Sun Cobalt™ Control Station

Administrator Manual



Copyright © 1997-2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at `http://www.sun.com/patents` and one or more additional patents or pending patent applications in the U.S. and other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube and the Sun Cobalt logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communication Corporation in the United States and other countries.

Legato NetWorker is a registered trademark of Legato Systems, Inc. Linux is a trademark of Linus Torvalds.

Federal Acquisitions: Commercial Software -- Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright © 1997-2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303-4900 États-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient des droits de propriété intellectuelle sur la technologie réunie dans le produit qui est décrit par ce document. Ces droits de propriété intellectuelle peuvent s’appliquer en particulier, sans toutefois s’y limiter, à un ou plusieurs des brevets américains répertoriés à l’adresse `http://www.sun.com/patents` et à un ou plusieurs brevets supplémentaires ou brevets en instance aux Etats-Unis et dans d’autres pays.

Ce produit ou document est distribué avec des licences qui en restreignent l’utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l’autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l’Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d’autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube et le logo Sun Cobalt sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Netscape et Netscape Navigator sont des marques de fabrique ou des marques déposées de Netscape Communication Corporation aux Etats-Unis et dans d'autres pays.

Legato NetWorker est une marque déposée de Legato Systems, Inc. Linux est une marque de fabrique de Linus Torvalds.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

Part Number / Numéro de pièce : 070-00356-01
Date : 11-2001

Preface

This user manual is for anyone who will set up the Sun Cobalt Control Station for a group of users. You should be familiar with Microsoft Windows, Macintosh or other operating systems, and Netscape Navigator™, Microsoft Internet Explorer or other Web browsers.

This manual consists of the following chapters and appendices:

Chapter 1 — "Introduction" includes an overview of the Sun Cobalt Control Station.

Chapter 2— "Station Settings" explains the features available to the Server Administrator under the Station Settings tab.

Chapter 3— "Control Modules" explains the features available to the Server Administrator under the Control Modules tab.

Appendix A— "Licenses" lists licensing information.

Appendix B— "Glossary" provides a glossary of terms used in the Administrator manual for the Sun Cobalt Control Station.

Contents

Preface v

1 Introduction 1

Services on the Sun Cobalt Control Station 3
Sun Cobalt Control Station user interface 3
Icons 4
Online Documentation 4
Software Notification 5
Active Monitor 5
Logout 5
Online documentation 5
Resetting the Server Administrator password 6
Password guidelines 7
Support for RAID-1 8

2 Station Settings 11

Accessing the Sun Cobalt Control Station 12
Station Settings screen 14
Network Services 15
FTP 15
Basic Firewall 16
Firewall Safeguard 17
Applying changes to the settings 17
Configuring an external firewall 17
Confiiguring the Basic Firewall 18
Enabling the firewall feature 19
Configuring the firewall settings 19
Policy definitions 20
Viewing a chain of input rules 21
Changing the default policy for a chain 22

Adding an input rule 22
Modifying an input rule 24
Changing the order of input rules in a chain 26
Deleting an input rule 27
Overview of the Basic Firewall 27
Rules and chains 27
The lifecycle of a packet 28
SNMP 29
Telnet 30
System 31
TCP/IP 32
TCP/IP Settings 32
Modify static routes 34
Internet 35
Configuration for a gateway on a LAN 35
Power 37
Power down 37
Reboot 38
Time 38
Information 39
BlueLinQ 40
Software Notification icon 41
New Software 41
Check availability of new software 43
Install new software manually 43
Updates 45
Check availability of software update packages 46
Install software updates manually 47
Installed Software 48
Settings 49
Maintenance 51
Backup 51
Creating a backup 51
Viewing details of a scheduled backup 53
Deleting a scheduled backup 54

Backup file locations 54
Restore 55
Restoring with the backup history 55
Viewing details of a history item 57
Deleting a history item 57
Restoring a backup file manually 58
Disaster recovery 59
Usage information 60
Network 60
Active Monitor 61
Active Monitor icon 61
Status 61
RAID failure 63
Settings 65
Administrator 66
Account 66
Modifying account information 66
Email 67
Email forwarding 67
Vacation message 69

3 Control Modules 71

Control Modules screen 72
Selector window 74
Appliance Manager 75
Add Appliance 75
Adding a single server appliance 75
Importing a list of server appliances 76
Creating a list of appliances 77
Appliance Groups 79
List Groups table 79
Adding a group 80
Modifying a group 81
Viewing details of a group 81

Adding an appliance to a group 82
Removing an appliance from a group 82
Removing a group 83
Edit Appliance 83
Removing an appliance 83
Modifying an appliance 84
Events 85
View Tasks 85
Tasks table 85
View Events 87
Events table 87
Cleanup 88
Administer Modules 89
Administer 89
Installed Control Modules table 89
Adding a control module 90
Viewing details for a control module 91
Re-installing a module on an appliance 91
Removing a control module 92

A Licenses 93

The BSD Copyright 93
GNU General Public License 94
SSL License 100
Acme Public License 101

B Glossary 103

Introduction

The Sun Cobalt™ Control Station is a server appliance that allows administrators to take control of their Sun Cobalt servers: tracking and applying software updates, deploying new services, monitoring the health and performance of server appliances. More than just a typical "systems" management device, the Sun Cobalt Control Station is a platform that will help you in the "life-cycle" management of your Sun Cobalt servers, from initial setup through eventual redeployment at the end of useful life. As an added benefit, customers can continue to use third-party or homegrown software in conjunction with the Sun Cobalt Control Station.

Based on the Sun Cobalt RaQ™ 4r platform with RAID capabilities, the Sun Cobalt Control Station consists of two parts: a core framework that is the engine for executing control modules, and the built-in control modules themselves. These control modules can come from Sun Microsystems™, Inc., from third-party vendors or from you own in-house design team. The Sun Cobalt Control Station ships with four pre-installed modules: Appliance Inventory, Performance Monitoring, Software Management and Health Monitoring.

Through the Sun Cobalt Control Station, you can fully control the distribution of software payloads, offering customized and tailor-made services to downstream and end-user customers. Service Providers can offer unique payloads, data or software monitoring services. By leveraging the Sun Cobalt BlueLinQ technology, all available software updates and patches can be accessed and distributed to Sun Cobalt RaQ™ server appliances and Sun Cobalt Qube™ appliances, as designated by the administrator. Custom-built and third-party software can also be distributed. Furthermore, software packages can be "published" so that BlueLinQ-enabled clients—including other Sun Cobalt Control Station—can view and download these packages.

The Sun Cobalt Control Station can manage the following Sun Cobalt server appliances:

- Sun Cobalt RaQ 2, English and Japanese
- Sun Cobalt RaQ 3 and 3i, English and Japanese
- Sun Cobalt RaQ 4, 4i and 4r, English and Japanese
- Sun Cobalt RaQ XTR, English and Japanese
- Sun Cobalt CacheRaQ™ 4, English
- Sun Cobalt Qube™ 2, English and Japanese



Note: The Sun Cobalt Qube 2 appliance must have OS Update 2.0 installed.

- Sun Cobalt Qube 3, English and Japanese
- Sun Cobalt Qube 3, multilingual version

The Sun Cobalt Control Station does not manage the following Sun Cobalt server appliances or products:

- Sun Cobalt RaQ 1, English and Japanese
- Sun Cobalt Qube 2700, English and Japanese
- Sun Cobalt StaQware, English and Japanese
- Sun Cobalt NASRaQ, any versions
- any Sun Cobalt CacheRaQ appliance previous to the CacheRaQ 4

Services on the Sun Cobalt Control Station

Here is a sample of what you can do with the Sun Cobalt Control Station:

- **Inventory Management.** You can import and group from hundreds up to thousands of server appliances, as well as obtain detailed information on the appliances.
- **Software Management.** The Server Administrator can keep systems current using the version-tracking feature for software patches and updates. You can also deploy custom software or data.
- **Local Software Repository.** In conjunction with Software Management, you can use the local software repository to "publish" software packages and allow the Server Administrator or end users of various server appliances to install available software packages as desired or needed. You can configure your Sun Cobalt Control Station to view "published" software and share software with other BlueLinQ-enabled appliances.
- **Health and Performance Monitoring.** These control modules provide system alerts and the metrics of the basic operations of the server appliances, allowing you to pinpoint potential causes of failure.

These services can be used within an extranet or an intranet environment, or across the Internet.

Sun Cobalt Control Station user interface

You access the Sun Cobalt Control Station through a browser-based user interface (UI), known as the Server Dekstop. The Server Desktop UI consists of the **Station Settings** tab and the **Control Modules** tab.

For more information on these tabs, see Chapter 2, "Station Settings" and Chapter 3, "Control Modules".

Icons

There are four icons in the top right corner of the Server Desktop UI:



Note: Depending on the control modules that you have installed on the control station, there may be other icons displayed as well.

- Online Documentation
- Software Notification
- Active Monitor
- Logout

Online Documentation



You can access the user manuals in PDF format from the Server Desktop UI. If you have installed third-party software on the Sun Cobalt Control Station, the relevant documentation is also available.

To access the PDF file for a user manual, click on the *Online Documentation* icon in the top right corner. A separate browser window opens displaying a list of PDF files available. Click the link for a PDF file; you can open the PDF file in the browser window or save it to your personal computer.

Software Notification



The *Software Notification* icon allows you to check for new or updated software packages for the Sun Cobalt Control Station itself. The icon turns red when new or updated software packages are available.

For more information on installing software, refer to “BlueLinQ” on page 40.

Active Monitor



The *Active Monitor* icon allows you to view status information. The icon flashes red if any of the components or services monitored by Active Monitor fails or is under heavy use.

For more information on the Active Monitor feature, see “Active Monitor” on page 61.

Logout



Click the *Logout* icon to log out of the system.

Online documentation

To access the online documentation, see “Online Documentation” on page 4.

Resetting the Server Administrator password

When the Server Administrator password is cleared, the root account is not accessible until a new password has been assigned.



Caution: This function resets the Server Administrator password to blank.

After you clear the password, enter a new one as soon as possible to protect the security of the Sun Cobalt Control Station. At this point, anyone on the network can assign the Server Administrator password until you assign a new one.

If you forget the Sun Cobalt Control Station Administrator password, you can reset the password.

1. Push and hold the end of a paper clip in the recessed Reset Password button (located between the LCD screen and the LCD arrow buttons, on the front of the Sun Cobalt Control Station). Hold the button in for approximately 2 seconds.

   The LCD screen displays

   ```
   RESETTING ADMIN
       PASSWORD
   ```

2. Release the button.
3. Enter the following URL In your Web browser to access the Server Desktop UI of the control station.

   ```
   http://<hostname>.<domainname>/login/
   ```

4. If a prompt appears asking for a username or password, enter *admin* as the user name and “admin” as the password.



Note: The system automatically sets the *admin* password to “admin” when you use the Password Reset button.

5. Click **OK**. The Server Desktop UI appears.
6. Select **Station Settings > Administrator**. The "Account Settings - admin" table appears.
7. Enter a new password in the fields. Enter the password twice for confirmation.

   For more information on choosing a password, see "Password guidelines" on page 7.
8. Click **Save**. The screen refreshes.

Password guidelines

Use the following guidelines when choosing a password:

1. Use between three and sixteen alphanumeric characters.

   The valid characters include: a-z A-Z 0-9 % ! @ $ ^ & * - _ = \ | . , / ? ; : +
2. Use both upper- and lower-case letters.



Note: A password is case-sensitive.

3. Do not use a proper name.
4. Do not use a word found in a dictionary.
5. Do not use a date.
6. Do not use a UNIX® command word.
7. Do not use a string of consecutive keys on a keyboard (for example, "qwerty").

Support for RAID-1

A redundant array of independent disks (RAID) is a way of storing the same data in different places (thus, redundantly) on multiple hard disk drives. A RAID appears to the operating system to be a single virtual hard disk drive.

Redundancy means that there is protection against the failure of any single hard disk drive. Redundant data is used by a RAID system in the event of a failure; this redundant data can either be a mirror copy or parity data used to reconstruct the actual data.

There are a variety of different types and implementations of RAID, each with its own advantages and disadvantages. The Sun Cobalt Control Station implements RAID Level 1 (RAID-1), also known as disk mirroring, which consists of a primary hard disk drive and a secondary hard disk drive; the secondary hard disk drive is an exact copy or "mirror image" of the primary hard disk drive.

Although RAID can protect your data in case of a hard-disk-drive failure, it does not protect against operator and administrator (human) error, or against loss due to programming bugs.

The Sun Cobalt Control Station server implements RAID services through software. Each hard disk drive has its own independent master channel to allow high performance without extra RAID hardware.

You do not need to enable RAID-1 on the Sun Cobalt Control Station; it is enabled by default. You cannot disable RAID-1 on the Sun Cobalt Control Station.

There are two possible causes for RAID failure on the Sun Cobalt Control Station:

- **Hardware failure**. If a hard disk drive fails, the Sun Cobalt Control Station can function with one hard disk drive, but the server can no longer provide disk mirroring. To restore RAID service, you must shut down the Sun Cobalt Control Station and replace the failed hard disk drive.
- **Software failure**. The RAID software should not fail. If it does, the likely cause is a failure of the whole kernel, in which case the Sun Cobalt Control Station just reboots.

In case of a failed hard disk drive, you will have to replace the hard disk drive. For more information on replacing a hard disk drive, refer to the PDF *Maintaining and Upgrading the Hardware*.

For a failed drive, Active Monitor indicates that the Left or Right hard disk drive has failed ("Right" and "Left" are in relation to looking at server with the front blue panel facing you.)

If RAID fails on the Sun Cobalt Control Station, the system indicates the non-RAID status in a number of ways:

- An email is sent to the Administrator of the Sun Cobalt Control Station.
- The Active Monitor icon in the top right corner flashes red.
- On the screen **Station Settings > Active Monitor > Status**, the Disk Integrity (RAID) circle changes to red.
- The "C" logo badge on the front panel of the server appliance blinks.

Once you replace a failed drive on a Sun Cobalt Control Station and reboot the server, the system detects the new hard disk drive. It then automatically begins to synchronize the new hard disk drive to the existing hard disk drive so that the server will be able to provide disk mirroring.



Note: During the synchronization process, the Sun Cobalt Control Station cannot provide disk mirroring.

Station Settings

This chapter describes the administrative functions available under the **Station Settings** tab. The Server Administrator, with the user name *admin*, has full control of the Sun Cobalt Control Station. The Server Administrator can:

- enter the network settings
- enable or disable the various services
- perform maintenance functions
- receive system alerts and warnings by email



Note: In most of the short procedures in this chapter, the first step is to click the **Station Settings** tab in the top menu bar and the second step is to click on a selection from the left menu bar.

To reduce the number of steps in each procedure, the menu commands are grouped together and shown in **bold** type face. Right angle brackets separate the individual items.

For example, select **Station Settings > System > Time** means to click the **Station Settings** tab in the top menu bar, click the **System** menu category in the left menu bar and finally click the **Time** sub-menu item.

Accessing the Sun Cobalt Control Station

To access the Sun Cobalt Control Station:

1. Enter one of the following into your browser:

   ```
   http://<hostname>.<domainname>/login/
   ```

   or

   ```
   http://<IP_address>/login/
   ```

2. At the login screen that appears, enter the user name:

   ```
   admin
   ```

3. Enter the *admin* password.

4. If you want to establish a secure connection when you log in to the Sun Cobalt Control Station, click the "Secure Connect" check box. This establishes a Secure Sockets Layer (SSL) connection between your browser and the control station. Sun Microsystems™ recommends that you enable the secure connection so that any data sent to or received from the control station is encrypted.

   If your browser does not support SSL or has problems accessing the Sun Cobalt Control Station, try connecting without enabling the secure connection. Some browsers do not handle SSL properly and the only option is not to use SSL.

5. Click **Login**. If you enabled the Secure Connect option, your browser may prompt you to accept a self-signed certificate. This certificate is generated automatically for you and is required for SSL encryption. If you do not accept the certificate, you cannot use the Secure Connect option.



Note: The Sun Cobalt Control Station generates a self-signed certificate during configuration. A self-signed certificate encrypts the data but it does not authenticate the identity of the server at the other end of the connection.

For more information, see the entries for *Authentication*, *Encryption* and *Secure Sockets Layer* in Appendix B, "Glossary".

6. The **Control Modules** screen of the Server Desktop UI appears.
7. Click the **Station Settings** tab at the top. The **Station Settings** screen appears. See Figure 1.

Figure 1. Station Settings screen



Station Settings screen

The following bullet items represent the fully expanded menu on the left side of **Station Settings** screen. These are the functions and services that the Server Administrator can manage from this screen. They are explained in this chapter.

- Network Services (see “Network Services” on page 15)
  - FTP
  - Basic Firewall
  - SNMP
  - Telnet
- System (see “System” on page 31)
  - TCP/IP
  - Internet
  - Power
  - Time
  - Information
- BlueLinQ (see “BlueLinQ” on page 40)
  - New Software
  - Updates
  - Installed Software
  - Settings
- Maintenance (see “Maintenance” on page 51)
  - Backup
  - Restore
- Usage Information (see “Usage information” on page 60)
  - Network
- Active Monitor (see “Active Monitor” on page 61)
  - Status
  - Settings
- Administrator (see “Administrator” on page 66)
  - Account
  - Email

Network Services

This section describes the network services available on the Sun Cobalt Control Station.

- FTP
- Basic firewall
- SNMP
- Telnet

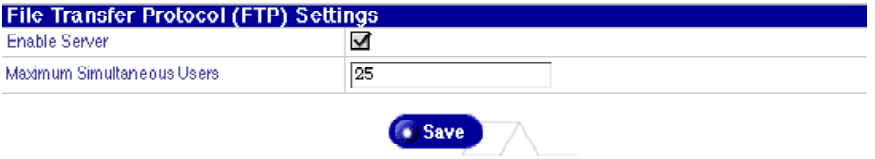
FTP

As the Server Adminisrator of the Sun Cobalt Control Station, you can enable the File Transfer Protocol (FTP) server and specify the number of simultaneous users.

