



Click IT Solutions

Simply Click It

Simply Click It

WANSECURER OVERVIEW AND MANUAL

- **DUAL STACK IPV4 AND IPV6 SUPPORT**
- **SSL/TLS PEER TO PEER & MULTI-CLIENT VPN TUNNELS**
- **EMAIL PROTECTION WITH SPAM/VIRUS FILTERS**
- **STATEFUL IPV4/6 FIREWALL & INTRUSION DETECTION**
- **WEB MANAGEMENT W/OPT. TOLL FREE VOIP SUPPORT**
- **S-TUNNELS, OPENSSL (CA), OPENVPN, PPTP & OSSIM**

WANSECURER APPLIANCES

Disclaimer:

This document make mention to the WANSecurer Appliance, Webmin, and third Party Modules. The WANSecurer is a Trade Mark name of Click IT Solutions network security appliance, while Webmin is a trade mark of www.webmin.com, and all other trade marks are of their respective authorities.

The WAN Securer Appliance

The WANSecurer Appliance is a dual IP stack complete suite of solutions within a single hardware unit, capable of securing against network intrusion, Worms, Botnets, Email borne Virus, SPAM, and Phishing. It also provides a number of tools embedded such as OpenSSL, OpenSSH, OpenVPN, OSSIM, Statefull Firewall and more, this appliance is all your company need to guarantee its security from inside and outside threats to your IT Infrastructure.

Features include:

- Apache SSL Web Service with MOD-Security + OpenSSL + IPv6
- Clam Anti-virus
- Domain Name Service (IPv4/6 support)
- Dynamic Host Configuration Protocol DHCP
- IPv4/IPv6 Stateful Firewall with Redirect, sNAT and dNAT support
- LDAP integration w/ Kerberos 5 Support
- MailScanner with Email Protection Service + ETRN support
- OpenSLP Service
- OpenSSH Server
- OpenSSL Certificate Authority / PKI
- Open Source Security Information Manager OSSIM
- OpenVPN Server w/ IPv6 support
- Point to Point Tunnel Protocol PPTP VPN Server
- Secure Socket Layer (SSL) Tunnelling
- SMS Tools 3.0 (send and receive text messages via Ethernet base GSM modems)
- SpamAssassin
- Squid (dual IPv4/6 stack support) Transparent Web Proxy + Caching Server
- Toll Free VoIP with Remote Support Service
- Transparent FTP Proxy Server with Anti-virus support
- Webmin Web Based Unix/Linux Manager

- **Table of Contents**

The Table of Content is divided into the various module features. The Standard Features by category includes some 113 standard modules, and there are at least as many third party modules add-ons. Some screenshots may vary based on Operating Systems of Appliance.

Web Admin	See Page 6.
Backup Configuration Files	6
Command Shell	8
Custom Commands	8
SSH and Telnet Login.	13
System and Server Status	13
Webmin Actions Log	18
Webmin Servers Index	19
Webmin Users	24
Read User Mail	<i>n/a</i>
System	See Chapter 2.
Bootup and Shutdown	X
Change Passwords	X
Disk Quotas	X
Disk and Network Filesystems	X
Filesystem Backup	X
File Manager	X
LDAP Client	X
LDAP Users and Groups	X
Log File Rotation	X
MIME Type Programs.	X
MON Service Monitor	X
PAM Authentication	X
Running Processes	X
Scheduled Cron Jobs	X
Scheduled Commands	X
Security Sentries	X
Software Packages	X
SysV Init Configuration	X
System Documentation	X
Public Key Infrastructure (PKI)	X
System Logs	X
Upload and Download	X
Users and Groups	X
Protected Web Directories	X
PHP Configuration	X
Perl Modules	X
Features/Servers	See Chapter 3.
Apache Webserver	X
BIND DNS Server	X
DHCP Server	X
Clam Anti-Virus	X
MailScanner SPAM/Virus Filter	X
Fetchmail Mail Retrieval	X

OpenSLP Server	X
Procmal Mail Filter	X
SSH Server	X
Sendmail Configuration	X
SpamAssassin Mail Filter	X
Squid Analysis Report Generator	X
Squid Web Proxy Server	X
Frox FTP Proxy Server	X

Networking See Chapter 4.

HTTP Tunnel	X
IPSec VPN Configuration	X
Kerberos5	X
Linux Firewall	X
NFS Exports	X
Network Configuration	X
OpenVPN Server	X
PPP Dialin Server	X
PPP Dialup Client	X
PPTP VPN Client	X
PPTP VPN Server	X
SSL Tunnels	X

Hardware See Chapter 5.

Linux Bootup Configuration	X
Linux RAID	X
Logical Volume Management	X
Partitions on Local Disks	X
Printer Administration	X
System Time	X

Cluster See Chapter 6.

Cluster Change Passwords	X
Cluster Copy Files	X
Cluster Cron Jobs	X
Cluster Shell Commands	X
Cluster Software Packages	X
Cluster Users and Groups	X
Cluster Web Admin Servers	X
Configuration Engine	X
Heartbeat Monitor	X

Web Admin

Web Admin - Webmin is a web-based interface for system administration for UNIX. Using any modern web browser, you can setup user accounts, Apache, DNS, file sharing and much more. Webmin removes the need to manually edit Unix configuration files like `/etc/passwd`, and lets you manage a system from the console or remotely.

See the following modules within this Category -:

- Backup Configuration Files
- Command Shell
- Custom Commands
- SSH and Telnet Login
- System and Server Status
- Webmin Actions Log
- Webmin Servers Index
- Webmin Users
- Read User Mail

Backup Configuration Files

Most Webmin modules work by editing configuration files on your system, like `/etc/exports` for NFS shares, `/etc/passwd` for users and `/etc/fstab` for filesystems. Each module knows which configuration files it manages, and what commands need to be run to activate them. Not all modules actually deal with config files though - for example, the MySQL module works by executing SQL commands. As such, it cannot participate in the configuration backup process.

The Backup Configuration Files module can collect information about config files from other modules, and create and restore backups containing some or all of those files. It is designed for saving the configuration of a single system, but not for migrating configs from one server to another - that would be far more complex. You can theoretically backup the configs from one system and restore them on another if they are running the exact same OS and version (like Fedora Core 5), but attempting this between systems of different types is almost certain to fail.

Using the Backup Configuration Files module

When this module (under the Web Admin category) is opened, it will display a set of tabs with the form for making a backup selected by default, as in the image below.

The screenshot shows the Webmin interface for the 'Backup Configuration Files' module. The page title is 'Backup Configuration Files'. There are three tabs: 'Backup now' (selected), 'Scheduled backups', and 'Restore now'. Under 'Backup now', there is a sub-tab 'Backup configuration now'. The main form area is divided into sections:

- Modules to backup:** A list of modules to be backed up, including Shorewall Firewall, SpamAssassin Mail Filter, Squid Analysis Report Generator, Squid Proxy Server, and SysV Init Configuration.
- Backup destination:** Radio buttons for selecting the backup location: Local file `/tmp/boobar.tgz`, FTP server, SSH server, and Download in browser.
- Include in backup:** Checkboxes for including Webmin module configuration files, Server configuration files, and Other listed files ..

To perform an immediate config backup, follow these steps:

1. Click on the Backup now tab.
2. In the Modules to backup list, select the modules you want to backup config files for, such as Users and Groups. Multiple modules can be selected by ctrl-clicking.
3. In the Backup destination field, select Local file and enter a path to write the backup to. This should be given a tar.gz extension, as that is the file format used.
4. Click the Backup Now button.

Assuming the path you entered is valid, a page should appear showing the list of modules whose configs were backed up, and the size of the resulting file.

Backups can also be made to a remote SSH or FTP server, provided you have a login, password and writable directory. This is done by selecting the FTP server or SSH server options in step 3 above, and filling in the appropriate fields.

Creating a scheduled backup

Once you have performed a manual backup, you can schedule it to run on a regular basis as follows:

Create Scheduled Backup

Scheduled backup options

Modules to backup
 ADSL Client
 Apache 2.2.0
 Apache Clone
 Apache Webserver
 BIND DNS Server

Backup destination
 Local file
 FTP server
 SSH server

Include in backup
 Webmin module configuration files
 Server configuration files
 Other listed files ..

Email result to address

When to send email
 Always
 Only when an error occurs

Scheduled backup enabled?
 No
 Yes, at times selected below ..

Simple schedule .. Hourly
 Times and dates selected below ..

Minutes	Hours	Days	Months	Weekdays
<input type="radio"/> All <input checked="" type="radio"/> Selected ..	<input type="radio"/> All <input checked="" type="radio"/> Selected ..	<input type="radio"/> All <input checked="" type="radio"/> Selected ..	<input type="radio"/> All <input checked="" type="radio"/> Selected ..	<input type="radio"/> All <input checked="" type="radio"/> Selected ..
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59	0 1 2 3 4 5 6 7 8 9 10 11 12	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	January February March April May June July August September October November December	Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months.

1. Click on the Scheduled backups tab.
2. Click the Add a new scheduled backup link, which will open the form shown below.
3. Select the modules whose config files you want to include from the Modules to backup list.
4. Enter a local or remote file destination in the Backup destination section.
5. If you want to be notified about the status of this backup, enter your email address in the Email result to address field.

6. In the Scheduled backup enabled? field select Yes, and choose the times and days for the backup to run from the Cron time selector below it.
7. Click the Create button.

Once a scheduled backup has been created, you can edit or remove it by clicking on the destination path in the table under the Scheduled backups tab.

Restoring a backup

If you find that a config file on your system has been corrupted, incorrectly edited or mistakenly deleted, it can be easily restored using this module. The steps to perform a restore are:

1. Click on the Restore now tab.
2. Select the module or modules whose config files you want to restore from the Modules to restore menu.
3. In the Restore from section, enter the path to a local or remote file that was originally created by this module. To be useful, it must contain backups for the modules that you selected above.
4. Click the Restore Now button.

If all goes well, a page will be displayed showing the number of modules and files restored. Files will be restored to their original locations on the system, rather than the paths that are set on the Module Config pages of the selected modules.

Command Shell

The Command Shell module

One problem with the SSH/Telnet Login module is its inability to connect if there is a firewall of some kind blocking telnet or SSH connections to your system. Even though the rest of Webmin may work fine using HTTP connections, the ports used by the applet may not be available. Even though it is possible to do almost everything in Webmin that you can do at the command line, sometimes it is useful to have a shell prompt for executing Unix commands.

To get around firewall restrictions that prevent an SSH or telnet connection, you can use the Command Shell module, found under the Others category. It allows you to enter shell commands into the field next to the *Execute command *button, which are run when the button is clicked or the return key pressed. All output from the command is displayed in the Command history section at the top of the page.

