full access to everything in the repository. Do not make any ACLs for anyone with Admin role, privilege, or group. If you need to exclude a user from certain files, assign that user another role without any use of the Admin privilege, role or group.

3.1.1 Special Permissions

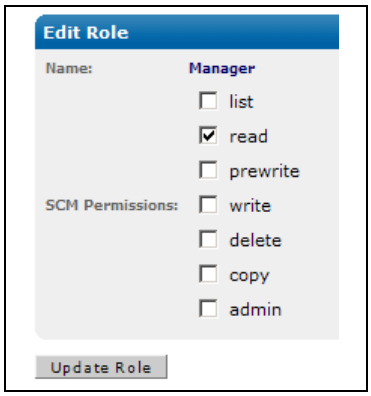
Special consideration should apply for list and read access rules. Unlike write operations, the read and list operations can traverse directory hierarchy. Therefore it makes sense to always allow/deny read and list privileges on all files under a directory. This can be done by specifying a wild-card pattern, for example: `allow read from /svnroot/trunk/module1|/svnroot/trunk/module1/.`

3.1.2 Creating New Roles

In the Security tab, select **Create Role**. Enter a name for the role and select the Subversion permissions you would like this role to have. Any user you assign to this role has the permissions you specify for this role.

3.1.3 Editing Existing Roles

Select **List Roles**: the defined roles display. Select the name of the role you wish to edit. The Edit Role page displays, listing all possible privileges. The role's existing privileges are checked.



Make any changes, and click **Update Role**. Any user assigned to that role, both for current and future assignments, has these same privileges.

3.1.4 Deleting Roles

Select **List Roles**. Use the checkboxes to mark the roles for deletion. Select **Delete Selected**. The role is deleted throughout Access Control, even if users are assigned to that role.

WARNING:

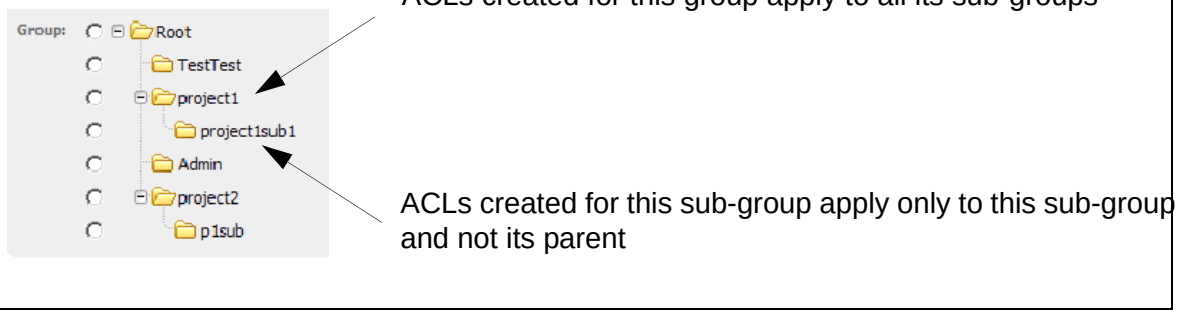
> Think carefully when deleting roles. If you delete a role, make sure no user is assigned to that role before you delete it.

3.2 Managing Groups

Creating groups allows you to manage projects, providing a convenient way of organizing many users into a related category for controlling access. You assign each group to a set of files, a directory hierarchy, or to individual directories, to either allow or deny access to specified files and directories.

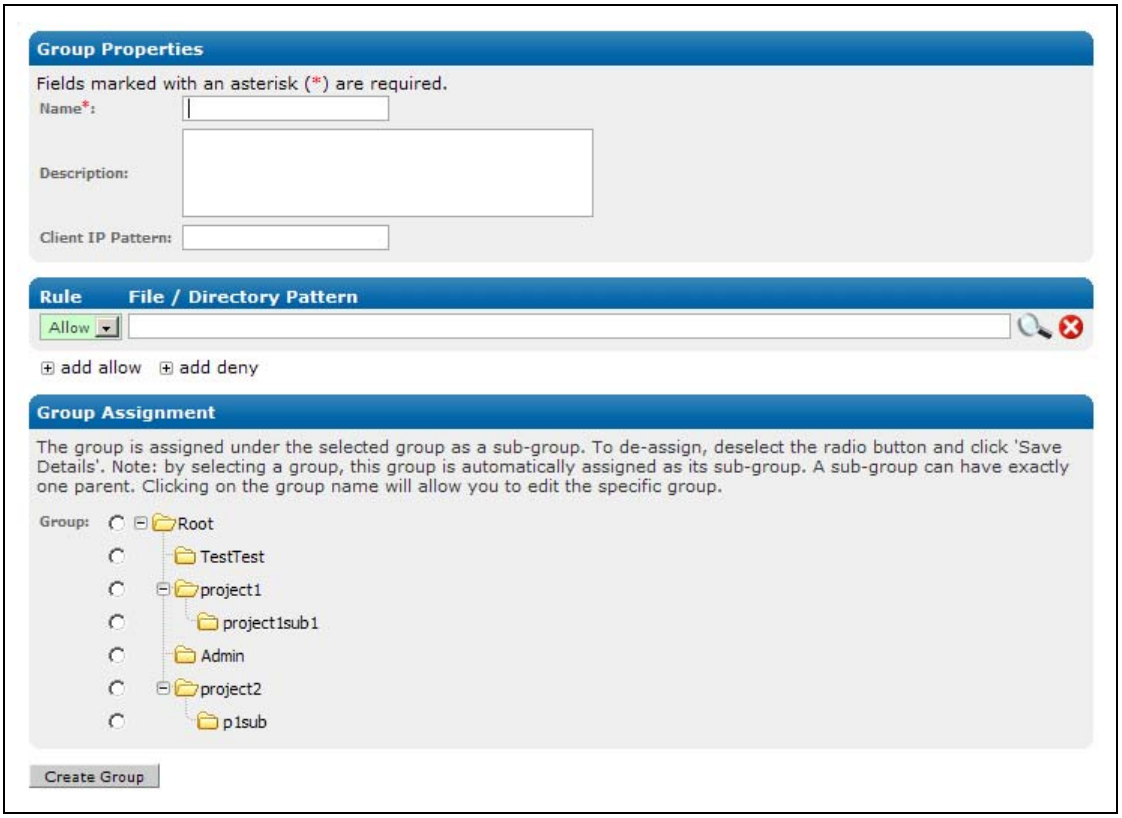
You can create and delete groups, associate files, directories and modules to a group, add to and remove users from a group, and perform bulk imports of existing groups. You can also restrict access to a group by client IP address.