By default, the FTP server is enabled. To configure the FTP settings for your control station:

1. Select **Station Settings > Network Services > FTP**. The" File Transfer Protocol (FTP) Settings" table appears; see Figure 2.

Figure 2. File Transfer Protocol (FTP) Settings table



2. Click the "Enable Server" check box.
3. Specify the maximum number of simultaneous users.
4. Click **Save**. The system saves the configuration and the screen refreshes.

Basic Firewall



Caution: Basic Firewall is an advanced feature of your Sun Cobalt Control Station. This feature is not recommended for novice users.

Check with your network administrator before configuring the Basic Firewall to ensure that your security rules are in line with you corporate security policy.

For more information on how the Basic Firewall feature works, see "Overview of the Basic Firewall" on page 27.

A firewall provides network security through a set of rules that restrict the flow of information between the Sun Cobalt Control Station and your network. It is also used to control the information that your control station allows to pass between different networks (such as your company's intranet and the public Internet).

On this screen, the Server Administrator can:

- enable and disable your firewall
- create and edit rules for the chain of input rules
- re-order your rules within each chain
- change the default policy for each chain

Firewall Safeguard

When enabling your firewall for the first time or applying changes to the configuration of the firewall currently functioning, the Sun Cobalt Control Station verifies that the Web browser that the you are currently using is still able to communicate with the Sun Cobalt Control Station after the firewall settings have been applied.

The purpose of this verification is to prevent the Server Administrator from accidentally misconfiguring the firewall and locking herself or himself out of the Sun Cobalt Control Station completely, rendering it inaccessible.

If, sixty seconds after the new firewall settings have been applied, the Sun Cobalt Control Station has not received any communication from the Server Administrator's Web browser, the control station automatically disables the firewall feature.

Applying changes to the settings

If you make changes to the Basic Firewall settings when the firewall is already enabled, the changes are not immediately reflected in the state of the firewall that is currently functioning.

You must click **Apply Changes Now** to make your changes take effect. The changes do not take effect in real time because that could cause the firewall to enter a temporary, insecure state while you are in the process of editing the firewall configuration.

If Basic Firewall is not enabled, the **Apply Changes Now** button is greyed out.

Configuring an external firewall

If you have an external firewall—which could be a router, a switch or any external product providing firewall functionality—between the control station and the managed appliances, you must leave open the following ports:

- For traffic from the control station to a managed appliance, you must leave open port 27000/tcp.
- For incoming traffic to the control station, you must leave open ports 80, 81 and 444/tcp.

Confiiguring the Basic Firewall

If you enable the Basic Firewall feature, at the minimum, you must create these five input rules so that the Sun Cobalt Control Station functions properly.

To add these rules, see “Adding an input rule” on page 22.



Note: For each rule, enter the information provided for the fields indicated. Leave all other fields blank.

As well as these five rules, change the default Policy to “Deny”. See “Changing the default policy for a chain” on page 22.

Rule 1

- **Destination Port Number(s)**. The low value is 1025; the high value is 65535.
- **Policy**. Accept

Rule 2

- **Destination Port Number(s)**. The low value is 444; the high value is 444.
- **Policy**. Accept

Rule 3

- **Destination Port Number(s)**. The low value is 80; the high value is 81.
- **Policy**. Accept

Rule 4

- **Source IP Address (Low)**. 127.0.0.1.
- **Source IP Address (High)**. 127.0.0.1
- **Policy**. Accept

Rule 5

- **Source IP Address (Low)**. Enter the IP address of the default gateway for the control station (see “Internet” on page 35).
- **Source IP Address (High)**. Enter the IP address of the default gateway for the control station
- **Network Protocol**. ICMP
- **Policy**. Accept

Enabling the firewall feature

To enable the firewall feature:

1. Select **Station Settings > Network Services > Basic Firewall**. The "Firewall Settings" table appears; see Figure 3.
2. Click to enable the check box "Enable Firewall".
3. Click **Save**. A popup window notifies you that you are about to enable packet filtering on your firewall.
4. Click **OK**.

Figure 3. Firewall Settings table



Configuring the firewall settings

To configure the Basic Firewall settings:

1. Select **Station Settings > Network Services > Basic Firewall**. The "Firewall Settings" table appears.
2. From the **Select Section** pull-down menu, select the option Input Rule Chain. The "Input Rules" table appears.

   The "Input Rules" table lists the IP filtering rules for the firewall currently functioning; see Figure 4. You can perform the following actions in the rules table:

   - Set the Default Policy for a rule chain. See "Changing the default policy for a chain" on page 22.
   - Click **Add** to add a new rule. See "Adding an input rule" on page 22.
   - Click the green *pencil* icon to edit a rule. See "Modifying an input rule" on page 24.
   - Change the order of the input rules. See "Changing the order of input rules in a chain" on page 26.
   - Click the red *trash can* icon to delete a rule. See "Deleting an input rule" on page 27.

- Click **Apply Changes Now** to apply rule changes to the firewall currently functioning. The **Apply Changes Now** button is greyed out until you modify rules that define your firewall.



Note: Your changes to the firewall rules do not take effect until you click the **Apply Changes Now** button.

3. After making changes in the "Firewall Settings" table, click **Save**.

Figure 4. Firewall Input Rules



Policy definitions

In the "Add Firewall Rule" and "Modify Firewall Rule" tables, the Server Administrator selects an action in the Policy pull-down menu. The policy determines the action taken if a packet matches the rule's criteria.

The following policies are supported:

- **ACCEPT** accepts the packet into the system. The packet "passes" the rule chain and no further rules within this chain are applied.
- **DENY** discards the packet. The packet is dropped from the system; the originator of the packet in not notified that the packet was discarded.
- **REJECT** rejects the packet. Like DENY, the packet is dropped from the system. However, unlike DENY, the sender of the packet is notified that the packet was discarded.
- **REDIRECT** redirects the packet to a local port number. Regardless of the port number or IP address to which the packet is actually addressed, the packet is instead routed to a port number on the Sun Cobalt Control Station itself. This port is specified in the "Redirect to Port Number" field. This feature is primarily used for features such as transparent proxy servers.

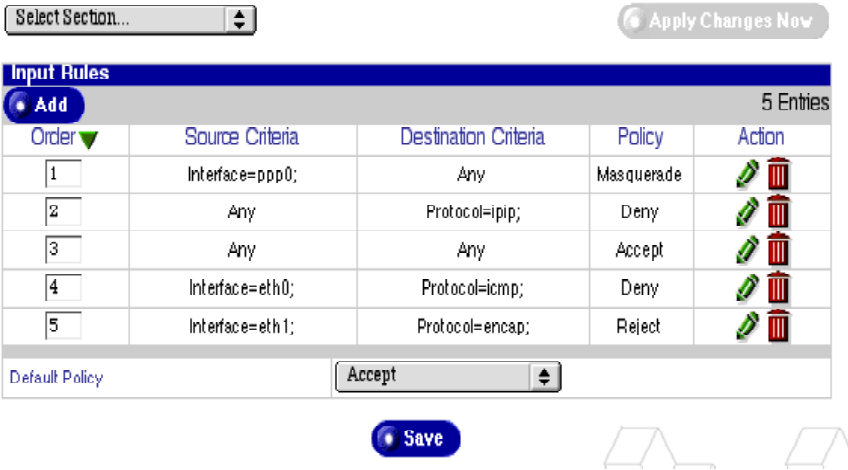
Viewing a chain of input rules

To view a chain of input rules:

1. Select **Station Settings > Network Services > Basic Firewall**.
   The "Firewall Settings" table appears; see Figure 5.
2. From the Select Section pull-down menu, select "Input Rule Chain".

   The "Input Rules" table for that chain appears, displaying the list of rules currently configured for that rule chain.

Figure 5. Sample of a list of Firewall rules



Changing the default policy for a chain

The default policy determines what happens to a packet that does not match any of the rules in the "Input Rules" table.

To change the default policy for a chain of input rules:

1. Select **Station Settings > Network Services > Basic Firewall**.
   The "Firewall Settings" table appears.
2. From the Select Section pull-down menu, select "Input Rule Chain".

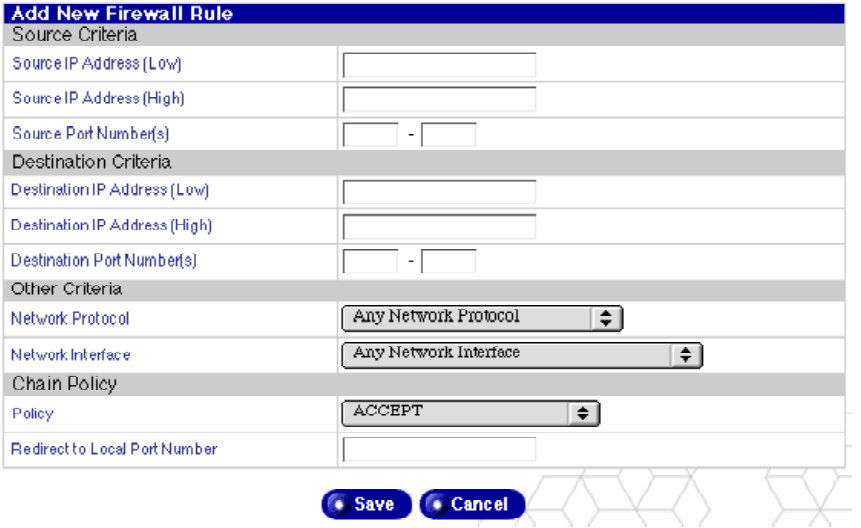
   The "Inpute Rules" table appears, displaying the list of rules currently configured for that rule chain.
3. In the Default Policy pull-down menu, select the default policy you want to apply to this rule chain. For more information, see "Policy definitions" on page 20.
4. Click **Save**.

Adding an input rule

To add an input rule:

1. Select **Station Settings > Network Services > Basic Firewall**.
   The "Firewall Settings" table appears.
2. From the Select Section pull-down menu, select "Input Rule Chain". The "Input Rules" table appears.
3. Click **Add**. The "Add New Firewall Rule" table appears; see Figure 6.

Figure 6. Add New Firewall Rule table



4. Configure the following settings:

- **Source IP Address (Low).** Enter the first or lowest source IP address in the range of IP addresses to be matched by this rule.
- **Source IP Address (High).** Enter the last or highest source IP address in the range of IP addresses to be matched by this rule.

  To match any source IP address, leave both the Low and High Source IP Address fields empty.
- **Source Port Number(s).** Enter the first and last source port number in the range of source IP addresses to be matched by this rule.

  To match any source port number, leave the Source Port Number fields empty.
- **Destination IP Address (Low).** Enter the first or lowest destination IP address in the range of IP addresses to be matched by this rule.
- **Destination IP Address (High).** Enter the last or highest destination IP address in the range of IP addresses to be matched by this rule.

  To match any destination IP address, leave both the Low and High Destination IP Address fields empty.

- **Destination Port Number(s).** Enter the first and last destination port number in the range of destination IP addresses to be matched by this rule.

  To match any destination port number, leave the Destination Port Number fields empty.

- **Network Protocol.** Enter the network protocol of the packets to be matched by this rule. The options are: Any Network Protocol, TCP, UDP, ICMP, IPIP and Encap.

- **Network Interface.** Enter the network interface of the packets to be matched by this rule. The options are: Any Network Interface, Primary Network Interface, Secondary Network Interface or PPP Dialup Interface.

- **Policy**. Select the policy for this rule chain. The policy determines the action applied to a packet that meets the criteria of this firewall rule. For definitions of the policies, see "Policy definitions" on page 20.

- **Redirect to Local Port Number.** If the REDIRECT policy has been selected, enter a local port number to which packets that meet the criteria of this firewall rule are redirected.

  If the REDIRECT policy has not been selected, this field is ignored.

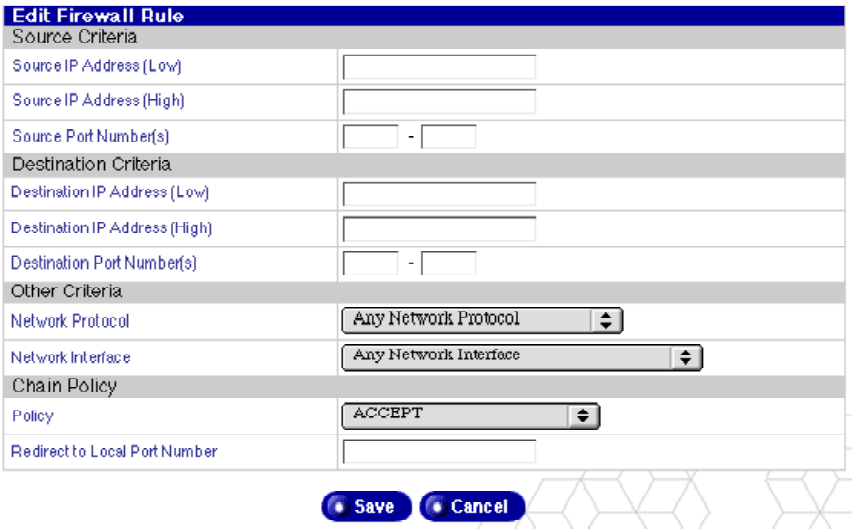
5. Click **Save**.

Modifying an input rule

To modify an input rule:

1. Select **Station Settings > Network Services > Basic Firewall**.
   The "Firewall Settings" table appears.
2. From the Select Section pull-down menu, select "Input Rule Chain". The "Input Rules" table appears.
3. Click the green *pencil* icon next to the rule you want to modify. The "Edit Firewall Rule" table appears; see Figure 7.

Figure 7. Edit Firewall Rule table



4. Modify one or all of the following fields. For a description of each field, see the procedure in "Adding an input rule" on page 22.
   - Source IP Address (Low)
   - Source IP Address (High)
   - Source Port Number(s)
   - Destination IP Address (Low)
   - Destination IP Address (High)
   - Destination Port Number(s)
   - Network Protocol
   - Network Interface
   - Policy
   - Redirect to Local Port Number
5. Click **Save**.

Changing the order of input rules in a chain

To re-order the input rules in a chain:

1. Select **Station Settings > Network Services > Basic Firewall**.
   The "Firewall Settings" table appears.
2. From the Select Section pull-down menu, select "Input Rule Chain". The "Input Rules" table appears.

   The first column in the table displays the order in which the system applies the firewall rules. Number 1 is the top-priority rule. For a sample chain of rules, see Figure 5.
3. To change the position of a rule in the hierarchy, simply enter the number of of the position that you want the rule to occupy in the small window in the first column.

   For example, let us say that a table holds five rules. If you want to move the rule at position 4 to position 2, enter "2" in the window for the rule at position 4.



Note: You can change the position of more than one rule at a time.

4. Click **Save**. The rules within this chain are sorted according to the values you entered into the Order column and the table refreshes with the re-numbered rules.

   Using the same example, the rule at position 4 now occupies position 2; the rule at position 2 shifts down to position 3 and the rule at position 3 shifts down to position 4. The rules at positions 1 and 5 do not shift.
5. If you have finished changing the order of the rules and your firewall is currently enabled, click **Apply Changes Now** so that your changes take effect in the firewall currently functioning.

Deleting an input rule

To delete an input rule:

1. Select **Station Settings > Network Services > Basic Firewall**. The "Firewall Settings" table appears.
2. From the Select Section pull-down menu, select "Input Rule Chain". The "Input Rules" table appears.
3. Click the red *trash can* icon next to the rule you want to delete. A confirmation dialog verifies the deletion.
4. Click **OK**.

Overview of the Basic Firewall

A firewall provides network security through a set of rules that restrict the flow of information between the Sun Cobalt Control Station and your network. It is also used to control the information that your control station allows to pass between different networks (such as your company's intranet and the public Internet.

When information is transmitted between the Sun Cobalt Control Station server and a network (for example, during an FTP file transfer or when fetching a Web page), the information is divided into small blocks of data called packets. Each packet contains a header which is used to direct the packet to its destination. The header contains information such as the destination address and source address of the packet, and indicates the software program that should receive the packet.

The Sun Cobalt Control Station ships with a type of firewall that allows you to accept or reject packets based on the information found in the header of a packet. This is known as an IP-packet-filtering firewall.

The type of IP-packet-filtering firewall implemented on the Sun Cobalt Control Station is the standard *ipchains* firewall system which is compiled into the Linux kernel. You can configure the ipchains firewall through the Server Desktop UI of the Sun Cobalt Control Station.

Rules and chains

A packet-filtering rule consists of a set of criteria, and an action to take if a packet matches the criteria (this action is called the rule's *policy*). Criteria for a rule can consist of items such as the machine from which the packet originated, the destination of the packet and the network interface through which the packet is moving. Typically, a rule's policy accepts or rejects the packet; if rejected, the packet is discarded from the system.

For the definitions of the policies, see "Policy definitions" on page 20.

Rules are organized into ordered lists called *chains*. When a chain of rules is applied, the firewall system tests the packet against each rule in sequence. If a packet meets the criteria of a rule, the action specified by the policy is taken; the packet is not evaluated against the subsequent rules. If a packet does not meet the criteria of a given rule, the packet is evaluated against the next rule in the chain.

Chains can also specify a default action to apply to packets that do not meet the criteria of any of the rules within the chain.

The Sun Cobalt Control Station allows you to configure chains of input rules, which are applied to packets at different stages of a packet's *lifecycle* within the Sun Cobalt Control Station. The *input* chain is applied against all packets entering the control station through a network interface.

The lifecycle of a packet

When a packet enters the Sun Cobalt Control Station server through a network interface, the firewall system applies the input chain against the packet before it is allowed to proceed any further into the system.