You can re-run old commands by selecting them from the menu next to the Execute previous command button and then clicking it. If the command history becomes too large, it can be wiped using the Clear history button. This will not effect the menu of previously run commands though.

The module's biggest limitation is that interactive commands like vi, passwd and telnet cannot be run. There is no support for providing input to a command once it has started, so you are limited to non-interactive programs like cp, ls and rm.

Custom Commands

This covers the Custom Commands module, which can be used to create buttons to run frequently used shell commands.

The Custom Commands module

Most system administrators like to create shell scripts to perform common tasks, like backing up a database or adding a new user of some kind. Because every system and organization is different, there will always be

tasks that a generalized tool like Webmin cannot do as easily as a simple customized script. Unfortunately, scripts run at the command line are not easy for an inexperienced user to use.

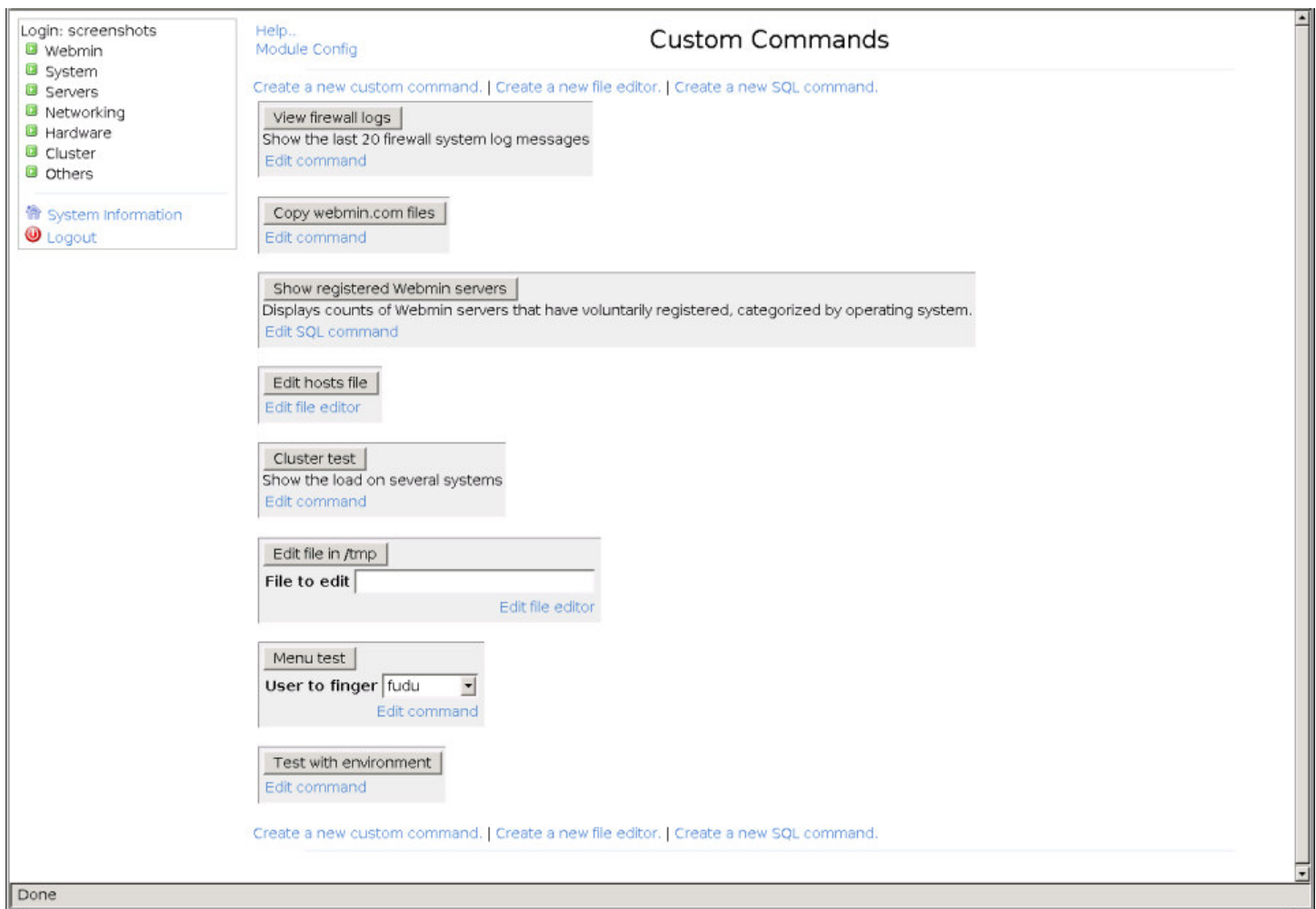
The Custom Commands module allows you to create simple web interfaces for shell scripts and commands, so that they can be run from within Webmin at the click of a button. It also allows you to define parameters of various types for each command that can be entered by the user and substituted into the shell command. This can be used to provide additional arguments or input to the scripts that are run, depending on selections made by the user before running it.

Another feature of the module is the ability to define file editors, so that frequently changed files can be edited through web interface. You can also define commands to be run before and after the file is edited, so that it can be validated, copied or backed up before editing.

Possibly the most useful feature of the module is its access control support. You can grant other Webmin users the rights to use some or all of the commands and editors, while giving only yourself and other trusted administrators permissions to create and edit commands. This means that the other users can only execute the scripts and edit the files that you allow them to, but with full root privileges.

Unlike most other modules, this one does not deal with the configuration of some separate server or service. Therefore it has the exact same user interface and functionality on all versions of Unix that Webmin can run on.

The screenshot below shows an example from a system with 1 file editor and 8 commands defined, two of which have a parameter. If you have not used the module before, the page will be empty though.



The screenshot displays the 'Custom Commands' module in Webmin. On the left is a navigation sidebar with categories like Webmin, System, Servers, Networking, Hardware, Cluster, and Others, along with System Information and Logout. The main content area is titled 'Custom Commands' and includes a 'Help.. Module Config' link. Below this are three links: 'Create a new custom command.', 'Create a new file editor.', and 'Create a new SQL command.'. The interface lists several predefined commands, each with a button to run it and a link to edit it:

- View firewall logs**: Shows the last 20 firewall system log messages. Edit command.
- Copy webmin.com files**: Edit command.
- Show registered Webmin servers**: Displays counts of Webmin servers that have voluntarily registered, categorized by operating system. Edit SQL command.
- Edit hosts file**: Edit file editor.
- Cluster test**: Show the load on several systems. Edit command.
- Edit file in /tmp**: Includes a 'File to edit' text input field and an 'Edit file editor' link.
- Menu test**: Includes a 'User to finger' dropdown menu with 'fudu' selected and an 'Edit command' link.
- Test with environment**: Edit command.

At the bottom of the main content area, the same three creation links are repeated. The status bar at the very bottom of the window shows 'Done'.

You can run any command shown on the main page by just clicking its button. However, if the command has parameters fields or choices you must fill them in or make the appropriate selections before running it. When

the button is clicked, you will be taken to a page showing all output from the command, so that you can see if it succeeded or failed.

To use a file editor, just click on its button on the main page. This will take you to an editing form showing the current file contents, which you can change freely. When done, click the Save button below the text box to write out the new file contents.

Creating a new command

To create a new command that can be run using a button on the module's main page, the steps to follow are :

1. Click on the Create a new custom command link above or below the existing buttons. This will bring up the creation form shown in the image below.
2. Enter a short description for your command into the Description field. Whatever text you enter will appear on the command's button on the main page. You can also enter additional text (including HTML tags) into the larger text box below it, to be displayed underneath the button.
3. In the Command field, enter the shell script or command that you want to execute. All standard shell metacharacters are supported, such as |, &, < and >. To enter multiple commands, separate them with ; or &&. If your command has parameters (set in step 10) they will be converted into environment variables when the command is run. So if you have a parameter called foo, all occurrences of \$foo in the command string will be replaced with whatever the user enters for that parameter. For example, a command that allowed the user to finger any user on the system might look like finger \$user .
4. By default, the command will run in the Webmin directory for this module. To change this, de-select Default for the Run in directory field and enter a different path into the text box next to it.
5. In the Run as user field, enter the name of the Unix user that the command should run as. You can select Webmin user instead, which will cause it to run as the Unix user with the same name as the Webmin user who runs it. When the command is executed, it will not normally have access to the same environment variables that the Unix user would have if he logged in via telnet or SSH. However, if you check the Use user's environment option then all variables set in the user's .profile, .cshrc and other login files will be available. Webmin runs the command with su, which switches to the user, executes his shell and then executes the command.
6. If your command produces HTML output that you want to appear in the browser when it is run, change the Command outputs HTML? field to Yes. Otherwise Webmin will escape all HTML tags in the output, which is the correct thing to do for commands that produce just normal text.
7. To control the placement of the new command on the module's front page, enter a number for the Ordering on main page option. Commands are ordered so that those with the highest number appear first. If Default is chosen, the ordering number is taken to be zero. If you do not set the ordering number for any of your custom commands, they will be displayed in the order that they were created.
8. To prevent the user seeing the actual shell command being run when its button is clicked, set the Hide command when executing? field to Yes. This is a good idea if your command contains passwords or other sensitive information you want to hide from the user.
9. If you want your command to have parameters that the user can set on the main page, you need to fill in the Command parameters section. Each row in the table in this section defines one parameter, and for each the following information must be entered :
 - a. Name A short unique name for this parameter, which can be used in the Command field (prefixed with a \$) to indicate where the value entered by the user should be substituted. The name should be made up of only letters, numbers and the _ character.
 - b. Description The text that will label the parameter on the module's main page. This can contain any characters including HTML tags, but should not be too long.
 - c. Type This menu controls how the parameter is displayed on the module's main page, and what inputs are allowed. The most common choice is Text, but all available options and their meanings are covered in the Parameter types section below.
 - d. Quote parameter? If set to Yes, the value entered by the user will be quoted with " characters before substitution.

When creating a new command, only one empty row for entering a single parameter is available. To add more, you will need to re-edit the command after saving it.

Finally, when you are done entering the details of your new command, click the Create button. As long as there are no errors in the form, you will be returned to the module's main page on which the new command button should be visible

The screenshot shows the 'Create Command' interface. On the left is a sidebar with a 'Login: screenshots' section containing links for Webmin, System, Servers, Networking, Hardware, Cluster, and Others, and a 'System Information' section with a Logout link. The main area is titled 'Create Command' and includes a 'Module index' and 'Help..' link. The 'Command details' section contains:

- Description: A large text input field.
- Command: A text input field.
- Run in directory: A dropdown menu with 'Default' selected.
- Run as user: A dropdown menu with 'Webmin user' selected, and a checkbox for 'Use user's environment?'.
- Command outputs HTML?: Radio buttons for 'Yes' and 'No'.
- Hide command when executing?: Radio buttons for 'Yes' and 'No'.
- Maximum time to wait for command?: Radio buttons for 'Forever' and a seconds input field.
- Run on Webmin servers: A dropdown menu with 'this server' selected, listing other servers like 'debian.home', 'bishan.home', 'clarke.home', and 'lentor.home'.

