ServiceWatch® Installation and User Guide

Version 2.0

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: March 2002
Part number: 100061-00 Rev 03

Contents

Preface

Figures

Tables

Preface

This preface provides an overview of the *ServiceWatch Installation and User Guide*, describes guide conventions, and lists other useful publications.

Introduction

This guide provides the required information to install and use the ServiceWatch® software. It is intended for use by network managers and system administrators who are responsible for monitoring and managing the performance and behavior of network and systems services, and it assumes a basic working knowledge of:

- Web browser interfaces
- Network management concepts

If the information in the release notes shipped with your software differs from the information in this guide, follow the release notes.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
ℹ	Note	Important features or instructions.
⚠	Caution	Risk of device configuration errors, loss of access, or loss of data.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Screen displays bold`	This typeface represents commands that you type.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names appear in text in one of two ways. They may be ■ referred to by their labels, such as “the Return key” or “the Escape key.” ■ written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). For example: Press [Ctrl]+[Alt]+[Del].
Words in **bold** type	Bold text indicates a button or field name.
Words in *italicized* type	Italics emphasize a point or denote new terms at the place where they are defined in the text.

Related Publications

The ServiceWatch documentation set includes the following:

- *ServiceWatch Installation and User Guide* (this manual)
- ServiceWatch online help pages, accessible through the browser client interface
- *ServiceWatch 2.0 Release Notes and Quick Start*

The Extreme Networks world-wide web site at **http://www.extremenetworks.com** provides much useful information:

- General information about Extreme Networks
- A link to the *ServiceWatch Installation and User Guide* in PDF format.
- A general description of ServiceWatch, and a link to a downloadable version of ServiceWatch version 2.0.
- Customers with a support contract can access the Technical Support pages, which provide the latest information on Extreme Networks software products, including the latest Release Notes, information on known problems, downloadable updates or patches as appropriate, and other useful information and resources.

Document Overview

This manual covers the following topics:

- Chapter 1: “ServiceWatch Overview.” A brief introduction to the features of ServiceWatch.
- Chapter 2: “Installing ServiceWatch.” Instructions for installing and running the ServiceWatch software and making server configuration changes, as well as uninstalling the ServiceWatch software.
- Chapter 3: “ServiceWatch Browser Client.” How to work with the browser-based client interface to set up and monitor network services monitoring requests.
- Chapter 4: “Using ServiceWatch Effectively.” Specific information about how to monitor most effectively the various services that the ServiceWatch software can handle.
- Chapter 5: “Summit Px1 Support.” Information on configuring optional ServiceWatch software support for the Summit Px1. These features will be displayed only with a license that includes the Summit Px1 features.
- Chapter 6: “Extending ServiceWatch via the API.” Documents how to use the optional extensibility features to develop monitoring modules for additional, custom monitoring capabilities.

1 ServiceWatch Overview

This chapter describes:

- The features of the ServiceWatch® software
- Information on technical support

Introduction

As local area and wide area networks have increased in number and grown in size, network services have become increasingly important to organizations. Users have come to depend on the network services as much as they do their computer. In today's Internet-enabled world, network services such as web hosting, bandwidth provisioning, usage-based billing—as well as traditional applications like electronic mail and ERP—are essential to the operation of service providers, web content providers, e-businesses and enterprises. The world wide web has become a lucrative source of revenue, as well as an important source of vital business information, and is growing at double-digit rates.

The possibility of downtime or poor performance is too high a risk in today's competitive business environment. Companies must eliminate potential points of failure and respond proactively to avoid problems before they occur. When network services go down or perform poorly, business suffers—in lost employee productivity, poor customer satisfaction, and lost revenue opportunities.

ServiceWatch software lets you proactively monitor the health and performance of your business-critical network services, and notifies you if response degrades or problems occur. ServiceWatch software identifies potential problems—including problems with underlying services such as name servers, file transfer servers, and so on—before they become catastrophic. You can take actions to correct the situation before more severe problems arise.

Combined with Extreme Networks' switched broadband infrastructure products, e-enabled businesses not only have scalable speed, bandwidth, size and quality of service across their networks, but also a proactive way to ensure that network services continue to perform at maximum efficiency.

ServiceWatch software monitors network services to make sure they are available and responding within a reasonable amount of time. ServiceWatch communicates with the network services using their native protocols (POP3, IMAP4, Telnet, NNTP, HTTP, FTP, DNS, etc.) and sends "test" queries to the specified servers. Depending on the protocol, ServiceWatch uses different methods to determine whether or not a particular network service is up and responding correctly. ServiceWatch also records the amount of time the network service takes to respond and reports any errors that occurred with the server.

Summary of Features

ServiceWatch software monitors the following network services:

- CIFS (Common Internet File System) Servers
- CVS (Concurrent Versions System)
- DHCP (Dynamic Host Configuration Protocol) Servers
- DNS (Domain Name System) Servers
- EPICenter Servers
- FTP (File Transfer Protocol) Servers
- HTTP (Web) Servers
- HTTPS (Secure Web) Servers
- IMAP4 Mail Servers
- LDAP (Lightweight Directory Access Protocol) Servers
- NFS (Network File System)
- News (NNTP) Servers
- ODBC

- Ping Protocol
- Pop3 Servers
- RADIUS Servers
- RPing Servers
- SMTP Mail Servers
- SNMP Agents
- TCP Layer 4
- Telnet Servers
- TFTP

ServiceWatch—Easy and Powerful Service Monitoring

ServiceWatch software is simple and easy to use. You log into the browser-based interface and enter the services you want to monitor along with response time thresholds and notification actions. The ServiceWatch software immediately begins monitoring your services. When a service does not respond correctly—reports an error or does not respond within your response-time threshold—ServiceWatch software can:

- Send email to an email address or an alphanumeric pager.
- Send SNMP traps to an SNMP manager.
- Run a program you specify, sending information about the failed network.
- Log an error report to the ServiceWatch software database for graphing or analysis.

You can also display real-time graphs and reports of response times or failure events for each service you monitor.

ServiceWatch software monitors any of the listed network services, regardless of which computer platform or operating system those services run on. For example, the web servers can run on a Solaris SPARC platform or a Windows NT platform, the NNTP servers can be on an SGI platform, the ftp server can be a Linux machine, or all these services can run on the same machine.

ServiceWatch software monitors the servers for performance and availability. If a server does not respond correctly, the ServiceWatch software returns information about the type of access error that occurred.

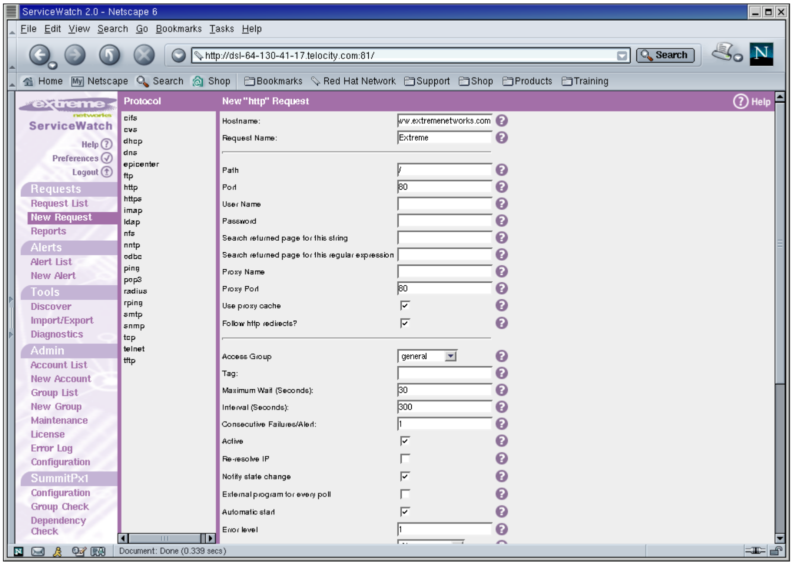
Easy to Set Up, Easy to Use

The browser-based client is login/password protected, and allows different users to have different levels of access. Some users can create and view all requests, some users can create requests in specific groups, and some users can only view requests, but not create or modify them.

You set up the services you want to monitor using a simple web browser-based interface. In addition to providing the service's contact information, you specify many options, including:

- How frequently to poll the service
- Response-time threshold (how long to wait for a response before deciding the service is down)
- How many consecutive failures must occur before creating an alarm
- What notification actions to take when a failure occurs, and which alerts to trigger
- User-defined error levels for service failures

All this is done through a simple form, shown in Figure 1-1, and typically takes just seconds to complete.



New "http" Request

Hostname:	ww.extremenetworks.com
Request Name:	Extreme
Path	/
Port	80
User Name	
Password	
Search returned page for this string	
Search returned page for this regular expression	
Proxy Name	
Proxy Port	80
Use proxy cache	☑
Follow http redirects?	☑
Access Group	general
Tag:	
Maximum Wait (Seconds):	30
Interval (Seconds):	300
Consecutive Failures/Alert:	1
Active	☑
Re-resolve IP	☐
Notify state change	☑
External program for every poll	☐
Automatic start	☑
Error level	1

Figure 1-1: Browser-based form for creating a ServiceWatch monitoring request

ServiceWatch Software Architecture

The main components of the ServiceWatch software are shown in Figure 1-2.

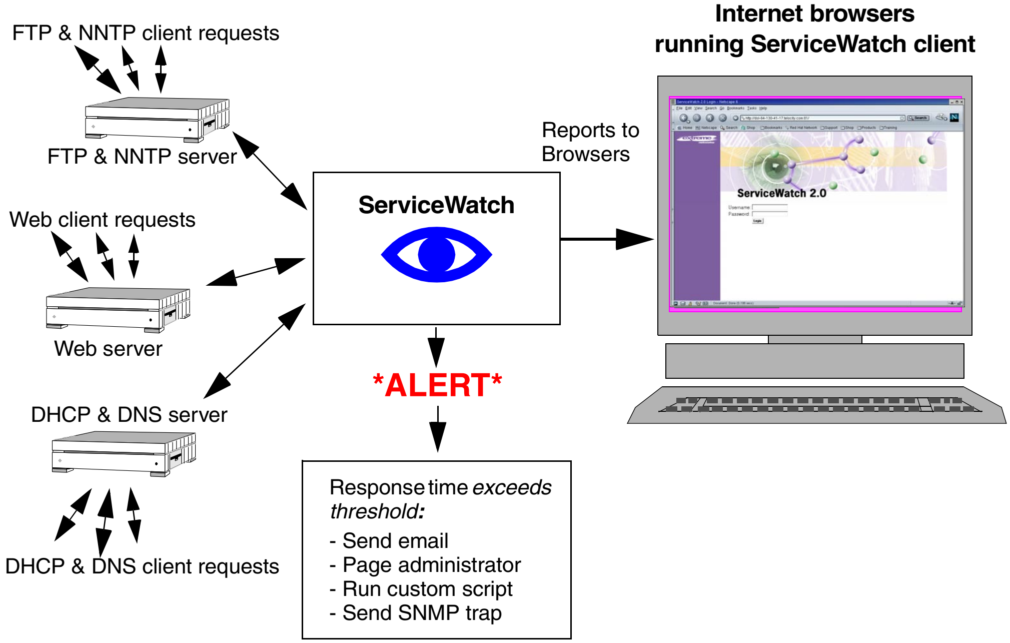


Figure 1-2: Overview of ServiceWatch

The ServiceWatch software "polls" a network service with a sample request appropriate to the service.

For example, to monitor a web server, it uses HTTP to request a page from the web server listed in the New Request form you filled out. If the web server responds with an error or does not respond within the response threshold (by default, 30 seconds), The ServiceWatch software takes whatever actions you specified. If the web server responds correctly, it records the poll results, including the round-trip response time.

The ServiceWatch web server provides the web pages that show the status of the monitored services, and it provides the interface for managing service monitoring requests.

Extensibility API

ServiceWatch software provides an extensibility API, shown in Figure 1-3, that allows you to develop scripts or programs to monitor the health and response times of additional services, such as databases or other mission-critical applications. New service monitoring programs are written in any programming language, and are easy for a programmer to create.

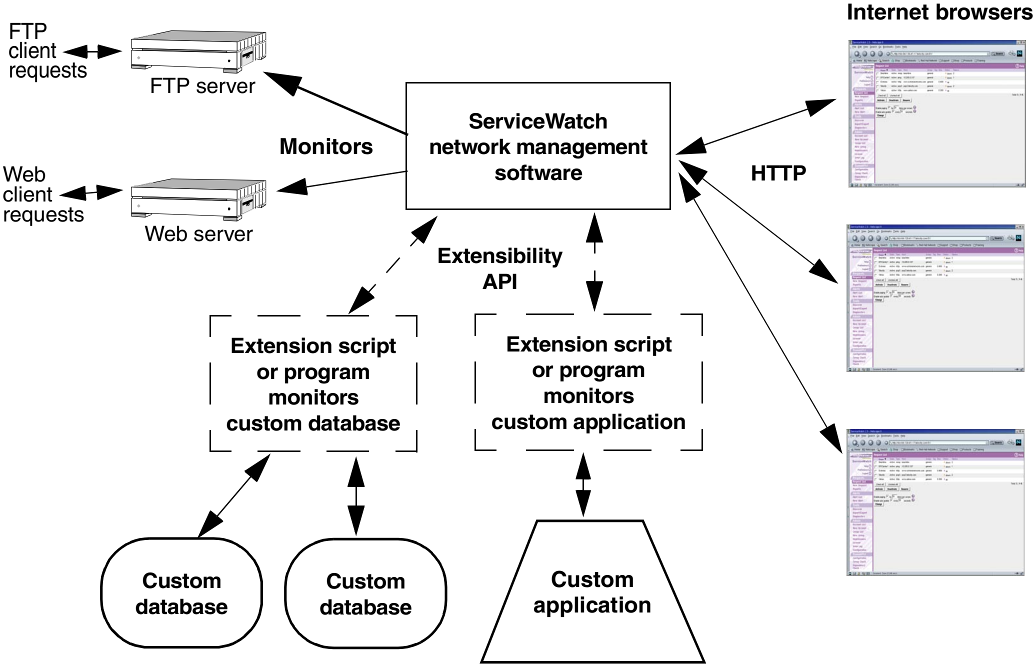


Figure 1-3: The ServiceWatch Extensibility API lets you create modules to monitor additional services

Technical Support

If you have problems installing the ServiceWatch software:

- Customers with a support contract can access the Technical Support pages at:

  ```
  http://www.extremenetworks.com/support/database.htm
  ```

  You must have a support contract before contacting Extreme Networks with any questions. ServiceWatch 2.0 allows you to monitor up to five services simultaneously without charge, however, it does not include technical support.