If the input chain rejects or denies the packet, the Sun Cobalt Control Station discards the packet.

If the input chain accepts the packet, the Sun Cobalt Control Station then passes the packet to a local process (such as the Web server on the control station).

Any packet entering the Sun Cobalt Control Station, destined for a local service on the control station, must pass the input chain of rules.

SNMP

You can specify the Simple Network Management Protocol (SNMP) communities that can have read-only and read-and-write access to this SNMP agent.

The default read-only access community is “public.”

The default read-and-write access community is “private.”



Note: Sun Microsystems recommends that you change the default string for the Read and Write SNMP Community to a unique value.

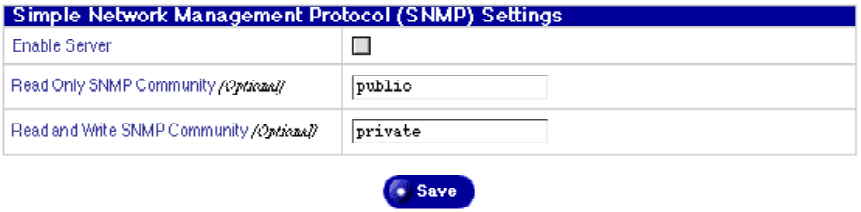
To specify the SNMP communities:

1. Select **Station Settings > Network Services > SNMP.** The “Simple Network Management Protocol (SNMP) Settings” table appears; see Figure 8.
2. Configure the following settings:
   - **Enable Server.** Click the check box to enable or disable the SNMP server.
   - **Read Only SNMP Community.** Enter the Read Only SNMP Community to which this Sun Cobalt Control Station belongs.

     The Read Only SNMP Community that you enter can only contain alphanumeric characters along with ‘-’ and ‘_’.
   - **Read and Write SNMP Community.** Enter the Read and Write SNMP Community to which this Sun Cobalt Control Station server belongs.

     The Read and Write SNMP Community that you enter can only contain alphanumeric characters along with ‘-’ and ‘_’.
3. Click **Save**. The system saves the configuration and the screen refreshes

Figure 8. SNMP Settings table



Telnet



Caution: You can adversely affect the performance of your Sun Cobalt Control Station if you modify system configuration files. Check your warranty card for details.



Caution: Only advanced users who need to run shell scripts or use shell commands should access the Sun Cobalt Control Station through the telnet function. An advanced user is someone who is proficient in using the UNIX® operating system.

Direct root logins are not allowed on the Sun Cobalt Control Station. To obtain a root shell, telnet to the control station and log in as the user *admin*. From the command prompt, type "**su -**" and press enter. Enter the Server Administrator password at the password prompt.

Only the Server Administrator can **su -** to root.

To specify the access settings for telnet:

1. Select **Station Settings > Network Services > Telnet**.The "Telnet Settings" table appears; see Figure 9.

Figure 9. Telnet Settings table



2. Select one of the following telnet access options to specify who has telnet access to the Sun Cobalt Control Station.



Note: The second and third options pose security risks; however, they allow the user to configure options supported by the Linux operating system that cannot be configured through the Server Desktop UI.

   - **Off - Do Not Allow Logins.** No telnet access is available. This is the most secure option for the Sun Cobalt Control Station.
   - **On - Telnet Access Enabled.** The Server Administrator can telnet into the Sun Cobalt Control Station. This option is less secure but provides more flexibility.

3. Click **Save**. The system saves the configuration and the screen refreshes.

System

This section describes how to use the following system administration screens:

- **TCP/IP.** Configure the TCP/IP settings.
- **Internet.** Configure settings specific to the type of internet connection for gateway on a LAN, cable modem or DSL, or analog modems and ISDN terminal adapters.
- **Power.** Reboot the Sun Cobalt Control Station.
- **Time.** Set the Sun Cobalt Control Station time settings.
- **Information.** Display information about the Sun Cobalt Control Station.

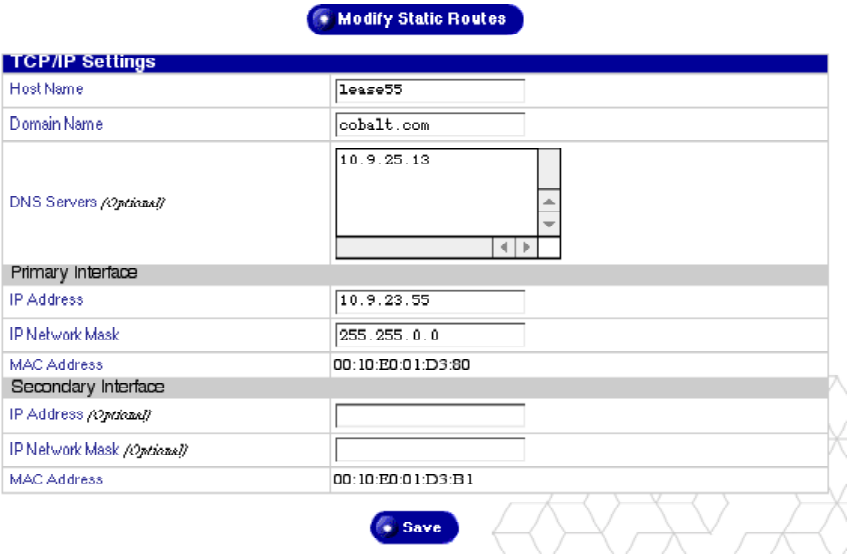
TCP/IP

TCP/IP Settings

To configure the Transmission Control Protocol/Internet Protocol (TCP/IP) settings for the Sun Cobalt Control Station:

1. Select **Station Settings > System > TCP/IP**. The "TCP/IP Settings" table appears; see Figure 10.

Figure 10. TCP/IP Settings table



2. Configure the following fields as appropriate for your situation.

   - **Host Name.** Enter the host name of this Sun Cobalt Control Station. The host name and the domain name combined together should uniquely identify this server. Enter only lowercase alphanumeric characters, dashes or periods. For example, www is a valid entry.
   - **Domain Name.** Enter the domain name of this Sun Cobalt Control Station. The host name and the domain name combined together should uniquely identify this server. Enter only lowercase alphanumeric characters, dashes or periods. For example, efgh123.com is a valid entry.
   - **DNS Servers.** *(optional)* Enter the IP address or addresses of your local Domain Name System (DNS) server or servers. A DNS server translates textual host names and domain names into numerical IP addresses, and vice-versa.

     Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry. Leaving this field empty prevents this machine from finding other machines by hostname or domain name, and can cause networking difficulties.



Note: Be sure to enter the IP address of your DNS server(s) here. Otherwise, the Simple Mail Transfer Protocol (SMTP) will not work. SMTP is used for transferring email messages.

   - **IP Address** (Primary Interface). Enter the IP address of the primary interface. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.
   - **IP Network Mask** (Primary Interface). Enter the network mask of the primary interface. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
   - **MAC Address** (Primary Interface). The Media Access Control (MAC) address is the hardware address of the network interface card. This hardware address is a unique identifier and cannot be changed after manufacture.
   - **IP Address** (Secondary Interface). Enter the IP address of the secondary interface. If you are using only one network interface connection to the server appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 209.43.21.5 is a valid entry.

- **IP Network Mask** (Secondary Interface). Enter the network mask of the secondary interface. If you are using only one network interface connection to the server appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
- **MAC Address** (Secondary Interface). The MAC address is the hardware address of the network interface card. This hardware address is a unique identifier and cannot be changed after manufacture.

3. Click **Save**. The system saves the configuration and the screen refreshes.

Modify static routes

If you have more than one router or gateway on a local are network (LAN), you need to configure the static routes so that TCP/IP traffic is delivered correctly.

You can configure static routes from the Sun Cobalt Control Station to other subnets.

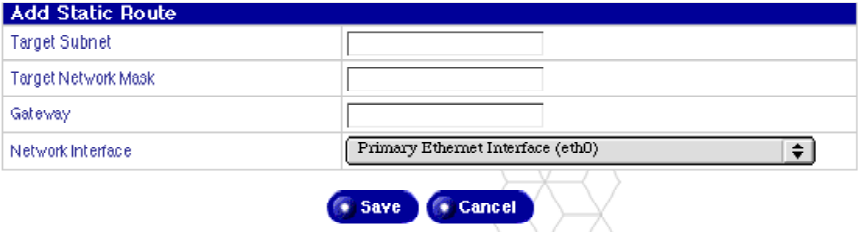
1. Select **Station Settings > System > TCP/IP**. The "TCP/IP Settings" table appears.
2. Click **Modify Static Routes**. The "Static Route List" table appears; see Figure 11.

Figure 11. Static Route List table



3. Click **Add**. The "Add Static Route" table appears; see Figure 12.

Figure 12. Add Static Route table



4. Configure the fields in the “Add Static Routes” table:
    - **Target Subnet.** Enter the IP address of the subnet to be re-routed. For example, 192.168.1.0 is a valid entry.
    - **Target Network Mask.** Enter the network mask of the subnet to be re-routed. For example, 255.255.255.0 is a valid entry.
    - **Gateway.** Enter the IP address of the network gateway through which the target subnet’s packets will be re-routed. For example, 192.168.1.1 is a valid entry.
    - **Network Interface.** Select the network interface through which the target subnet’s packets will be re-routed. If no device is specified, a device will be selected based on the IP address of the network gateway. The choices are:
        - Primary Interface (eth0)
        - Secondary Interface (eth1)
        - Point-to-Point Protocol Interface (ppp0)
5. Click **Save**. The system saves the configuration and the screen refreshes.

Internet

You can connect the Sun Cobalt Control Station to the Internet through a gateway on a local area network (LAN).

Configuration for a gateway on a LAN

Complete this section only if you intend to connect the Sun Cobalt Control Station to the Internet through an existing gateway located on a local area network (LAN). This gateway may be connected to the outside world through a T1/E1 line or other type of leased line.

You need a network connection and the IP address for the gateway.



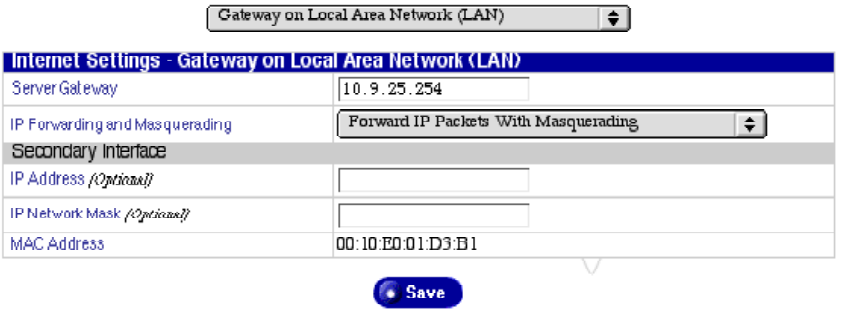
Note: If the gateway is on the secondary network interface, ensure that you connect the secondary network interface on the back of the Sun Cobalt Control Station to the network on which the gateway is located.

See Figure 14 on page 37.

To configure the Internet settings for an existing gateway on a LAN:

1. Select **Station Settings > System > Internet**. The "Internet Settings" table appears.
2. If it does not open in the desired mode, click on the **Change Internet Connection** pull-down menu and select **Gateway on Local Area Network (LAN)**. The "Gateway on a LAN" table appears; see Figure 13.

Figure 13. Internet Settings for Gateway on a LAN table

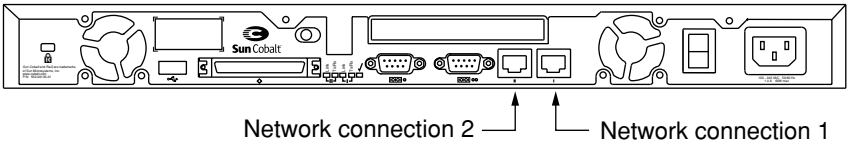


3. Configure the following settings:
   - **Server Gateway.** Enter the IP address of your local network gateway. A network gateway allows you to connect to the world outside of your LAN. For example, 192.168.1.254 is a valid entry.

     Leaving this field empty prevents this machine from communicating with other networks.
   - **IP Address.** *(optional)* Enter the IP address of the secondary interface. If you are using only one network interface connection to the server appliance, use the primary interface and leave the secondary interface empty. For example, 192.168.1.1 is a valid entry.
   - **IP Network Mask.** *(optional)* Enter the network mask of the secondary interface. If you are using only one network interface connection to the server, use the primary interface and leave the secondary interface empty. For example, 255.255.255.0 is a valid entry.
   - **MAC Address.** The Media Access Control (MAC) address is displayed in the last field. The MAC address is the hardware address of the network interface card; it is a unique identifier and cannot be changed.
4. Click **Save**. The system saves the configuration and the screen refreshes.

Figure 14 shows the network connectors on the back of the Sun Cobalt Control Station.

Figure 14. Network connectors



Power

Rebooting the Sun Cobalt Control Station sometimes fixes problems with certain services. The Active Monitor software recommends when a reboot is necessary.

Power down

For security reasons, you cannot power down the Sun Cobalt Control Station through the Desktop Server UI; you have to power down the control station through the LCD console. This screen lists the steps for powering down.

For more information on powering down the control station, see “Powering down” in the PDF *Using the LCD Console*.



Caution: Turning off the power switch before the Sun Cobalt Control Station tells you to do so can result in lost or corrupted data.

Reboot

To reboot the Sun Cobalt Control Station through the Server Desktop UI:

1. Select **Station Settings > System > Power.** The **Reboot** screen appears with the following button.



2. Click the **Reboot Now** button. A confirmation dialog appears.
3. Click **OK**. A dialog appears stating that the server is rebooting and that the reboot can take as long as a few minutes.
4. Once the Sun Cobalt Control Station reboots, the browser should refresh to the Login screen. If it does not, point your browser to the IP address of the Sun Cobalt Control Station.

You can also reboot the Sun Cobalt Control Station through the LCD console. For more information, see "Rebooting" in the PDF *Using the LCD Console*.

Time

To specify the time, date, and time zone settings for the Sun Cobalt Control Station:

1. Select **Station Settings > System > Time**. The "Time Settings" table appears; see Figure 15.
2. Use the pull-down menus to set the time, date and time zone.
3. As an option, you can enter the host name or IP address of a Network Time Protocol (NTP) server if you want the Sun Cobalt Control Station to automatically synchronize its internal clock every night.

   You can find a list of publicly available NTP servers at: http://www.eecis.udel.edu/~mills/ntp/servers.html.
4. Click **Save**. The system saves the configuration and the screen refreshes.

Figure 15. Time Settings table



Information

To view information about your Sun Cobalt Control Station, select **Station Settings > System > Information**. The “System Information” table appears; see Figure 16.

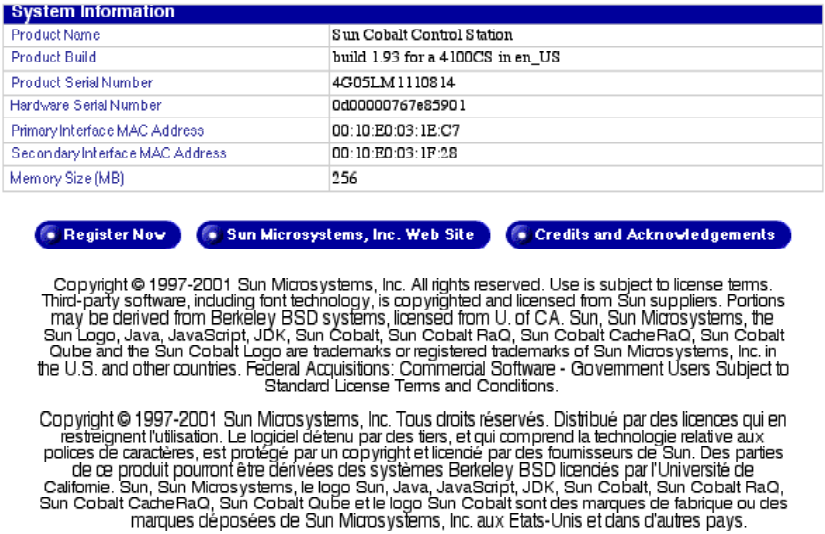
You can see the following information:

- the product name
- the serial number of the product
- the serial number of the hardware
- the MAC address for the primary network interface
- the MAC address for the secondary network interface
- the amount of memory in the server
- the proprietary rights notices (PRNs) from Sun Microsystems

In addition to viewing information about your Sun Cobalt Control Station, you can click the following buttons.

- Click **Register Now** to register your Sun Cobalt Control Station online.
- Click **Sun Microsystems, Inc. Web Site** to go to http://www.sun.com/cobalt.
- Click **Credits and Acknowledgements** to view credits about some of the software installed on the Sun Cobalt Control Station.

Figure 16. System Information table



System Information	
Product Name	Sun Cobalt Control Station
Product Build	build 193 for a 4100CS in en_US
Product Serial Number	4G05LM1110814
Hardware Serial Number	0d00000767e85901
Primary Interface MAC Address	00:10:E0:03:1E:C7
Secondary Interface MAC Address	00:10:E0:03:1F:28
Memory Size (MB)	256

Register Now | Sun Microsystems, Inc. Web Site | Credits and Acknowledgements

Copyright © 1997-2001 Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers. Portions may be derived from Berkeley BSD systems, licensed from U. of CA. Sun, Sun Microsystems, the Sun Logo, Java, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube and the Sun Cobalt Logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Federal Acquisitions: Commercial Software - Government Users Subject to Standard License Terms and Conditions.

Copyright © 1997-2001 Sun Microsystems, Inc. Tous droits réservés. Distribué par des licences qui en restreignent l'utilisation. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun. Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. Sun, Sun Microsystems, le logo Sun, Java, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube et le logo Sun Cobalt sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

BlueLinQ

The BlueLinQ Application Delivery Service provides instant access to product updates and new services as they become available. Using the BlueLinQ technology, the Sun Cobalt Control Station informs you when new software is available.