Groups are hierarchical, with a parent-child association between a group and a sub-group.



3.2.1 Creating New Groups

To add a new group, select **Create Group**. The Group Properties page appears.

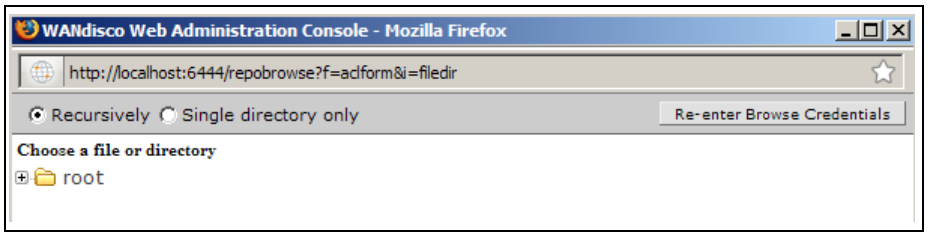


The name can contain any character, including white space, except the underscore character. The group name is the primary key into the group database, therefore it cannot be changed once it is created. Enter relevant text in the description field. Access Control automatically tracks the creation and modification time on the groups, which you can see in `groups-reports.txt` in **Log Viewer**.

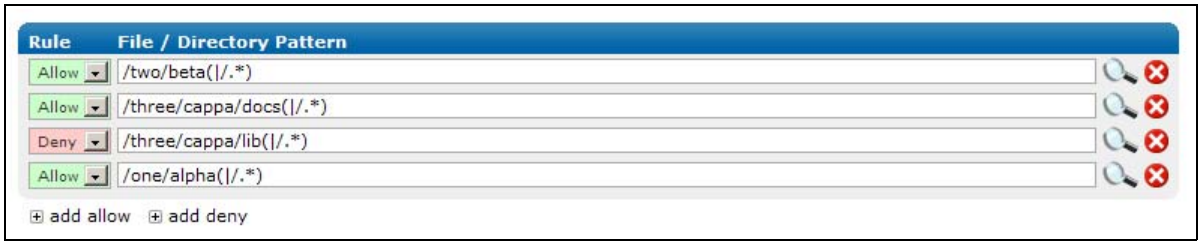
You can optionally create this group for a specific client IP pattern. If you do enter an IP pattern in the Client IP Pattern field, no other client IPs are allowed unless you create specific ACLs for those other client IP addresses. You must use regular expressions.

3.2.1.1 Defining Group Rules

The **Rule** section allows you to define the files and directories for this group. Select **add allow** or **add deny**, and browse to the file or directory. You can identify a file or directory, and use the radio buttons to check either Recursively or Single directory only.



Add as many entires as necessary for this group, ensuring that all allows and denies for all files and directories are accounted for.



3.2.2 Creating a Sub-Group

A group inherits all of the resources and privileges of its sub-groups.

Follow these steps to create a sub-group.

Step 1 Make the sub-group as you would a group.

Step 2 Go to **List Groups**.

Step 3 Click **Edit** for the sub-group. The Group Properties page appears.

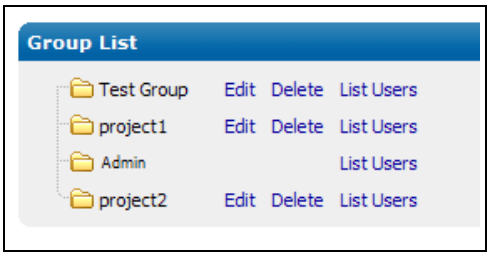
Step 4 In the **Group Assignment** section, check the radio button of the sub-group's parent.

Step 5 Click **Save Changes**.

Step 6 Go back to **List Groups** and verify the correct structure.

3.2.3 Deleting a Group

To delete a group, click **List Groups**.



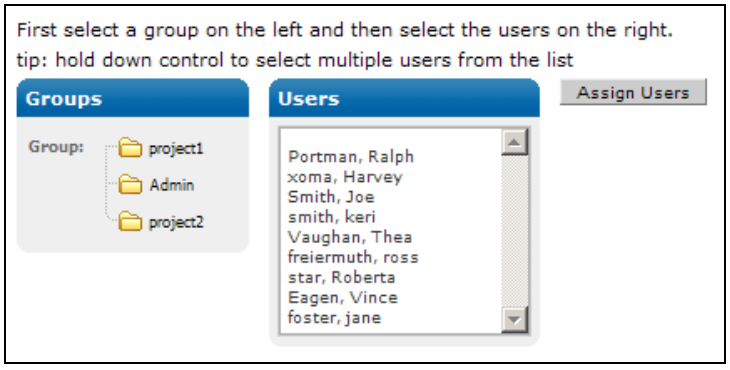
Click **Delete**. You are asked to confirm your action.

When you delete a group, the association between the group and any users who belonged to that group is broken. The associations between any sub-groups and users are also deleted.

If you want to keep a sub-group, first select a new parent for that sub-group, and then delete the old parent group. The sub-group then does not get deleted.