 The 'Command parameters' section is a table with columns: Name, Description, Type (with a dropdown menu showing 'Text'), and Quote parameter? (with radio buttons for 'Yes' and 'No'). A 'Save' button is located below the table. At the bottom, there is a 'Return to commands' link.

Once a command has been created, you can edit it by clicking on the Edit command link below it on the module's main page. All the fields described above can be changed, and an additional parameter added. Once you are done making changes, click the Save button at the bottom of the page. Or to get rid of the command, click the Delete button in the bottom-right corner instead.

Parameter types

For each parameter in a command, you can choose a type from its menu under the Type column. The available options and their meanings are:

This area Not done yet ... we ask your patience of ask support agent for guidance in configuring module.

Creating a new file editor

To add a new button to the module's main page for editing a file, you must follow these steps:

1. Click on the Create a new file editor link above or below the existing buttons. This will bring up the editor creation form shown in the image below.
2. Enter a short description for the file to be edited into the Description field. Whatever text you enter will appear on the editor's button on the main page. You can also enter additional text (including HTML tags) into the larger text box below it, to be displayed underneath the button.
3. Enter the full path to the file to be edited into the File to edit field. The file does not necessarily have to exist yet.
4. To have the file's owner changed when it is saved, set the File ownership field to User and enter a Unix username and group name into the fields next to it. This is especially useful when editing a file that does not exist yet, so that the ownership of the newly created file is set properly. If you leave the field set to Leave as it, the file's ownership will not be changed when it is saved. Newly created files will be owned by root.
5. To have the file's access permissions changed when it is saved, set the File permissions field to Set to octal and enter the permissions (like 700 or 664) into the field next to it. To you select Leave as it, the

file's permissions will not be changed when it is saved. The permissions on newly created files depend on the Webmin processes's umask.

6. To have a command run just before the file is saved by the user, fill in the *Command to run before saving *field. This could be useful for making a backup copy, checking the file out of RCS or anything else that you can come up with.
7. Similarly, to have a command run just after the file is saved fill in the C*ommand to run after saving* field. This can be useful for validating the file's contents, copying it to another system or checking it back into RCS.
8. To control the placement of the new editor's button on the module's front page, enter a number for the Ordering on main page option. Commands and editors are ordered so that those with the highest number appear first. If Default is chosen, the ordering number is taken to be zero. If you do not set the ordering number for any of your file editors, they will be displayed in the order that they were created.
9. Finally, click the Save button. If there are no errors in the form, you will be returned to the module's main page which will include a button for the new editor.

The screenshot shows the 'Create File Editor' interface. On the left is a navigation menu with 'Login: screenshots' and various system categories. The main content area has a title 'Create File Editor' and a 'Help..' link. Below the title are two sections: 'File editor details' and 'Command parameters'. The 'File editor details' section contains several form fields: 'Description' (a large text area), 'File to edit' (a text field with a browse button), 'File ownership' (radio buttons for 'Leave as is', 'User', and 'Group'), 'File permissions' (radio buttons for 'Leave as is' and 'Set to octal'), 'Command to run before saving' (a text field), 'Command to run after saving' (a text field), 'Ordering on main page' (a radio button for 'Default' and a text field), and 'Available in Usermin?' (radio buttons for 'Yes' and 'No'). The 'Command parameters' section is a table with three columns: 'Name', 'Description', and 'Type'. The 'Type' column has a dropdown menu currently set to 'Text'. A 'Save' button is positioned below the table. At the bottom left, there is a 'Return to commands' link with a left-pointing arrow.

Once an editor has been created, you can edit it by clicking on the *Edit file editor *link below it on the module's main page. Once you are done making changes, click the Save button at the bottom of the page. Or to get rid of the editor, click the Delete button in the bottom-right corner instead.

Module access control

The access control options in the Custom Commands module are designed to allow a master Webmin user to give some other users the rights to run selected commands, but not edit or create them. From a security point of view, it makes no sense to give an un-trusted user permissions to create his own custom commands, because that would allow him to run any command as root and so compromise the security of the entire system. Similarly, you can restrict the file editors that a Webmin user can use, and prevent him from creating new editors.

Once you have created a user or group with access to the Custom Commands module, the steps to follow to limit his access are:

1. In the Webmin Users module, click on Custom Commands next to the name of the user or group that you want to grant access to. This will bring up the access control form for the module.
2. Change the Can edit module configuration? field to No.

3. Unless you want the user to be able to run all commands and use all editors, set the Commands this user can run field to Selected and choose those that he should be allowed to use from the list below. Alternately, you can choose All except selected and select from the list the commands that he should not be allowed to use. All others will be available to him.
4. Change the Can create and edit commands? field to No.
5. Click the Save button. The access control settings will be activated and you will be returned to the main page of the Webmin Users module.

SSH and Telnet Login

This module combines the best features of both SSH/Telnet Login and Command Shell - it allows you to make a fully interactive login that is tunneled through an HTTP connection, thus avoiding any firewall restrictions. It is not included as one of the standard Webmin modules.

When you enter the module, its main page is taken up entirely by a Java applet. To start the login process, click the Connect button in the lower right-hand corner. A normal login: prompt should appear at the top of the window, allowing you to enter a username and password to login and get a shell prompt. When you are done, just click the Disconnect button to logout.

The module's biggest disadvantage is that it uses compiled Linux x86 code, and so cannot be run on other Unix systems or on non-PC hardware. It also uses up a lot of CPU time on the server due to the high number and frequency of HTTP requests that it makes.

System and Server Status

The System and Server Status module

This module allows you to monitor the status of various servers and daemons running on your system, so that you can easily see which are running properly and which are down. It can also be configured to check the status of servers on a regular schedule, and to email you or run a command if something goes down. This can be useful if your system runs critical servers that other people depend upon, such as web or DNS servers.

The module can also monitor servers running on other hosts. This can be done in two ways - by making a TCP or HTTP connection to the port that the server runs on, or by communicating with the Webmin server on the remote host and asking it to check the status of the server. The latter method is more powerful, because it can be used to monitor things such as disk space and daemons that do not accept any network connections.

Each server or service that you want to watch using the module must have a monitor defined. Every monitor has a type that indicates what kind of server it is supposed to check, such as Apache or BIND. Monitors also have additional parameters, some of which are specific to their type. The module allows you to create many different types of monitors, for things like checking if Sendmail or Squid is running, watching for excessive network traffic or a shortage of disk space, or pinging or connecting to some host.

A monitor can run either on the system that you are using the module on, or another server running Webmin. In the latter case the server must be defined in the Webmin Servers Index module, explained in chapter 53. Alternately, you can check another system that does not have Webmin installed using the remote TCP, HTTP and ping monitor types.

Many monitors use other Webmin modules to find the locations of the servers and daemons that they checked. For this reason, those other modules must be configured and working properly for the associated monitor to work as well. For example, if you have compiled and installed Apache in a different directory to the standard for your Linux distribution, the module configuration for Apache Webserver will have to be adjusted to use the correct paths. If not, this module will not know where to look for the Apache PID file.

When you enter the System and Server Status module from the Others category on the Webmin menu, its main page will display a table of all configured monitors. By default, several monitors for common servers and services will be defined, but you can edit, delete or add to them as you wish. The screenshot below shows an example of the module's main page.

The screenshot displays the 'System and Server Status' module in Webmin. On the left is a navigation menu with categories like Webmin, System, Servers, Networking, Hardware, Cluster, and Others. The main content area shows a 'Module Config' section with a dropdown menu set to 'Alive System'. Below this, it indicates the status from the last scheduled check at 'Wed May 16 16:00:35 2007'. A table lists various monitors, each with a checkbox, a description, the host it runs on, and its last check status. The 'Home DNS server' monitor is highlighted in yellow. All monitors show a green checkmark in the 'Last check' column, indicating they are up.

Monitoring	On host	Last check
<input type="checkbox"/> Apache Webserver	Local, www.pic.com.au	✓✓
<input type="checkbox"/> DNS server www.webmin.com	Local	✓
<input type="checkbox"/> Disk Space on /	Local	✓
<input type="checkbox"/> Disk Space on /backup	Local	✓
<input type="checkbox"/> Disk Space on /home	Local	✓
<input type="checkbox"/> Disk Space on /var/mail	Local	✓
<input type="checkbox"/> Disk Space on /video	Local	✓
<input type="checkbox"/> Free Memory	Local	✓
<input type="checkbox"/> Hacked ttyload	Local	✓
<input type="checkbox"/> Hacked ttymon	Local	✓
<input type="checkbox"/> Home DHCP server	Local	✓
<input type="checkbox"/> Home DNS server	Local	✓
<input type="checkbox"/> Internet and RPC Server	Local	✓
<input type="checkbox"/> Internet connection	Local	✓
<input type="checkbox"/> Local FTP server	Local	✓
<input type="checkbox"/> Mail queue size	Local	✓
<input type="checkbox"/> MySQL Database Server	Local	✓
<input type="checkbox"/> NFS Server	Local	✓
<input type="checkbox"/> PIC DNS server www.webmin.com	Local	✓
<input type="checkbox"/> PostgreSQL Database Server	Local	✓
<input type="checkbox"/> ProFTPD Server	Local	✓
<input type="checkbox"/> SQL Query	Local	✓
<input type="checkbox"/> SSH bugs	Local	✓
<input type="checkbox"/> Samba Servers	Local	✓
<input type="checkbox"/> Secondary DNS server	lentor.home	✓
<input type="checkbox"/> Sendmail Server	Local	✓
<input type="checkbox"/> Squid Proxy Server	Local	✓
<input type="checkbox"/> Usermin Webserver	Local	✓
<input type="checkbox"/> Webmin Webserver	Local	✓
<input type="checkbox"/> Website www.google.com	Local	✓
<input type="checkbox"/> Website www.pic.com.au	Local	✓
<input type="checkbox"/> Website www.test20.com (CFI)	Local	✓

For each monitor, a description, the Webmin server that it runs on and its current status are shown. A monitor can be in one of the following states:

- Up, meaning that the monitored server or service is running correctly. This state is indicated by a green tick on the main page.
- Down, meaning that the monitored server is down. This state is indicated by a red X on the module's main page.
- Not installed, meaning that the server being monitored is not installed on your system. This state is indicated by a black circle with a line through it.
- Timed out, meaning that the monitor took too long to execute. This state is indicated by a clock icon.
- Webmin error, meaning that the remote Webmin server to run the monitor on could not be contacted. This is represented by a red letter W.