When you click the BlueLinQ menu item on the left, a sub-menu allows you to add new software, update the current software on the Sun Cobalt Control Station, view the installed software and change the settings for the BlueLinQ feature.



Note: The BlueLinQ feature under the **Station Settings** tab provides software packages for the Sun Cobalt Control Station itself. This feature does not apply to appliances managed by the control station.

For information on configuring BlueLinQ servers under the Software Management Module, refer to the PDF *Software Management Module*.

The following functions are available on the Server Desktop UI.

1. New Software
2. Updates
3. Installed Software
4. Settings

Software Notification icon



The Software Notification icon in the top right corner of the Server Desktop UI allows you to check for new or updated software packages for the Sun Cobalt Control Station itself, and to install them if any are found. The icon turns red when new or updated software packages are available.

If you click this icon, the "Available New Software List" table under the BlueLinQ menu item appears.

New Software

To install new software through the BlueLinQ feature:

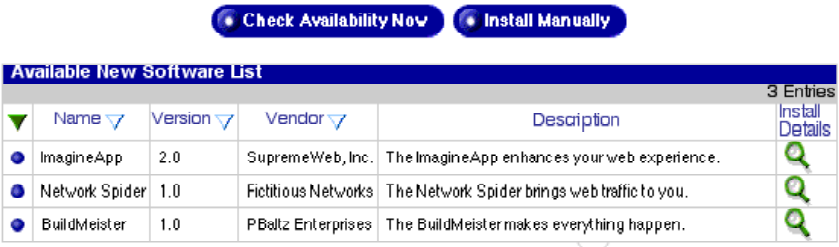
1. Select **Station Settings > BlueLinQ > New Software.** The "Available New Software List" table appears; see Figure 17.

   The table displays the name of the software, the version number, the vendor, a short description of the software and green *magnifying-glass* icon to view the installation details.

   The first column displays either a solid or hollow blue circle.

   - A solid blue circle indicates that you have not seen this new software package before.
   - A hollow blue circle indicates that you have already seen this software package.

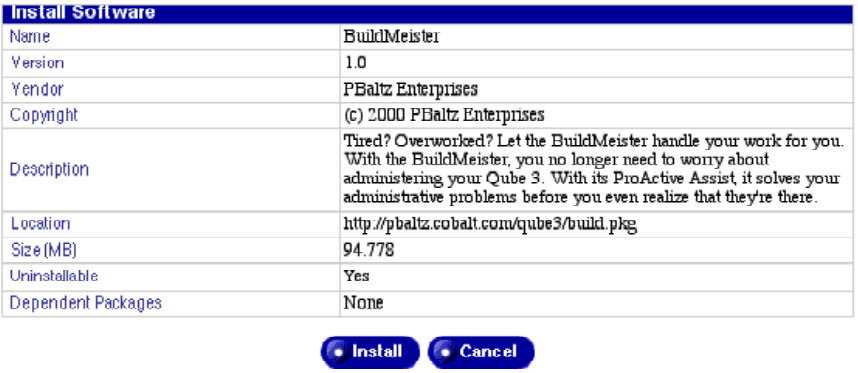
Figure 17. Available New Software List table



2. To install a software package listed in the table, click the green *magnifying-glass* icon. The “Install Software” table appears; see Figure 18. In addition to the information listed in Step 1, the following information is also provided for the software package:

   - the copyright information
   - a longer description of the software
   - the URL location
   - the size of the software package (in MB)
   - whether the software package is uninstallable
   - a list of software packages that must be installed on the system before this new package can be safely installed.

Figure 18. Install Software table



3. Click **Install**. If a License Agreement has been included in the initial splash screen of the software package, a License screen appears. After reviewing the terms of the License Agreement, you may either accept or decline the license.

   If you do not agree with the terms of the License Agreement, click **Decline**., You do not receive the software package and you return to the "Available New Software List" table.

   If you agree with the terms of the License Agreement, click **Accept**. Following your acceptance of the software package License Agreement and clicking **Accept**, a status table appears. The first field indicates the state of the software package during the operation; the second field indicates the progress of the upload with a percentage bar. Once it is completed, a message appears indicating that the software was loaded successfully or that an error occurred.

Check availability of new software

You can force the system to check for new software immediately.

1. Select **Station Settings > BlueLinQ > New Software**. The "Available New Software List" table appears.
2. Click **Check Availability Now**. If new packages are available, they are added to the "Available New Software List" table.

   To install a new software package, see "New Software" on page 41.

Install new software manually

You can install new software manually if you know the location of the software package.

1. Select **Station Settings > BlueLinQ > New Software**. The "Available New Software List" table appears.
2. Click **Install Manually**. The "Install Manually" table appears; see Figure 19.

3. To specify the location of the software package, do one of the following:

   - Click the URL radio button.

     Enter a URL beginning with either http:// or ftp:// to download the package from a location on the Internet.

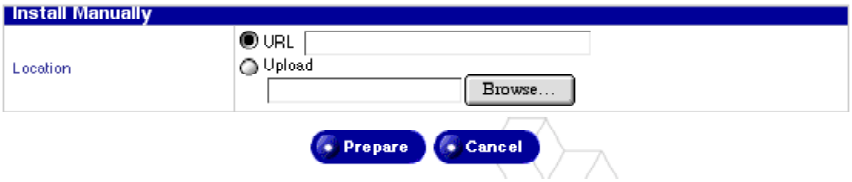
   - Click the Upload radio button.

     Click **Browse** to locate a file on your local hard disk drive.

   - If you have previously downloaded software packages to the /home/packages directory on your Sun Cobalt Control Station server, you can choose one of these packages from the table.

4. Click **Prepare**. The system verifies that the file is in the correct .pkg format. The system then begins to load the software.

Figure 19. Install Manually table



Updates

To install a software update through the BlueLinQ feature:

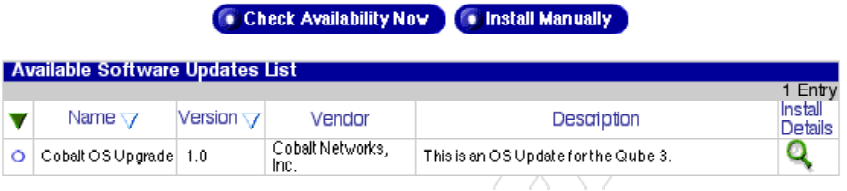
1. Select **Station Settings > BlueLinQ > Updates**.The “Available Software Updates List” table appears; see Figure 20.

   The table displays the name of the software, the version number, the vendor, a short description of the software and green *magnifying-glass* icon to view the installation details.

   The first column displays either a solid or hollow blue circle.

   - A solid blue circle indicates that you have not seen this software update package before.
   - A hollow blue circle indicates that you have already seen this software update package.

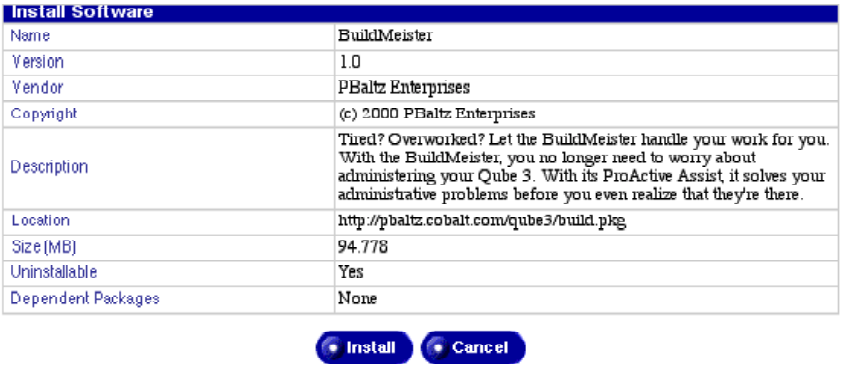
Figure 20. Available Software Updates List table



2. To install a software update package listed in the table, click the green *magnifying-glass* icon. The “Install Software” table appears; see Figure 21. In addition to the information listed in Step 1, the following information is also provided for the software package:

   - the copyright information
   - a longer description of the software
   - the URL location
   - the size of the software package (in MB)
   - whether the software package is uninstallable
   - a list of software packages that must be installed on the system before this new package can be safely installed.

Figure 21. Install Software table



3. Click **Install**. If a License Agreement has been included in the initial splash screen of the software package, a License screen appears. After reviewing the terms of the License Agreement, you may either accept or decline the license.

   If you do not agree with the terms of the License Agreement, click **Decline**., You do not receive the software package and you return to the "Available Software Updates List" table.

   If you agree with the terms of the License Agreement, click **Accept**. Following your acceptance of the software package License Agreement and clicking **Accept**, a status table appears. The first field indicates the state of the software package during the operation; the second field indicates the progress of the upload with a percentage bar. Once it is completed, a message appears indicating that the software was loaded successfully or that an error occurred.

Check availability of software update packages

You can force the system to check for software update packages immediately.

1. Select **Station Settings > BlueLinQ > Updates**. The "Available Software Updates List" table appears.
2. Click **Check Availability Now**. If software update packages are available, they are added to the "Available Software Updates List" table.

   To install a software update package, see "Updates" on page 45.

Install software updates manually

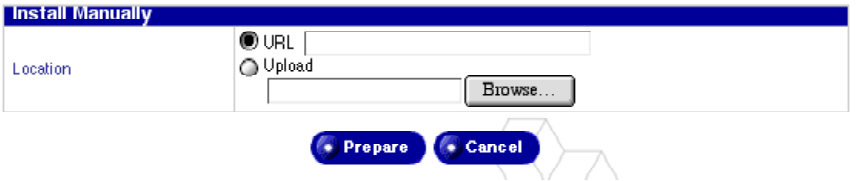
You can install software update packages manually if you know the location of the software update package.

1. Select **Station Settings > BlueLinQ > Updates**. The "Available Software Updates List" table appears.
2. Click **Install Manually**. The "Install Manually" table appears; see Figure 22.
3. To specify the location of the software package, do one of the following:
   - Click the URL radio button.

     Enter a URL beginning with either http:// or ftp:// to download the package from a location on the Internet.
   - Click the Upload radio button.

     Click **Browse** to locate a file on your local hard disk drive.
   - If you have previously downloaded software packages to the `/home/packages` directory on your Sun Cobalt Control Station server, you can choose one of these packages from the table.
4. Click **Prepare**. The system verifies that the file is in the correct .pkg format. The system then begins to load the software.

Figure 22. Install Manually table



Installed Software

On the Sun Cobalt Control Station, the package *Cobalt OS* is installed on the control station at the factory.



Note: You cannot un-install the default packages.



Note: Control modules installed on the Sun Cobalt Control Station do not appear in this table. To view the control modules, see "Administer Modules" on page 89.

To view the software installed on the Sun Cobalt Control Station:

1. Select **Station Settings > BlueLinQ > Installed Software.** The "Installed Software List" table appears; see Figure 23.

   The columns show the name of the software, the version number, the vendor and a short description of the software.

2. Click the icon in the Uninstall column if you wish to uninstall a particular software. A confirmation dialog appears to proceed with the uninstall procedure.

   Software packages for which the *uninstall* icon is disabled (grayed-out) cannot be uninstalled from the Sun Cobalt Control Station server.

3. Click **OK**.

Figure 23. Installed Software List table

Installed Software List

2 Entries

Name	Version	Vendor	Description	Uninstall
Cobalt DiskMirror	1.0	Cobalt Networks	Cobalt DiskMirror provides enhanced reliability by actively mirroring content across a pair of hard drives.	
Cobalt OS	6.0	Sun Microsystems	The Cobalt OS is the base software for the Sun Cobalt Control Station. This software package is required in order for your server appliance to function.	

Settings

To view or modify the settings for the BlueLinQ feature:

1. Select **Station Settings > BlueLinQ > Settings**. The "BlueLinQ Settings" table appears; see Figure 24 for the Basic settings and Figure 25 for the Advanced settings. The active tab shows up as a light grey.

Figure 24. BlueLinQ Settings - Basic table

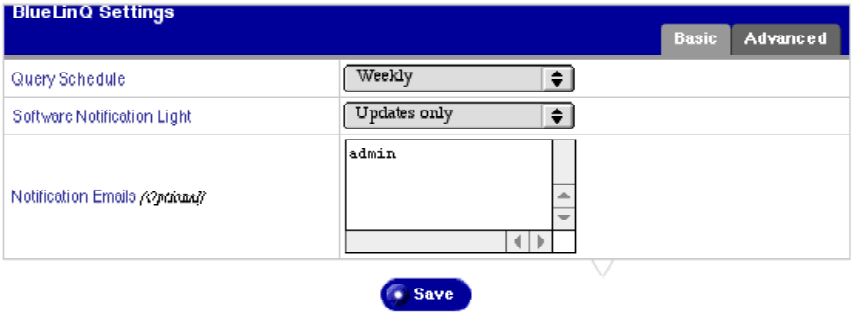
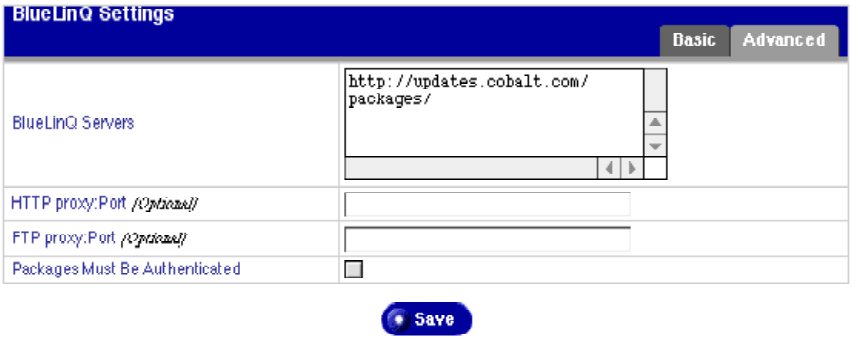


Figure 25. BlueLinQ Settings - Advanced table



2. Configure the fields in the "BlueLinQ Settings" tables.

   Basic settings:

   - **Query Schedule**—Specify how frequently the Sun Cobalt Control Station checks the BlueLinQ server for new or updated software packages: daily, weekly, monthly or never.
   - **Software Notification Light**—Specify the type of software that activates the Software Notification Light and, if applicable, the type of new software that appears in notification email messages.

     You can select "All software" or "Updates only".
   - **Notification Emails** *(optional)* —Enter an email address(es) to which notification of new software or errors in queries for software update are sent. The notification email is sent in accordance with the Software Notification Light setting.

     If you do not want to receive these notifications, leave this field blank.

   Advanced Settings:

   - **BlueLinQ Server(s)**—Enter the HTTP address(es) of the location(s) to query for software updates. You can enter more than one address in this scrolling window; enter each HTTP address on a separate line.

     The default location of the Sun Cobalt Update Server is http://updates.cobalt.com/packages/.



Note: To receive updates from Sun Microsystems for the Sun Cobalt Control Station, you must retain the URL http://updates.cobalt.com/packages/ in this field.



Note: The host name of the BlueLinQ server that you enter must be resolvable by a Domain Name System (DNS) server that your Sun Cobalt Control Station accesses.

To configure a DNS server for your control station, see "TCP/IP" on page 32.

   - **HTTP proxy:port** *(optional)*—Enter the proxy server and port for HTTP queries if a proxy server is needed to reach outside your firewall.

     For example: proxy.mycompany.com:8080.
   - **FTP proxy:port** *(optional)*—Enter the proxy server and port for FTP queries if a proxy server is needed to reach outside your firewall.

     For example: proxy.mycompany.com:8080.

- **Packages must be authenticated**—If enabled, the BlueLinQ feature installs only packages that have passed an authentication check.

3. Click **Save**.

   The screen refreshes to the "BlueLinQ Settings - Basic" table.

Maintenance

The Maintenance menu provides access to utilities for backing up and restoring the Sun Cobalt Control Station.

Backup

You can perform both scheduled backups and manual backups on the Sun Cobalt Control Station.

Creating a backup

To create a backup of the data on the Sun Cobalt Control Station:

1. Select **Station Settings > Maintenance > Backup.** The "Scheduled Backup List" table appears.
2. Click **Add**. The "Add Scheduled Backup" table appears; see Figure 26.
3. Complete the fields in the table.

   - **Backup Name.** This is a unique name assigned to a backup job which can be used to identify backup sets at a later time. The backup name must be a unique name.

     The default value is the current date. You can change this value.

   - **Files to Backup.** This pull-down menu allows you to specify whether this job is a full backup or an incremental backup.

     You can choose to back up All Files (a full backup) or All files modified in the last 31 days, 14 days, 7 days, 2 days or 1 day (incremental backups).

- **Method of Backup.** This field allows you to specify the backup method to use (SMB, FTP or NFS) and the necessary information for that method. For more details on each of these methods, see "Backup file locations" on page 54.

  When a backup runs, it creates a new directory in the location specified in these fields. The directory name is the time at which the backup was started and has the form: Year Month Day Hour Minute Second. For example, the directory name "20010720174533" indicates that the backup was run at 17:45:33 on July 20, 2001.

- **Backup Interval.** This field allows you to specify how often a backup job runs once it is scheduled. You can schedule a backup to run immediately, once a day, once a week or once a month.
  - Once a day means each day soon after midnight.
  - Once a week means every Sunday morning after midnight (Saturday night going into Sunday morning).
  - Once a month means after midnight on the first of every month.

4. Click **Cancel** to discard any changes you have made or click **Save** to schedule the backup as specified. The "Scheduled Backup List" table refreshes with the new job displayed; see Figure 27.

   If you selected Backup Immediately, the backup job begins and proceeds in the background. Administering the Sun Cobalt Control Station while a backup is running is not recommended.