- All customers can access manuals and patches at:

  ```
  http://www.extremenetworks.com/support/techsupport.asp
  ```

2 Installing ServiceWatch

This chapter describes how to:

- Install the ServiceWatch software.
- Obtain a license if you downloaded the free evaluation version of the software.
- Start and stop the ServiceWatch software.

See the *ServiceWatch 2.0 Release Notes and Quick Start*, included with the ServiceWatch software, for the most current information about the procedures described in this chapter. The release notes are found on the CD in the `qstart.pdf` file.

You must have administrator privileges (Windows) or super-user (root) (Solaris and Linux) to perform most of the functions discussed in this chapter.

ServiceWatch System Requirements

Windows

ServiceWatch software version 2.0 runs under Microsoft Windows NT or Windows 2000. The requirements for installation on Windows NT or Windows 2000 are:

- Microsoft Windows NT 4.0 with service pack 6a or Microsoft Windows 2000 with service pack 2 running on an Intel platform
- 500 MHz or faster Pentium-compatible CPU
- 128 MB RAM (256 MB recommended)

- 20 MB disk space for the installation, plus a variable amount of disk space (from 10 to 100 megabytes) for the database
- CD-ROM drive (if installed via CD-ROM)
- Ethernet network interface card (NIC)

The ServiceWatch software is delivered and installed by a self-extracting file. The program files are found in the **\Program Files\Extreme Networks\ServiceWatch 2.0** directory.

Solaris

ServiceWatch software version 2.0 runs under Sun Microsystems Solaris Operating Environment, SPARC Platform Edition. The requirements for installation on Solaris are:

- An UltraSPARC system running Solaris 8
- Approximately 20 MB of disk space in `/opt` for the installation, plus a variable amount of disk space (from 10 to 100 megabytes) in `/var` for the database

Linux

ServiceWatch software version 2.0 runs under the Red Hat Linux Operating Environment version 7.1 or 7.2 on an Intel (X86/Pentium) platform. The requirements for installation on Linux are:

- Red Hat Linux version 7.1 or 7.2
- 500 MHz or faster Pentium-compatible CPU
- 128 MB RAM (256 MB recommended)
- 20 MB disk space for the installation, plus a variable amount of disk space (from 10 to 100 megabytes) in `/var` for the database
- CD-ROM drive (if installed via CD-ROM)

ServiceWatch Client Requirements

The ServiceWatch browser client runs on any system that supports the following browsers:

- Microsoft Internet Explorer 5 and later, under Windows NT or Windows 2000
- Netscape Navigator 6.2.1 and later, under Linux, Windows NT or Windows 2000
- Netscape Navigator 6.2.1 beta or later, under Solaris
- Netscape Navigator 4.78 and later, under Solaris, Linux, Windows NT or Windows 2000

Obtaining ServiceWatch

To obtain a copy of the ServiceWatch software you can:

- Purchase the packaged product on CD-ROM.
- Download a free evaluation copy the from Extreme Networks web site.

The ServiceWatch evaluation version will allow you to monitor up to five sites (requests). If you want to monitor more sites, you must purchase a packaged version with a permanent license key. See "Obtaining a License Key" on page 2-3 for more details.

You should install the software on a machine that has a static IP address rather than a dynamic IP address. If you install it on a machine with a dynamic IP address, it is possible that after every system reboot, the machine uses a different IP address.

Obtaining a License Key

To purchase the packaged version of the ServiceWatch software on CD, contact your Extreme Networks sales representative or Extreme Networks authorized distributor. An Activation Password is included in the package you receive. Use the Activation Password to obtain a permanent license key via the Extreme Networks web site.

To obtain a permanent license key:

1 Call +1 (888) 257-3000 or +1 (408) 579-2800 or contact your distributor, and purchase the product as usual.

2 When you receive the ServiceWatch product box, find a page (the "License Agreement Information" sheet) that contains an Activation Password.

3 Go to the Extreme Networks ServiceWatch registration web site at `http://www.extremenetworks.com/go/swlicense.htm`

The ServiceWatch software registration page appears. Fill in the requested information, including the following:

- The Activation Password from the “License Agreement Information” sheet. If you purchased multiple products or additional service licenses, you enter an Activation Password for each product.
- An email address to which the permanent license key should be sent.

4 Return email sends a 12-character permanent license key, which you enter after the installation process.

ServiceWatch license keys are available based on the total number of simultaneous network services to be monitored.

See “Licensing ServiceWatch” on page 2-13 for more details.

Installing ServiceWatch in Windows 2000 or NT

Installing from an Internet Download

If you obtained the ServiceWatch software by downloading it over the Internet from the Extreme Networks web site, the self-extracting WinZip file is named `swatch2-win.exe`.

To install this file, follow these steps:

1 Select and open the file:

`swatch2-win.exe`

A pop up window appears:

```
To unzip all files in swatch2-win.exe to the specified folder press
the UnZip button.
```

Make sure you select the box:

```
When done unzipping open: setup.exe.
```

2 Click **Unzip** to extract the ServiceWatch files to your system. The following dialog box appears:

```
WinZip Self-Extractor:... file(s) unzipped successfully.
```

3 Click **OK** to begin the ServiceWatch installation automatically.

4 For additional installation instructions, see step 4 in "Installing from CD-ROM" on page 2-5.

Installing from CD-ROM

If you obtained the ServiceWatch software by purchasing the CD-ROM, follow these steps to install ServiceWatch onto your system:

1 Close any open applications.

2 Insert the CD-ROM into the CD-ROM drive.

3 In most cases, the ServiceWatch Welcome screen appears automatically. If it does not:

   a From the **Start** menu, choose **Run**.

   The Run dialog box appears.

   b Type `d:\win32\setup` in the text box and click **OK**.

   If the CD-ROM is not drive `d`, substitute the correct drive letter.
   The ServiceWatch Welcome screen appears.

4 Follow the on-screen instructions to progress through the Welcome screen.

5 Click **Yes** to accept the license agreement.

6 Enter your company information.

7 In the Destination dialog box, choose one of two options:

   — Accept the default target drive and folder displayed in the Destination Directory box.

   — Click **Browse** and select or enter a new folder, a new drive, or both.

8 In the Web Server Port dialog box, enter the port number into the **Port** field that ServiceWatch uses to communicate with the monitored network services. The default port is 80. If you already have a web server installed on your system at port 80, select another port that is not being used.

   If you selected port 80 already during an install and that port is being used by another web server, stop the server, edit the `<swatch2-install-directory>swatch.ini` file, manually change the serverport line with the port you would like it to use, then start the server again.

9 In the Email Data dialog box, enter the hostname or IP address of your SMTP email server in the **IP** field.

10 Click **Next** to copy the files to your system.

11 Click **Finish** to complete the installation process. You should now install your ServiceWatch license, if you purchased the packaged version.

12 ServiceWatch is installed by default at:

```
C:\Program Files\Extreme Networks\ServiceWatch 2.0.
```

Installing ServiceWatch on Solaris

Installing from an Internet Download

If you obtained the ServiceWatch software by downloading it over the Internet from Extreme Networks' web site, the package file is named **EXTRsw2.bin.Z**.

To install this package, follow these steps:

1 Uncompress the file:

```
uncompress EXTRsw2.bin.Z
```

The uncompress command creates a file with the name **EXTRsw2.bin**.

2 Use the **pkgadd** command to add the package to your system.

```
pkgadd -d EXTRswa2.bin
```

*You must be super-user/root before you use the **pkgadd** command.*

3 Now skip to "Pkgadd Dialogue" on page 2-8.

Installing from CD-ROM

Mounting the CD-ROM Using the Volume Manager

1 Insert the CD-ROM into the system. If you are running the volume manager, or if you have no idea what the volume manager is, you can run the following command, which informs the volume manager to check and mount a new CD-ROM[1]. Type:

```
/usr/bin/volcheck
```

[1] If you are not sure if the volume manager is running, you can still type **volcheck**.

If you are running the File Manager you may see a window pop up with a CD-ROM icon, and the “swatch” label below the icon. If you do not see a window pop up, that is fine.

2. To make sure that the volume manager both found and mounted the ServiceWatch installation disk, type the **mount** command with no arguments, and look for a line that shows the CD-ROM is mounted, as shown below:

```
/usr/sbin/mount

/cdrom/swatch2 on /vol/dev/dsk/c0t2d0/swatch2 read only/nosuid on Mon
Apr 8 09:09:50 2000
```

3. If the CD-ROM appears to be mounted correctly, skip to “Adding the ServiceWatch Package” on page 2-8.

If you do not see a message similar to the **/cdrom/swatch2** line or other CD-ROM-related line from the **mount** command, then one or more of the following conditions may exist:

- The volume manager **(vold)** is not running.
- The volume manager is configured to not access CD-ROMs on your system. (Other applications, such as Wabi, for example, disable the volume manager’s use of the CD-ROM.)
- The volume manager is confused. **volcheck** and the volume manager do not always work as documented.

If the volume manager is running, but does not work correctly, it sometimes causes the CD-ROM to be difficult to mount. In this case, the quickest approach is to do the following:

1. Take the CD-ROM out of the CD-ROM drive.
2. Reboot the machine.
3. Disable the volume manager via the command:
   /etc/init.d/volmgt stop
4. Follow the instructions next in “Mounting a CD-ROM Without the Volume Manager,” to mount the CD-ROM without using the volume manager.

Mounting a CD-ROM Without the Volume Manager

To mount the CD without using the volume manager, follow these steps:

1 Make sure the volume manager is not running. Type:

```
/etc/init.d/volmgt stop
```

2 Make a new directory that is used to mount the CD-ROM, or find an existing empty directory that you know is available, such as **/mnt**. Since the **/mnt** directory exists, by default, on all machines we use that as an example. Mount the CD-ROM:

```
/usr/sbin/mount -F hsfs -r /dev/dsk/<devicename> /mnt
```

— The **-F hsfs** specifies the CD-ROM in “High Sierra” format.

— The **-r** specifies mounting the CD-ROM **read-only**.

— The *<devicename>* argument is the name of the “special” CD-ROM device on your system, in the form **c**<*n*>**t**<*n*>**d**<*n*>**s**<*n*> (for example, **c0t2d0s0**).

— The **/mnt** argument is the name of the empty directory where the CD-ROM file system is made available to you (this directory is known as the “mount point”).

Adding the ServiceWatch Package

Add the package to your system by typing:

```
pkgadd -d /cdrom/cdrom0/solaris/EXTRsw2.bin
```

You must be super-user/root before you use the ***pkgadd*** *command.*

Pkgadd Dialogue

After you run the **pkgadd** command, as described previously, the following message appears:

```
The following packages are available:
  1  EXTRswa2        ServiceWatch 2 - Network Services Monitoring
                     (sparc) 2.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

To continue with the installation process, follow these steps:

1 Type either **1** or **all** and press the return key. The following message appears:

```
Processing package instance <EXTRswa2> from </cdrom/EXTRsw2.bin>
```

```
ServiceWatch - Network Services Monitoring
(sparc) 2.0_EXTRswa2 Extreme Networks

If the window you are running the pkgadd command in is not
scrollable, you should turn scrolling on at this point. Then press
the Return key.
```

2 When you press **[Enter]**, the Extreme Networks license agreement appears. When it is finished, you are asked the following question:

```
Do you agree to the above terms [yes, no, repeat]?
```

If you answer “**`no`**,” the installation is terminated. If you answer “**`repeat`**,” the license agreement is displayed again.

If you answer “**`yes`**,” the installation continues with the following message:

```
You have agreed to the above terms. Continuing with installation.
```

3 You must now select a web server port for ServiceWatch to use.

```
You appear to have a web server already installed on your system at
the default web port 80
Web Server port number to use [81]:
```

4 You must now specify an SMTP mail server.