By default, the status of every monitor is queried every time you view the module's main page. Because this may take a long time if you have many monitors or are checking the status of servers on remote hosts, there is a module configuration option that can be used to display the status from the last scheduled check instead.

Adding a new monitor

To have Webmin check on the status of a new server or service, you must add an additional monitor in this module. Before you can do this, you must decide on the monitor's type, which is determined by the type of

service that you want it to check. See the **Monitor types** section below for a list of all those that are available, their purposes and optional parameters.

Once you have chosen a type, the steps to follow to add it are:

1. Select the type from the menu next to the Add monitor of type button on the module's main page. When you click the button, the browser will display a form for adding a new monitor as shown in the image below.
2. Fill in the Description field with a short description of this monitor, such as Office webserver. This will appear on the main page and in any status emails.
3. To have the monitor executed on another Webmin server, select it from the Run on host menu. If you have no servers defined in the Webmin Servers module (covered in Webmin Servers Index – see below), no menu will appear.
4. If you have scheduled monitoring enabled and want this service to be checked regularly by it, make sure the Check on schedule? field is set to Yes. If it is set to No, scheduled checking will be turned off for this particular monitor. The other options starting with Yes allow you to control when email is sent if the monitor goes up or down. They correspond to the options for the Send email when field, explained in the Setting up scheduled monitoring section.
5. To have a command executed when a scheduled check determines that the monitor has gone down, enter it into the If monitor goes down, run command field. This could be used to attempt to re-start the monitored server, or to notify a system administrator by some method other than email.
6. Similarly, you can fill in the In monitor comes up, run command field with shell commands to execute when a scheduled check determines that the service has come back up again.
7. If the Run on host field is set to another Webmin server, you can choose whether the up and down commands in the previous two steps are run on this system or the remote server. This is controlled by the Run commands on field.
8. If the monitor is being run locally and is checking a server configured in another Webmin module for which multiple clones exist, the Module to monitor field will appear on the form. This menu can be used to choose which of the clones the monitor should get its configuration from. So for example if you had two versions of Apache installed on your system and two Apache Configuration modules set up to configure them, you would be able to choose which one should be checked when creating an Apache Webserver monitor. See chapter 51 for more information on how module clones work.
9. Depending on the type of monitor being created, there may be several additional options that you can set on this form. See the Monitor types section below for the details.
10. When done, click the Create button to have the monitor created and added to the main page. Its status should be immediately displayed.

The screenshot shows the 'Edit Monitor' form for 'Disk Space' in Webmin. The form is titled 'Monitor details' and contains the following fields and options:

- Description:** Disk Space on /
- Current status:** 54.63 GB free
- Run on hosts:** A dropdown menu with options: <Local>, bishan.home, clark.home, debian.home, and virtualmin-ec2-demo.homelinux.com.
- Run on host groups:** A dropdown menu with options: home (6 members), bacula (One member), redhat (One member), and test (One member).
- Check on schedule?:** Yes, and use default reporting mode
- Failures before reporting:** 1
- Notification methods:** Email SNMP
- Also send email for this service to:** (empty text field)
- Don't check if monitor is down:** (empty dropdown menu)

On the left side of the interface, there is a sidebar with navigation links: Login: screenshots, Webmin, System, Servers, Networking, Hardware, Cluster, Others, System information, and Logout. At the top, there is a 'Module index' link.

Existing monitors can be edited by clicking on their description on the main page. When editing, all the same fields as described above are available, in addition to a Current status field that indicates whether the service is up or down. For some monitor types, additional information is displayed when it is up, such as the time that the server being checked was started.

After you have finished editing a monitor, click the Save button at the bottom of the page to record your changes. To get rid of a monitor, use the Delete button instead. Either way, the changes will be applied immediately.

Monitor types

The System and Server Status allows you to monitor many different kinds of servers and daemons, using different monitor types. All types perform some kind of check, and either succeed or fail depending on whether the check passes or not. In some cases, a monitor can return a third result indicating that the server being checked is not installed or that the check that it is trying to perform is impossible.

Not all monitors are available on all operating systems. Because they use Linux specific files in /proc, the Free Memory and Network Traffic monitors are only available on that OS. The Load Average type can only be used on systems that support the Running Processes module, and the Disk Space monitor will only work on systems that the Disk and Network Filesystems module has been ported to.

In addition, many monitors depend upon other Webmin modules. For example, if the Apache Configuration module has been deleted from your Webmin installation, you will not be able to use the Apache Webserver monitor type. If you attempt to add a new monitor that depends upon a module that is not installed or will not work on your operating system, an error message will be displayed when the Create button is clicked.

Setting up scheduled monitoring

The monitors that you can configure using this module are most useful when they are run on schedule, so that you can be automatically notified via email if a monitored server or daemon goes down. When scheduled checking is enabled, all your monitors will be run at a periodic interval, just as they are all run when you visit the module's main page.

To set up scheduled monitoring, the steps to follow are:

1. On the module's main page, click on the Scheduled Monitoring button below the table of monitors. This will take you to the form shown in the screenshot below.
2. Change the Scheduled monitoring enabled? field to Yes.
3. The Check every *field controls when the scheduled check is run. The first lets you set the period, such as every 1 hour or 5 minutes, while the second part controls how many hours or minutes into the period it is run. For example, to have the monitors checked at 3:00am every day, you would set the *Check every *field to 1 days, and the *with offset field to 3.
4. To limit the check to only certain hours of the day, de-select those hours that you don't want it to run on from the Run monitor during hours list. This does not make much sense if the scheduled check is being run only once per day.
5. Similarly, to limit the check to certain days of the week, de-select the days that you don't want it to run from the Run monitor on days list.
6. The Send email when field determines which events will cause an email message to be sent by the scheduled check. If When a service changes status is chosen, email will be sent when a service goes down or up. If When a service goes down is chosen, email will only be sent when a service is detected to have gone down. If Any time service is down *is chosen, email will be sent as long as any service is down, and will be sent again at each check until it comes back up. It is possible to override this field on a per-monitor basis using the *Check on schedule field on the monitor creation form.
7. To receive email when a service goes down, enter your address into the Email status report to field. If it is left set to Nobody, then no email will be sent.

8. To set the source address of the status email, change the From: address for email field. The default is just `webmin@_yourhostname_`.
9. By default, any status email will be sent by running the `sendmail` program on your system. To have it sent via an SMTP server on another system, change the Send mail via field to SMTP server and enter the hostname of the mail server into the field next to it.
10. If you want to receive on email for each monitor that goes down, change the Send one email per service? field to Yes. Otherwise all services that are determined to have failed by a single check will be reported in a single email.
11. If you have a pager command set up and working on the module's configuration, you can enter a pager number into the Page status report to number field. It will receive a shortened version of the message that is sent via email.
12. Click the Save button at the bottom of the page to activate scheduled monitoring. Webmin will automatically set up a Cron job that runs a script on the chosen schedule.

The screenshot displays the 'Scheduled Monitoring' configuration interface. On the left, there is a navigation menu with options like 'Webmin', 'System', 'Servers', 'Networking', 'Hardware', 'Cluster', and 'Others'. The main content area is titled 'Scheduled Monitoring' and contains the following settings:

- Scheduled background monitoring options**
- Scheduled checking enabled?** Yes No
- Check every** 1 hours with offset 0
- Run monitor during hours**: A grid of time slots from 00:00 to 23:00 in 1-hour increments.
- Run monitor on days**: A dropdown menu set to 'Sunday'.
- Send one email per service?** Yes No
- Send email when**: When a service changes status When a service goes down Any time service is down
- Email status report to**: Don't send email Email status report to `cameron@webmin.com`
- From: address for email**: Default (webmin) [text field]
- Send mail via**: Local mail server SMTP server [text field]
- Send SMS to**: Nobody Phone on carrier T-Mobile with number [text field]

At the bottom, there is a 'Save' button and a 'Return to service list' link.

Once scheduled monitoring is active, you should begin receiving email messages notifying you when services go down and come back up. However, if a service is down when scheduled checking is first enabled and you have chosen to be only notified when services go down or come up, you will not receive a message about it.

To modify any of the scheduled monitoring options, just repeat the steps above again. To turn it off altogether, change the *Scheduled monitoring enabled?* field to No and click Save. If you want to change the monitoring schedule, it is best to do it in this module instead of in the Scheduled Cron Jobs module covered in Scheduled Cron Jobs.

Module access control

You can grant Webmin user the right to only see the current status of configured monitors but not to create or edit them. This can be done in the Webmin Users module, which is covered in chapter 52. Once you have created a user who has access to the module, follow these steps to give him read-only access :

1. In the Webmin Users module, click on System and Server Status next to the name of the user or group that you want to restrict.
2. Change the Can edit module configuration? option to No, to prevent him changing display options.
3. Set the Can create and edit monitors? field to No, so that he can only view the status of existing monitors.
4. Set the Can change scheduled monitoring? field to No.
5. Click the Save button to make the module access control restrictions active.

Webmin Actions Log

Introduction to logging

When logging is enabled, Webmin will record every action taken using it that has some effect on your system, such as the creation of a user or the changing of an Apache setting. Pages that do not actually change anything on your system, such as those that just display icons, list users or show the current settings for some object will not write anything to the action log. In this way it is different to the separate CLF log file that Webmin writes to `/var/webmin/miniserv.log`, which records every single page visited and image loaded.

Most actions performed in Webmin change configuration files, run commands or execute SQL statements. When the recording of these file changes is enabled the details of each will be included in the actions log so that you can see exactly what Webmin did when you told it to create a Unix user or delete a DNS zone. This can be helpful for understanding what is really going on behind the scenes if you are new to system administration or want to see how actions are implemented. Not all modules perform action logging though, particularly those that are old or have been written by third-party developers.