Note: Do not interrupt or cancel the backup job. If the backup job fails, delete the partial backup file from your computer. If you try to restore a partial backup file, you can corrupt the data on your Sun Cobalt Control Station.

Figure 26. Add Scheduled Backup table

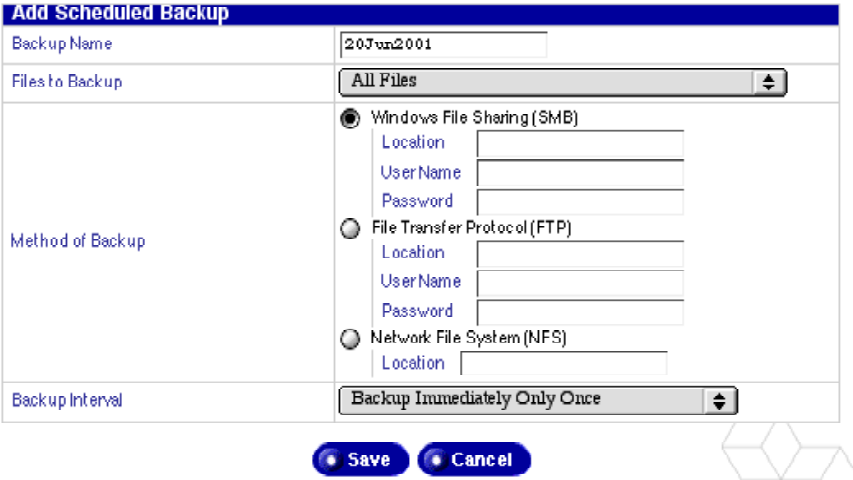
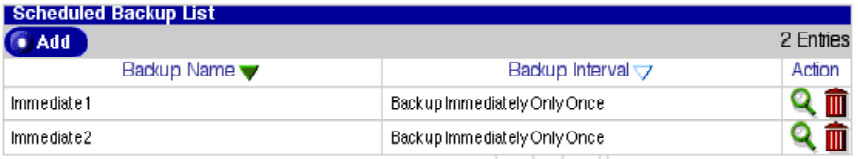


Figure 27. Scheduled Backup table



Viewing details of a scheduled backup

To view the details for a scheduled backup job:

1. Select **Station Settings > Maintenance > Backup.** The "Scheduled Backup List" table appears.
2. Click the green *magnifying-glass* icon next to the backup that you want to view. The "Scheduled Backup Details" table appears, showing the details about the backup job.
3. Click **Back** to return to the "Scheduled Backup List" table.
4. Click **Remove** to permanently delete this backup job. A confirmation dialog verifies the deletion.

   Click **OK**.

Deleting a scheduled backup

To delete a scheduled backup job:

1. Select **Station Settings > Maintenance > Backup.** The "Scheduled Backup List" table appears.
2. Click the red *trash can* icon next to the backup that you want to delete. A confirmation dialog verifies the deletion.
3. Click **OK**.

Backup file locations

Windows File Sharing (SMB) server

For a backup by a **Windows File Sharing (SMB**) server:

- specify a location (fileserver and directory), user name and password
- a location is in the form `\\server\share\dir1\dir2`

File Transfer Protocol (FTP) server

For a backup by an **FTP Server**:

- specify a location (fileserver and directory), user name and password
- a location is in the form `server.name.com/dir1/dir2`



Note: For FTP backups, portions of the data set must be stored on the Sun Cobalt Control Station's hard disk while being transferred. There must be at least 1 GB of disk space free on the Sun Cobalt Control Station to perform an FTP backup.

Network File Sharing (NFS) server

For a backup by an **NFS Server**:

- specify a location only
- a location is in the form `server:/dir1/dir2`
- a password is not required

All scheduled backups

For **All Scheduled** backups, ensure that the target location is available and has enough disk space to hold the backup archive. Failure to do this may result in zero-length or truncated archives.

Restore

There are two ways to restore a data set to the Sun Cobalt Control Station: use the backup history or restore the data set manually.

When a backup runs, it creates a new directory in the location specified in the Method of Backup section of the "Add Scheduled Backup" table; see "Creating a backup" on page 51. The directory name is the time at which the backup was started and has the form: Year Month Day Hour Minute Second. For example, the directory name "20010720174533" indicates that the backup was run at 17:45:33 on July 20, 2001.

Restoring with the backup history

If your system failed and you have cleansed your system with the Sun Cobalt OS Restore Disc, your backup history is not available. To retrieve your history file, you must transfer the most recent history file of one of your data sets to the Sun Cobalt Control Station. This is a separate file within a data set and it always includes the backup data set with which it was associated. The directory names created by the backups can be used to determine the most recent backup.

To retrieve a history file, create the directory `/home/users/admin/.cbackup/` and load the history file in the new directory. This file must be named *history*. You can use any method to transfer the file there.

If you have not cleansed your system with the Sun Cobalt OS Restore Disc or you have restored your history file, the history of all executed backups is available in the "Backup File List" table in the **Maintenance > Restore** screen.

To restore the data set with the backup history:

1. Select **Station Settings > Maintenance > Restore**. The "Backup File List" table appears; see Figure 28.



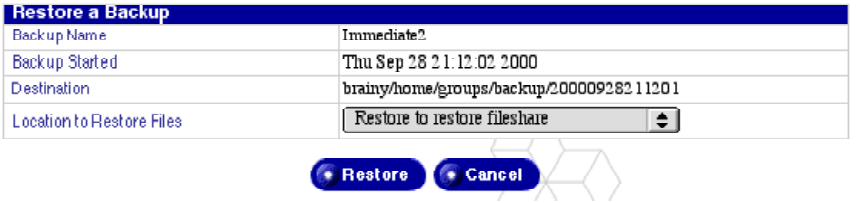
Note: For an unsuccessful backup or for a backup that is still running, the *file-restore* icon for that file is greyed out in the Action column.

Figure 28. Backup File List table



2. Click the *file-restore* icon (a tape with a green arrow) for the history file that you want to restore to the Sun Cobalt Control Station. The "Restore a Backup" table appears with information about the history file; see Figure 29.

Figure 29. Restore a Backup table



3. From the Location to Restore Files pull-down menu, choose a location for the restored files: restore to "restore" fileshare or replace existing files.

   Replacing existing files overwrites files on your hard drive if there is a file with the same name and location as the file being restored. This option should only be used for disaster recovery, as it irreversibly alters the state of the system.



Note: If you select the "Replace existing files" option to restore a full backup, the Sun Cobalt Control Station automatically reboots when the restore is complete.

   The restore fileshare is the directory

   ```
   /home/groups/restore/<BACKUPTIME>
   ```

   where `<BACKUPTIME>` is the directory name used for the backup (for example, 20010720174533). You cannot select or change this location, and there must be enough space in the `/home/` partition for the files.

   This allows you to manually copy only those files you wish to restore.

4. Click **Cancel** to discard any changes you have made or click **Restore** to restore the files. The restore job begins and proceeds in the background. Administering the Sun Cobalt Control Station while a restore is underway is not recommended.



Caution: Interrupting a restore can corrupt your data. If the restore process is interrupted, the Server Administrator can try to restore again.

Viewing details of a history item

To view the details for a history item:

1. Select **Station Settings > Maintenance > Restore.** The "Backup File List" table appears.
2. Click the green *magnifying-glass* icon next to the history file that you want to view. The "History Item Details" table appears, showing the details about the history file.
3. Click **Back** to return to the "Backup File List" table.
4. Click **Restore** to restore the files. The "Restore a Backup" table appears with information about the history file. To continue, go to Step 3 in the procedure under "Restoring with the backup history" on page 55.
5. Click **Remove** to permanently delete this history file. A confirmation dialog verifies the deletion.

   Click **OK**.

Deleting a history item

To delete a history item:



Note: This operation deletes just the history item; it does not delete the backup itself

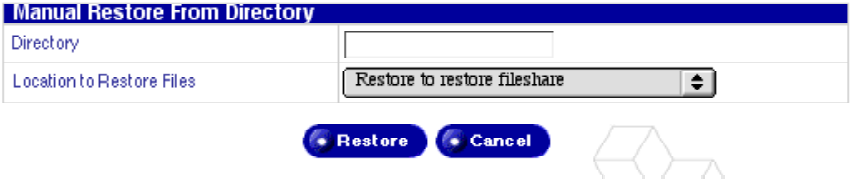
1. Select **Station Settings > Maintenance > Restore.** The "Backup File List" table appears.
2. Click the red *trash can* icon next to the history file that you want to delete. A confirmation dialog verifies the deletion.
3. Click **OK**.

Restoring a backup file manually

To restore a data set manually, you must make the desired data set available to the Sun Cobalt Control Station either by mounting the network share or by transferring the files to the Sun Cobalt Control Station.

1. Mount the network share or transfer the data set to the Sun Cobalt Control Station.
2. Select **Station Settings > Maintenance > Restore.** The "Backup File List" table appears.
3. Click **Restore Manually** above the table. The "Manual Restore From Directory" table appears; see Figure 30.

Figure 30. Manual Restore From Directory table



4. In the Directory field, enter the name of the directory on the Sun Cobalt Control Station to which the data has been transferred or mounted, and within which the data set is found (for example, `/home/restoredata/20010720174533`).
5. From the Location to Restore Files pull-down menu, choose a location for the restored files: restore to "restore" fileshare or replace existing files.

   Replacing existing files overwrites files on your hard drive if there is a file with the same name and location as the file being restored. This option should only be used for disaster recovery, as it irreversibly alters the state of the system.



Note: If you select the "Replace existing files" option to restore a full backup, the Sun Cobalt Control Station automatically reboots when the restore is complete.

The restore fileshare is the directory

```
/home/groups/restore/<BACKUPTIME>
```

where `<BACKUPTIME>` is the directory name used for the backup (for example, 20010720174533). You cannot select or change this location, and there must be enough space in the `/home/` partition for the files.

This allows you to manually copy only those files you wish to restore.

6. Click **Cancel** to discard any changes you have made or click **Restore** to restore the files. The restore job begins and proceeds in the background. Administering the Sun Cobalt Control Station while a restore is underway is not recommended.



Caution: Interrupting a restore can corrupt your data. If the restore process is interrupted, the Server Administrator can try to restore again.

Disaster recovery

To restore your Sun Cobalt Control Station to a known state after a disaster:

1. Restore the Sun Cobalt Control Station to a factory-fresh state with the Sun Cobalt OS Restore Disc that was shipped with the control station.
2. Locate the most recent history file from your backups (use the directory name to identify the most recent backup).
3. Transfer this history file to the directory `/home/users/admin/.cbackup/`
4. Select **Station Settings > Maintenance > Restore.** The “Backup File List” table appears.
5. Restore your backup using from the history item. See “Restoring with the backup history” on page 55.



Important: When restoring your backups, start with the oldest dataset you want to restore. Restore each dataset from oldest to most recent until you reach either the most recent backup or the backup you wish to restore.

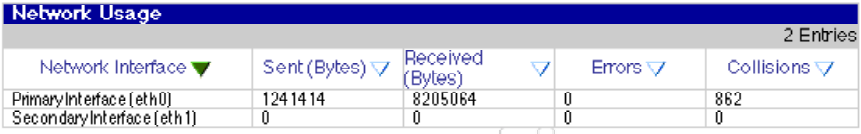
Usage information

Network

You can view statistics about the network interfaces on your Sun Cobalt Control Station .

1. Select **Station Settings > Usage Information > Network**. The "Network Usage" table appears; see Figure 31.

Figure 31. Network Usage table



Network Usage

2 Entries

Network Interface	Sent (Bytes)	Received (Bytes)	Errors	Collisions
Primary Interface (eth0)	1241414	8205064	0	862
Secondary Interface (eth1)	0	0	0	0

2. The table displays the following information:
   - **Network Interface**
   - **Sent (Bytes)**: the total number of bytes sent on the network interface
   - **Received (Bytes)**: the total number of bytes received by the network interface
   - **Errors**: the total number of errors sent or received on the network interface
   - **Collisions**: the total number of collisions detected on the network interface

Active Monitor

The Sun Cobalt Control Station uses Active Monitor software. Active Monitor is a utility that runs on Sun Cobalt server appliances and updates key system and service status every 15 minutes.

Active Monitor icon



The Active Monitor icon in the top right corner of the Server Desktop UI allows you to view status information. The icon flashes red if any of the components or services monitored by Active Monitor fails or is under heavy use.

Status

To view the status of a system component or a service:

1. Select **Station Settings > Active Monitor > Status**. The “Active Monitor Status” table appears; see Figure 32**.**
2. You can click the **Check Status Now** button to begin updating system and service status information immediately. This may take as long as several minutes and proceeds in the background.
3. To view detailed status information for a particular system component or service, click the colored circle to the left of the item’s name in the table or click the gree *magnifying-glass* icon in the Action column that corresponds to the name of the item. See Figure 33.

   The status of each of the above items is indicated by a green, yellow, red or grey circle beside each item. The colors have the following significance:

   - **Grey.** No information is available, or the service or the monitoring feature is not enabled.
   - **Green**. The services and components are functioning normally.
   - **Yellow.** There is moderate use on the server or a component is recovering.
   - **Red.** There is heavy use on the server or a failure.

Figure 32. Active Monitor Status table

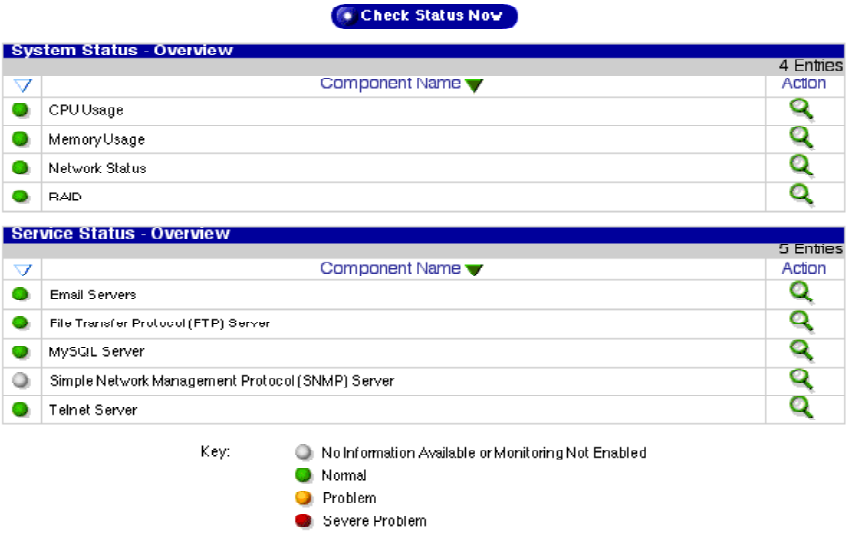
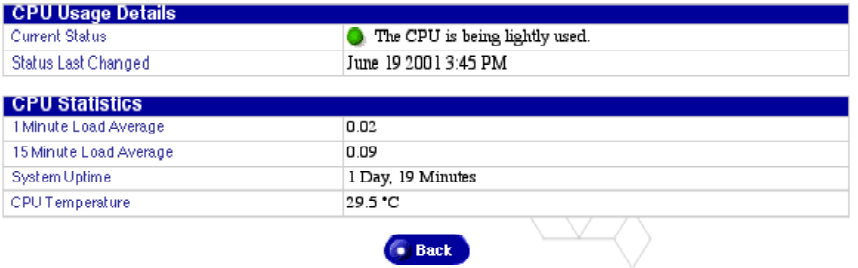


Figure 33. Sample details table



RAID failure

If a hard disk drive in a RAID-1 configuration fails and the control station is still operating, the system indicates the non-RAID status in a number of ways:

- An email is sent to the Administrator of the Sun Cobalt Control Station.
- The Active Monitor icon in the top right corner flashes red.
- On the screen **Station Settings > Active Monitor > Status**, the Disk Integrity (RAID) circle changes to red.
- The "C" logo badge on the front panel of the server appliance blinks.

To view the status of the RAID configuration:

1. Select **Server Management > Active Monitor**. The status tables appear**.**
2. Click the green *magnifying-glass* icon to see the detailed view of Disk Integrity (RAID).

If a single hard disk drive fails, the control station can continue to operate. To restore the RAID-1 configuration (disk mirroring), you must replace the failed hard disk drive and reboot the server appliance.

The replacement drive must be the same model number by the same manufacturer as the failed hard disk drive, and it should have the same storage capacity. If you cannot find a hard disk drive to match the failed drive, you can use a replacement drive that has a larger storage capacity than the failed drive.

For more information on replacing a failed hard disk drive, refer to the PDF *Maintaining and Upgrading the Hardware*.

Once you replace a failed drive on a Sun Cobalt Control Station and reboot the server, the system detects the new hard disk drive and automatically begins to re-integrate it. The system synchronizes the new hard disk drive to the existing drive to recreate a mirrored disk drive.



Note: While the server appliance server is re-integrating the new hard disk drive, the server is not in a RAID configuration.

You can verify that the control station is re-integrating the replacement hard disk drive through Active Monitor.

1. Select **Station Settings > Active Monitor > Status**. The status tables for the system components and services appear.

   The status for "Disk Integrity (RAID)" should be yellow.

2. Click the green *magnifying-glass* icon to see the detailed view of the re-integration process.



Important: If the detailed view of the "Disk Integrity (RAID)" component does not show the replacement hard disk drive being re-integrated, the replacement drive is not compatible with the remaining drives.

Verify that the replacement drive matches the make and model of the failed hard disk drive.