3.2.4 Assigning Users to a Group

To add users to a group, click **Assign Users**.



Select a group on the left. The list of users on the right updates to reflect potential new members for the group you selected. Users already in the group are excluded from the Users list.

If a user belongs to a parent group, they automatically belong to any sub-groups underneath it, even though the list does not reflect that. However, a user can belong to a sub-group and not belong to the parent group.

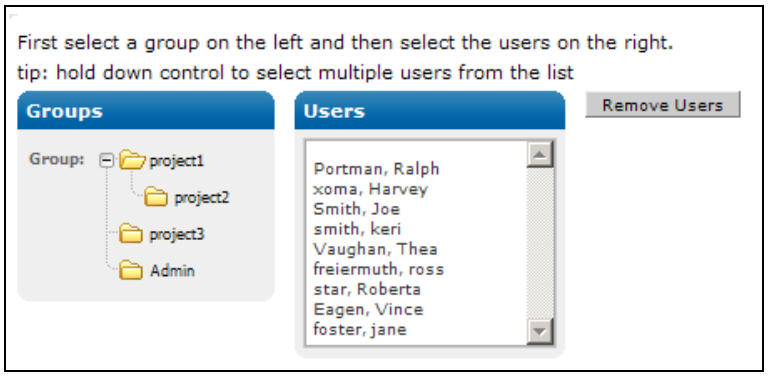
Select the users to add to the group. To add several users at once, hold down the Control key while you click on your selections.

3.2.5 Assigning Users to a Sub-Group

You can assign a user to any number of groups with the **Assign Users** command. Note by selecting a group, the user is automatically assigned to the group and all its sub-groups. To un-assign, check the checkbox and click **Save Details**.

3.2.6 Deleting Users from a Group

To delete users from a group, click **Remove Users**.



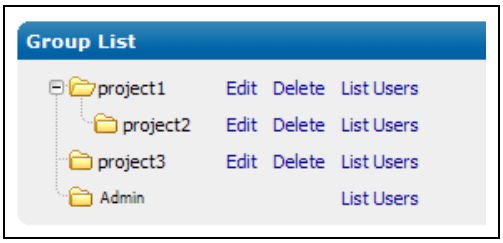
Select a group on the left. The list of users on the right updates to reflect that group's users.

Select the users to remove from the group. To remove many users at once, hold down the Control key while you click on your selections. Click **Remove Users**.

If a user belongs to a parent group, they automatically belong to any sub-groups underneath it; however, the screen does not reflect this. If a user is removed from a parent group, they are also removed from any sub-groups.

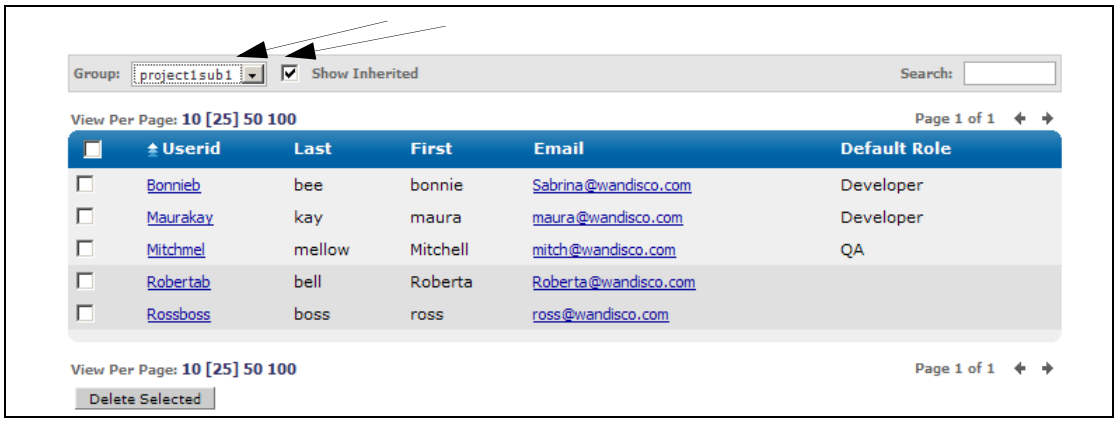
3.2.7 Who Is In a Group?

To view a list of which users belong to which groups, click **List Groups**.



All the groups are displayed. Click **List Users**. All the users in that group are displayed.

To view users who are explicitly members of this sub-group and those members inherited from any parent groups, check the **Show Inherited** checkbox. Use the Group drop-down list to view the users belonging to another group.

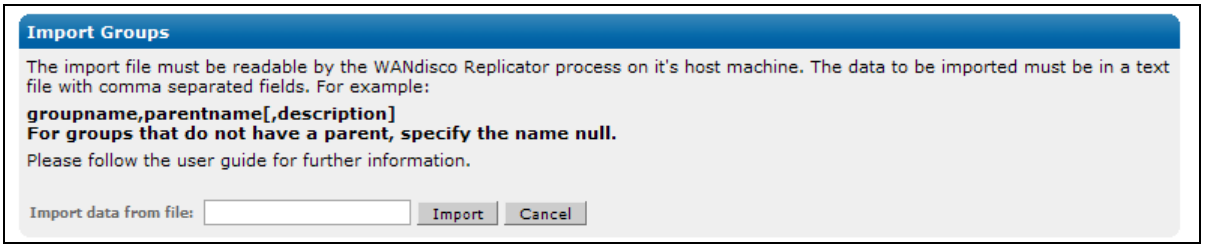


The userids are linked to the User Properties page, in case you need to edit a user. You can also edit and delete groups from this page.

3.2.8 Importing Existing Groups

You may have groups already set up outside Access Control. If so, you can import them using the **Import Groups** command, in a comma separated text file, of the format `groupname,parent-name<,description>`.

Type in the pathname to the file, and click **Import**. The new groups are added to the existing groups. Define the resources for this group or subgroup, and assign users.