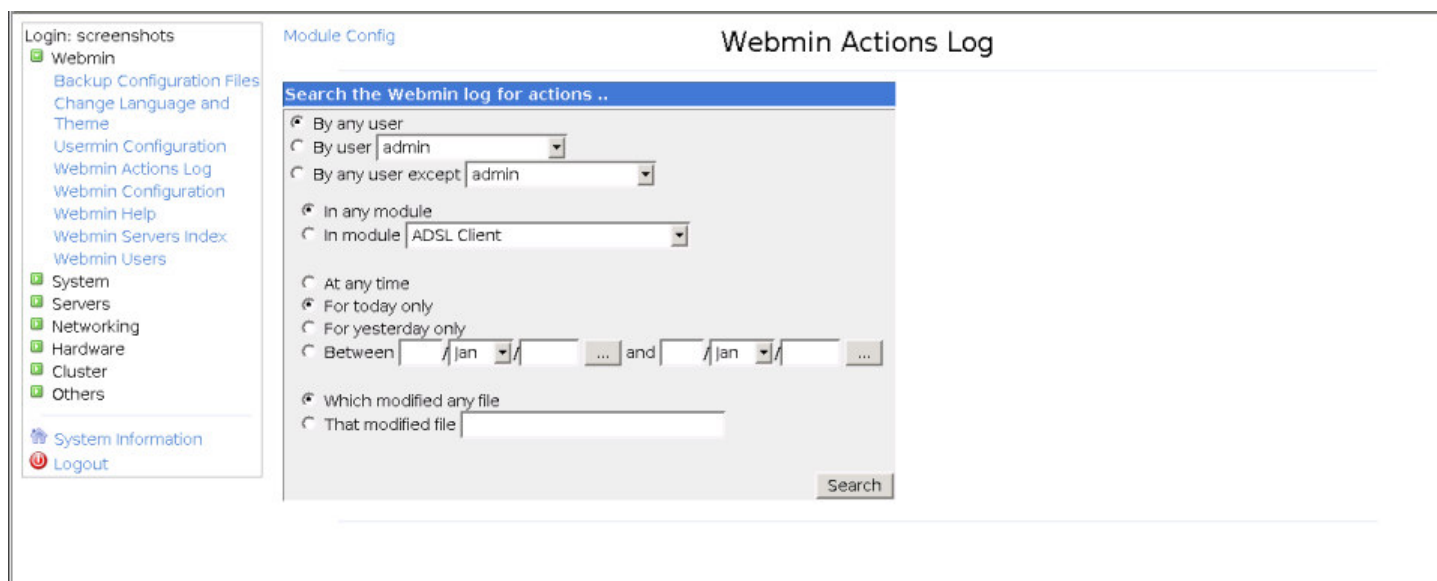
Basic action logging is enabled by default, but the recording of file changes is not. To gain the most benefit from the Webmin Actions Log modules, file changes should be logged as well. This will slow down the program slightly though, and consume more disk space for recording the changes.

Some types of action will never have any associated file changes logged, even if this feature is enabled. Such actions might perform all their work with network connections, or modify a file so large that generating the differences between the old and new contents is impractical. Or file change logging may not have been implemented in the module at all.

The actual file in which actions are recorded is called `/var/webmin/webmin.log`. Its format is unique to Webmin, but records the details of each action on a separate line in a simple text format. If the logging of file changes is enabled the directory `/var/webmin/diffs` is used to store files containing the details of changes and commands used. Each file in this directory is named to match the ID of an action, and contains in diff format the changes made to one file.

If you are looking for the files in `/var/webmin` on your system and cannot find them, check in `/var/log/webmin` instead. Some packaged versions of the software created by other Linux distribution vendors use this alternate directory instead, to better fit in with the normal Linux log file layout.

The Webmin Actions Log module



The screenshot shows the Webmin interface for the 'Webmin Actions Log' module. On the left is a navigation menu with categories like 'Webmin', 'System', 'Servers', 'Networking', 'Hardware', 'Cluster', and 'Others'. The main content area is titled 'Webmin Actions Log' and contains a search form. The search form has a title 'Search the Webmin log for actions ..' and several options:

- By any user
- By user
- By any user except
- In any module
- In module
- At any time
- For today only
- For yesterday only
- Between and
- Which modified any file
- That modified file

A 'Search' button is located at the bottom right of the search form.

This simple module exists solely for viewing action logs created by Webmin. It can be useful for finding out what a particular user is up to, or who has been doing what in some module. On a system with multiple administrators, tracking down who broke a particular server's configuration could ordinarily be tough but this module makes it relatively easy.

The module can be found under the Web Admin category on the main menu, and clicking on its icon will bring up the search page shown in the image below. Before you can view the details of a particular action, it must be found using the search form.

Displaying logs

The form on the module's main page lets you find actions using three different search criteria. Only actions that match all three will be displayed, rather than those that match any one of the criteria. You can find actions by the Webmin user that performed them, the module they were carried out in and the date and time that they occurred.

The steps to follow are:

1. In the first section of the form, select By user and if you want to display only actions by a particular user, and choose it from the adjacent menu. To instead exclude some user's actions from your search, use the By any user except option instead. To include all users in the search choose By any user.
2. In the second section, to limit the search to actions performed in some module choose In module and select it from the menu. Only modules that are currently installed will be listed. To search all modules' actions select In any module instead.
3. The final section determines which date range an action must fall into to be included in the results. If Between is chosen you can select or enter one or two dates using the fields next to it. If the first date is omitted, all actions up to the second date will be included. Similarly if the second date is missing, all actions from the first date onwards will match. If For today only is selected, only actions that have occurred during the current local time day will be included in the result. If At any time is chosen, the date on which an action occurred will be ignored.
4. Hit the Search button to display a page of actions that match the chosen criteria. This may take a few seconds to display if your Webmin log is large. If any were found, the resulting page will provide a short description for each action (such as Created user fred), the module it comes from, the Webmin user responsible, the client system he was connected from and the date and time it occurred.
5. Click on the description in the Action column to go to a page showing more details about the action. If logging of file changes was enabled at the time it occurred, the changes made to any files by the action will be shown as well, along with any commands executed or SQL statements run. Only actions from the MySQL? and PostgreSQL? modules will include SQL statements, used to do things like creating a table or modifying a column.
6. When Webmin is in session authentication mode, a Session ID field will be shown in this form. Clicking on the ID will bring up a list of all actions performed by the user in a single browser instance from the time he logged in till the time he logged out.

It is possible to display every single action logged on your system by leaving the options on the search form set to their defaults. However, this is likely to take quite a while to generate and produce a lengthy HTML page.

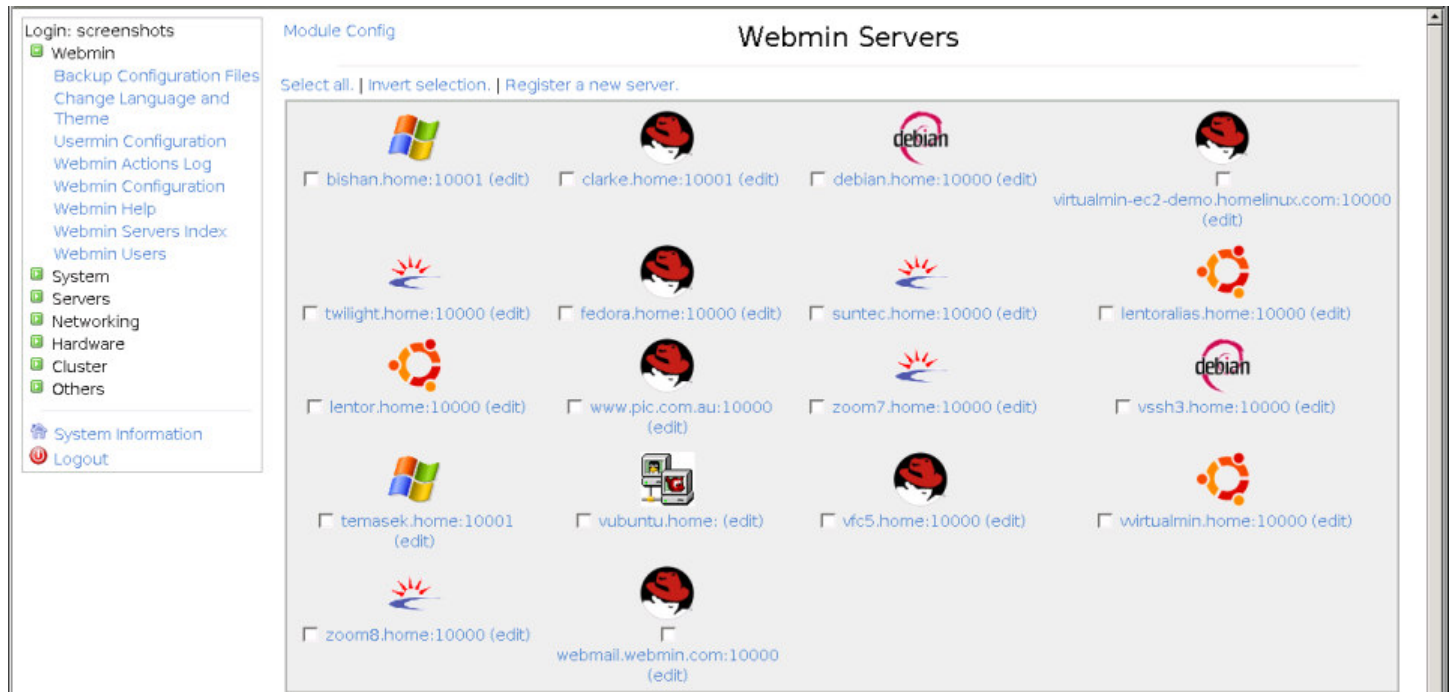
Webmin Servers Index

The Webmin Servers Index module

This module really serves two purposes, one simple and one quite complex. You can use it to create a master index of other systems running Webmin on your network, each of which is shown as an icon that you can click on to link to the server. Each icon can either be a normal link, or a 'tunnel' that logs you into another server automatically with all traffic sent via the first system.

As well, the module can be used to define systems which can be controlled by a master Webmin server, using the System and Server Status module and the modules in the Cluster category. Each of these other systems must also have Webmin installed, and a special RPC (Remote Procedure Call) protocol is used by the master to communicate with and control the slaves. How this all works is explained in detail in this chapter.

When you click on the module's icon in the Webmin category, a page like the one shown in the image below will be displayed. Most of the page is taken up with a table of icons, one for each of the other servers that you have added. Of course, if this is the first time the module has been used, no server icons will appear initially. At the bottom are buttons for automatically finding other Webmin servers on your local network.



Even though it was designed for creating an index of Webmin web servers, there is no reason that you cannot create icons for other types of web server instead. However, the module's RPC features will naturally only work when communicating with a host running Webmin.

Adding a Webmin server

To add a new server to this module, either to provide a link to it or so that it can be managed with one of the Cluster group modules, follow these steps:

1. Click on the Register a new server link on the main page above or below the existing icons.
2. In the Hostname field enter the Internet hostname or IP address of the other server, such as server.example.com.
3. In the Port field enter the port that Webmin is listening on, usually 10000.
4. From the Server type menu choose the operating system that the other host runs. This only sets the icon that will be used to represent the server.
5. If the other Webmin server is in SSL mode, select Yes in the SSL server? field. This option can only be used if the master system has the Net::SSLeay Perl module and the OpenSSL? library installed, so that it can make a client-mode SSL connection.
6. When the Description field is set to From hostname and port, the server's hostname and port number are shown under its icon on the module's main page. However, you can select the second option and enter an alternate description to be shown instead, such as Corporate Web Server.
7. Servers defined in this module can be categorized into groups for easier addition in the Cluster category modules. In the Member of server group field you can select one of the following options :
 - *None *The system you are adding will not be in any group.
 - *Existing group *If some groups have already been defined, this server will be in the group selected from the menu next to this option. If no groups exist yet, this option will not even appear.
 - *New group *The server will be added to the new

group whose name you enter in the adjacent text field. A group will cease to exist as soon as all the of servers in it have been deleted or changed to another group.