Settings

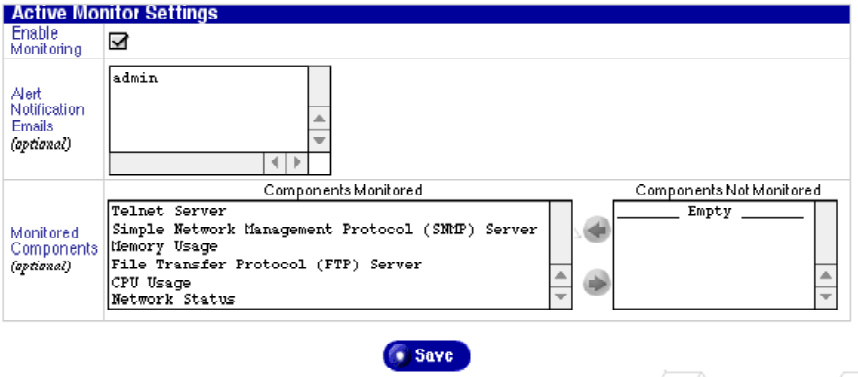
To configure the Active Monitor settings:

1. Select **Station Settings > Active Monitor > Settings**. The "Active Monitor Settings" table appears; see Figure 34.
2. Configure the settings in the "Active Monitor Settings" table.
   - **Enable Monitoring.** This check box enables or disables Active Monitor. Enabling this feature allows the system components to be regularly checked for proper operation.
   - **Alert Notification Emails.** *(optional)* Specify the email address(es) to which the Active Monitor sends email alert messages. The default is the user *admin*.

     If you add more than one email address, enter each one on a separate line or separate the addresses with spaces.
   - **Monitored Components.** *(optional)* Select the specific system components to be regularly checked by Active Monitor. The left column shows the system components which are currently being monitored. The right column shows the system components which are not being monitored.

     To move a component or service between columns, click to highlight the component or service and then click the arrow to move it to the other column.
3. Click **Save**. The system saves the configuration and the screen refreshes.

Figure 34. Active Monitor Settings table



Administrator

The Administrator section allows you to view and modify the information for the user *admin*.

- Account
- Email

Account

In the Account section, you can change the name on your account, select a language and change your password.

Modifying account information

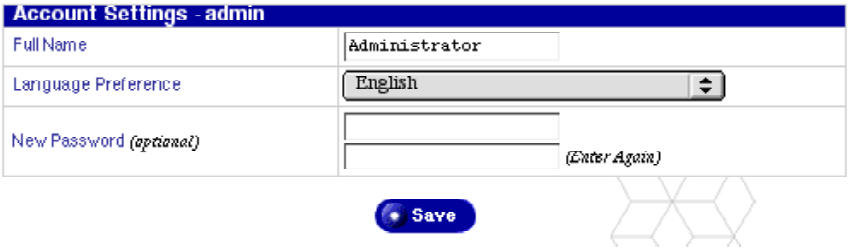
To modify your account information:

1. Select **Station Settings > Administrator**. The "Account Settings - admin" table appears; see Figure 35.
2. Modify any of the following fields.
   a. **Full Name**. This field is mandatory. Modify the name for your account.
   b. **Language Preference.** You can select a language from the pull-down menu.

      You can also have the Sun Cobalt Control Station use the language option selected in your browser software (as long as the text strings for that language are available on the Sun Cobalt Control Station). If the language selected in your browser is not available, the Sun Cobalt Control Station defaults to English.
   c. **New Password.** *(optional)* You can change your password. Enter the password twice for confirmation.

      For more information on choosing a password, see "Password guidelines" on page 7.
3. Click **Save**. The system saves the configuration and the screen refreshes.

Figure 35. Account Settings table



Email

There are two options available in the Email section: Email Forwarding and Vacation Message.

Email forwarding

The Forwarding feature allows you to forward incoming messages to another email address or addresses.

Enabling email forwarding

To enable email forwarding:

1. Select **Station Settings > Administrator > Email**. The "Email Settings - admin" table appears; see Figure 36.
2. In the Email Forwarding section of the table, click to enable the check box Enable.
3. In the scrolling text window labeled Email Addresses, enter an email address in the format "user@domain.com".

   For more than one email address, separate the addresses with a comma or enter each address on a separate line.
4. You can save a copy of the email messages that you forward.

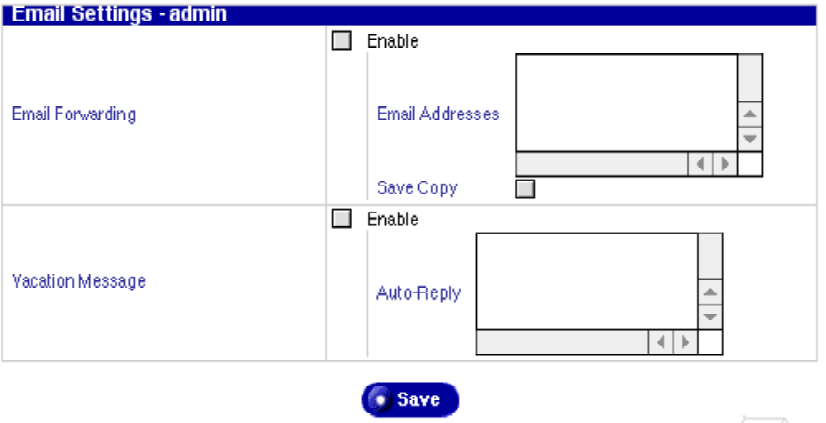
   Click to enable the check box Save Copy.
5. Click **Save**. The system saves the configuration and the screen refreshes.

Disabling email forwarding

To disable email forwarding:

1. Select **Station Settings > Administrator > Email**. The "Email Settings - admin" table appears; see Figure 36.
2. In the Email Forwarding section of the table, click to disable the check box Enable.
3. Click **Save**. The system saves the configuration and the screen refreshes. The email address(es) that you had entered remains in the scrolling text window.

Figure 36. Email Settings table



Vacation message

The Vacation Message feature allows you to enter a vacation-reply message that is automatically sent to each person who sends you email. This feature is useful when you know that you will not be reading or responding to incoming email messages for a period of time.

A particular sender receives the vacation-reply message only once a week; the sender does not receive the vacation-reply message for each email sent.

Enabling the vacation message

To enable the vacation message:

1. Select **Station Settings > Administrator > Email**. The "Email Settings - admin" table appears; see Figure 36.
2. In the Vacation Message section of the table, click to enable the check box Enable.
3. In the scrolling text window labeled Auto-Reply, type the text of the message you want to send to users while you are away.
4. Click **Save**. The system saves the configuration and the screen refreshes.

Disabling the vacation message

To disable the vacation message:

1. Select **Station Settings > Administrator > Email**. The "Email Settings - admin" table appears; see Figure 36.
2. In the Vacation Message section of the table, click to disable the check box Enable.
3. Click **Save**. The system saves the configuration and the screen refreshes. The message that you had entered remains in the scrolling text window.

Control Modules

This chapter describes the functions available under the **Control Modules** tab. The Server Administrator can:

- add or remove managed appliances
- create groups of managed appliances
- view tasks and events
- install and administer the control modules



Note: In most of the short procedures in this chapter, the first step is to click the **Control Modules** tab in the top menu bar and the second step is to click on a selection from the left menu bar.

To reduce the number of steps in each procedure, the menu commands are grouped together and shown in **bold** type face. Right angle brackets separate the individual items.

For example, select **Control Modules > Events > View Tasks** means to click the **Control Modules** tab in the top menu bar, click the **Events** menu category in the left menu bar and finally click the **View Tasks** sub-menu item.

The Sun Cobalt Control Station ships with four pre-installed modules:

- Appliance Inventory
- Performance Monitoring
- Software Management
- Health Monitoring

Each module is explained in detail in its own PDF document, available online through the Server Desktop UIor on the Documentation CD. For more information, see “Online Documentation” on page 4.

Control Modules screen



Note: The control modules also appear in the menu on the left side of the **Control Modules** screen.

For more information on an individual control module, refer to the relevant user document.

The following bullet items appear in the menu on the left side of **Control Modules** screen. These are the functions and services that the Server Administrator can manage from this screen. They are explained in this chapter.

- Appliance Manager (see "Appliance Manager" on page 75)
  - Add Appliance
  - Appliance Groups
  - Edit Appliance
- Events (see "Events" on page 85)
  - View Tasks
  - View Events
  - Cleanup
- Administer Modules (see "Administer Modules" on page 89)
  - Administer

Figure 37 shows the **Control Modules** screen of the Server Desktop UI.

Figure 37. Control Modules screen



Selector window

A number of functions in the Sun Cobalt Control Station use a selector window. This section describes the selector.

In the selector window, depending on the control module that you are using, you select the managed appliances upon which to perform various operations, for example:

- remove or modify an appliance(s)
- add an appliance(s) to a group
- remove an appliance(s) from a group
- view software package information
- publish, install or download software packages
- update performance or inventory information for an appliance

There are two options in the top frame of the selector:

- **Select all.** This option allows you to select all of the managed appliances in the list for that operation.
- **Deselect all.** This option allows you to de-select all of the selected appliances.

To select an appliance or appliances on which to perform an operation, click on the items in the list or click **Select all** at the top. You can also select all appliances within a group by clicking on the group name.

A single selected item is highlighted in blue; if a single item within a group is selected, the group name is highlighted in grey. If all items within a group are selected, the group name is highlighted in dark blue.

To de-select an appliance or appliances, click on the the highlighted item or click **Deselect all** at the top. You can also de-select all the appliances within a group by clicking on the group name.

Once you have selected the appliance(s), click the button in the bottom right corner. The caption on this button reflects the operation you have chosen from the menu items on the left side (for example, Modify or Remove). In the bottom left corner, the selector displays the number of appliances selected (for example, 3 of 10 items).

Appliance Manager

The Appliance Manager menu item allows you, as the Server Administrator, to add, remove or modify server appliances to be managed by the Sun Cobalt Control Station. You can also create groups of server appliances and check on the status of the server appliances being managed by the control station.

Add Appliance

You can add a server appliance to the Sun Cobalt Control Station in two ways:

- add a single server appliance
- import a file containing a list of server appliances

Adding a single server appliance

To add a single server appliance:

1. Select **Control Modules > Appliance Manager > Add Appliance.** The "Add Appliance" table appears; see Figure 38.
2. Configure the following settings:
   - **Appliance Network Address.** Enter the IP address or the fully qualified domain name of the server appliance.



Note: The host name of the appliance that you enter must be resolvable by a Domain Name System (DNS) server that your Sun Cobalt Control Station accesses.

To configure a DNS server for your control station, see "TCP/IP" in the PDF *Administrator Manual*.

   - **User Name.** Enter the user name of the Server Administrator of the server appliance. This name is always *admin*.
   - **Password.** Enter the password of the Server Administrator of the server appliance. Enter the password a second time for confirmation.
   - **Email Address.** (*optional*) Enter the email address of the contact person for the control station.
   - **Description.** (*optional*) Enter a description of the server appliance. For example, "Server in Joe's office".

3. Click **Add Appliance**. The "Progress" table appears. This table has a Status field indicating the current status of the Add operation and a progress bar. When the progress bar displays 100%, the appliance has been added.

   To view the list of events associated to adding a server appliance, click **View Events** below the progress bar. The "Events" table appears.

   To add another appliance, click **Done** below the progress bar. The "Add Appliance" table appears.

Importing a list of server appliances

For more information on creating the list of server appliances, see "Creating a list of appliances" on page 77.

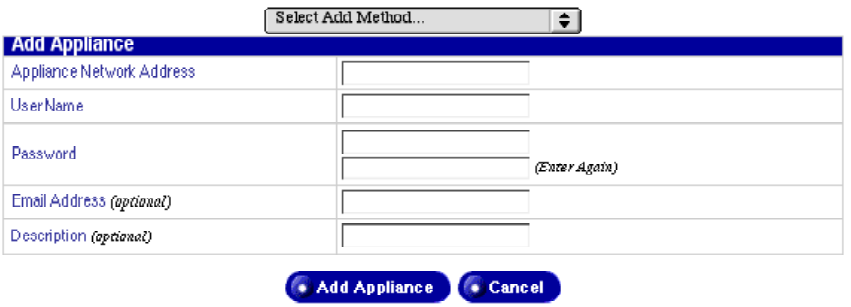
To add a list of appliances from a file:

1. Select **Control Modules > Appliance Manager > Add Appliance.** The "Add Appliance" table appears; see Figure 38.
2. From the pull-down menu above the table, select "Add Appliances from a file".
3. In the Source File field, enter the path and filename of the file to import. You can also click **Browse** and locate the file.
4. Click **Add Appliances**. The "Progress" table appears. This table has a Status field indicating the current status of the Add operation and a progress bar. When the progress bar displays 100%, the appliance has been added.

   To view the list of events associated to adding a server appliance, click **View Events** below the progress bar. The "Events" table appears.

   To add another appliance, click **Done** below the progress bar. The "Add Appliance" table appears.

Figure 38. Add Appliance table



Creating a list of appliances

You can create a file containing a list of appliances, and then import this file into the Sun Cobalt Control Station.

The first step in importing a list of appliances is to generate a text file in the required format. The order of the data fields is the following (enter the data on continuous line):

<hostname_or_IP_address>|<username>|<admin_password>|
<email_address>|<description>

The following criteria explain the structure of the file.

1. Include the following data for each appliance
   a. host name or IP address of the appliance



Note: To import the appliance by host name, you must first specify a Domain Name System (DNS) server on the Sun Cobalt Control Station. For more information, see "TCP/IP" on page 32.

If you have not specified a DNS server, you must import the appliance by IP address.

   b. user name for the Server Administrator
   c. Server Administrator password
   d. an email address for notifications (*optional*)
   e. a description of the appliance (*optional*)
2. Use one line for each appliance in the file.
3. Separate the data fields with the "|" character. Do not insert a space before or after the "|" character. You can use commas or tabs in the data string.
4. If you do not add an email address for the appliance, enter two consecutive "|" characters at the end of the line; this indicates a null field.

   The control station does not verify that an email address works.
5. If you do not add a description for the appliance, simply leave the end of the line blank. You do not need to enter a final "|" character to close the description data field.
6. Save the file in plain-text format.

Example file

An example file with seven appliances might look like this:

raq4|admin|abc123||

raq3|admin|abc123| joe@asdfg.com

10.9.32.100|admin|abc123||

10.9.32.111|admin|abc123| joe@asdfg.com

10.9.32.114|admin|abc123| joe@asdfg.com|Sun Cobalt Qube 3 at home

10.9.32.115|admin|abc123||Server appliance on top shelf

10.9.32.116|admin|abc123||Sun Cobalt RaQ 4 in server room

Appliance Groups

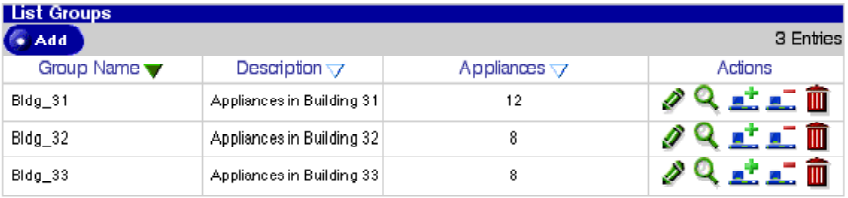
You can group a number of server appliances under a single group name.

List Groups table

The “List Groups” table has four columns; Figure 39 shows an example of the table.

- Group Name
- Description
- Appliances
- Actions

Figure 39. List Groups table



You can sort the list of groups according to the name of the group, the description of the group or the number of appliances in a group, in ascending or descending order.

Ascending order means from lowest value to the highest value (a–z or 1–9). Descending order means from highest value to the lowest value (z–a or 9–1). By default, the “ List Groups” table is sorted by group name in ascending order.

In the heading of the column which has been sorted, a green *triangle* icon points down (ascending order) or up (descending order). In the heading of the column which has not been sorted, a hollow *triangle* icon indicates that the column is not sorted.

Actions column

Once a group is created, you can perform various operations on that group. These operations are found in the Actions column of the "List Groups" table. These operations are explained further along in this section.

- Modify a group
- View details of a group
- Add an appliance(s) to a group
- Remove an appliance(s) from a group
- Remove a group

Adding a group

To create a group of managed appliances:

1. Select **Control Modules > Appliance Manager > Appliance Groups.** The "List Groups" table appears.
2. Click **Add** at the top of the table. The "Add a Group" table appears.
3. Fill in the following fields:
   - **Group Name.** Enter a name for the group.
   - **Description.** *(optional)* Enter a short description for this group. The description can contain up to 255 characters.
   - **Choose appliances to add.** Check this box if you want to add appliances to the group in this same procedure.
4. Click **Save**.

   If you did not click the check box Choose appliances to add, the "List Groups" table appears with the new group; the new group contains no appliances.
5. If you did click the check box Choose appliances to add, the selector appears, displaying the list of managed appliances.
6. In the selector, click to highlight the appliance(s) you want to add to the group. You can also click **Select All Rows** at the top to choose all appliances in the list.
7. Click **Add** in the bottom right corner. The "List Group" table appears with the new group added. The groups are sorted by group name in ascending order.

Modifying a group

You can change the name or the description for a group.

To modify a group:

1. Select **Control Modules > Appliance Manager > Appliance Groups.** The "List Groups" table appears.
2. Locate in the list the group that you want to modify.
3. Click the green *pencil* icon in the Actions column. The "Update Group" table appears.
4. You can modify the group name or the description of the group. The Description field is optional.
5. Click **Save**. The "List Groups" table appears with the modified information.

Viewing details of a group

You can see which appliances belong to a given group.

To view the details for a group:

1. Select **Control Modules > Appliance Manager > Appliance Groups.** The "List Groups" table appears.
2. Locate in the list the group for which you want to view the details.
3. Click the green *magnifying-glass* icon in the Actions column. The selector appears, displaying the list of managed appliances within that group.
4. To return to the list of groups, click **Appliance Groups** on the left. The "List Groups" table appears.