4 About Access Control Lists

Many people find that managing users' roles and groups offer enough access control. However, Access Control allows you to have very specific control of users through the use of Access Control Lists (ACLs).

4.1 How WANdisco Enforces Rules

When a user tries to execute a Subversion command, Access Control's ACL engine always follows the same process to make an allow or deny decision.

First, the ACL engine checks if a user is registered or licensed in the WANdisco user database. If the user is not registered or licensed, the user is denied access.

In order for a rule to be matched, the ACL engine verifies that a user's name or the group(s) a user belongs to, IP address and file/directory matches the patterns specified in the ACLs.

Rules applicable to a specific user override the rules applicable to a group.

User's access rights	Group's access rights	WANdisco allows or denies?
none specified	allowed	allowed
none specified	multiple groups, any of which is allowed	allowed
none specified	multiple groups, any of which is denied	denied
denied	multiple groups, any of which is allowed	denied
allowed	denied	allowed
denied	denied	denied

WANdisco allows you to atomatically edit multiple rules. When you submit changes to ACLs, WANdisco guarantees either all the rules are updated or none at all.

When setting up a rule on a specific directory, note that the directory name is treated as a regular expression pattern. For example, if you want to allow write access to all the files under a directory `/svnroot/trunk/docs`, you need to specify one of the following patterns:

```
/svnroot/trunk/docs|/svnroot/trunk/docs/.*
```

or

```
/svnroot/trunk/docs.*
```

The first pattern allows write into the directory (to create new files or directories) as well as all files under the `.../docs/` subdirectory. The second pattern allows access to all files and subdirecties that match `/svnroot/trunk/docs`, including, `/svnroot/trunk/docs`, `/svnroot/trunk/docsmaker`, `/svnroot/trunk/docs2`, etc.

Special considerations should apply for list and read access rules. Unlike write operations, the read and list operations can traverse directory hierarchy. Therefore it makes sense to always allow or deny read and list privileges on all files under a directory. This can be done by specifying a wild-card pattern, for example:

```
allow read from /svnroot/trunk/module1|/svnroot/trunk/module1/.*.
```

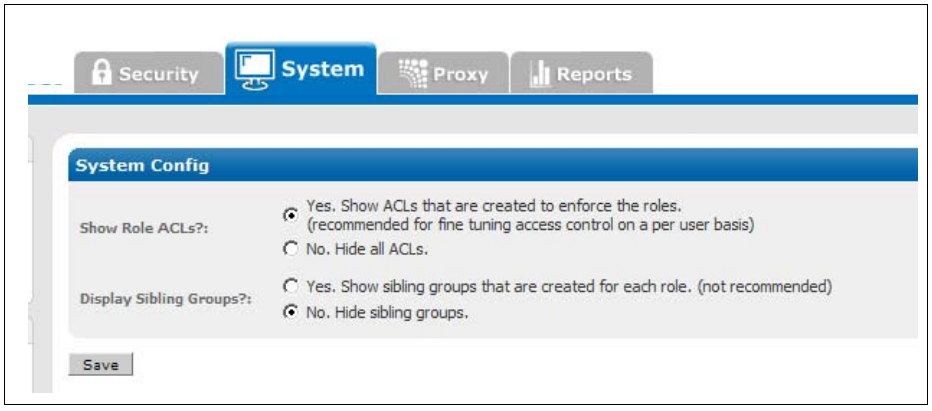
To use the copy privilege, specify it on the source directory. It allows a user to copy from a given directory. Make sure you enable the write privilege on the parent directory of the intended destination. Granting write privilege does not imply the user has delete or copy privilege. This allows the administrator to control who can create tags or branches and who can delete version controlled files. For example, to allow copy from `/trunk` to `/tags/rel1`, you create two access rules:

- Allow Copy from `/trunk.*`
- Allow Write to `/tags/rel1`

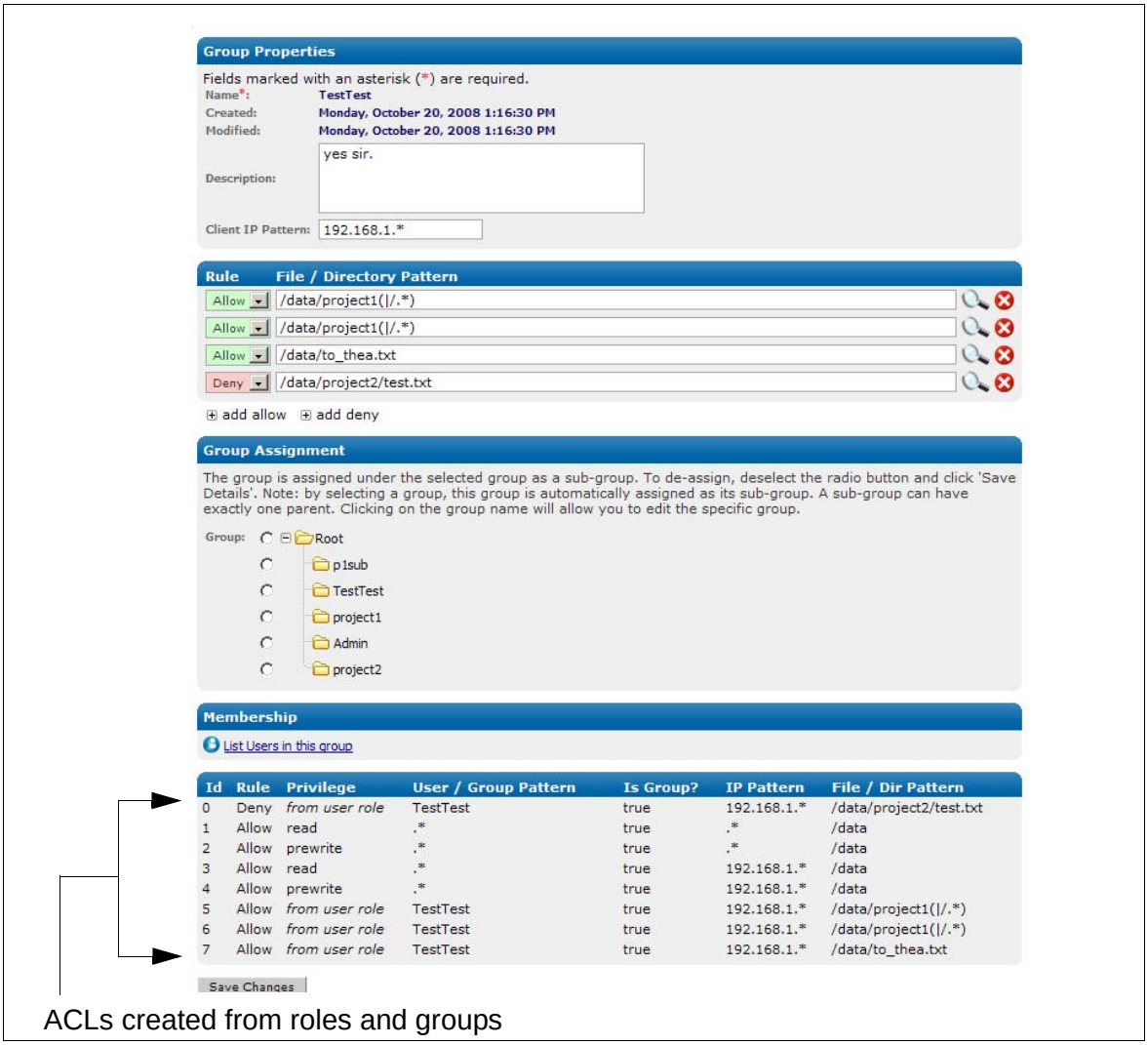
4.2 Toggling the ACL Display

You can toggle the display of role ACLs. The default is on.

Go to the System page, and click **System Config**. Select the **Yes** or **No** radio button for Show ACLs?

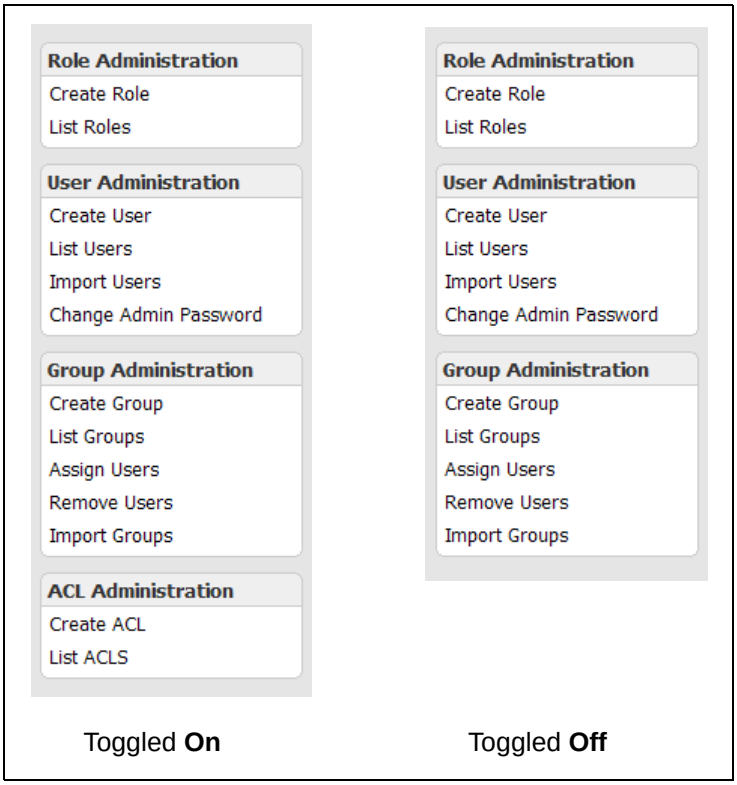


When toggled on, you see any ACLs created by roles and groups listed on the Group Properties page, shown in the next illustration.



ACLs created from roles and groups

Toggling the ACL display also displays the available ACL Administration commands in the Security tab.



4.3 Creating ACLs

To create ACLs, go to the Security tab and click **Create ACL**. If you are creating multiple ACLs, click on **List ACLs**. Refer to the field descriptions in ACL Administration in Using the Admin Console.

4.4 Toggling the Use of Access Control Lists

The following properties in the prefs.xml file can be used to control the ACL engine.

```
<Security>
   <AccessControl>
     <Enable>true</Enable>
     <Replicate>true</Replicate>
     <ClientTimeout>15s</ClientTimeout>
   </AccessControl>
</Security>
```

By default, Access Control has access control enabled. To turn it off, add the lines to `prefs.xml` and set `Enable` to `false`.

5 About Audit Reports

Access Control logs any Subversion user access (allowed or denied) in an audit trail file. WANdisco supplies a standard report, Users and Groups, but recommends you import the data into a database such as MySQL, so that you can make complex queries. WANdisco offers three such reports when set up with a database: Transaction History, Access Violation Report, and File.

To set up the more detailed reports, you need to:

- install php and the appropriate Apache module for your system
- install a database such as MySQL
- make sure you have the `svn-security/config/reports.tar` file, which contains WANdisco-supplied php scripts. This is part of the standard distribution.

To ensure no audit records are lost, WANdisco recommends you schedule a job (using `cron`, for example) to import the audit records into a database periodically.

5.1 Setting Up the Reports

Use this procedure to set up the reports. WANdisco does not automatically import data into the database. You can do this manually or set up a `cron` job.

Step 1 Download and install a database such as MySQL.