8. The Link type field is possibly the most important on this form, as it determines if the new server can be used in the Cluster modules and System and Server Status module. It also determines if the icon is a normal link, or a tunnel. Your options are: *Normal link to server *RPC calls cannot be made to the other server, and its icon on the module's main page will just be a normal web link. If the system is running some other webserver specified port you should select this option. *Login via Webmin with username *This option must be chosen if you want to use Webmin's RPC features to control this server, such as with the Cluster category modules. If selected, you must enter a username and password for Webmin on the remote host into the fields next to it. The user should be root or admin, as other Webmin users are not by default allowed to receive RPC calls unless specifically authorized. RPC can be used to run any command or modify any file on a server, which is why access to it must not be granted to un-trusted Webmin users. If this mode is chosen, the server's icon on the main page will be a tunnel that automatically logs whoever clicks on it into the remote server as the specified user. *Login when icon is clicked on *If this option is chosen the server cannot be used for RPC, but its icon will still be a tunnel to the remote host. However, when first clicked on it will prompt the user for a login and password for the remote system, which will be stored in a cookie in the user's browser. This option is handy if you want various users to be able to to make use of the tunnelling feature, but still login to the remote system as themselves.
9. If Login via Webmin with username was selected above, the Make fast RPC calls? field determines if the new fast RPC protocol will be used, or the older slow protocol. You can either select Yes to force the use of fast mode, No to force slow mode or Decide automatically to have Webmin use fast mode only if it is available. If the automatic option is chosen and the server cannot be contacted or logged into, an error message will be displayed when you hit the Create button later. Versions of Webmin before 0.89 did not support the fast protocol, but most systems should have been upgraded beyond that by now. Generally you will want to use the faster mode all the time, unless a firewall is blocking the direct TCP connections that it uses. See the 'How RPC works' section later in the chapter for more details on the differences between the two modes.
10. Finally, hit the Create button to add this new server. As long as there were no errors in the form you will be returned to the module's main page, which should include a new icon.

The icons for servers not created in Normal link to server mode will actually be links to a program on this master server that connects to the remote system for you. This can actually be useful if your master server is accessible from the Internet but internal hosts are not, for example if you only have a single Internet IP address and are using NAT. When you access those internal servers by clicking on their icons in this module on the master system, your browser is only really connecting to the master server, which is then tunneling the requests though to the chosen slave.

On a Webmin system with multiple users you should be careful about giving access to this module to un-trusted users. Anyone who can click on an icon for a server in Login via Webmin with username mode will be connected to the remote system as the user specified for that server, not himself. This will probably allow him to do things with root privileges on that remote host that he would not be able to do on the master system.

The 'Module access control' section later explains how you can control which server icons a particular user can use, so that un-trusted people can be limited to those in the safe *Normal link to server* or *Login when icon is clicked *on modes.

Editing or deleting a Webmin server

Once a server has been added to this module you can edit all of its details or even delete it altogether. The steps to follow are:

1. On the main page, click on the (edit) link next to the name of the server that you want to change. This will bring up an editing form almost identical to the one for adding a server.
2. All of the fields can be edited, and have the same options and meanings as explained in the 'Adding a Webmin server' section. The only exception is the Make fast RPC calls? field, which will not have the

Decide automatically selection if the module has already worked out the RPC mode that the remote server supports.

3. Hit the Save button to activate your new settings. Or if you want to remove this server from the module, hit Delete instead. Any other modules (such as those in the Cluster category) that made use of this server will automatically remove it from their lists.

Using server tunnels

When you click on an icon for a Webmin server in one of the tunnel modes you will be connected to it via this master system. The user interface of the remote host will be almost exactly the same as if you logged in normally, except that every page will include a special Webmin Servers link. When clicked on this will take you back to the Webmin Servers Index module on the master system, which is more convenient than hitting the back button in your browser a few hundred times.

For tunnelling to work, the master server must analyze and modify the HTML sent back by the remote host that you are logging in to. Currently this works well for Webmin servers, but may fail if you are tunnelling through to some other web-based application or website that uses HTML not supported by this module. Symptoms of this include links pointing to non-existent pages on the master server, and images that are not loaded properly.

Clicking on the icon for a server *Login when icon is clicked *mode will initially display a login form for entering a username and password for the remote system. This will appear even if the remote host does not actually run Webmin on the chosen port, but can be used to login to any web server that uses standard HTTP authentication. After you login your username and password will be remembered until you either quit your browser (thus discarding the cookie), or click on the (logout) link that appears below server's icon on the module's main page.

Broadcasting and scanning for servers

If you have a large number of Webmin servers on your network, adding them one by one to this module can be tedious. There is a better way though - the master system can broadcast on your local LAN for other Webmin servers, or send requests to hosts within a specific network to probe for servers. Any found will be automatically added to this module, although only in Normal link to server mode. There is no way for the master system to automatically determine a login and password for a remote system as this would be a huge security hole if it were possible!

To find other Webmin servers, follow these steps:

1. If you only want to search your local LAN, click on the Broadcast for servers button at the bottom of the module's main page. To search some other network, enter its address into the field to the right of the Scan for servers button before hitting it. This must be a class C network, entered like 192.168.1.0.
2. A page listing the URLs of servers found will be displayed. New ones will have Found new server before their URLs, those already on the main page will have Found known server, and responses from the master system itself will have Found this server.
3. When the process is complete you can return to the main page, which will now contain an extra icon for each of the newly found servers. Then can be edited to switch to Login via Webmin with username mode to use them for RPC.

All versions of Webmin since 0.75 listen on UDP port 10000 for the broadcast and scan packets sent out by this module, and reply with their hostname, port number and SSL mode. A server will not be found if a firewall is blocking this port or if UDP listening has been turned off for security reasons.

How RPC works

RPC is a protocol that one Webmin system can use to control another. An RPC request is usually a call to a function in the library of some module, and includes the parameters to that function. However, there are other RPC request types for transferring data to and from a server, checking if a module is available, getting a

module's configuration and executing a piece of Perl code. This section explains the technical details of how it works, and can be skipped if you are not a programmer and is not having any trouble with RPC connections.

When you set up the System and Server Status module to fetch some status information from a remote system, an RPC call is made to functions in the same module on that system to determine if a service is up or down. Similarly, when a user is added in the Cluster Users and Groups module, multiple RPC calls are made to add him to the password file, create his home directory and copy files into it. Chapter 56 explains how to make use of RPC in your own modules, and what its limitations are.

As explained earlier, RPC has two different modes - fast and slow. Slow mode is simplest, as it uses an HTTP request from the master to the slave for each RPC function call, file transfer or request for information. All parameters, data and return values are included in that request and its response, and no other TCP connections are made. The advantage of this mode is that it can work through firewalls and proxies, as long as HTTP requests to port 10000 are allowed.

Apart from being slow, this mode has one big down-side - HTTP is a stateless protocol, but Webmin RPC calls are not stateless. It is quite possible for one function call to set a global variable that the next function call depends upon. This means that a background process in which state is kept must be started on the remote system for each master that opens an RPC session. But there is no way for a slave system to automatically detect when the master CGI program has finished and thus shut down the background process, because no direct connection between the two exists!

Webmin's solution is to have the process exit when the master makes a special RPC call, or after 30 seconds of inactivity. If a master CGI program does not invoke the `remote_finished` function the remote process will hang around consuming memory until the timeout elapses. If for some reason more than 30 seconds passed between RPC calls to the same host, the background process will exit and future RPC calls will fail.

The newer fast RPC protocol solves these problems using only one initial HTTP request to have a background process started on the remote system. The master server then makes a TCP connection to this process (which is listening on a free port), and sends RPC requests through that connection instead. When the master program exits this connection will be automatically torn down, and the remote background process will exit. No special function calls or timeouts are needed.

Fast RPC mode has much better support for transferring large files to and from remote systems. The slow mode attempts to encode files inside an HTTP request, which can fail if they are too large. The newer mode instead transfers them un-encoded through a separate TCP connection, which is quicker and far more reliable. The Cluster Software Packages and Cluster Webmin Configuration modules may fail when installing a large package in slow mode.

The only problem with fast mode is that some firewalls may block the TCP connection, which is typically made on a port 1 or 2 above the remote host's base Webmin port, such as 10001 or 10002. Multiple connections may be made if data is transferred with RPC, so any firewall on your network between the two servers must be configured to allow connections from the master to the remote host on ports in the range 10000 up to 10100.

Module access control

If you have more than one Webmin user on your system, you may want to make this module available to other people without giving them access to all server icons or the ability to add servers. This is useful if you want others to see only icons for servers not in Login via Webmin with username mode, thus turning the module into just an index of other systems on your network.

The first step is to assign this module to a user, as explained on Webmin Users. You can then restrict him to only being able to see and use the tunnels for certain servers by following these steps :

1. Click on Webmin Servers Index next to the name of the user or group in the Webmin Users module to bring up the access control form.

2. Change the Can edit module configuration? field to No, so that he cannot change the user interface for other people.
3. In the Can use servers field chose Selected and select the ones that you want to make visible from the list below.
4. Change the Can edit servers? and Can find servers? fields to No.
5. Hit the Save button to activate the new restrictions.

Hiding a server from a user in this module does not stop him from using it in other modules that make use of RPC.

Webmin Users

Introduction to Webmin users, groups and permissions

A standard, out-of-the-box Webmin installation has only one user (called root or admin) who can use every feature of every module. On a home or office system used by just one person, that is all you need. Even if your system has multiple users, there may be only one who needed to perform system administration tasks.

However, there are many situations in which the administrator may want to give some people access to a subset of Webmin's features. For example, you may have a person in your organization whose job it is to create and edit DNS zones and records. On a normal Unix system, this person would have to be given root access so that he can edit the zone files and re-start the DNS server when necessary. Unfortunately, once someone is able to login as root he has full control of the system and can do whatever he wants.

Webmin solves this kind of problem by allowing you to create additional users who can login, but only access a few modules. You can further restrict what the user can do within each module, so that he cannot abuse its features to perform actions that he is not supposed to. Because Webmin still runs with full root privileges even when used by a restricted user, it still has access to all the configuration files and commands that it needs.

Some examples of the kind of access control restrictions that you can set up are:

- Creating a user with the right to edit directives in only a few Apache virtual servers that he owns. Global settings or directives in other virtual hosts cannot be edited.
- Giving a user the rights to edit and create Unix users with UIDs within a certain range and with home directories under a restricted directory. Important system users such as root or bin cannot be edited or even viewed.
- Allowing a user access to only one MySQL? database, but not to other databases or user permissions. Similar access control can be set up for PostgreSQL? .
- Giving a user access to the Squid access control list, but not to other functions. The user could be allowed to apply his configuration changes, but not to start or stop the proxy server.
- Creating custom commands and then giving a user the rights to run only some of them, but not create or edit any.
- Allowing a user to view and cancel print jobs in the Printer Administration module, but not edit or create actual printers.