Adding an appliance to a group

You can add an appliance or appliances to an existing group.

To add an appliance(s):

1. Select **Control Modules > Appliance Manager > Appliance Groups.** The "List Groups" table appears.
2. Locate in the list the group to which you want to add an appliance.
3. Click the green *plus-appliance* icon in the Actions column. The selector appears, displaying the list of managed appliances and the groups on the Sun Cobalt Control Station.
4. In the selector, click to highlight the appliance(s) you want to add to the group. You can also click **Select All Rows** at the top to choose all appliances in the list.

   You can select an appliance in another group to add to the current group. The appliance will then appear as a member of both groups.
5. Click **Add** in the bottom right corner. The "List Group" table appears with the updated information. The groups are sorted by group name in ascending order.

Removing an appliance from a group

You can remove an appliance or appliances from an existing group.

To remove an appliance(s):

1. Select **Control Modules > Appliance Manager > Appliance Groups.** The "List Groups" table appears.
2. Locate in the list the group from which you want to delete an appliance.
3. Click the red *minus-appliance* icon in the Actions column. The selector appears, displaying the list of managed appliances that belong to the group.
4. In the selector, click to highlight the appliance(s) you want to remove from the group. You can also click **Select All Rows** at the top to choose all appliances in the list.
5. Click **Remove** in the bottom right corner. The "List Group" table appears with the updated information. The groups are sorted by group name in ascending order.

Removing a group

You can remove an existing group.



Note: Removing a group does not remove the managed appliances in that group from the Sun Cobalt Control Station.

To remove an appliance(s), see "Removing an appliance" on page 83.

To remove a group:

1. Select **Control Modules > Appliance Manager > Appliance Groups.** The "List Groups" table appears.
2. Locate in the list the group that you want to remove.
3. Click the red *trash can* icon in the Actions column. The "Confirm Group Removal" table appears, asking you to confirm the removal.
4. Click **Remove**. The "List Groups" table appears with the updated information.

Edit Appliance

You can remove or modify a managed appliance.

If you have tried to add an appliance and the operation failed, the selector window has a group entry named "All Management Failed". The appliances for which the Add Appliance operation failed are listed under this group name.

Removing an appliance

To remove a managed appliance(s):

1. Select **Control Modules > Appliance Manager > Edit Applaince**. The selector appears, displaying the list of managed appliances and the appliance groups.
2. In the selector, click to highlight the appliance(s) you want to remove. You can also click **Select All Rows** at the top to choose all appliances in the list:
3. Click **Remove** in the bottom right corner. A confirmation table appear, asking you to confirm the removal of the selected appliances.

   To cancel the operation and return to the selector, click **Cancel**.

   To proceed with the operation, click **Remove**.

4. The “Progress” table appears. This table has a Status field indicating the current status of the Remove operation and a progress bar. When the progress bar displays 100%, the appliance(s) has been removed.

   To view the list of events associated to removing a server appliance, click **View Events** below the progress bar. The “Events” table appears.

   To remove another appliance, click **Done** below the progress bar. The “Edit Appliance” table appears.

Modifying an appliance

You can modify the host name of an appliance, the email address for notifications or the description of an appliance.

To modify a managed appliance(s):

1. Select **Control Modules > Appliance Manager > Edit Appliance.** The selector appears, displaying the list of managed appliances and the appliance groups.
2. In the selector, click to highlight the appliance(s) you want to modify. You can also click **Select All Rows** at the top to choose all appliances in the list
3. Click **Modify** in the bottom right corner. The “Modify Appliance <IP address>” table appears.
4. You can modify the following settings:
   - **Host Name.** Enter the host name of the server appliance.
   - **Email Address.** (*optional*) Enter the email address of the contact person for this server appliance.
   - **Description.** (*optional*) Enter a description of this server appliance. For example, “Sun Cobalt RaQ 4 server appliance”.
5. To cancel the operation and return to the previous list, click **Cancel**.

   To proceed with the operation, click **Save**. The selector appears displaying the modified information.

Events

Operations performed on the Sun Cobalt Control Station are called tasks and events.

A *task* is an executed operation that has a determined start and end point, such as adding an appliance or uploading a control module. A task is invoked by a user.

Invoking a task generates one or more events. An *event* is a notification message providing information on one part of a task. A task can comprise several events. An event is generated by the control station or by an agent on a managed appliance.

View Tasks

You can view a list of the tasks invoked by a user.

Tasks table

The "Tasks" table has eight columns; Figure 40 shows an example of the table.



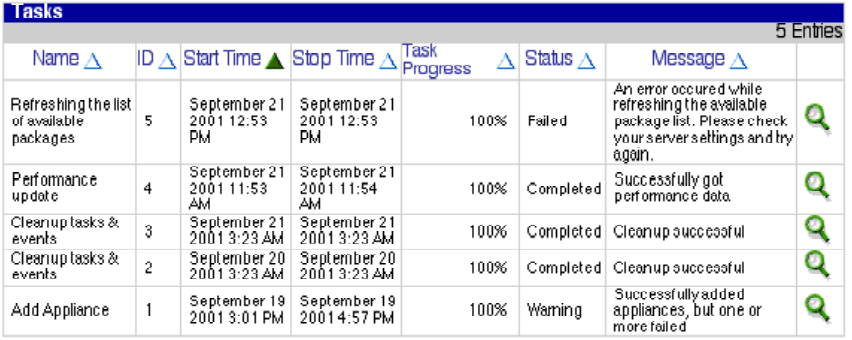
Note: If there are more than 50 entries in the table, the table lists the first 50 entries.

At the top of the table, you can use a pull-down menu to choose the range of entries that you want to view.

The columns are:

- **Name**: the string name of the functional component that created the task
- **ID**: a unique identification number for the task
- **Start Time**: the time that the task started
- **Stop Time**: the time that the task completed
- **Task Progress**: the progress of the task
- **Status**: the status of the task (either running or completed)
- **Message**: a descriptive message for the admin
- **Details**: Clicking the green *magnifying-glass* icon allows you to see the individual events associated with a task. A new table appears listing the events. Click **Done** to return to the "Tasks" table.

Figure 40. Tasks table



Tasks

5 Entries

Name △	ID △	Start Time ▲	Stop Time △	Task Progress △	Status △	Message △	
Refreshing the list of available packages	5	September 21 2001 12:53 PM	September 21 2001 12:53 PM	100%	Failed	An error occured while refreshing the available package list. Please check your server settings and try again.	
Performance update	4	September 21 2001 11:53 AM	September 21 2001 11:54 AM	100%	Completed	Successfully got performance data.	
Cleanup tasks & events	3	September 21 2001 3:23 AM	September 21 2001 3:23 AM	100%	Completed	Cleanup successful	
Cleanup tasks & events	2	September 20 2001 3:23 AM	September 20 2001 3:23 AM	100%	Completed	Cleanup successful	
Add Appliance	1	September 19 2001 3:01 PM	September 19 2001 4:57 PM	100%	Warning	Successfully added appliances, but one or more failed	

You can sort the list of tasks according to the the name of the task, the ID number of the task , the start time or stop time for the task, the progress, the status or the message for the task, in ascending or descending order.

Ascending order means from lowest value to the highest value (a–z or 1–9). Descending order means from highest value to the lowest value (z–a or 9–1). By default, the " Task" table is sorted by name in ascending order.

In the heading of the column which has been sorted, a green *triangle* icon points down (ascending order) or up (descending order). In the heading of the column which has not been sorted, a hollow *triangle* icon indicates that the column is not sorted.

View Events

You can view a list of the events generated on the control station.

Events table

The “Events” table has six columns; Figure 41 shows an example of the table.



Note: If there are more than 50 entries in the “Events” table, the table lists the first 50 entries.

At the top or bottom of the table, you can use a pull-down menu to choose the range of entries that you want to view.

The columns are:

- **Type**: the type of event generated (information, warning and so on)
- **Task ID**: the task ID to which the event is associated
- **Source**: the IP address of the appliance from which the event was generated; the local host shows up as IP address 127.0.0.1
- **Generating Process**: the process name that generated the event
- **Message**: a message associated with the event
- **Timestamp**: the time at which the event was generated

Figure 41. Events table

Events

Entries 1 - 50 — 554 Entries

Type	task	Source	Generating Process	Message	Timestamp
warning	5	127.0.0.1	Update Package List	BlueLinQ Server devblueling returned an unexpected result	September 21 2001 12:53 PM
info	4	127.0.0.1	Performance update	Successfully got performance data from 10.9.3.160	September 21 2001 11:54 AM
info	3	127.0.0.1	Cleanup tasks & events	Cleanup successful	September 21 2001 3:23 AM
info	3	127.0.0.1	Cleanup tasks & events	Verified database integrity	September 21 2001 3:23 AM
info	3	127.0.0.1	Cleanup tasks & events	No tasks at least 14 days old to delete	September 21 2001 3:23 AM
info	3	127.0.0.1	Cleanup tasks & events	No events at least 14 days old to delete	September 21 2001 3:23 AM
info	2	127.0.0.1	Cleanup tasks & events	Cleanup successful	September 20 2001 3:23 AM
info	2	127.0.0.1	Cleanup tasks & events	Verified database integrity	September 20 2001 3:23 AM
info	2	127.0.0.1	Cleanup tasks & events	No tasks at least 14 days old to delete	September 20 2001 3:23 AM
info	2	127.0.0.1	Cleanup tasks & events	No events at least 14 days old to delete	September 20 2001 3:23 AM
warning	1	127.0.0.1	Add Appliance	Successfully added appliances, but one or more failed	September 19 2001 4:57 PM
info	1	127.0.0.1	Performance update	Successfully got performance data from 10.9.23.104	September 19 2001 4:57 PM
info	1	127.0.0.1	Update	Successfully got inventory information from 10.9.23.104	September 19

You can sort the list of events according to the type of event, the task to which it is associated, the source (the IP address of the appliance) of the event, the generating process, a description of the event or the timestamp for an event, in ascending or descending order.

Ascending order means from lowest value to the highest value (a–z or 1–9). Descending order means from highest value to the lowest value (z–a or 9–1). By default, the " Events" table is sorted by type of event in ascending order.

In the heading of the column which has been sorted, a green *triangle* icon points down (ascending order) or up (descending order). In the heading of the column which has not been sorted, a hollow *triangle* icon indicates that the column is not sorted.

Cleanup

You can clean up the list of tasks and events retained by the Sun Cobalt Control Station.

You can configure the control station:

- to remove items from the list once they reach a certain age, measured in days (between 1 day and 100 days). Items older than 100 days are deleted from the list.
- to run the cleanup operation at a certain time each day.

To configure the cleanup feature:

1. Select **Control Modules > Events > Cleanup.** The "Task and Event Cleanup" table appears.
2. In the first row of the table, use the pull-down menu to select the period of time (in days) after which tasks and events are removed.
3. In the second row of the table, use the pull-down menus to select the time of day at which to run the cleanup operation each day.
4. Click **Save**. The screen refreshes.

Administer Modules

Administer

You can view the list of control modules currently installed on the Sun Cobalt Control Station. You can also add or remove a control module, or view the details on a control module.

Installed Control Modules table

The "Installed Control Modules" table has six columns; Figure 42 shows an example of the table. The columns are:

- **Module Name**: the name of the control module
- **Version**: the version number of the control module
- **Vendor**: the vendor of the control module
- **Installed On**: the date and time on which the control module was installed on the control station
- **Successful Appliances**: the number of managed appliances on which this control module is successfully installed
- **Failed Appliances**: the number of managed appliances on which this control module failed to install
- **Action**: to view the details for a control module or to delete a module from the control station

Figure 42. Installed Control Modules table

Installed Control Modules

Add — 4 Entries

Application Name	Version	Vendor	Installed On	Appliances	Failed Appliances	Action
Appliance Inventory	1.0-23	Sun Microsystems, Inc.	September 19 2001 2:12 PM	39	0	
Appliance Performance	1.0-16	Sun Microsystems, Inc.	September 19 2001 2:12 PM	39	0	
Health Monitoring	1.0-26	Sun Microsystems, Inc.	September 19 2001 2:12 PM	35	0	
Software Management	1.0-33	Sun Microsystems, Inc.	September 19 2001 2:12 PM	39	0	

You can sort the list of control modules according to the name of the module, the version number, the vendor, the date and time on which the module was installed or the number of appliances on which the module successfully installed or failed to install, in ascending or descending order.

Ascending order means from lowest value to the highest value (a–z or 1–9). Descending order means from highest value to the lowest value (z–a or 9–1). By default, the " Installed Control Modules" table is sorted by module name in ascending order.

In the heading of the column which has been sorted, a green *triangle* icon points down (ascending order) or up (descending order). In the heading of the column which has not been sorted, a hollow *triangle* icon indicates that the column is not sorted.

Adding a control module

When you add a control module to the control station, a menu item for this new module appears in the list on the left side of the Server Desktop UI.

To add a control module:

1. Select **Control Modules > Administer Modules > Administer**. The "Installed Control Modules" table appears.
2. Click **Add** at the top of the table. The "Install New Control Module" table appears.
3. In the Package to upload field, enter the path and filename of the module to install. You can also click **Browse** and locate the module.
4. Click **Install**. The "Progress" table appears. This table has a Status field indicating the current status of the Install operation and a progress bar. When the progress bar displays 100%, the module has been installed on the appliance. A green *checkmark* icon appears in the bottom left corner.

   To view the list of events associated to installing a module on an appliance, click **View Events** below the progress bar. The "Events" table appears.

   To add another control module, click **Done** below the progress bar. The "Installed Control Modules" table appears.



Note: If the newly added module does not appear in the menu of the left, "refresh" your browser window.

If there is documentation available for this module, it is added to the list of online documentation. For more information, see "Online Documentation" on page 4.

Viewing details for a control module

To view the details for a control module:

1. Select **Control Modules > Administer Modules > Administer**. The "Installed Control Modules" table appears.
2. Locate in the list the module for which you want to view the details.
3. Click the green *magnifying-glass* icon in the Actions column. A table appears, showing the appliances on which the module has been installed.

   The table shows the IP address and the host name of the managed appliance, and the installation status of the module for each appliance.
4. Click **Back** to return to the "Installed Control Modules" table.

Re-installing a module on an appliance

The "Installed Control Modules" table indicates if a module has failed to install on a managed appliance. You can drill down to the detailed information tables and try again to install the module on these appliances.

To re-install a module on a managed applicance:

1. Select **Control Modules > Administer Modules > Administer**. The "Installed Control Modules" table appears.
2. Locate in the list the module that has an entry or entries in the Failed Appliance column.
3. Click the green *magnifying-glass* icon in the Actions column. A table appears, showing the appliances on which the module has been installed.

   The table shows the installation status of the module for each appliance. If the module failed to install on an appliance, there is a **Retry install** button in th e Action column for that appliance.
4. Click **Retry install** in the Actions column. The "Progress" table appears. This table has a Status field indicating the current status of the Install operation and a progress bar. When the progress bar displays 100%, the module has been installed on the appliance. A green *checkmark* icon appears in the bottom left corner.

   To view the list of events associated to installing a module on an appliance, click **View Events** below the progress bar. The "Events" table appears.

   To return to the "Installed Control Modules" table, click **Done** below the progress bar. The "Installed Control Modules" table appears.

Removing a control module



Note: If you remove one of the four pre-installed control modules (for example, Health Monitoring), you cannot re-install it later (the modules are not stored on the Sun Cobalt Control Station).

See page 71 for the list of the pre-installed control modules.

To obtain another copy of one of the pre-installed control modules, visit the Sun Cobalt Web site at http://www.cobalt.com/support/download/index.html.

From the product pull-down menu, select Sun Cobalt Control Station. Locate the correct module and save it to your local machine.

Now add the module to the control station; see "Adding a control module" on page 90.

To remove a control module:

1. Select **Control Modules > Administer Modules > Administer**. The "Installed Control Modules" table appears.
2. Locate in the list the module that you want to remove.
3. Click the red *trash can* icon in the Actions column. The "Confirm Removal of Control Module" table appears, asking you to confirm the removal.
4. Click **Remove**. The "Installed Control Modules" table appears with the updated information.

Licenses

The BSD Copyright

Copyright ©1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program,” below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification.”) Each licensee is addressed as “you.”

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above, provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated, so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING, THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SSL License

Copyright (c) 1998-1999 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.engelschall.com/sw/mod_ssl/)."

4. The name "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.engelschall.com/sw/mod_ssl/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Acme Public License

Copyright (c) 2000 by Jef Poskanzer <jef@acme.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

The entries in this glossary are for your information. Not all of the concepts, technologies and protocols apply to the Sun Cobalt Control Station.

10/100 BaseTX

An Ethernet connection over twisted-pair cables with a throughput of 10 Mb/s or 100 Mb/s.

10BaseT

A 10-Mb/s baseband Ethernet specification using two pairs of twisted-pair cabling (Category 3, 4, or 5): one pair for transmitting data and the other for receiving data. 10BaseT (part of the IEEE 802.3 specification) has a distance limit of approximately 328 feet (100 meters) per segment.

100BaseTX

A 100-Mb/s baseband Fast Ethernet specification using two pairs of either unshielded twisted pair (UTP) or shielded twisted pair (STP) wiring. The first pair of wires is used to receive data; the second pair is used to transmit. To guarantee proper signal timing, a 100BaseTX segment cannot exceed 328 feet (100 meters) in length. 100BaseTX is based on the IEEE 802.3 standard.

Authentication

The process whereby a user or information source proves they are who they claim to be; in other words, the process of verifying the identity of a user, device or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. Authentication is any technique enabling the receiver to automatically identify and reject messages that have been altered either deliberately or by channel errors.

See also *Encryption* and *Secure Sockets Layer (SSL)*.

AppleShare

A file-sharing protocol in Apple system software that allows sharing of files and network services through a file server in the Apple Macintosh environment.