Step 2 Download and install php.

Step 3 Set up a user in the database. Grant that user all privileges to manage the database `wd_audit_db` (created in the next step).

Step 4 Create a database called `wd_audit_db` to manage the database. The database schema is created upon the import tool's first population, which you perform at a later step.

Step 5 Decompress the php scripts at `svn-security/config/reports.tar`.

Step 6 Edit the `reports/config.php` to point to the database you just created. Modify the `config.php` file to update the server, username and password entries along with the `scm` type, which is `svn`.

Step 7 Edit the `importauditdb` script to match the changes to `config.php`: `dbhost`, `dbuser`, and `dbpass`. It is recommended to not use the default user, `root`.

Step 8 Update your Apache `httpd.conf` file to point to the scripts. Make sure to replace `/home/wandisco/reports` with your installation directory. You may also want to rename the `/reports/` alias (e.g. `/wandisco_reports`). For example,

```
Alias /reports/ "/home/wandisco/reports/"
<Directory "/home/wandisco/reports">
Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

Step 9 Restart Apache.

Step 10 Run the import tool. See Using the Import Tool.

Step 11 You can now run the reports. See Running a Report.

5.1.1 Using the Import Tool

The import tool requires `Perl::DBI` module to be installed. Please run `svn-security/bin/checkdbi` to verify that the module is installed, and the correct database driver is available on your system.

The import tool is called `importauditdb`, and its usage is as follows:

```
perl importauditdb -host dbserver -user dbuser -pass dbpassword -f ../
audit/audit-trail.0
```

Here is an example of how to use the import command:

```
[admin@smp1 ~/svn-replicator]$ bin/importauditdb -h
Usage:
     importauditdb [-host <db-host>] [-port <db-port>] [-user <db user>]
                   [-pass <db user password>] [-db <database to use>]
                   -f file-pattern1 file-pattern2 .. file-pattern-N
```

```
Defaults:
host : localhost
port : Default DB Port
user : root
password : empty
Database : wd_audit_db
```

NOTE:

> Before using import, you must create a database on the database server.

The import tool automatically creates the table schema in that database, the first time it runs. The import tool uses standard SQL syntax, and makes use of a system function `FROM_UNIXTIME`. Please ensure your database version supports it. MySQL and Microsoft SQLServer both support this function.

Here is an example of how you would import a file:

```
perl importauditdb -host dbserver -user dbuser -pass dbpassword -f ../
audit/audit-trail.0
```

The `audit-trail.0` file is located in the `svn-security/audit` directory. The file has a complete history of all Subversion actions, listed in the following format:

```
# Column syntax -
# 0 seq | 1 time | 2 txid | 3 cmd | 4 user | 5 ipaddress | 6 access |
# 7 dir | 8 file | 9 rev
```

The columns are described in this table:

Column No.	Description
0	Record Sequence Number
1	UNIX Timestamp
2	Transaction Id
3	Subversion Command Name
4	Subversion User id
5	IP Address of User
6	Access Decision (Allow or Deny)
7	Subversion Directory being accessed
8	Subversion File being accessed
9	User's File Revision

5.2 Configuring Audit Properties

Auditing is controlled in the `prefs.xml` file. By default, Access Control enables auditing. You can turn it off by setting the `Disable` element to `true`.