```
In order for ServiceWatch to send email alerts when there is a
service failure, you need to provide an SMTP mail server that can
send email for this host. If you do not know what machine is
configured as an SMTP server for you, please contact your site's
system administrator or Internet Service Provider. What is the SMTP
mail server that ServiceWatch can use to send email alerts?
```

The following messages appear:

```
You have 1186 megabytes free on the /var partition which is where
the ServiceWatch database is stored.
Installing ServiceWatch...
Using </opt> as the package base directory.
## Processing package information.
## Processing system information.   4 package pathnames are already
properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs. This package contains scripts
which will be executed with super-user permission during the process
of installing this package.
```

```
Do you want to continue with the installation of <EXTRsw2> [y,n,?] y
Installing ServiceWatch 2 - Network Services Monitoring as <EXTRsw2>
## Installing part 1 of 1.
```

ServiceWatch begins installing on your system, listing the names of various files that it is installing.

The following messages appear:

```
## Executing postinstall script.
********************************************************************
Creating /etc/swatch.conf Creating Sybase links....
Copying Default Database to /var/swatch/swatch.db
********************************************************************
ServiceWatch is now installed.
********************************************************************
Modifying configuration file /opt/swatch2/swatch.ini...
********************************************************************
Your ServiceWatch web page is:  http://beachline:81
********************************************************************
Use the following for the initial configuration:
Username: admin     [With no password]
********************************************************************
Starting ServiceWatch 2:
swatch2 startup succeeded
It can now take 5-20 seconds for the ServiceWatch web server to
initialize before it can communicate with browsers.
Installation of <EXTRsw2> was successful.
```

5. Type **q** to quit. The installation is complete. You should now install your ServiceWatch license, if you purchased the packaged version.
6. ServiceWatch is installed under `/opt/swatch2` and the ServiceWatch database is installed under `/var/swatch`.

Installing ServiceWatch on Linux

Installing from an Internet Download

If you obtained the ServiceWatch software by downloading it over the Internet from Extreme Networks' web site, the file is named **swatch2-linux.sh**. To install this file, follow these steps:

1 Become super-user.

2 Type the installation command to install the ServiceWatch package to your system:

```
sh swatch2-linux.sh
```

*You must be super-user/root before you use the **install** command.*

3 Now skip to "ServiceWatch Install" on page 2-12.

Installing from CD-ROM

If you obtained the ServiceWatch software by purchasing the CD-ROM, follow these steps to install ServiceWatch onto your system:

1 Insert the CD-ROM into the CD-ROM drive.

2 The CD-ROM automatically mounts onto **/mnt/cdrom**. If the CD-ROM does not mount onto the system, enter one of the following commands:

```
mount /mnt/cdrom
mount /dev/scd0 /mnt/cdrom
```

3 If the CD-ROM appears to be mounted correctly, type the installation command to install the ServiceWatch package to your system:

```
/mnt/cdrom/linux/swatch2-linux.sh
```

*You must be super-user/root before you use the **install** command.*

ServiceWatch Install

After you run the **install** command, as described previously, the following message appears:

```
Welcome to the ServiceWatch 2.0 installation for Linux

If the window you are running in is not scrollable, you should turn
scrolling on at this point. Then press the Return key.
```

To continue with the installation process, follow these steps:

1 When you press **[Enter]**, the Extreme Networks license agreement appears. When it is finished, you are asked the following question:

```
Do you agree to the above terms [yes, no, repeat]?
```

If you answer “**`no`**,” the installation is terminated. If you answer “**`repeat`**,” the license agreement is displayed again.

If you answer “**`yes`**,” the installation continues with the following message:

```
You have agreed to the above terms. Continuing with installation.
```

2 You must now specify a directory in which to install ServiceWatch.

```
The ServiceWatch directory must be a local directory, and NOT an
NFS-mounted directory.
Where would you like ServiceWatch installed: [/opt/swatch2]
```

3 You must now select a web server port for ServiceWatch to use.

```
You appear to have a web server already installed on your system at
the default web port 80
Web Server port number to use [81]:
```

4 You must now specify an SMTP mail server.

```
In order for ServiceWatch to send email alerts when there is a
service failure, you need to provide an SMTP mail server that can
send email for this host. If you do not know what machine is
configured as an SMTP server for you, please contact your site's
system administrator or Internet Service Provider.
What is the SMTP mail server that ServiceWatch can use to send email
alerts? sol

You have 332 megabytes free on the /var partition which is where the
ServiceWatch database is stored.
```

```
Press the RETURN key to continue installation.
```

5 Press the Return key.

The following messages appear:

```
Installing ServiceWatch...

The installation is complete.
********************************************************************
** ServiceWatch 2 is now installed.
********************************************************************
** Modifying configuration file /opt/swatch2/swatch.ini...
********************************************************************
** Your ServiceWatch web page is:
http://linuxcorp.extremenetworks.com:81
********************************************************************
** Use the following for the initial login: Username: admin [With no
password]
********************************************************************
** Starting ServiceWatch 2:
 It can now take 5-20 seconds for the ServiceWatch web server to
initialize before it can communicate with browsers.
```

The installation is now complete. You should now install your ServiceWatch license, if you purchased the packaged version.

Licensing ServiceWatch

ServiceWatch software licenses are available based on the total number of simultaneous network services to be monitored.

You can purchase optional licenses that allow you to monitor more requests, or add support for Summit Px1 switches.

To add support for HTTPS/SSL, fill out a form at the Extreme Networks web site `http://www.extremenetworks.com/go/SW20Encrypt.htm` If approved, you are told how to add HTTPS/SSL to ServiceWatch 2.0.

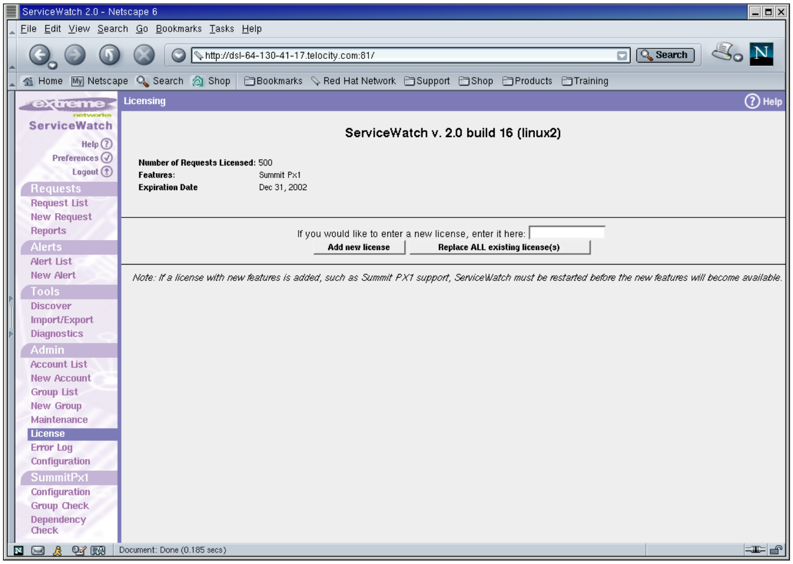
For more information on obtaining additional ServiceWatch licenses, see “Obtaining a ServiceWatch License” on page 4-38.

Installing the ServiceWatch License

After you have installed the ServiceWatch software and obtained your license key, follow these steps to install the license:

1 Start ServiceWatch and login as Admin.

2 From the ServiceWatch main page, click the **License** button. The License page appears as shown in Figure 2-1.



ServiceWatch v. 2.0 build 16 (linux2)

Number of Requests Licensed: 500
Features: Summit Px1
Expiration Date Dec 31, 2002

If you would like to enter a new license, enter it here:

Note: If a license with new features is added, such as Summit PX1 support, ServiceWatch must be restarted before the new features will become available.

Figure 2-1: ServiceWatch License page

3 Enter your license key into the box. An example of a key is:

`JBwHDzF5BZDDXIBVC`

4 Click **Add New License** to add a new license, or click **Replace ALL Existing Licenses** to replace your current licenses.

For more information on the ServiceWatch License feature, see “License” on page 4-37.

Removing ServiceWatch

Windows

To remove the ServiceWatch software from a Windows NT or Windows 2000 system, follow these steps:

1 From the **Start** menu highlight **Settings**, pull right, and select **Control Panel**. This displays the Control Panel folder.

2 From the Control Panel folder, double-click **Add/Remove Programs**. This displays the Add/Remove Program Properties window.

3 From the list of installed programs, select **ServiceWatch 2.0** and click **Add/Remove**. Follow the instructions to remove the component.

Solaris

*You must be super-user (root) to use the **pkgrm** command.*

You can remove ServiceWatch from your system by typing:

```
pkgrm EXTRsw2
```

You are navigated through the following type of dialog:

```
The following package is currently installed:
   EXTRsw2          ServiceWatch 2 - Network Services Monitoring
                      (sparc) 2.0

Do you want to remove this package? y

## Removing installed package instance <EXTRsw2>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q]
```

Answer **y** to continue with the uninstall.

```
## Verifying package dependencies.
## Processing package information.
## Executing preremove script.
## Removing pathnames in class <none>
Shutting down ServiceWatch 2: Shutdown was successful.
Removing database files in /var/swatch...done
## Removing pathnames in class <none>
/opt/swatch2/unixrecover
/opt/swatch2/swatchunix.pyc
/opt/swatch2/swatch.pyc
/opt/swatch2/swatch.ini.dist
/opt/swatch2/px1engine/px1db.pyc
..........................
..........................
/opt/swatch2/Alerts/Email/__init__.pyc
/opt/swatch2/Alerts/Email/Email.pyc
/opt/swatch2/Alerts/Email
/opt/swatch2/Alerts
/opt/swatch2 <non-empty directory not removed>
/etc/rc3.d/S91swatch2 /etc/rc3.d <shared pathname not removed>
/etc/rc2.d/K91swatch2 /etc/rc2.d <shared pathname not removed>
/etc/init.d/swatch2 /etc/init.d <shared pathname not removed>
/etc <shared pathname not removed> ## Executing postremove script.
********************************************************************
Cleaning up remaining files...
********************************************************************
## Updating system information.  Removal of <EXTRsw2> was successful.
```

After this sequence of messages, ServiceWatch is removed from your system.

Linux

*You must be super-user (root) to use the **remove** command.*

You can remove the ServiceWatch software from your system by typing:

```
   /<install-directory>/swatch.remove
```

where <install-directory> is the directory where you installed ServiceWatch.

```
   # ./swatch.remove
   Extreme Networks ServiceWatch Removal
```

```
Are you sure you wish to remove ServiceWatch? [n] y

Where is ServiceWatch installed: [/opt/swatch2]

Do you wish to remove the ServiceWatch database files and directory?
[y]
The ServiceWatch database files will be removed.
Shutting down ServiceWatch 2:
[OK]

done
Removing database /var/swatch...done
Removing RC scripts...Removing ServiceWatch contents in
/opt/swatch2...
Finished removing ServiceWatch.
```

After this sequence of messages, ServiceWatch is removed from your system.

Determining Whether ServiceWatch is Installed

Windows

To determine whether or not the ServiceWatch software is already installed on a machine, follow these steps:

1. From the **Start** menu, highlight **Settings**, pull right, and select **Control Panel**. This displays the Control Panel folder.
2. From the Control Panel folder, double-click **Add/Remove Programs**. This displays the Add/Remove Program Properties window.
3. From the list of installed programs, locate **ServiceWatch 2.0**. If the program is listed, it is installed on your machine. If the program is not listed, it is not installed on your machine.

See “Installing from CD-ROM” on page 2-5 for more details.

Solaris

To determine whether or not the ServiceWatch software is already installed on a machine, type:

```
pkginfo | grep -i EXTRsw2
```

If the ServiceWatch software is installed on the machine, the following message appears:

```
Application EXTRsw2 ServiceWatch 2 - Network Services Monitoring
```

If it is not installed on the machine, the **pkginfo** command ends without displaying the above line.

Linux

To determine whether or not the ServiceWatch software is already installed on a Linux machine, type:

```
cat /etc/swatch.conf
```

If the ServiceWatch software is installed on your machine, your system reports the installation location of ServiceWatch 2 on your system, for example:

```
/opt/swatch2
```

If it is not installed on your machine, your system reports:

```
cat: /etc/swatch.conf: No such file or directory
```

ServiceWatch Client Access Permissions

The ServiceWatch browser-based client is login/password protected, and allows different users to have different levels of access. Some users can create and view all requests, some users can create requests in specific groups, and some users can only view requests in specific access groups, but not create or modify them.

For more information on changing access permissions, adding users, and creating groups, see "Managing Accounts and Groups" on page 3-32.

Changing Passwords

By default, the username for ServiceWatch is "admin" with no password.

If you want to change the Admin password, see "Setting User Preferences" on page 4-41.

ServiceWatch Configuration File

The ServiceWatch configuration file under Windows is located at: **Program Files\Extreme Networks\ServiceWatch****swatch.ini.**

The ServiceWatch configuration file under Solaris or Linux is located at: **/<install-directory>/swatch.ini,** where **<install-directory>** is where you installed ServiceWatch.

You may need to modify the following the port on which your web server is running.

You must have administrator privileges (Windows) or be super-user (root) (Solaris and Linux) to modify the configuration file.

A sample configuration file is shown here.