Many of these rights would be impossible to grant using command-line tools without giving root access to the entire system. Even programs like sudo are limited when it comes to allowing a user to edit only part of a file, or run a command with only certain arguments.

You must be very careful when granting access to un-trusted Webmin users though, as even a small mistake in the access control configuration may allow the user to edit arbitrary files on your system or run commands as root. All it takes is a small hole for an attacker to sneak through and take total control of your system. Webmin's access control capabilities give you the power to lock down users, but only if used properly.

Even though it is possible to create a user with access to only his own email, home directory and password, Webmin is not always the best way to provide this kind of single-user web interface. A superior program is

Usermin, which was developed by the same author and shares much of the Webmin code and user interface. It is designed to give each Unix user access to only those things that he would be able to access at the command line, such as his email, home directory files and GNUPG configuration. Usermin runs most of its code with the permissions of the logged-in user, so there is far less chance of a user doing things that he is not supposed to, or even gaining root access. See chapter 47 (Usermin Configuration) for more details on how you can manage Usermin from within Webmin.

The Webmin Users module

If you want to create, edit or grant permissions to a Webmin user or group, it must be done in this module. When you enter it from the Webmin category, the main page displays all users and groups on your system and the modules that they have access to, as shown in the image below. If a user is a member of a group, his membership and only those modules that did not come from the group will be shown.

On a normal Webmin system, only the root or admin user that you login as will appear, which access to all modules that are supported on your operating system.

Creating a new Webmin user

If you want to create a new user who can login to Webmin, possibly with limited privileges, it must be created in this module. The steps to do this are:

1. On the module's main page, click on the Create a new Webmin user link above or below the list of existing users. This will bring up the creation form shown in Figure 52-2.
2. Enter a login name into the Username field. The name cannot be already in use by any other user or group.

3. To make the user a part of a group, select it from the Member of group field. Any modules that the group has will be granted to the user in addition to modules that you select on this page, and any access control restrictions that apply to the group in those modules will apply to the user as well. See the Creating and editing Webmin groups section for more information on how to add new groups to the list.
4. To give the user a normal password, select Set to from the menu in the Password field and enter it into the adjacent field. If the new user has the same name as a Unix user, you can select Unix authentication instead to have Webmin use PAM or read the /etc/shadow file to validate the user. To prevent the user from logging in at all, select No password accepted. This might be a good idea when creating a user who will have limited privileges, so that he cannot login until you have finished restricting his access.
5. To have Webmin use a different language for the user than the global default, select one from the Language field menu.
6. In most themes, module icons on Webmin's main page are displayed under categories. If this new user is going to be granted access to only a few modules, this is not really necessary and so you can change the Categorize modules? field to No.
7. To have the Webmin user interface displayed using a different theme for the user, set it in the Personal theme field.
8. To limit the addresses from which the new user can login to Webmin, change the IP access control field to Only allow listed addresses. Then fill in the text box next to it with hostnames, IP addresses, network/netmask pairs or wildcard hostnames (like *.foo.com). Note that these restrictions are checked only after any global IP access control set in the Webmin Configuration module have been passed.
9. Select all the modules that you want the user to have access to in the Modules section.
10. When done, click the Save button to have the new user created. You will be returned to the module's main page, and he will be able to login immediately.

The screenshot shows the 'Create Webmin User' configuration page. The 'Webmin user access rights' section includes fields for Username, Password (with a dropdown menu), Member of group (set to '<None>'), SSL certificate name, Language (set to 'Afrikaans (AF)'), Categorise modules? (set to 'Default'), Inactivity logout time (set to 'Default'), and Personal theme (set to 'Old Webmin theme'). The 'IP access control' section has radio buttons for 'Allow from all addresses', 'Only allow from listed addresses', and 'Deny from listed addresses'. The 'Allowed days of the week' section has radio buttons for 'Every day' and 'Only selected days ..', with checkboxes for Sunday through Saturday. The 'Allowed times of the day' section has radio buttons for 'Any time' and 'From [] : [] to [] : []'. The 'Modules' section is titled '(In addition to modules from group)' and includes a 'Select all Invert selection' link. It lists modules under three categories: Webmin (Backup Configuration Files, Teacher Logins, Webmin Actions Log, Webmin Help, Webmin Users, Change Language and Theme, Usermin Configuration, Webmin Configuration, Webmin Servers Index), Virtualmin (AWstats Reporting, Virtualmin LDAP, Virtualmin Mailman Mailing Lists, Virtualmin MySQL Users, Virtualmin Password Recovery, Virtualmin Protected Directories, Virtualmin SQLite Databases, Virtualmin System Manager, Virtualmin Virtual Servers (GPL), Virtual Server Signup, Virtualmin Mailbox Signup, Virtualmin Message of the Day, Virtualmin Oracle Databases, Virtualmin PowerDNS, Virtualmin Qmail+LDAP, Virtualmin SubVersion Repositories, Virtualmin Virtual Servers), and System (Bootup and Shutdown, Disk Quotas, FTP Backup, LDAP Client, Change Passwords, Disk and Network Filesystems, Filesystem Backup, LDAP Users and Groups).

To further restrict what the new user can do in each module that you have granted him access to, see the [*Editing module access control*](#) section below.

You can speed up the process of creating a new user who has the same attributes and access permissions as an existing user by using the module's cloning feature. To clone a user, the steps to follow are:

1. Click on the username of the existing user that you want to clone on the module's main page.
2. Click on the Clone button at the bottom of the editing form. This will take you to the creation form shown in Figure above, but with most fields already filled in with the attributes of the original user.
3. Fill in the Username field and set the Password, as they do not get copied from the cloned user. You can also adjust the values in any of the other fields.
4. When done, click the Create button. The new user will receive a copy of all module access control settings from the original user, but they will not be updated if the original user is changed in future.

If you want to create many users with access to the same modules and the same access control settings, it is better to create a group and assign the users to it. That way you can change the settings for all members at once by just editing the group.

Editing a Webmin user

You can change the username, password, language or any other attribute of a Webmin user (including the one you are logged in as) using this module. To edit a user, the steps to follow are:

1. Click on his username on the module's main page. This will bring you to an editing form, similar to the one shown in the image above.
2. By default, the password will be left unchanged. To edit it, select Set to *from the *Password field menu and enter a new password into the field next to it.
3. Change any of the other fields on the form, as explained in the Creating a new Webmin user section. You can even move the user to another group, which will cause him to lose access to all modules in the original group and gain access to those in the new group. If you are editing yourself, Webmin will not allow you to take away access to the Webmin Users module. This is to protect you from locking yourself out of the module and not being able to grant yourself access back again.
4. When you are done, click the Save button to have the changes applied immediately. If the username or password was changed and the user is currently logged in and Webmin is not in session authentication mode, he will have to login again.

You can delete a user by clicking the Delete button at the bottom of the editing form, which will also take effect immediately. Webmin will not allow you to delete yourself though.

Editing module access control

Many Webmin modules allow you to further restrict the actions that each user can perform using them. The actual access control options are different for each module, and are documented in detail in the Module access control section of the page that covers it. This section only describes the common process that you need to follow to configure what a user (or group) can do with a particular module :

1. On the Webmin Users main page, find the user or group that you want to restrict and click on the name of the module next to his name that you want to edit the restrictions for. This will bring up the access control editing form, an example of which is shown in the image below. That screenshot is from the Users and Groups module, so if you select a different module the available options will not be the same.
2. To stop the user from changing the module's configuration, set the Can edit module configuration? field to No. This should always be done, as in most modules the configuration settings could be changed to allow the user to gain root access or otherwise escape the access control restrictions that you have set up.
3. Change other options on the form to restrict the user in whatever way you wish. Each module covered in this book has a section in its chapter that explains exactly what the fields mean, and gives examples of how to set up common types of access control.
4. Click the Save button to make your changes immediately active and return to the module's main page.

The module access control form for Users and Groups

Not all modules allow you to limit what a user can do, as it would not make any sense. For example, the Software Packages module does not allow access control restrictions to be configured. Its primary purpose is the installation of new packages, and any user with the rights to install a package could build and install his own that gives him root access. In modules like these, only the Can edit module configuration? Option appears on the access control form. For modules that have no options other than this, there is no Module access control section in their chapter of the book.

At the start of the list of modules next to every user is an entry called Global ACL. If you click on this, it will take you to an access control form that allows the editing of restrictions that apply in all modules. The fields and their meanings are:

- Root directory for file chooser *There are many fields in Webmin for entering a file or directory name, and next to most of them is a button that pops up a simple fill chooser window. Users will not be able to use this file chooser to list directories outside whatever path you enter into this field. By default, it is set to / so that the entire Filesystem can be browsed. This option only controls which directories can be browsed using the file chooser. A user can still enter ANY path into a filename field manually, unless the module has its own access control restrictions.
- Users visible in user chooser *In most Webmin modules when a username field is displayed, next to it is a button that pops up a window for selecting either a single or multiple users. This option allows you to control which users appear in that pop-up window, so that a particular Webmin user cannot see all of the Unix users on your system. This access control option does nothing to stop the user from manually entering any username that he chooses - it just limits that list that appears in the pop-up window.
- Groups visible in group chooser *This option works in exactly the same way as the one above, but applies to the pop-up group selection window instead.
- Can send feedback email? *When using the Webmin theme that is enabled by default, a Feedback button appears on every page in the upper-right corner. Changing this option to No will remove the button, while changing it to Yes, but not with config files will prevent the user from sending feedback with the *Include module configuration in email* option selected. Because all feedback goes to the author of Webmin by default, disabling it makes sense for users other than the master administrator.
- Can accept RPC calls? *Webmin has its own RPC (remote procedure call) mechanism that is used by the cluster modules, System and Server Status and others modules. Any client program that makes an RPC call to a Webmin server must first login as a normal user using a web browser client would. However, an RPC client can access all of the features of Webmin, edit arbitrary files and execute commands as root - regardless of any access control settings. For this reason, users without full access to Webmin should have this option set to No. The default is Only for root or admin, which means that only if the user is called root or admin can it be used to login for RPC. Because the root and admin users typically have full access to Webmin anyway, this is not a security problem. However, if you create a new user with one of these two names and grant only limited Webmin access, make sure this option is set to No.

For almost all Webmin users, even those that are granted only limited access to some modules, the default Global ACL options will work fine and do not need to be changed.