```
<Audit>
   <MaxFileSize>10485760</MaxFileSize>
   <MaxFileCount>10</MaxFileCount>
   <Disable>false</Disable>    <!-- this is the default -->
</Audit>
```

By default, Access Control automatically rotates the files up to 10 times when they get to 10 megabytes. You can change these defaults in the `prefs.xml` file. The `MaxFileSize` element specifies a size in bytes, and the `MaxFileCount` element specifies how many files to rotate before recycling the files.

To create audit files in a different directory, create a symbolic link (`svn-security/audit`) to another directory.

NOTE:

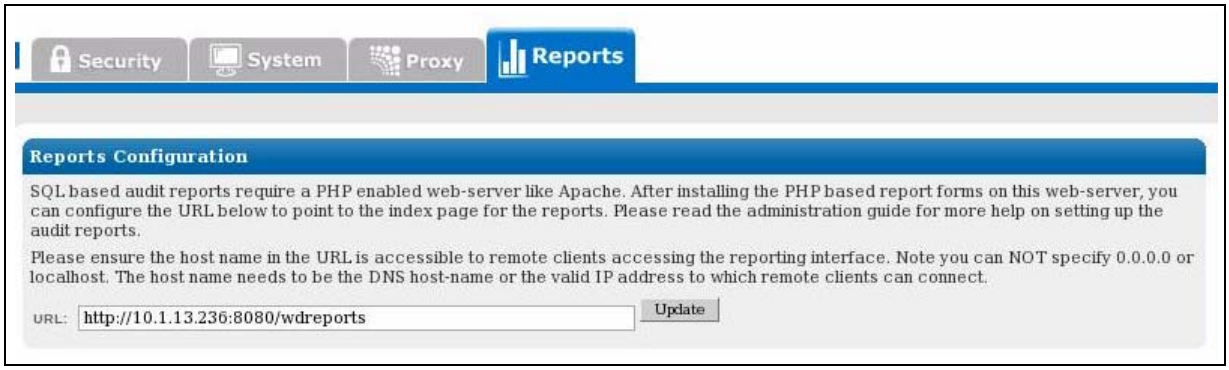
You do not want to loose any audit history. Make sure that any interval you schedule to import the files into a database is short enough (not longer) so that all files in the `MaxFileCount` element are captured (and not overwritten).

5.3 Running a Report

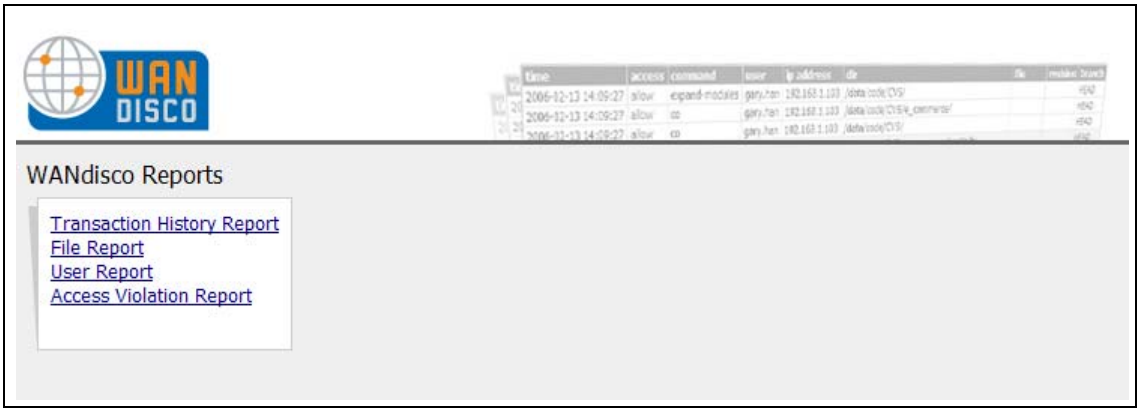
Step 1 Configure the report URI. Go to the Reports tab in the Admin Console. Click **Configure URI**. Enter in the IP address of the `"reports apache server":8080/<reports direcotry>`. For example,

`http://10.1.13.236:8080/wdreports`

Click **Update**.



Step 2 Go to that URL.



Step 3 Select **File Report** from the main menu.

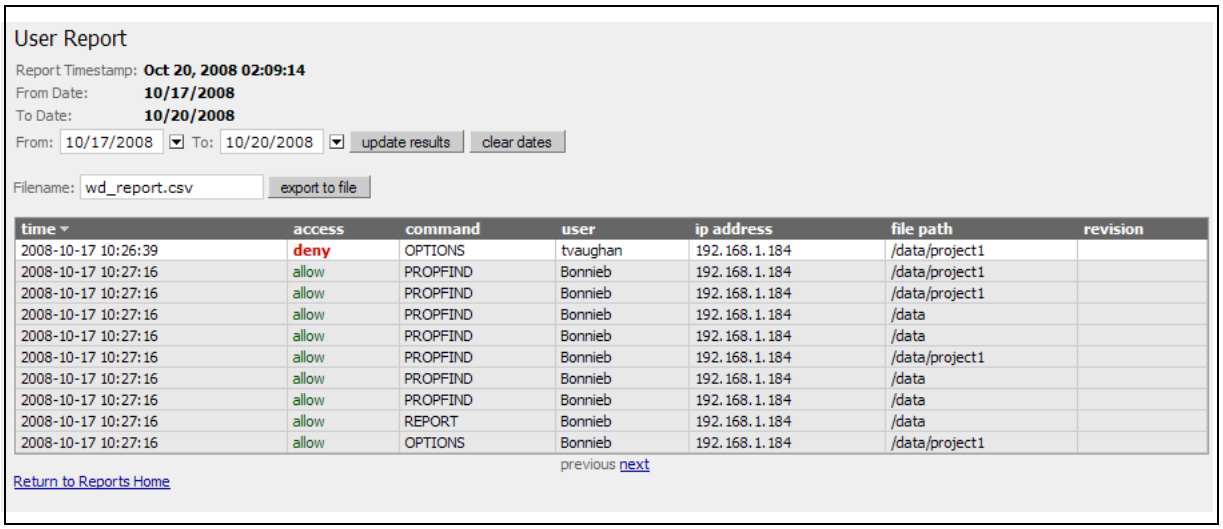
Step 4 Enter the criteria for the report. For example, select a user from the drop-down, specify an access level or a Subversion command to filter the results. Note: use % for wildcards.

Step 5 Click **Run Report**.

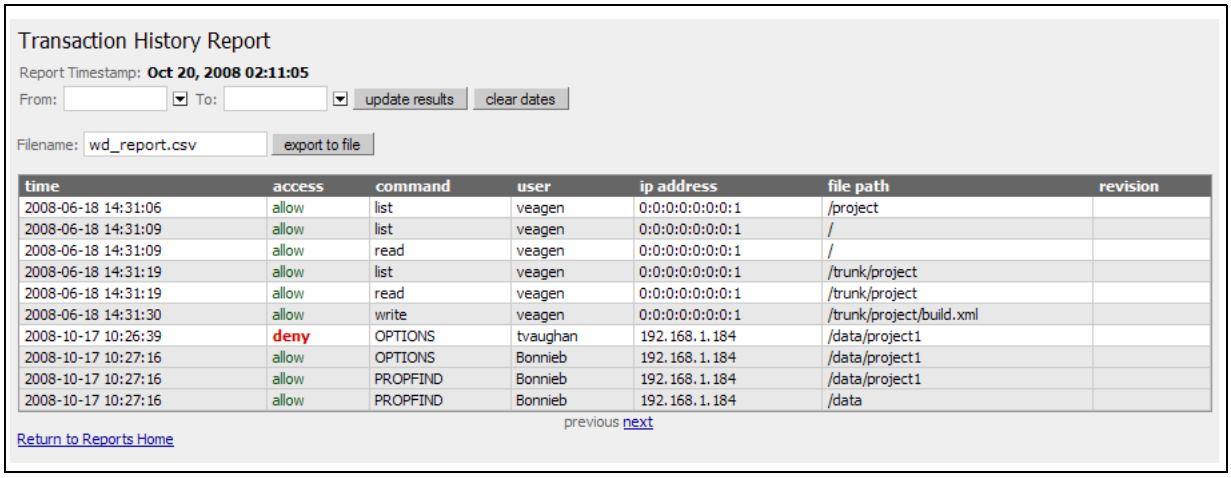
5.3.1 Report Types

Report Name	Description
Transaction History	Shows all transactions against Subversion.
File	List file access and filter by parameters such as: date, access, command, user, ip address, directory, filename, revision or branch.
User	Show Subversion allowed / denied access per user.
Access Violation	Display all denied access to Subversion.

5.3.1.1 The User Report