```
; ServiceWatch customized INI file

[Web]
serverport = 80
```

```
[DataEngine]
smtp_server = mail.telocity.com
self_check_interval = 3600
min_thread = 10
log_level = 1
max_thread = 200

[DataBase]
port = 9966
```

Starting and Stopping ServiceWatch

By default, the ServiceWatch software automatically starts when your system is booted, and stops when the system is shut down. The ServiceWatch script is run at boot up and shutdown.

All requests are automatically started, expect for those requests that have autostart turned off (via the Automatic Start option).

Windows

An administrator can manually start and stop the ServiceWatch software two ways:

1 From the **Start** menu highlight **Programs**, pull right, highlight **ServiceWatch 2.0** and and select **Stop ServiceWatch**.

2 From the Start menu highlight Settings, pull right, and click on the Control Panel. This displays the Control Panel folder.

  a From the Control Panel folder, double-click **Services** (Windows NT) or double-click **Admin Tools** and double-click Services (Windows 2000). This displays the Services window.

  b From the list of services, select **ServiceWatch** and select the **Start** or **Stop** button. The service is running if **Started** is listed in the status column. The service is **Stopped** if the status column is blank.

If you try these methods, but ServiceWatch is unable to start, look at the Task Manager. Press CTRL+ ALT + DEL, click the Task Manger button, and click the Processes tab. Check for `PythonService.e` and `dbeng7.exe`, and make sure they are stopped before another try. The log file (in `<install directory>\Log`) should list why the service cannot be started.

The most common cause of not being able to start ServiceWatch is because the database cannot be started. The database file may have pending transactions from a previous run. To recover the database file, make sure the service applet does not have the `PythonService.exe` and `dbeng7.exe` files, then use the `dbrecovery.bat` utility to recover the database (by double clicking the icon). After that try to start ServiceWatch again.

Sometimes the `dbeng7.exe` process cannot be stopped. In that case, you may need to restart your computer.

Solaris

By default, the ServiceWatch software automatically starts when your system is booted, and stops when the system is shut down. The `/etc/rc3.d/S89swatch2` script is run at boot up, and the `/etc/rc2.d/K89swatch2` script is run on shutdown.

All requests are automatically started, expect for those requests that have autostart turned off (via the Automatic Start option).

As super-user you may also manually start and stop ServiceWatch as shown below:

```
# Start ServiceWatch:
/etc/init.d/swatch2 start

# Stop ServiceWatch:
/etc/init.d/swatch2 stop
```

Sometimes the dbeng7 and python swatchunix.pyc processes do not stop. In that case you need to kill the processes:

```
dbeng7
python swatchunix.pyc
```

You can do that entering the following commands:

1 `ps -ef | grep dbeng7`

2 `kill -9 <process-id of dbeng7>`

3 `ps -ef | grep python2.1`

4 `kill -9 <process-id of python2.1>`

Linux

By default, the ServiceWatch software automatically starts when your system is booted, and stops when the system is shut down. The `/etc/rc.d/init.d/swatch` script is run at boot up and shutdown.

All requests are automatically started, expect for those requests that have autostart turned off (via the Automatic Start option).

As super-user you may also manually start and stop ServiceWatch as shown below:

```
# Start ServiceWatch:
/etc/rc.d/init.d/swatch2 start

# Stop ServiceWatch:
/etc/rc.d/init.d/swatch2 stop
```

Sometimes the dbeng7 and python swatchunix.pyc processes do not stop. In that case you need to kill the processes:

```
dbeng7
python swatchunix.pyc
```

You can do that entering the following commands:

1. `ps -ef | grep dbeng7`
2. `kill -9 <process-id of dbeng7>`
3. `ps -ef | grep python2.1`
4. `kill -9 <process-id of python2.1>`

Tips on Using ServiceWatch

The following tips describe how to effectively use and run ServiceWatch.

Where to Run ServiceWatch

You should run the ServiceWatch agent on a machine *different* than the network services you plan to monitor. For example, if you are monitoring a web server on www.cnn.com, then run it on a machine other than www.cnn.com.

If you run the ServiceWatch software on the same machine as the service you are monitoring, you are not testing the *network* connection to the service, though you are testing the response time for queries as if a user was logged into the www.cnn.com machine. Having the ServiceWatch software monitor a web server from a machine *other* than the web server also tests the network connection between the remote machine and the web server. For Internet servers, it is useful to run the ServiceWatch software from an Internet machine at a remote site (depending on the reliability of the Internet near you).

Impact of ServiceWatch on Network Services

The impact of the ServiceWatch software on network services should be insignificant. In the case of web servers, a typical, well-performing web server should be able to process far more than 500 web "operations" (such as GET and PUT) per second. As an example, assume ServiceWatch polls a web server once every 30 seconds. In 30 seconds, a web server that processes 500 web operations a second would have the capacity of performing 900,000 web operations. A ServiceWatch query every 30 seconds would take up .00001% of the capacity of the web server.

Similarly, for other servers, such as FTP, DNS, etc. the impact on the server should be quite low, due to the infrequent (every 30 or so seconds) queries being generated by the ServiceWatch software. To ensure that it does not adversely affect very busy services, you can set the polling interval to a longer time.

Restarting Failed Servers Automatically

After you run the ServiceWatch software for a while and have a feel for the response time of a network services server during different days and times, you might consider having it or your SNMP network management software restart failed servers.

For example, if a web server does not respond to queries for a certain amount of time, you can configure the ServiceWatch software to run a program that restarts the web server. Similarly, a trap request can cause your SNMP management program to run such a program (not all SNMP managers have this capability, however). You probably want to wait until multiple (two or three) consecutive events are generated, showing that the web server is really down, rather than restarting a web server immediately after the first event. This depends on the reliability of your network and web server.

Multiple Email Servers

During the installation, you are asked to enter the hostname or IP address for your SMTP mail server. Make sure you enter a hostname or IP address for an SMTP server.

If your site has multiple email servers, it is possible that the Microsoft Exchange Server where you receive your email is not an SMTP server. If you are unable to export saved requests via email, contact your local system administrator to locate the hostname or IP address of the SMTP server.

Database Password Encryption

The database stores passwords in unencrypted form. For example, the following pollers have password fields: HTTP, HTTPS, FTP, IMAP, POP3, NNTP. When you create a new request and enter a password in the web browser, the password characters appear as asterisks, rather than the real password.

However, be aware that the database stores these passwords in an unencrypted format. Also, when you perform an export of the requests to a file, the passwords are also exported in an unencrypted form.

Troubleshooting ServiceWatch

Problem: I tried to stop the ServiceWatch processes, but they aren't stopping (possibly because ServiceWatch ran out of disk space, for example). How do I make sure ServiceWatch is stopped?

Solution: To make sure ServiceWatch is stopped on Linux or Solaris, kill the python2.1 processes and dbeng7 processes. On Linux, as super-user enter:

```
killall -9 python2.1
killall -9 dbeng7
```

On Solaris, as super-user enter:

```
ps -ef | grep python
```

Then kill the python processes:

```
ps -ef | grep dbeng7
```

Then kill the dbeng7 processes. The dbeng7 process(es) are the imbedded database.

In Windows, use ctrl+alt+delete to start the Task manager, find the processes `PythonService.e` and `dbeng7.exe` on the Processes tab, and stop them by selecting them and clicking the End Process button.

Problem: I can't start the server and the log file reports:

```
Failed to connect to database. Will try 3 times more
Failed to connect to database. Will try 2 times more
Failed to connect to database. Will try 1 times more
Failed to connect to database. Will try 0 times more
swDatabaseDown, “Database connection refused”
```

Solution: You should:

Try to kill all the python processes and `dbeng7` (UNIX), or `PythonService.e` and `dbeng7.exe` (Windows).

In UNIX, run unixrecover, in Windows, double click the icon dbrecovery.bat, and a dialog box appears showing the recovery status.

After the recover script finishes, try to restart the server as usual.

Problem: I am not receiving email or pages.

Solution:

Solaris and Linux: Check the SMTP Server configuration under Admin/Configuration. The machine listed must have sendmail or other valid SMTP server set up correctly in order for you to send email to your email address or pager.

Win32: Make sure the SMTP email server is set up correct under the Admin/Configuration section. Make sure your email server uses SMTP and will send SMTP mail on behalf of the ServiceWatch client machine.

Problem: I know a web server is up, but ServiceWatch says it is down.

Solution: You may need to specify a proxy host (in many networks, machines need to specify a proxy host, due to the firewall configuration). The proxy host is specified in http and https requests. For example:

```
Proxy Name: 10.0.1.60
Proxy Port: 80
```

Problem: I am getting messages saying I couldn't communicate correctly with the Summit Px1.

Solution: The Summit Px1 needs to be running version 1.1.0 or later of the Px1 software.

Problem: The browser does not display the right information (sometimes a menu is not being updated when it should, and it's basically a bit off).

Solution: Is the browser supported? Make sure the cache usage is configured correctly by following these steps.

Internet Explorer:

1. From the Tools menu, click Internet Options.
2. From the General tab, Temporary Internet Files section, click Settings.
3. Make sure Automatically is set.

Netscape 6.2:

1. From the Edit menu, click Preferences.
2. Click the Advanced drop list and click Cache.
3. In the Compare the page in the cache to the page on the network section, make sure Automatic is selected.

Problem: Everything was running fine for months and suddenly the log reports the database failed. Why?

Solution: Check to make sure you didn't run out of disk space where the database resides (/var/swatch on Linux and in the swatch2-installation directory for Windows).

Problem: My request is in infinite loop status.

Solution: This means the poller is in an infinite waiting status. This situation is complicated, but it could be due to the service hanging on the client, or simply because the poller did not timeout as it should have. Check the service first, then manually change the request's status to active, and see if it still happens.

You must manually activate the request once the problem is solved. An alert may or may not be sent in this case, depending on where the request was blocked.

3 ServiceWatch Browser Client Interface

The ServiceWatch browser client uses an Internet browser such as Netscape Navigator or Microsoft Internet Explorer to provide an easy-to-use interface for managing ServiceWatch requests, viewing service status, and creating reports and graphs.

This chapter describes how to do the following:

- Launch the ServiceWatch browser client interface.
- Access the ServiceWatch online Help system.
- Use the ServiceWatch client to create, modify, and remove ServiceWatch monitoring requests.
- Create reusable alerts, allowing you to be notified in various ways when a service is up or down.
- Control user access through accounts and groups.
- Log out of the ServiceWatch browser.

ServiceWatch Browser Client

The ServiceWatch browser client user interface runs within a JavaScript or Jscript-enabled browser, including:

- Microsoft Internet Explorer 5 and later, under Windows NT or Windows 2000
- Netscape Navigator 6.2.1 and later, under Linux, Windows NT or Windows 2000
- Netscape Navigator 6.1.2 beta or later, under Solaris
- Netscape Navigator 4.78 and later, under Solaris, Linux, Windows NT or Windows 2000

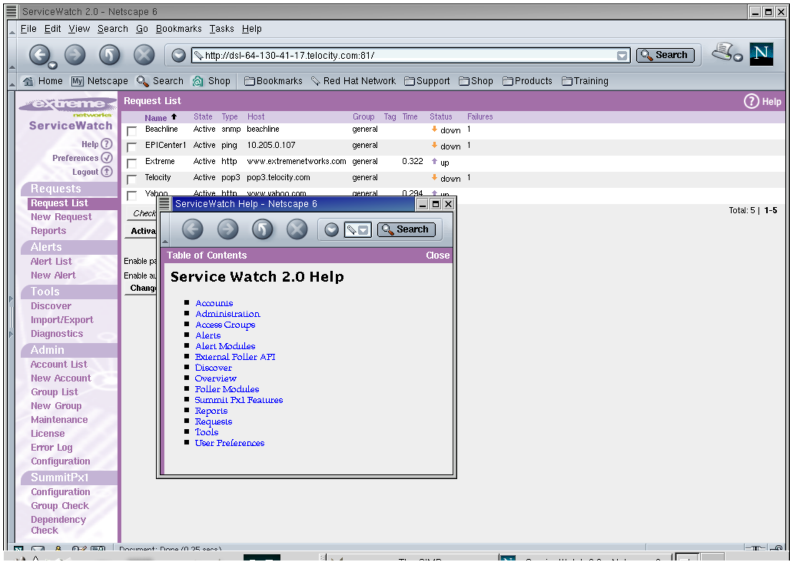
The ServiceWatch browser-based client is login/password protected, and allows different users to have different levels of access. Some users can create and view all requests, some users can create requests in specific groups, and some users can only view requests in specific access groups, but not create or modify them.

ServiceWatch Help

The **Help** button at the top of the ServiceWatch navigation pane, on the left side of the browser window, starts the ServiceWatch Help system. Tabs and links in the navigation pane, and various pages let you access an overview of ServiceWatch and detailed information about the functional areas of the product.

In addition, you can click the Help button, as shown in Figure 3-1, on any ServiceWatch page to open a Help window that describes the specific item as shown in Figure 3-2.

Figure 3-1: ServiceWatch Help button



Request List

	Name	State	Type	Host	Group	Tag	Time	Status	Failures
□	Beachline	Active	snmp	beachline	general			down	1
□	EPICenter1	Active	ping	10.205.0.107	general			down	1
□	Extreme	Active	http	www.extremenetworks.com	general		0.322	up	
□	Telocity	Active	pop3	pop3.telocity.com	general			down	1
□	Yahoo	Active	http	www.yahoo.com	general		0.294	up	

Service Watch 2.0 Help

- Accounts
- Administration
- Access Groups
- Alerts
- Alert Modules
- External Poller API
- Discover
- Overview
- Poller Modules
- Summit Px1 Features
- Reports
- Requests
- Tools
- User Preferences

Figure 3-2: ServiceWatch Help system

Running the ServiceWatch Client

The ServiceWatch agent and web server must be running before you can use a ServiceWatch client.

To run one of the ServiceWatch client interfaces, follow these steps:

1 Start your web browser.

2 Enter the following URL:

`http://<host>`

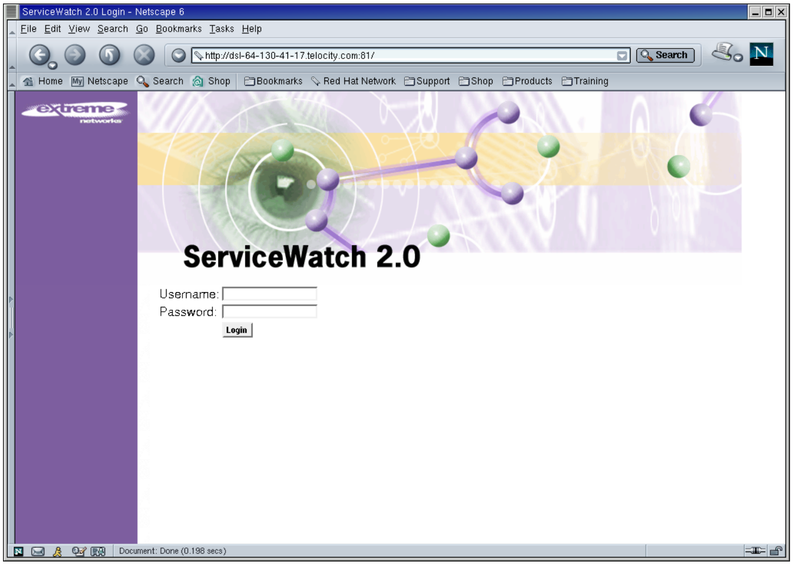
In the URL, replace *<host>* with the name or IP address of the system where the ServiceWatch software is running.

If ServiceWatch is assigned to use a HTTP port other than the default (80), enter the port number along with the host name:

`http://<host>:<port>`

Replace <port> with the TCP port number that you assigned to the ServiceWatch web server during installation.

If you are logging in for the first time, a login screen appears, as shown in Figure 3-3.



ServiceWatch 2.0 Login - Netscape 6

http://dsl-64-130-41-17.telocity.com:81/

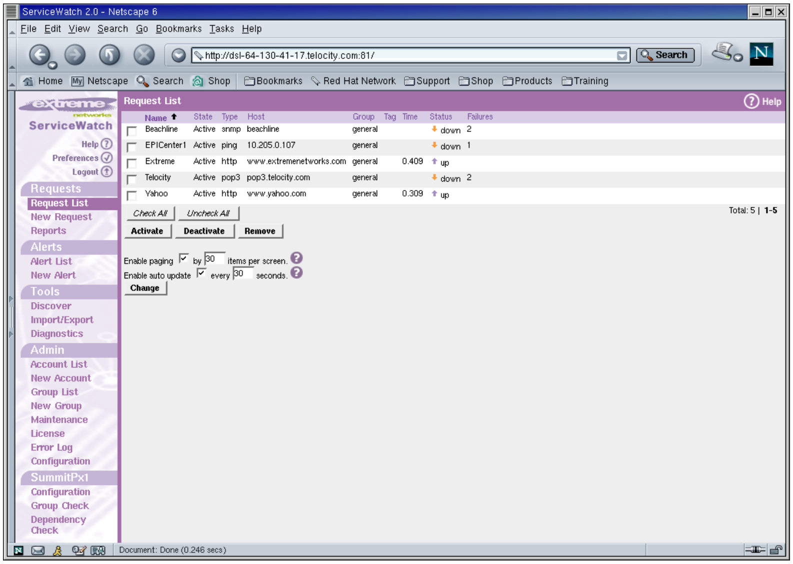
Document: Done (0.198 secs)

Figure 3-3: ServiceWatch Login screen

3 Enter your username and password, and click **Login**.

— By default, the username for ServiceWatch is “admin” with no password.

After logging in successfully, the ServiceWatch Request List appears. Figure 3-4 shows the Request List as it appears in the browser client running in Netscape Navigator.



	Name ↑	State	Type	Host	Group	Tag	Time	Status	Failures
□	Beachline	Active	snmp	beachline	general			↓ down	2
□	EPICenter1	Active	ping	10.205.0.107	general			↓ down	1
□	Extreme	Active	http	www.extremenetworks.com	general		0.409	↑ up	
□	Telocity	Active	pop3	pop3.telocity.com	general			↓ down	2
□	Yahoo	Active	http	www.yahoo.com	general		0.309	↑ up	

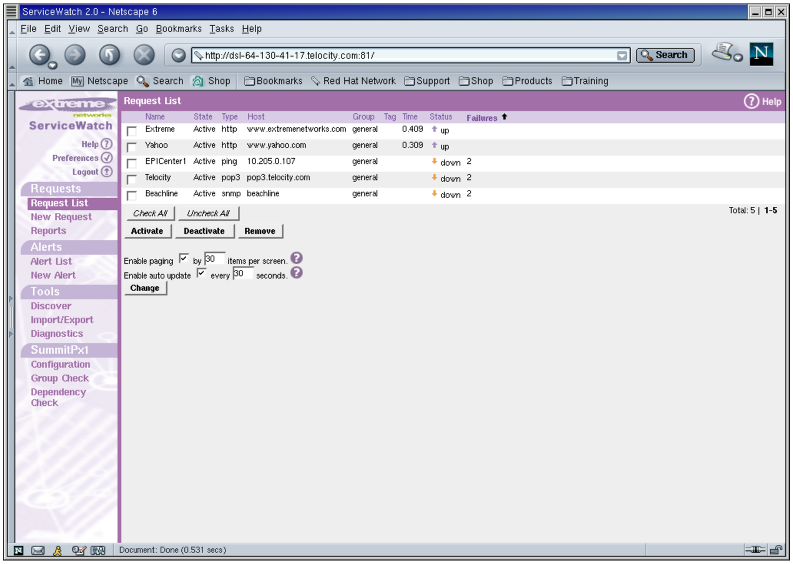
Total: 5 | **1-5**

Enable paging ☑ by 30 items per screen.
Enable auto update ☑ every 30 seconds.

Figure 3-4: ServiceWatch Request List, for a user with Admin access

If you logged in as Admin, you have a **Requests** tab, which provides a menu for viewing the Request List, creating a new request, and generating Reports. You also have an **Alerts** tab, a **Tools** tab, an **Admin** tab, and a **Summit Px1** tab, if the Summit Px1 option is enabled.

Figure 3-5 shows the Request List as it appears for a user logged in with User access, running in Netscape Navigator.



Request List

	Name	State	Type	Host	Group	Tag	Time	Status	Failures ↑
□	Extreme	Active	http	www.extremenetworks.com	general		0.409	↑ up	
□	Yahoo	Active	http	www.yahoo.com	general		0.309	↑ up	
□	EPICenter1	Active	ping	10.205.0.107	general			↓ down	2
□	Telocity	Active	pop3	pop3.telocity.com	general			↓ down	2
□	Beachline	Active	snmp	beachline	general			↓ down	2

Total: 5 | **1-5**

Check All | Uncheck All

Activate | Deactivate | Remove

Enable paging ☑ by 30 items per screen.

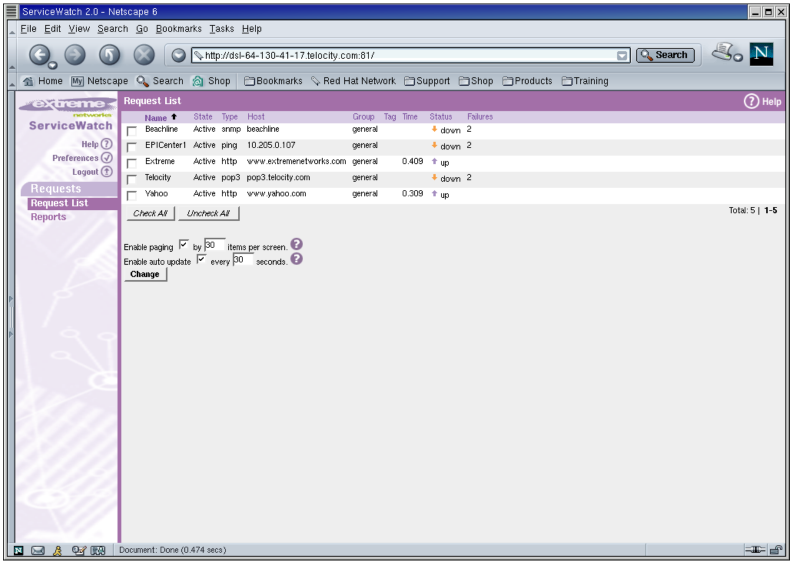
Enable auto update ☑ every 30 seconds.

Change

Figure 3-5: ServiceWatch Request List, for a user with User access

If you logged in as User, you have a **Requests** tab, which provides a menu for viewing the Request List, creating a new request, and generating reports. You also have an **Alerts** tab, and a **Tools** tab.

Figure 3-6 shows the Request List as it appears for a user with Guest access, running in Netscape Navigator.



Request List

	Name	State	Type	Host	Group	Tag	Time	Status	Failures
□	Beachline	Active	snmp	beachline	general			↓ down	2
□	EPICenter1	Active	ping	10.205.0.107	general			↓ down	2
□	Extreme	Active	http	www.extremenetworks.com	general		0.409	↑ up	
□	Telocity	Active	pop3	pop3.telocity.com	general			↓ down	2
□	Yahoo	Active	http	www.yahoo.com	general		0.309	↑ up	

Check All   Uncheck All

Total: 5 | **1-5**

Enable paging ☑ by 30 items per screen.

Enable auto update ☑ every 30 seconds.

Change

Figure 3-6: ServiceWatch Request List, for a user with Guest access

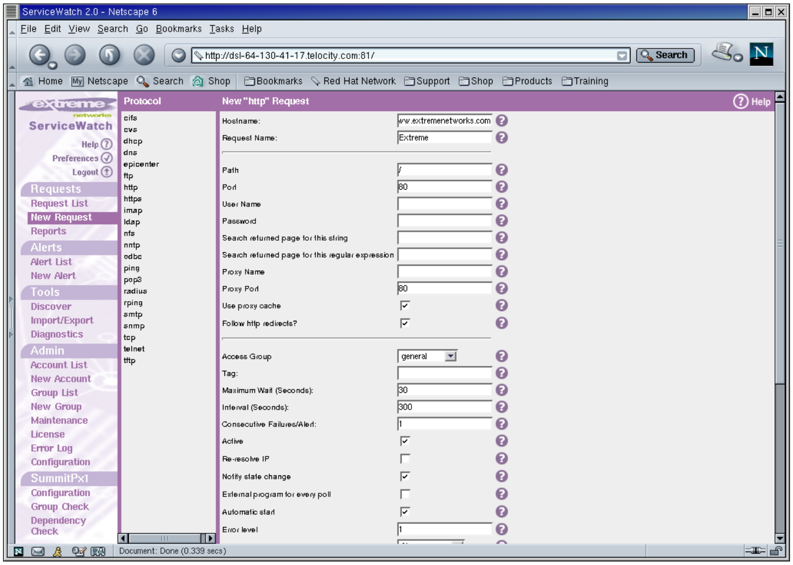
If you logged in as Guest, you have a **Requests** tab, which provides a menu for viewing the Request List, and generating reports.

For more information about Admin privileges, and creating and managing Users and Guests, see “Managing Accounts and Groups” on page 3-32.

Creating Your First Request

If you logged in as Admin or User, you are ready to create your first request. To create an easy ServiceWatch request, follow these simple steps:

1 From the ServiceWatch navigation pane, click **New Request**.
The New Request page appears, as shown in Figure 3-7.



New "http" Request

Hostname:	ww.extremenetworks.com
Request Name:	Extreme
Path	/
Port	80
User Name	
Password	
Search returned page for this string	
Search returned page for this regular expression	
Proxy Name	
Proxy Port	80
Use proxy cache	☑
Follow http redirects?	☑
Access Group	general
Tag:	
Maximum Wait (Seconds):	30
Interval (Seconds):	300
Consecutive Failures/Alert:	1
Active	☑
Re-resolve IP	□
Notify state change	☑
External program for every poll	□
Automatic start	☑
Error level	1

Figure 3-7: Creating your first request with ServiceWatch

2 In the **Hostname** box, enter the name of the host, for example, `www.extremenetworks.com`

3 In the **Request Name** box, type a descriptive name for your request, for example, *Extreme*. If you leave the name blank, ServiceWatch will create one for you.

4 For the rest of the parameters, just leave them blank and accept the defaults.

5 Click the **Create Request** button at the bottom of the page.
Your new request now appears in the Request List.

Requests

Requests let you view the current status of the network services you are actively monitoring.

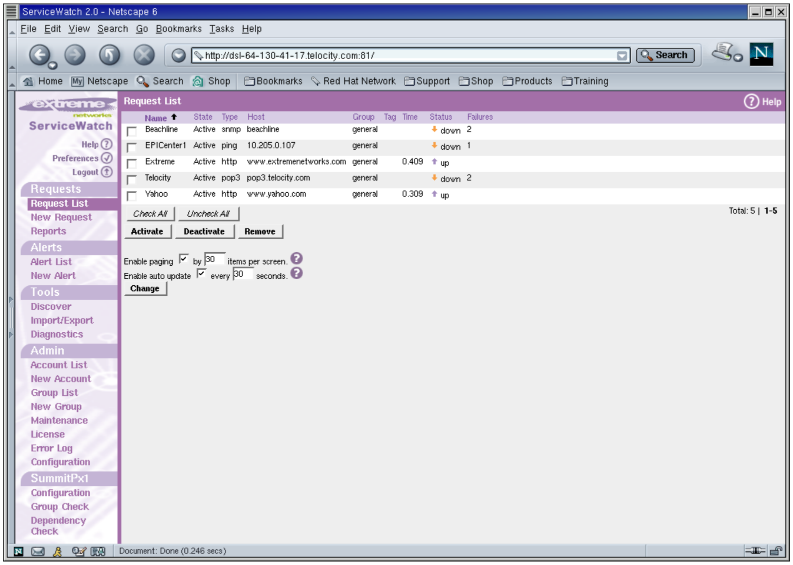
- To display ServiceWatch requests, click **Request List** under the **Requests** tab in the navigation pane.

All users can view the **Request List**. Users can view the status of the requests, sort requests by a specific column, and sort requests in ascending or descending order for each group that they have read access to. Users logged in as Admin or User can create new requests, and modify or remove existing requests.

You can access these functions through the links in the navigation pane.

Request List

The Request List displays a summary of all the requests, as shown in Figure 3-8.



Request List

	Name ↑	State	Type	Host	Group	Tag	Time	Status	Failures
□	Beachline	Active	snmp	beachline	general			↓ down	2
□	EPICenter1	Active	ping	10.205.0.107	general			↓ down	1
□	Extreme	Active	http	www.extremenetworks.com	general		0.409	↑ up	
□	Telocity	Active	pop3	pop3.telocity.com	general			↓ down	2
□	Yahoo	Active	http	www.yahoo.com	general		0.309	↑ up	

Check All | Uncheck All

Total: 5 | **1-5**

Activate | Deactivate | Remove

Enable paging ☑ by 30 items per screen.
Enable auto update ☑ every 30 seconds.
Change

Figure 3-8: Request List

To sort by a particular column, click the column heading, and it becomes bold. Clicking the column again reverses the list sort order.

Select requests by marking the check box on their left. They then can be Activated, Deactivated, or Removed.

Clicking anywhere on a request displays its Request Details page.

Paging

The Request List can be either shown as one continuous list or as pages with a specified number of items per page. To enable paging, check the **Enable paging** checkbox, enter the number of requests per page, and click **Change**.

Auto Update

By default, ServiceWatch refreshes the Request List page every 30 seconds. This can be disabled by unchecking the **Enable auto update** check box. The time delay can also be changed by entering a number in seconds. Click the **Change** button for either change to take effect.

The Request List displays the current request results in a tabular format, with one row for each request. The fields in the table are listed in Table 3-1.

Table 3-1: Request List fields

Name The name of the request. If you didn't specify a name in the New Request page, ServiceWatch calls the first unnamed request "request", the next one, "request-1", etc.

Click the name or index number to view the detailed definition of the request.

State The state of the request.

Active indicates that the request is polling the service at defined intervals.

Inactive indicates that the request is currently suspended (is not polling).

Type The type of the network service that this request is monitoring, for example, HTTP, or Ping.

Hostname The host where the service is running.

Group The access group of this request. This is used to determine which other users can view and modify this request. For example, users without read access to this group do not see these requests.

Table 3-1: Request List fields

Tag A tag is a user-defined string that can be used to classify requests into user-defined categories. For example, you may want all requests that monitor services running in building 1 to have the tag “bldg1”, and all requests that monitor services running in building 2 to have the tag “bldg2”.

Time The time, in seconds, that it took for the monitored service to respond to the last ServiceWatch poll. If the service failed to respond correctly within the time period specified by a user-defined threshold, the time is left blank.

Status The status of the service being monitored.

- Purple arrow (up) indicates that the service is responding correctly within the defined threshold.
- Orange arrow (down) indicates that the service is down and is returning an error condition.
- Unknown means that the status of the service cannot be determined (as when the request is “inactive” or polling has not yet occurred on a new request).

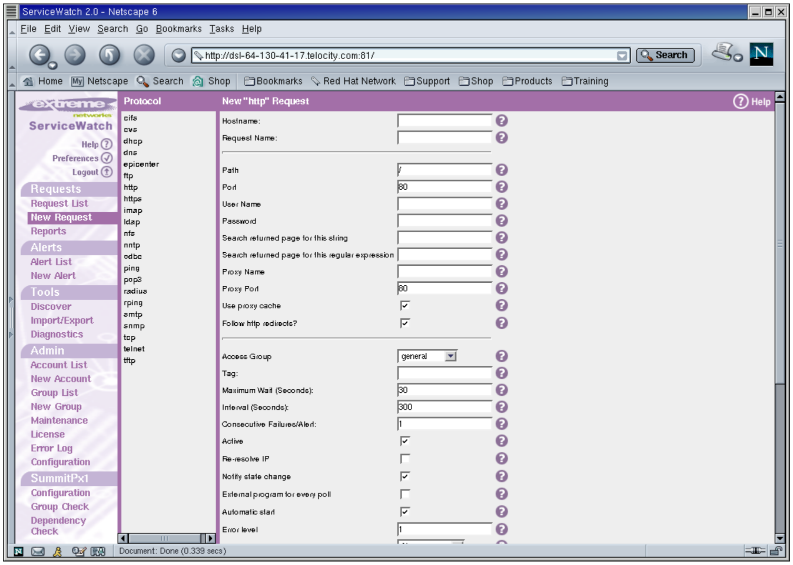
Failures The number of consecutive ServiceWatch polls that did not complete correctly within the specified time period.

Creating a New Request

If you are logged in as Admin or User, you can create new requests for monitoring network services.

To create a new request, follow these steps:

1 Click **New Request** in the navigation pane. The New Request page appears, as shown in Figure 3-9. If you are logged in as Guest, this link is not available.



New "http" Request

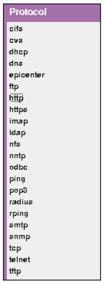
Hostname:	
Request Name:	
Path	/
Port	80
User Name	
Password	
Search returned page for this string	
Search returned page for this regular expression	
Proxy Name	
Proxy Port	80
Use proxy cache	☑
Follow http redirects?	☑
Access Group	general
Tag:	
Maximum Wait (Seconds):	30
Interval (Seconds):	300
Consecutive Failures/Alert:	1
Active	☑
Re-resolve IP	□
Notify state change	☑
External program for every poll	□
Automatic start	☑
Error level	1

Figure 3-9: New Request

In this page, you enter all the information and specifications necessary to monitor the network service and to determine and respond to the service's status.

Help ? Click the **Help** button to display a definition or description of any parameter.

2 On the left side of the page, select the protocol from the Protocol list, as shown in Figure 3-10. By default, the last protocol selected is automatically chosen.



Protocol

cifs
cvs
dhcp
dns
epicenter
ftp
http
https
imap
ldap
nfs
nntp
odbc
ping
pop3
radius
rping
smtp
snmp
tcp
telnet
tftp

Figure 3-10: Protocol type selection list

3 Enter a hostname in the **Hostname** box.

The hostname is the fully qualified name or IP of the server that is to be polled.

4 Enter a request name in the **Requestname** box.

The request name is a textual name for the request. If left blank, one is assigned. Names must be unique. If they are not, a number is appended to make them unique.

5 In the second section of the New Request page, enter the parameters for polling the service. These vary, depending on the service. You can accept the defaults or refer to more specific details in section "Definition of Network Services," on page 4-2.

General Request Parameters

You can set the following parameters, as shown in Table 3-2, for every request in the third section of the New Request page. The poller-specific parameters that apply only to particular pollers are described in detail in "Definition of Network Services" on page 4-2.

Table 3-2: General Request Parameters

Access Group	The access group to which this request belongs. This affects: ■ Who can view and modify the request, and ■ Which alerts can be added to the request, since only alerts belonging to the same access group as the request, or to the special access group General, can be used.
Tag	A text field used for sorting and identifying groups of requests.

Table 3-2: General Request Parameters

Maximum Wait
The maximum number of seconds to wait for a server to respond. If it does not respond after this time, it is considered down. The default is 30 seconds. This means that after 30 seconds without a response, ServiceWatch times-out that particular query, and set the Response Time to -1.0, the Response Type to 405, and the Error to Connection Time Out.

Interval
How often to poll a server, in seconds.

Consecutive Failures/Alert
The number of times a server can fail before an alert is triggered. To avoid creating alerts on transient, short-lived response failures, you can specify that the service is not considered down unless the failure occurs repeatedly some number of times.

Active
If this box is checked, the request is considered active, and polls the server. Otherwise, the request is inactive and does not poll, collect data, or trigger alerts.

Re-resolve IP
If checked, resolves the IP address from the host name every time a poll is executed. Otherwise, the IP is only resolved once and is cached for future use. Setting this option enables the following:

- Continuous testing of your name service, since the resolution is done before each request.
- "Round-robin" DNS servers are used to make requests go to different servers (round-robin DNS servers have the ability to return a different IP address on subsequent DNS requests).

Notify State Change
If this box is checked, an alert is sent when the server becomes active again. With this option set, you are notified when a web server is first detected to be down, and you are notified next when the web server is detected as back up. You are not notified while the web server remains down.

You are notified only if:

- A service is down exactly the number of times set in Consecutive Failures/Alert, or
- A service that is down comes back up.

External Program for Every Poll
If checked, ServiceWatch runs any external script/program alert after every poll attempt. If not checked, ServiceWatch runs the external script/program alert only if an alert is triggered from the poll request.

Automatic Start
If checked, start the request when ServiceWatch starts. Otherwise, it is left in the inactive state, and must be started manually.

Table 3-2: General Request Parameters

Error Level

A user-defined integer that lets you define how important a service failure is. By convention, error levels range from 1–9 where an error level 1 is a low level error and a level 9 error is the most serious. A few uses of this are:

- An external alert program/script could be run on every poll attempt and determine other actions to perform, depending on the error level.
- If an SNMP trap alert is sent, the receiving network management platform may perform different actions (like changing the color of an icon) depending on the error level.

Gateway Request

If a gateway request is specified, the new request only triggers an alert if the gateway request is alive. This is useful if there are several servers behind a router, for example.

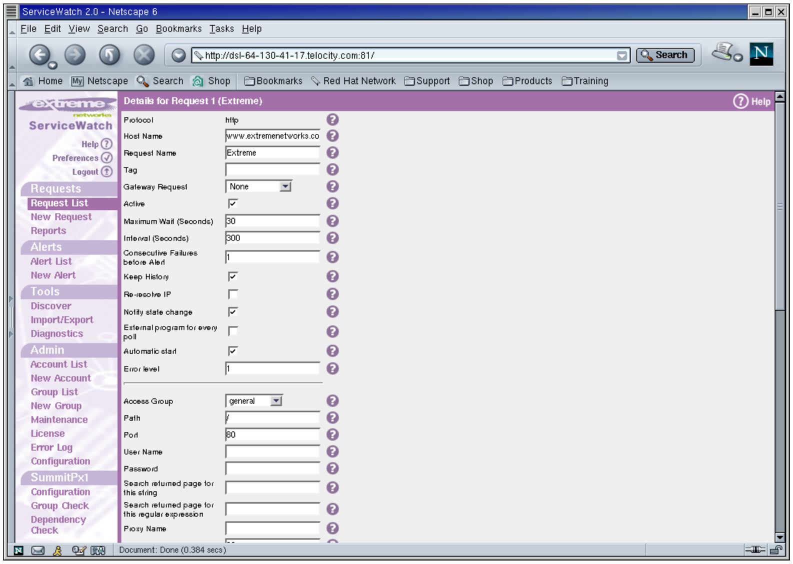
Alerts

Here you can associate alerts with a request. Note, however, that only alerts belonging to the same request group as the new request, or the special group General can be assigned.

If you are already monitoring the maximum number of requests for which you are licensed, the ServiceWatch software gives you an error if you try to create additional requests. You need to remove one or more requests before you can start new ones.

Request Details

The Request Details page, as shown in Figure 3-11, shows and allows modification of request parameters. It also displays the last polling results for the request.



Details for Request 1 (Extreme)

Protocol	http
Host Name	www.extremenetworks.co
Request Name	Extreme
Tag	
Gateway Request	None
Active	☑
Maximum Wait (Seconds)	30
Interval (Seconds)	300
Consecutive Failures before Alert	1
Keep History	☑
Re-resolve IP	☐
Notify state change	☑
External program for every poll	☐
Automatic start	☑
Error level	1
Access Group	general
Path	/
Port	80
User Name	
Password	
Search returned page for this string	
Search returned page for this regular expression	
Proxy Name	

Figure 3-11: Request Details

Table 3-3: Request details

Keep History	When checked, the history data collected for the request is saved on update. Otherwise, it is cleared.
Last Poll	Displays the last time the service was polled.
Server Status	Indicates whether a server is up or down.
Response Time	The number of seconds the request took.
Response Type	The “server response code” similar to that defined by HTTP.
Code Range	-1 Site was down or did not respond 100-199 Informational 200-299 Client request successful 300-399 Client request redirected, further action necessary 400-499 Client request incomplete 500-599 Server errors 600-999 ServiceWatch specific error

Table 3-3: Request details

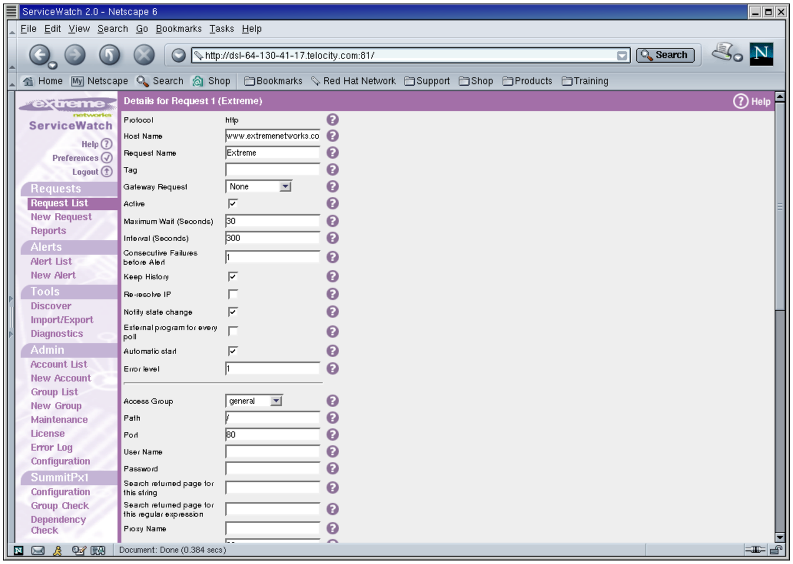
Error	The error that the request generated. If the server is up, the error is None.
Reason	Shows extra information on why a server responded the way it did.
Query Number	The number of queries that have been performed so far for this request.
Consecutive Failures	The number of consecutive failures since the first failure was detected.
Last IP	The last known IP of the server.

Modifying a Request

You can view the details of an individual request, which includes both the values of the monitoring parameters you can set, as well as the results values returned from a monitoring request. You can then change the values of any of the monitoring parameters.

To view the details of an individual monitoring request, from the Request List page click the name or index number of the request. This displays the details for the request, as shown in Figure 3-12.

If you are logged in as Guest, you see the same display, but are not be able to make any changes or delete or update the request.



Details for Request 1 (Extreme)

Protocol	http
Host Name	www.extremenetworks.co
Request Name	Extreme
Tag	
Gateway Request	None
Active	☑
Maximum Wait (Seconds)	30
Interval (Seconds)	300
Consecutive Failures before Alert	1
Keep History	☑
Re-resolve IP	☐
Notify state change	☑
External program for every poll	☐
Automatic start	☑
Error level	1
Access Group	general
Path	/
Port	80
User Name	
Password	
Search returned page for this string	
Search returned page for this regular expression	
Proxy Name	

Figure 3-12: Request Details page

This report displays the status of all the variables associated with a request.

For an explanation of the meaning of each item, click the **Help** button to display the definition and examples of its use.

To make changes to the request, follow these steps:

1 Enter the new values into the appropriate fields, or set/reset the checkboxes.

2 Click the **Modify Request** button, at the bottom of the page, to have your changes take effect.

For example, you may want to change the polling interval (**Interval**) or the maximum time to wait for a request to complete (**Maximum Wait**).

You can make a request inactive (which suspends the request without removing it from the Request List) by clearing the **Active** check box, then clicking **Modify request**. You can also activate and deactivate the request from the Request List.

The changes take effect immediately.

Activating, Deactivating, or Removing a Request

When you are logged in as Admin or User, you can activate, deactivate, or remove requests from ServiceWatch, by using the **Activate**, **Deactivate** and **Remove** buttons on the Request List.

If you are logged in as Guest, these buttons do not appear.

To activate, deactivate, or remove one or more requests, follow these steps:

1 Click the check box next to the name of the requests you want to change.

To select all requests, click the **Check All** button.

To clear the check boxes and start over, click the **Uncheck All** button.

2 After you make your selections, click the button for the type of change you want to make.

The **Remove** button stops and removes the selected requests. Requests are deleted from the ServiceWatch software, and must be recreated if needed again.

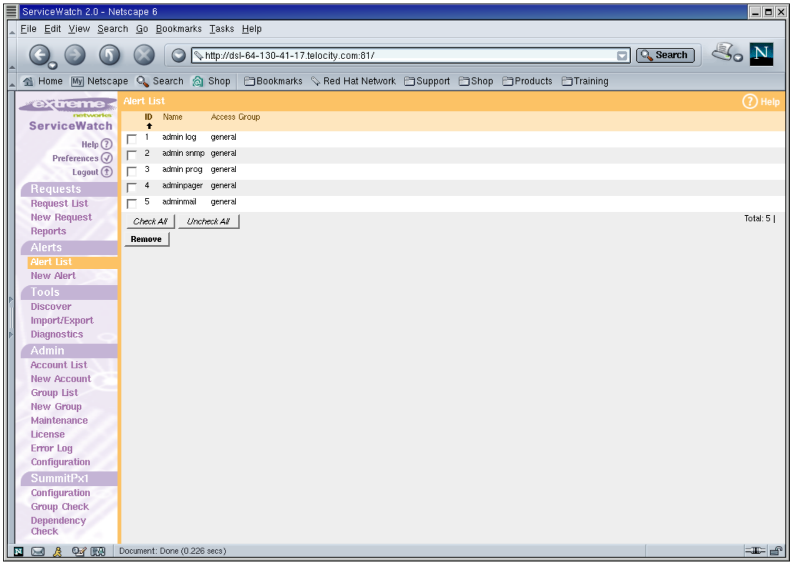
If you want to stop a request from running temporarily, you can modify the Status parameter (see "General Request Parameters" on page 3-13 for more details) by deselecting the ***Active*** *checkbox in the Request Details page. This stops the request from running, but leaves it in the Request List.*

Alerts

ServiceWatch alerts allow you to be notified in various ways when a service is up or down. ServiceWatch alerts are “reusable.” After you create an alert, you can select it anytime you create a new request, or modify an existing request.

To create and work with your alerts, click the **Alert List** link from the ServiceWatch navigation pane.

The Alert List appears, as shown in Figure 3-13, listing the alert names and the access groups to which they belong.



Alert List

	ID	Name	Access Group
□	1	admin log	general
□	2	admin snmp	general
□	3	admin prog	general
□	4	adminpager	general
□	5	adminmail	general

Total: 5 |

Figure 3-13: ServiceWatch Alert List

The five types of alerts are:

- Email
- Epager
- Eprog
- SNMP Trap
- Syslog

Creating Alerts

To create new alerts, follow these steps:

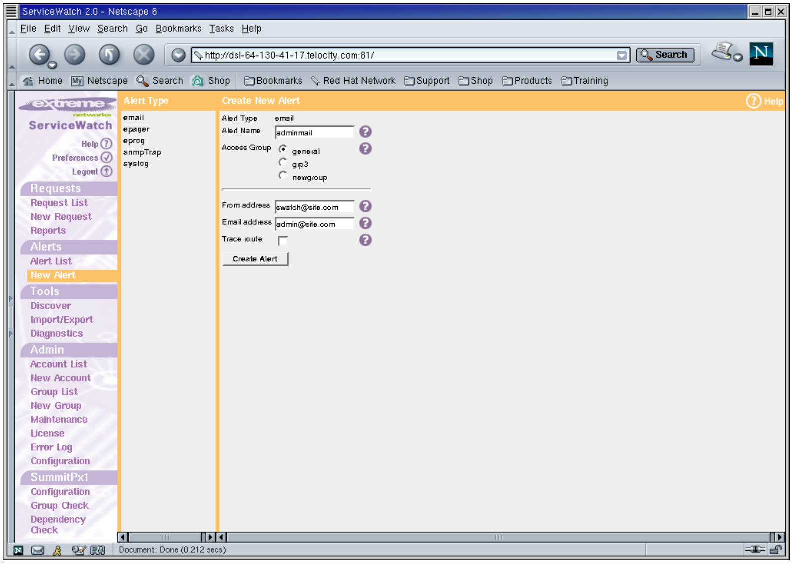
1. Click the **New Alert** link from the ServiceWatch navigation pane. The Create New Alert page appears.
2. Select one of the types of alerts detailed below from the Alert Type list.
3. Fill in the appropriate fields.
4. Click the **Create Alert** button.

After you create a new alert, for example, one titled *adminmail*, the next time you create a new request, you see the adminmail alert listed under email alerts. If you want that alert to be used, then you can check the adminmail email alert check box. You can create many requests using that same alert type.

Email Alert

You can configure the ServiceWatch software to automatically send email to one or more specified email addresses when an event occurs. This feature assumes that the SMTP server specified in the Configuration section is set to a mail server that will send email on behalf of your host.

To create an email alert, on the Create New Alert page shown in Figure 3-15, follow these steps:



Create New Alert

Alert Type email

Alert Name adminmail

Access Group ● general ○ grp3 ○ newgroup

From address swatch@site.com

Email address admin@site.com

Trace route □

Create Alert

Figure 3-14: Create New Alert page for email alert

1 In the **Alert Name** box, enter a name for the alert that is easy for you to remember, for example, *adminmail*.

2 In the **Access Group** options, select the access group you want this alert to belong to.

3 In the **From Address** box, enter the email address used to sending the email alert, for example *swatch@site.com*.

4 In the **Email Address** box, enter the recipient’s email address, for example *admin@site.com*.

5 Check the **Trace Route** check box to perform a traceroute between the ServiceWatch server and the host of the service when a failure occurs. The output from the traceroute is included in the event notification email.

6 Click the **Create Alert** button.

This is an example of an email message that the ServiceWatch software sends if a network service is down:

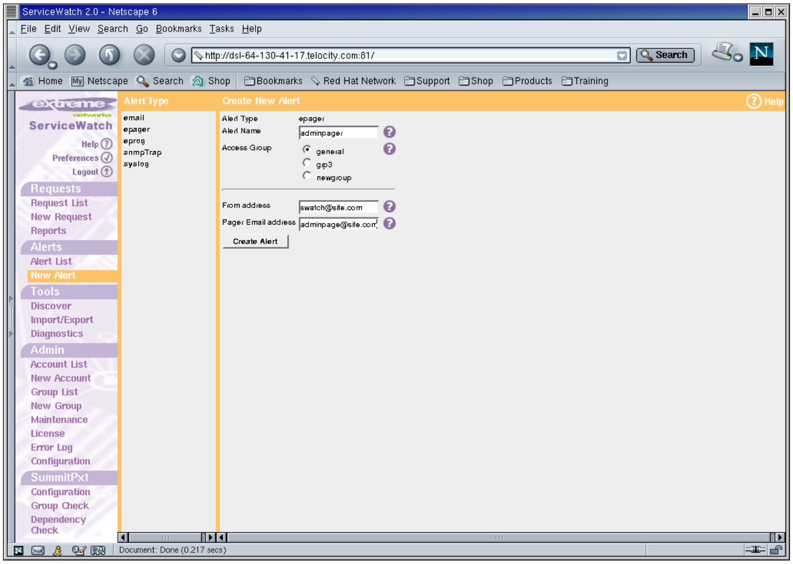
```
From: servicewatch@extremenetworks.com
To: msmith@extremenetworks.com
Subject: ServiceWatch Alert -- Request-2
```