Carrier sense

In a local area network (LAN), an ongoing activity of a data station to detect whether another station is transmitting.

Carrier sense multiple access with collision detection (CSMA/CD)

A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting stops sending, sends a jam signal and then waits for a variable period of time before sending again. Used in ethernet LAN technology.

CGI

See *Common gateway interface (CGI).*

Common gateway interface (CGI)

A set of rules that describe how a Web server communicates with another application running on the same computer and how the application (called a CGI program) communicates with the Web server. Any application can be a CGI program if it handles input and output according to the CGI standard.

Collision

In an ethernet network, a collision is the result of two devices attempting to transmit data at exactly the same time. The network detects the "collision" of the two transmitted packets and discards them both. Collisions are a natural occurrence on an ethernet network.

Ethernet technology uses carrier sense multiple access/collision detect (CSMA/CD) to allow devices to take turns using the signal carrier line. When a device wants to transmit, it checks the signal level of the line to determine whether another device is already using it. If the line is already in use, the device waits and tries again, perhaps in a few seconds. If the line is not in use, the device transmits.

However, two devices can transmit at the same time in which case a collision occurs and both devices detect it. Each device then waits a random amount of time and retries until successful in getting the transmission sent.

Control module

A package file (.pkg) containing a list of executable commands that is integrated into, and executed from, the Sun Cobalt Control Station. Modules can be created by Sun Microsystems, by third-party developers or by the end user (using the Software Developers Kit for the control station).

Control Station

The Sun Cobalt Control Station consists of two parts: a management framework for deploying control modules and adding appliances to be managed, and several built-in modules for performing specific tasks on the managed appliances.

CSMA/CD

See *carrier sense multiple access with collision detection (CSMA/CD)*.

DHCP

See *Dynamic Host Configuration Protocol (DHCP)*.

Digital Subscriber Line (DSL)

A technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. The term xDSL refers to different variations of DSL, such as asymmetric DSL (ADSL), high-bit-rate DSL (HDSL) and rate-adaptive DSL (RADSL). If your home or small business is close enough to a telephone company central office that offers DSL service, you may be able to receive data at rates of up to 6.1 Mb/s. More typically, individual connections provide from 512 Kb/s to 1.544 Mb/s downstream and about 128 Kb./s upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected.

DNS

See *Domain Name System (DNS)*.

Domain name

The location of an organization or other entity on the Internet. For example, the address www.cobalt.com locates an Internet address for the domain name “cobalt.com” at a particular IP address and a particular host server named “www.”

Domain Name System (DNS)

The Internet service responsible for translating a human-readable host name such as cobalt.com into a numeric IP address (111.123.45.67) for TCP/IP communications.

DSL

See *Digital Subscriber Line (DSL)*.

Dynamic Host Configuration Protocol (DHCP)

A protocol that provides a mechanism for allocating IP addresses dynamically so that an address can be reused when a host no longer needs it.

Encryption

The transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. In the area of security, encryption is the ciphering of data by applying an algorithm to plain text to convert it into cipher text.

See also *Authentication* and *Secure Sockets Layer (SSL)*.

ESMTP

See *Extended Simple Mail Transfer Protocol (ESMTP)*.

Ethernet

The most widely used technology for local area networks (LANs). Standard ethernet runs at 10 Mb/s, 100 Mb/s or 1000 Mb/s. It balances speed, price, ease of installation and availability.

ETRN

ETRN (Extended Turn) is an extension to the Simple Mail Transfer Protocol (SMTP) that allows an SMTP server to send a request to another SMTP server to send any email messages it has. Typically, SMTP is used with two other protocols, Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP), to request messages from a server; SMTP by itself cannot request mail to be sent.

ETRN is designed for use by anyone who is traveling and wants to access their email. ETRN can only be used with Internet service providers (ISPs) that support ETRN.

Event

A notification message providing information on one part of a *task*. A task can comprise several events. An event is generated by the control station or by an agent on a managed appliance.

Invoking a task generates one or more events.

See also *Task*.

Extended Simple Mail Transfer Protocol (ESMTP)

The Extended Simple Mail Transfer Protocol specifies extensions to the original SMTP protocol for sending email that supports graphics, audio and video files, and text in various national languages. ESMTP provides the capability for a client email program to inquire of a server email program about which capabilities it supports and then communicate accordingly.

File sharing

The public or private sharing of computer data or space in a network with various levels of access privileges.

File Transfer Protocol (FTP)

A standard Internet protocol and a way to exchange files between computers connected to the Internet. FTP is an application protocol that uses TCP/IP protocols. FTP is commonly used to transfer Web page files from the computer that was used to create the files to the computer that acts as the server for these files. It is also used to download programs and other files to your computer from other servers.

Using FTP, you can update—delete, rename, move and copy—files at a server. You need to log on to an FTP server. However, publicly available files are easily accessed using anonymous FTP.

FTP

See *File Transfer Protocol (FTP)*.

Gateway

A network device that acts as an entrance to another network. A gateway can also be any device that passes packets from one network to another network across the Internet.

HTML

See *HyperText Markup Language (HTML)*.

HTTP

See *HyperText Transfer Protocol (HTTP)*.

HyperText Markup Language (HTML)

A set of "markup" symbols or tags inserted in a text file intended for display on a World Wide Web browser. The markup tags tell the Web browser how to display a Web page's content, words, and images. HTML is a subset of Standardized Generalized Markup Language (SGML).

HyperText Transfer Protocol (HTTP)

A set of rules for exchanging files (text, graphic images, sound, video and other multimedia files) on the World Wide Web.

ICANN

See *Internet Corporation for Assigned Names and Numbers (ICANN)*.

IEEE 802.3

IEEE local area network (LAN) protocol that specifies an implementation of the physical layer and the media access control (MAC) sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet. Physical variations of the original IEEE 802.3 specification include 10Base2, 10Base5, 10BaseF, 10BaseT and 10Broad36. Physical variations for Fast Ethernet include 100BaseT, 100BaseT4 and 100BaseX.

IMAP

See *Internet Message Access Protocol (IMAP)*.

Integrated Services Digital Network (ISDN)

A system of digital telephone connections. This system allows data to be transmitted simultaneously across the world using end-to-end digital connectivity.

With ISDN, voice and data are carried by bearer channels (B channels) occupying a bandwidth of 64 Kb/s (some switches limit B channels to a capacity of 56 Kb/s). A data channel (D channel) handles signaling at 16 Kb/s or 64 Kb/s, depending on the type of service.

There are two basic types of ISDN service: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI consists of two 64 Kb/s B channels and one 16 Kb/s D channel for a total of 144 Kb/s. This basic service is intended to meet the needs of most individual users.

PRI is intended for users with greater capacity requirements. Typically, the channel structure is 23 B channels plus one 64 Kb/s D channel for a total of 1536 Kb/s. In Europe, PRI consists of 30 B channels plus one 64 Kb/s D channel for a total of 1984 Kb/s.

Internet Corporation for Assigned Names and Numbers (ICANN)

The private (non-government) non-profit corporation that has been formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system (DNS) management and root server system management functions. These functions were previously performed by the Internet Assigned Numbers Authority (IANA). The U.S. government is essentially turning over control of the Internet to ICANN, although domain name registration performed by Network Solutions, Inc. (NSI) will continue to be under U.S. government contract for a limited time.

Internet domain

An Internet domain is a host naming convention used to ensure that no two individual hosts on the global Internet have the same host name. An Internet domain should not be confused with an NT Domain.

Internet Message Access Protocol (IMAP)

Internet Message Access Protocol is a standard protocol for accessing email from your local server. IMAP is a client/server protocol in which email is received and held for you by your Internet server. You (or your email client) can view just the heading and the sender of the letter and then decide whether to download the mail from the server. You can also create and manipulate folders or mailboxes on the server, delete messages or search for certain parts or an entire note. IMAP requires continuous access to the server during the time that you are working with your mail.

IMAP can be thought of as a remote file server. Another protocol, Post Office Protocol (POP), can be thought of as a store-and-forward service.

POP and IMAP deal with receiving email from your local server; Simple Mail Transfer Protocol (SMTP) is a protocol for transferring email between points on the Internet. You send email with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP.

See also "Post Office Protocol 3 (POP3)" on page 113 and "Simple Mail Transfer Protocol (SMTP)" on page 116.

Internet Protocol (IP)

A network-layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. IP is defined in RFC 791.

InterNIC

The former organization responsible for registering and maintaining the com, edu, gov, net and org domain names on the World Wide Web. Domain name registration is now performed by Network Solutions, Inc. who will continue to be under U.S. government contract for a limited time.

IP address

A 32-bit address assigned to hosts using Transmission Control Protocol/ Internet Protocol (TCP/IP). An IP address belongs to one of five classes (A, B, C, D or E) and is written as four octets separated by periods (for example, 192.168.10.10), also called the dotted decimal format. Each address consists of a network number, an optional subnetwork number and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. Also called an Internet address.

ISDN

See *Integrated Services Digital Network (ISDN).*

LAN

See *local area network (LAN).*

Leased IP address

An IP address assigned by the Dynamic Host Configuration Protocol (DHCP) to an unrecognized computing device. This method involves setting up a leased pool of IP addresses that are allocated dynamically when new devices are booted and recognized on the network.

Local area network (LAN)

A high-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). A LAN connects workstations, peripherals, terminals and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the Open Systems Interconnection (OSI) model. Widely used LAN technologies include Ethernet, fiber distributed data interface (FDDI) and token ring.

See also *wide area network (WAN).*

Logical memory

See *virtual memory.*

Media access control (MAC) sublayer

The lower of the two sublayers of the data link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention is used.

Media access control (MAC) address

A standardized data-link-layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network, and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as a hardware address, a MAC-layer address and a physical address.

When your computer is connected to the Internet, a correspondence table relates your IP address to your computer's physical (MAC) address on the network

Name server

A program that constitutes the server half of the DNS client-server mechanism. A name server contains information about a segment of the DNS database and makes it available to a client called a resolver. A resolver is often just a library routine that creates queries and sends them across a network to a name server.

NAT

See *Network Address Translation (NAT)*.

Netmask

See *subnet mask*.

Network Address Translation (NAT)

A mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

Network Time Protocol (NTP)

A protocol built on top of the Transmission Control Protocol (TCP) that synchronizes the time of a local computer client or server to radio clocks and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods. Some configurations include cryptographic authentication to prevent accidental or malicious protocol attacks.

NTP

See *Network Time Protocol (NTP)*.

Packet

The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. The packet includes a header containing control information and (usually) user data. Packets are most often used to refer to network layer units of data.

PCI

See *Peripheral Component Interface (PCI)*.

Peripheral Component Interconnect (PCI)

Peripheral Component Interconnect (PCI) is an interconnection system between a microprocessor and attached devices in which expansion slots are spaced closely for high-speed operation. PCI is designed to be synchronized with the clock speed of the microprocessor, in the range of 20 MHz to 33 Mhz.

PCI transmits 32 bits at a time in a 124-pin connection (the extra pins are for power supply and grounding) and 64 bits in a 188-pin connection in an expanded implementation. PCI uses all active paths to transmit both address and data signals, sending the address on one clock cycle and data on the next. Burst data can be sent starting with an address on the first cycle and a sequence of data transmissions on a certain number of successive cycles.

Point-to-Point Protocol (PPP)

A protocol for communication between two computers using a serial interface, typically a personal computer connected by telephone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet and forward your requested Internet responses back to you. PPP uses the Internet protocol (and is designed to handle others).

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair, fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control for packet encapsulation. PPP can handle synchronous as well as asynchronous communication.

Point-to-Point Protocol over Ethernet (PPPoE)

A specification for connecting multiple computer users on an ethernet to a remote site through common customer-premises equipment such as a modem and similar devices. PPPoE can be used to allow an office or building full of users share a common digital subscriber line (DSL), cable modem or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dial-up connections, with the ethernet protocol, which supports multiple users in a local area network (LAN). PPP information is encapsulated within an Ethernet frame.

POP3

See *Post Office Protocol (POP3)*.

Post Office Protocol 3 (POP3)

Post Office Protocol (POP) is a standard protocol for receiving email. POP is a client/server protocol in which email is received and held for you by your Internet server. When you read your mail, all of it is immediately downloaded to your computer and no longer maintained on the server. POP3 is built into the Netscape Navigator and Microsoft Internet Explorer browsers.

POP can be thought of as a store-and-forward service. Another protocol, Internet Message Access Protocol (IMAP), can be thought of as a remote file server.

POP and IMAP deal with receiving email from your local server; Simple Mail Transfer Protocol (SMTP) is a protocol for transferring email between points on the Internet. You send email with SMTP and a mail handler receives it on your recipient's behalf. The mail is then read using POP or IMAP.

See also "Internet Message Access Protocol (IMAP)" on page 109 and "Simple Mail Transfer Protocol (SMTP)" on page 116.

PPP

See *Point-to-Point Protocol*.

PPPoE

See *Point-to-Point Protocol over Ethernet*.

RAID

See *Redundant Array of Independent Disks (RAID)*

Redundant Array of Independent Disks (RAID)

A redundant array of independent disks is a way of storing the same data in different places (thus, redundantly) on multiple hard disks. A RAID appears to the operating system to be a single logical hard disk.

There are a variety of different types and implementations of RAID, each with its own advantages and disadvantages. RAID Level 1 (RAID-1), also known as disk mirroring, consists of at least two drives that duplicate the storage of data.

Although RAID can protect against disk failure, it does not protect against operator and administrator (human) error, or against loss due to programming bugs.

RAID can be implemented in hardware or in software. Hardware RAID is always a “disk controller”, that is, a device to which one can cable up the disk drives. Software RAID is a set of kernel modules, together with management utilities that implement RAID purely in software, and require no extraordinary hardware.

Root name server

On the Internet, the root name server system is the manner in which an authoritative master list of all top-level domain names (such as .com, .net, .org and individual country codes) is maintained and made available.

SCSI

See *Small Computer System Interface (SCSI)*.

Secure Sockets Layer (SSL)

Secure Sockets Layer is a program layer created by Netscape Communications for managing the security of message transmissions in a network. Netscape's idea was that the programming for keeping your messages confidential ought to be contained in a program layer between higher-level protocols (such as HTTP or IMAP) and the TCP/IP layers of the Internet. The "sockets" part of the term refers to the sockets method of passing data between a client and a server program in a network or between program layers in the same computer.

SSL allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

These capabilities address fundamental concerns about communication over the Internet and other TCP/IP networks:

- SSL server authentication allows a user to confirm the identity of a server. SSL-enabled client software can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs. This confirmation can be important if, for example, the user is sending a credit card number over the network and wants to check the receiving server's identity.
- SSL client authentication allows a server to confirm a user's identity. Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the server's list of trusted CAs. This confirmation can be important if, for example, the server is a bank sending confidential financial information to a customer and wants to check the recipient's identity.
- an encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality. Confidentiality is important for both parties to any private transaction. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering—that is, for automatically determining whether the data has been altered in transit.

See also *Authentication* and *Encryption*.

Server

A system program that awaits requests from client programs in the same computer or across a network, and services those requests. A server can be dedicated, in which case this is its sole function, or non-dedicated, where the system can be used in other ways, such as a workstation.

Server Message Block (SMB)

A protocol that enables client applications in a computer to read and write files on a computer network and to request services from server programs in a computer network for systems running Microsoft Windows.

Simple Mail Transfer Protocol (SMTP)

The TCP/IP standard protocol for transferring electronic mail messages between points on the Internet. SMTP specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

SMTP is a protocol for transferring email between points on the Internet; Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) deal with receiving email from your local server. You send email with SMTP and a mail handler receives it on your recipient's behalf. The mail is then read using POP or IMAP.

See also "Internet Message Access Protocol (IMAP)" on page 109 and "Post Office Protocol 3 (POP3)" on page 113.

Simple Network Management Protocol (SNMP)

A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance and security on a network.

Small Computer System Interface (SCSI)

A parallel interface standard used by Apple Macintosh computers, PCs and many Unix systems for attaching peripheral devices to computers. SCSI interfaces provide for faster data transmission rates (up to 80 Mb/s) than standard serial and parallel ports. In addition, you can attach many devices to a single SCSI port, so that SCSI is really an input/output bus rather than simply an interface. Although SCSI is an ANSI standard, there are many variations, so two SCSI interfaces can be incompatible. For example, SCSI supports several types of connectors.

SMB

See *Server Message Block (SMB)*.

SMTP

see *Simple Mail Transfer Protocol (SMTP)*.

SNMP

See *Simple Network Management Protocol (SNMP)*.

SSL

See *Secure Socket Layer (SSL)*.

Subnet mask

A number that, in conjunction with an IP address, defines the set of IP addresses that are considered "local." For example, if your IP address is 192.168.25.77 and your subnet mask is 255.255.255.0, then addresses between 192.168.25.1 and 192.168.25.255 are considered local. Also known as netmask.

Swap file

A space on a hard disk used as the virtual memory extension of a computer's random access memory (RAM). Having a swap file allows the computer's operating system to pretend that it has more RAM than it actually does. The least-recently-used files in RAM are "swapped out" to your hard disk until they are needed later; in their place, new program segments or data can be "swapped in" to RAM.

Task

An executed operation that has a determined start and end point, such as adding an appliance or uploading a management application. A task is invoked by a user.

See also *Event*.

Transmission Control Protocol (TCP)

A connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A common name for the suite of protocols developed in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite. The TCP/IP protocols enable computers and networks to connect to an intranet or Internet.

Virtual memory

A concept that, when implemented by a computer and its operating system, allows programmers to use a very large range of memory or storage addresses for stored data.

Wide area network (WAN)

A data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Asynchronous transfer mode (ATM), frame relay, Switched Multimegabit Data Service (SMDS) and X.25 are examples of WANs.

See also *local area network (LAN)*.