5.3.1.2 The Transaction History Report



Transaction History Report

Report Timestamp: **Oct 20, 2008 02:11:05**

From: To: update results clear dates

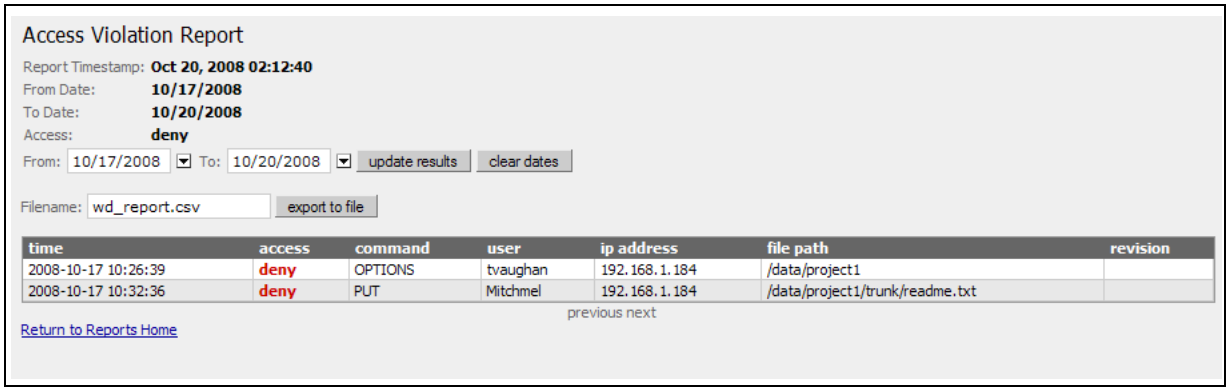
Filename: wd_report.csv export to file

time	access	command	user	ip address	file path	revision
2008-06-18 14:31:06	allow	list	veagen	0:0:0:0:0:0:0:1	/project	
2008-06-18 14:31:09	allow	list	veagen	0:0:0:0:0:0:0:1	/	
2008-06-18 14:31:09	allow	read	veagen	0:0:0:0:0:0:0:1	/	
2008-06-18 14:31:19	allow	list	veagen	0:0:0:0:0:0:0:1	/trunk/project	
2008-06-18 14:31:19	allow	read	veagen	0:0:0:0:0:0:0:1	/trunk/project	
2008-06-18 14:31:30	allow	write	veagen	0:0:0:0:0:0:0:1	/trunk/project/build.xml	
2008-10-17 10:26:39	deny	OPTIONS	tvaughan	192.168.1.184	/data/project1	
2008-10-17 10:27:16	allow	OPTIONS	Bonnieb	192.168.1.184	/data/project1	
2008-10-17 10:27:16	allow	PROPFIND	Bonnieb	192.168.1.184	/data/project1	
2008-10-17 10:27:16	allow	PROPFIND	Bonnieb	192.168.1.184	/data	

previous next

Return to Reports Home

5.3.1.3 The Access Violation Report



Access Violation Report

Report Timestamp: **Oct 20, 2008 02:12:40**
From Date: **10/17/2008**
To Date: **10/20/2008**
Access: **deny**

From: 10/17/2008 To: 10/20/2008 update results clear dates

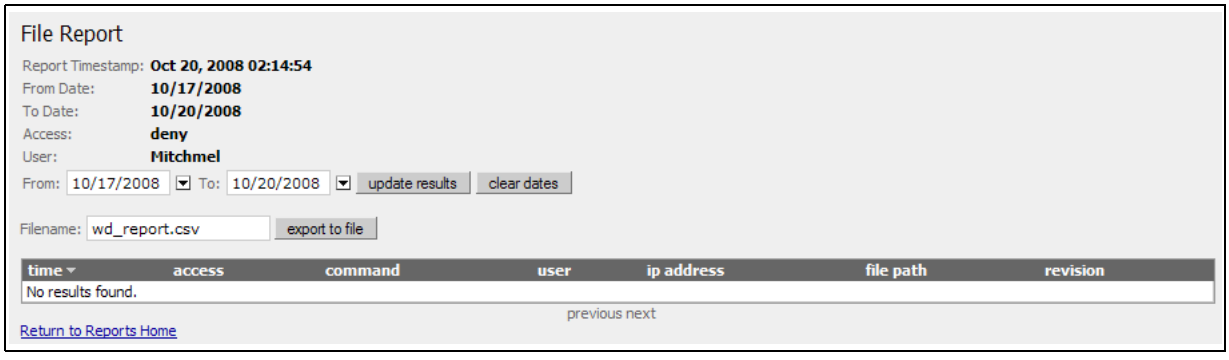
Filename: wd_report.csv export to file

time	access	command	user	ip address	file path	revision
2008-10-17 10:26:39	deny	OPTIONS	tvaughan	192.168.1.184	/data/project1	
2008-10-17 10:32:36	deny	PUT	Mitchmel	192.168.1.184	/data/project1/trunk/readme.txt	

previous next

Return to Reports Home

5.3.1.4 The File Report



File Report

Report Timestamp: **Oct 20, 2008 02:14:54**
From Date: **10/17/2008**
To Date: **10/20/2008**
Access: **deny**
User: **Mitchmel**

From: 10/17/2008 To: 10/20/2008 update results clear dates

Filename: wd_report.csv export to file

time	access	command	user	ip address	file path	revision
No results found.						

previous next

Return to Reports Home