Creating and editing Webmin groups

If you want to create a large number of users who will all have access to the same modules with the same access control options, the best solution is to create a Webmin group. Like users, groups have access to a subset of the available Webmin modules and have access control permissions in those modules. If you change the available modules or permissions for a group, those of all member users will change as well.

A group can itself be a member of another group, which it will inherit all allowed modules and access control settings from. If parent group is changed in any way, those changes will flow through to all member groups and their member users. There is no limit to the number of levels of group nesting that you can create.

To create a new group, the steps to follow are:

1. On the Webmin Users module main page, click on the Create a new Webmin group link near the bottom of the page under the Webmin Groups section. This will take you to the group creation form shown in Figure below.
2. Fill in the Group name field with a unique name that is not used by any other existing user or group.
3. To make this new group a member of an existing one, select it from the Member of group menu.
4. Select all the modules that you want members of this group to have access to from the Members' modules list. Those from any parent group will be automatically included.
5. Click the Save button to have the new group created, and your browser returned to the module's main page.
6. Configure access control settings for members of the group by clicking on module names next to the group name on the main page, as described in the Editing module access control section above.
7. You can now create new Webmin users or edit existing ones to become members of the new group.

The screenshot displays the 'Create Webmin Group' form. The 'Members' modules' section is as follows:

Members' modules	Member of group
Webmin	
<input type="checkbox"/> Backup Configuration Files	<input type="checkbox"/> Change Language and Theme
<input type="checkbox"/> Teacher Logins	<input type="checkbox"/> Usermin Configuration
<input type="checkbox"/> Webmin Actions Log	<input type="checkbox"/> Webmin Configuration
<input type="checkbox"/> Webmin Help	<input type="checkbox"/> Webmin Servers Index
<input type="checkbox"/> Webmin Users	
Virtualmin	
<input type="checkbox"/> AWstats Reporting	<input type="checkbox"/> Virtual Server Signup
<input type="checkbox"/> Virtualmin LDAP	<input type="checkbox"/> Virtualmin Mailbox Signup
<input type="checkbox"/> Virtualmin Mailman Mailing Lists	<input type="checkbox"/> Virtualmin Message of the Day
<input type="checkbox"/> Virtualmin MySQL Users	<input type="checkbox"/> Virtualmin Oracle Databases
<input type="checkbox"/> Virtualmin Password Recovery	<input type="checkbox"/> Virtualmin PowerDNS
<input type="checkbox"/> Virtualmin Protected Directories	<input type="checkbox"/> Virtualmin Qmail+LDAP
<input type="checkbox"/> Virtualmin SQLite Databases	<input type="checkbox"/> Virtualmin SubVersion Repositories
<input type="checkbox"/> Virtualmin System Manager	<input type="checkbox"/> Virtualmin Virtual Servers
<input type="checkbox"/> Virtualmin Virtual Servers (GPL)	
System	
<input type="checkbox"/> Bootup and Shutdown	<input type="checkbox"/> Change Passwords
<input type="checkbox"/> Disk Quotas	<input type="checkbox"/> Disk and Network Filesystems
<input type="checkbox"/> FTP Backup	<input type="checkbox"/> Filesystem Backup
<input type="checkbox"/> LDAP Client	<input type="checkbox"/> LDAP Users and Groups
<input type="checkbox"/> Log File Rotation	<input type="checkbox"/> MIME Type Programs
<input type="checkbox"/> MON Service Monitor	<input type="checkbox"/> PAM Authentication
<input type="checkbox"/> PostgreSQL Backup	<input type="checkbox"/> Qmail LDAP Users
<input type="checkbox"/> Running Processes	<input type="checkbox"/> Scheduled Commands
<input type="checkbox"/> Scheduled Cron Jobs	<input type="checkbox"/> Security Sentries
<input type="checkbox"/> Software Packages	<input type="checkbox"/> SysV Init Configuration
<input type="checkbox"/> System Documentation	<input type="checkbox"/> System Logs
<input type="checkbox"/> System Logs NG	<input type="checkbox"/> Users and Groups
Servers	
<input type="checkbox"/> Apache 2.2.0	<input type="checkbox"/> Apache Webserver
<input type="checkbox"/> BIND DNS Server	<input type="checkbox"/> CVS Server
<input type="checkbox"/> DHCP Server	<input type="checkbox"/> Dovecot IMAP/POP3 Server
<input type="checkbox"/> Fetchmail Mail Retrieval	<input type="checkbox"/> Firewall Configuration
<input type="checkbox"/> Frox FTP Proxy	<input type="checkbox"/> Jabber IM Server
<input type="checkbox"/> Majordomo List Manager	<input type="checkbox"/> Manage HTTPasswd File
<input type="checkbox"/> MySQL Database Server	<input type="checkbox"/> OpenSLP Server
<input type="checkbox"/> Postfix Configuration	<input type="checkbox"/> PostgreSQL Database Server

Once a group has been created, it can be edited by clicking on its name from the table under Webmin Groups on the module's main page. This will take you to the group editing form on which you can change any of its attributes, before applying them with the Save button. Or you can delete the group altogether with the Delete button, as long as it does not have any member users or groups.

Requesting a client SSL key

Normally, users authenticate themselves to Webmin with a username and password. However, if you are running in SSL mode and using a modern browser like IE or Netscape, it is possible to set up Webmin to authenticate you via a client-side SSL key instead. Usually an SSL web server sends its certificate to the client for authentication purposes, but the protocol also allows clients to send their certificates to the server as well.

The advantages of this method are that there is no need to remember a username and password any more, and that the old method of authentication can be disabled so that only clients with the SSL key can connect. Attackers thus cannot break in by guessing your password, or looking over your shoulder as you type it. Some browsers even support the storage of SSL keys on removable smart cards, which is even more secure.

Before a client key can be issued, Webmin must be switched to SSL mode and a certificate authority key generated. Once this is done, the steps to request a key are:

1. Login to Webmin as the user that you want to create a key for, using the browser that the key should be stored in. Browsers keep a list of client-side keys, usually protected by some password that must be entered only once when a key is first needed. It is usually possible to export keys to another browser of the same type though.
2. Go to the Webmin Users module, and click on the Request an SSL Certificate icon at the bottom of the page.
3. The form that appears will be different depending on whether you are running IE or Netscape. The following instructions apply to Netscape and Mozilla, as they are the most common browsers on Unix systems.
4. Enter a name into the Your name field, such as Joe Bloggs.
5. Enter your email address into the Email address field, such as joe@example.com.
6. If your Webmin system is on a company or organization network, fill in the Department and Organization fields. Otherwise, they can be left blank.
7. Enter the state your system is in into the State field, such as California.
8. Enter a two letter country code like US into the Country code field.
9. From the Key size menu select the number of bits in the SSL key that will be created. The higher the number, the more secure, but the longer it will take to be authenticated. 1024 bits should be secure enough for anyone.
10. Click on the Issue Certificate button. Your browser should pop up a window showing the key generating progress, which is done on the client system. When it is complete and have been send back to Webmin, a success page will be displayed.
11. Click on the pick up your certificate link to store the newly generated and signed key in your browser. You may be asked by the browser for a password to secure your certificates.
12. To test that everything worked, logout of Webmin and quit your browser. The re-run it and attempt to connect, the login page should be bypassed, and the main menu displayed. The text SSL certified should appear next to your username in the browser's status bar.
13. Once SSL client authentication is working, you may no longer want clients to be able to login as this Webmin user with a username and password. To enforce this, go to the Webmin Users module, click on your username, select No password accepted from the Password menu and hit Save.

Viewing and disconnecting login sessions

When Webmin is in session authentication mode (as it is by default), it keeps track of all currently logged-in users. You can view this information and cancel sessions that seem to be invalid by following these steps:

1. Click on the View Login Sessions icon at the bottom of the Webmin Users module main page.
2. On the page that appears, the ID, login name and connection time of each active session will be listed, with the newest shown first. It is quite possible for several sessions to exist for the same user, as many people do not bother to properly logout of Webmin. However, old sessions will be automatically removed after 1 week.
3. To view the actions performed in some session, click on the View logs link in the last column. This will take you to a list of actions in the Webmin Actions Log module, covered in chapter 54.

4. To cancel a session, click on its ID. This will immediately log the user out, but will not kill any CGI programs that Webmin is currently running for him.

Module access control

Interestingly, the Webmin Users module has its own set of access control options that can be used to determine which other users a particular Webmin user can edit. This is typically used to give a sub-administrator user the rights to create and edit only a subset of Webmin users, and to grant them access to only a few modules. To set up this kind of access, the steps to follow are:

1. In the Webmin Users module, click on Webmin Users next to the name of the sub-administrator you want to restrict.
2. Change Can edit module configuration? to No.
3. Set the Users who can be edited option to Selected users, and choose those accounts that you want the sub-administrator to be able to edit.
4. Change the Can grant access to field to either Selected modules, and choose from the list below the modules that the administrator is allowed to grant to new or edited users. There is not much point choosing modules that the sub-admin cannot already access.
5. Change Can rename users?, Can edit module access control?, Can request certificate?, Can configure user synchronization?, Can configure unix authentication?, Can view and cancel login sessions? And Can edit groups? To No. All the other yes/no fields can be set to Yes.
6. Change the Newly created users get field to Same module access control as creator. Because the sub-administrator is not allowed to edit the access control settings of modules that he grants to other users, they will always get the same settings that he does.
7. To force all new and edited users to be a member of a single group, change the Can assign users to groups field to Selected and choose the group from the list below. Or to prevent the sub-admin from choosing any group, select the <None> option. It may make sense for you to allow the creation of users who must be members of a group which has been set up with the appropriate restricted modules and permissions. If so, in step 4 you should not select any modules at all from the list so that only those from the group are available to created users.
8. Click the Save button to return to the module's main page.
9. If you are not forcing all new users to be a member of a particular group, make sure that the access control settings in other modules for the sub-administrator have been set correctly. They will be inherited by any new users that he creates.

The Webmin Users access control settings can also be configured to allow a user to change some of his own settings, but not edit other users or grant himself additional privileges. To set this up, the steps to follow are:

1. Click on Webmin Users next to the name of the user or group to whom you want to grant the rights to edit himself. Naturally, the user must have already been granted access to the module.
2. Change Can edit module configuration? to No.
3. Set the Users who can be edited option to This user.
4. Set the Can grant access to field to Selected modules, but do not select any from the list below. This will prevent the user from giving himself any additional module access.
5. Change Can request certificate?, Can change language?, Can change categorization? and Can change personal theme? to Yes, and all of the other yes/no fields to No.
6. Change Can edit groups? to No, and set Can assign users to groups? to Selected but do not select any from the list.
7. Finally, click Save. The Webmin user will now be able to use the module to change only his own password, language, theme and categorization mode, and request a client-side SSL certificate.

Read User Mail

This area Not done yet ... we ask your patience of ask support agent for guidance in using this module.