```
Request name: Request-2
Host name: localhost
-------------------------------------
filetype: ''
response_time: -1.0
port: 82
ip_address: '127.0.0.1'
response_reason: "(111, 'Connection refused')"
bytes_read: 0
error: 10
data: ''
service_status: 2
Request_number: 1
Request_id: 2
moving_average: -1.0
create: <DateTime object for '2002-01-30 11:01:41.36' at 8482648>
response_type: 600
sr: 1
gate_host_name: ''
ncfails: 1
throughput: -1.0
```

Epager Alert

You can configure the ServiceWatch software to automatically send email to an alphanumeric pager when an event occurs. The epager alert is identical to the email alert except the email message sent is shortened to one line for an alphanumeric pager.

To create an epager alert, on the Create New Alert page shown in Figure 3-15, follow these steps:



Alert Type

email
epager
eprog
snmpTrap
syslog

Create New Alert

Alert Type: epager

Alert Name: adminpager

Access Group: ● general ○ grp3 ○ newgroup

From address: swatch@site.com

Pager Email address: adminpage@site.com

Create Alert

Figure 3-15: Create New Alert page for epager alert

1 In the **Alert Name** box, enter a name for the alert that is easy for you to remember, for example, *adminpager.*

2 In the **Access Group** options, select the access group you want this alert to belong to.

3 In the **From Address** box, enter the email address used to sending the email alert, for example *swatch@site.com*.

4 In the **Pager Email Address** box, enter the recipient’s email address, for example *adminpage@site.com*.

5 Click the **Create Alert** button.

This is an example of an email message that the ServiceWatch software sends if a network service is down:

```
From: swatch@extremenetworks.com
To: msmith@extremenetworks.com
Subject: ServiceWatch Alert -- pagereq

localhost (http) - Down
```

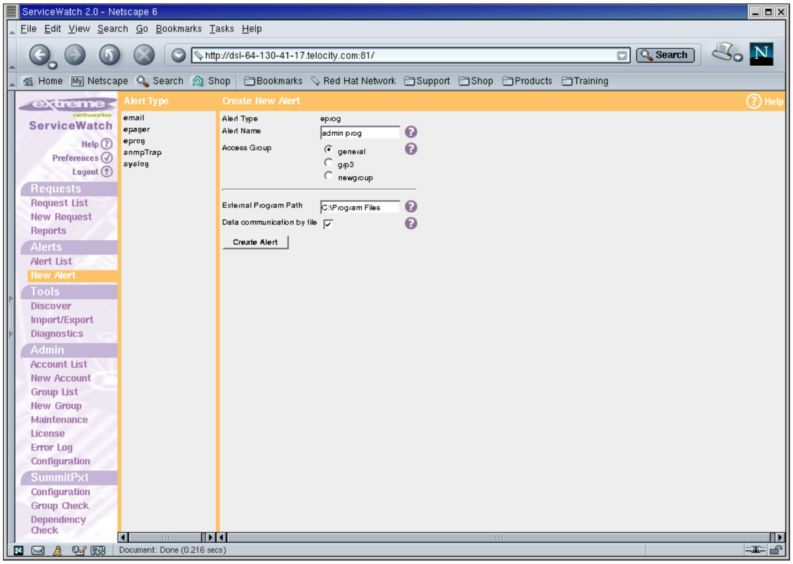
Eprog Alert

The eprog alert allows you to specify a program to run. You enter the filename path of the program that you would like to run when the alert is triggered.

For example, this feature allows you to run a program to restart a web server if it becomes unavailable.

For testing and debugging eprog, and any external API for ServiceWatch, it is best to set the log level in ServiceWatch to Extension Debug. This level will filter out irrelevant entries, and log the communication and external command calls.

To create an eprog alert, on the Create New Alert page shown in Figure 3-16, follow these steps:



Create New Alert

Alert Type eprog

Alert Name admin prog

Access Group ● general ○ grp3 ○ newgroup

External Program Path C:\Program Files

Data communication by file ☑

Create Alert

Figure 3-16: Create New Alert page for eprog alert

1 In the **Alert Name** box, enter a name for the alert that is easy for you to remember, for example, *admin prog*.

2 In the **Access Group** options, select the access group you want this alert to belong to.

3 In the **External Program Path** box, enter the path to the program you want to run.

4 If you want, select the **Data Communication by File** check box. For more information on this option, see the section below.

5 Click the **Create Alert** button.

For Win32 environments:

- Before the eprog program is run, the current directory is set to WINNT\system32.
- You may specify a batch file as an eprog program.

Communication by File

If the communication channel between the external alert program and ServiceWatch is by file, then the following tagged format of data is sent to the external alert program:

```
<sw>
   <hostinfo>
       <nc_fails_alert>1</nc_fails_alert>
       <query>1</query>
       <request_id>118</request_id>
       <auto_start>1</auto_start>
       <request_group_name>general</request_group_name>
       <gate_host>128</gate_host>
       <poller_type>http</poller_type>
       <eprog_all_poll>1</eprog_all_poll>
       <re_resolution>0</re_resolution>
       <logic_group_name></logic_group_name>
       <hostname>www.extremenetwork.com</hostname>
       <error_level>1</error_level>
       <average_time>0</average_time>
       <maxwait>5</maxwait>
       <description></description>
       <request_name>extr</request_name>
       <notify_state_change>1</notify_state_change>
       <interval>10</interval>
       <status>1</status>
   </hostinfo>
   <response>
       <filetype></filetype>
       <response_time>-1.0</response_time>
       <port>80</port>
       <moving_average>-1.0</moving_average>
       <create>2002-02-01 14:50:30.48</create>
       <bytes_read>0</bytes_read>
       <error>19</error>
       <response_type>-1</response_type>
       <throughput>-1.0</throughput>
       <request_number>1</request_number>
       <response_reason>unknown</response_reason>
       <data></data>
       <service_status>2</service_status>
       <gate_host_name>www.yahoo.com</gate_host_name>
       <sr>1</sr>
       <ip_address>unknown</ip_address>
       <nc_fails>1</nc_fails>
       <request_id>118</request_id>
   </response>
</sw>
```

Some of the parameters are meaningful to ServiceWatch only, like the tag. However, most of the info will be useful to the eprog alert.

The file name that contains the above data is passed to the external alert program as the first argument.

Communication Without a File

When the program or script is run, the program or script determines what request caused the alert, the hostname, poller type, error level, and so on. If the **Data communication by file** check box is not checked, then the following arguments are passed to the program or script, in the following order:

1. REQUEST_ID
2. REQUEST_NAME
3. HOST_NAME
4. POLLER_TYPE
5. ERROR_LEVEL
6. NC_FAILS_ALERT
7. NOTIFY_STATE_CHANGE
8. INTERVAL
9. MAX_WAIT
10. GATE_HOST
11. SERVICE_STATUS
12. RESPONSE_TIME
13. ERROR
14. IP
15. PORT
16. NC_FAILS
17. BYTES_READ
18. RESPONSE_TYPE
19. REQUEST_NUMBER

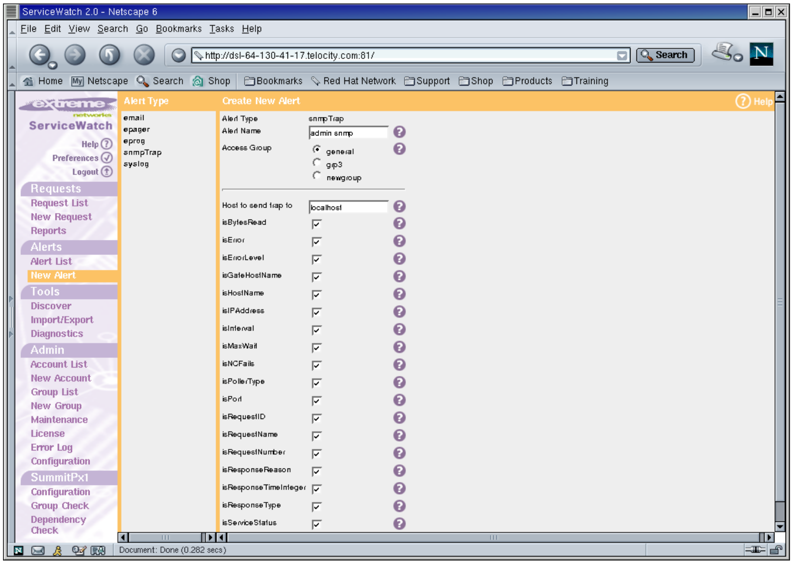
For example, a call to the eprog “test.exe” would be:

test.exe “118” “amd” “www.amd.com” “http” “1” “1” “1” “10” “5” “128” “2” “-1.0” “19” “unknown” “-1” “6” “0” “-1” “6”

SNMP Trap

The SNMP Trap alert allows you to specify an SNMP trap to be sent as an alert. You can specify which variables are sent in an SNMP Trap.

To create an SNMP Trap alert, on the Create New Alert page shown in Figure 3-17, follow these steps:



Alert Type snmpTrap
Alert Name admin snmp
Access Group ● general ○ grp3 ○ newgroup

Host to send trap to localhost
isBytesRead ☑
isError ☑
isErrorLevel ☑
isGateHostName ☑
isHostName ☑
isIPAddress ☑
isInterval ☑
isMaxWait ☑
isNCFails ☑
isPollerType ☑
isPort ☑
isRequestID ☑
isRequestName ☑
isRequestNumber ☑
isResponseReason ☑
isResponseTimeInteger ☑
isResponseType ☑
isServiceStatus ☑

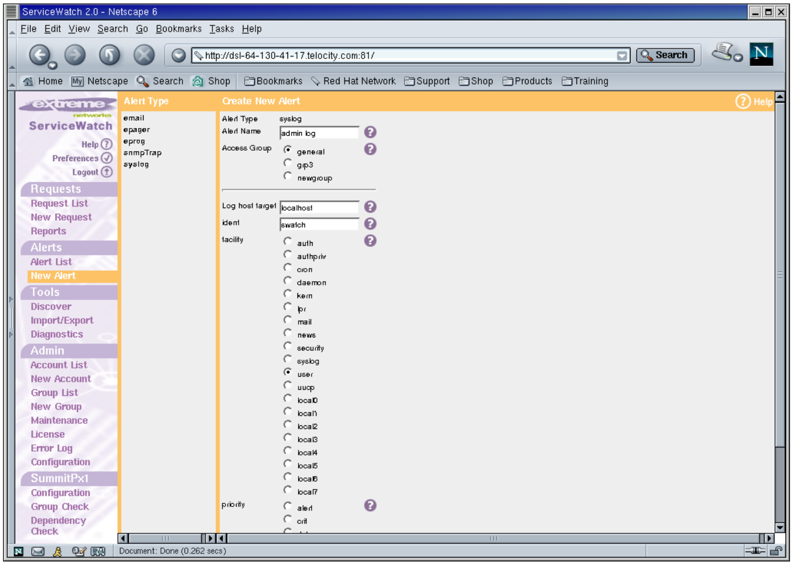
Figure 3-17: Create New Alert page for SNMP Trap alert

1. In the **Alert Name** box, enter a name for the alert that is easy for you to remember, for example, *admin snmp*.
2. In the **Access Group** options, select the access group you want this alert to belong to.
3. In the **Host to Send Trap to** box, enter host name to send the trap to, for example *localhost*.
4. In the Trap check box section, select or deselect the traps you want sent.
5. Click the **Create Alert** button.

Syslog Alert

The syslog alert allows you to specify a syslog entry to be sent to a syslog daemon.

To create a syslog alert, on the Create New Alert page shown in Figure 3-18, follow these steps:



Alert Type syslog

Alert Name admin log

Access Group ● general ○ grp3 ○ newgroup

Log host target localhost

ident swatch

facility ○ auth ○ authpriv ○ cron ○ daemon ○ kern ○ lpr ○ mail ○ news ○ security ○ syslog ● user ○ uucp ○ local0 ○ local1 ○ local2 ○ local3 ○ local4 ○ local5 ○ local6 ○ local7

priority ○ alert ○ crit

Figure 3-18: Create New Alert page for syslog alert

1. In the **Alert Name** box, enter a name for the alert that is easy for you to remember, for example, *admin log*.
2. In the **Access Group** options, select the access group you want this alert to belong to.
3. In the **Log Host Target** box, enter the target for the log host, for example *localhost*.
4. In the **Ident** box, enter an identifier, for example *swatch*.
5. In the **Facility** section, select any options you want.
6. In the **Priority** section, select any priority you want.
7. Click the **Create Alert** button.

The ServiceWatch MIB is located at:

```
<install-directory>/SharedLib/swsnmp/mibs/SWATCH2-MIB.txt
```

You would typically tell your SNMP manager application to import the ServiceWatch MIB, since it makes reading the trap easier with symbolic names rather than OIDs. Refer to your SNMP Manager documentation for information on how to load MIBs for use within it.

Modifying Alerts

If you need to change any of the alerts you have already created, follow these steps:

1. Click the **Alert List** link on the ServiceWatch navigation pane.
2. From the Alert List page, click the name of the alert you want to modify.
3. Change any information necessary.
4. Click the **Modify Alert** button.

Changes take effect immediately.

Removing Alerts

When you are logged in as Admin or User, you can remove ServiceWatch alerts from the Alert List.

To remove one or more alerts, follow these steps:

1. Click the check box next to the name of the alert you want to remove.

   To select all alerts, click the **Check All** button.

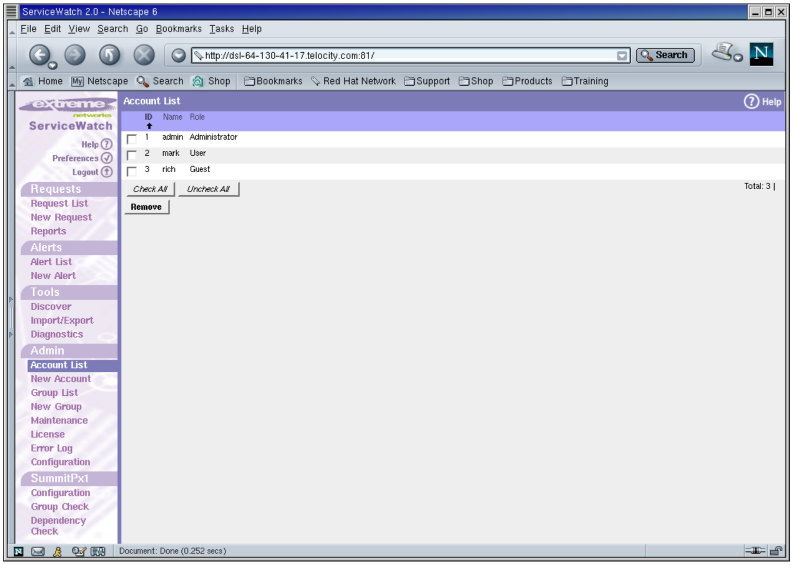
   To clear the check boxes and start over, click the **Uncheck All** button.
2. After you make your selections, click the **Remove** button.

Managing Accounts and Groups

ServiceWatch software access is controlled by an Admin user through accounts and groups. Accounts consist of a username and password.

To manage accounts, follow these steps:

1. Click the **Account List** link on the ServiceWatch navigation pane.
2. The Account List appears, as shown in Figure 3-19, which displays a list of users and roles.



	ID	Name	Role
□	1	admin	Administrator
□	2	mark	User
□	3	rich	Guest

Total: 3 |

Figure 3-19: Account List

Each account has one role. The three types of roles are:

- **Admin**, which has full access to all ServiceWatch functions.
- **User**, which is normal type of role that an account would have: A User is assigned read, read/write, or no access to each access group.
- **Guest**, which can only read and view, but not write or modify requests in the assigned access groups.

Accounts

When you log in to the ServiceWatch software, you enter your account information, in the form of your username and password.

When an account is created, the account is assigned:

- A role, which is the type of access: Admin, User, or Guest.
- The list of groups the user is allowed access to and the type of access the user is allowed in that group: read only, read/write, or no access.

A role refers to the type of access granted.

- Admin role, which allows full access to ServiceWatch functionality.

  Only users with the Admin role are able to create Accounts and Groups and change other user passwords. Only users with the Admin role see the following links:

  — Account list

  — New Account

  — Access Group List

  — New Access Group

  — Maintenance

  — License

  — Error Log

  — Configuration

  Accounts with the Admin role can read, write, and create requests in any and all request groups.

- User role, which allows read/write in request groups as set up by a user with the Admin role.

  When a User creates a request, the User chooses which access group the request belongs to. The User can choose the new request to be in any group that the User has read/write access to.

- Guest role, which allows read/view requests only (cannot create new requests, cannot modify/write requests). A user with the Guest role can never create request groups. If a user is in only Guest groups (not User groups), then the user cannot create/write any requests. Consequently, the following links do not appear in the browser:

  — New Request

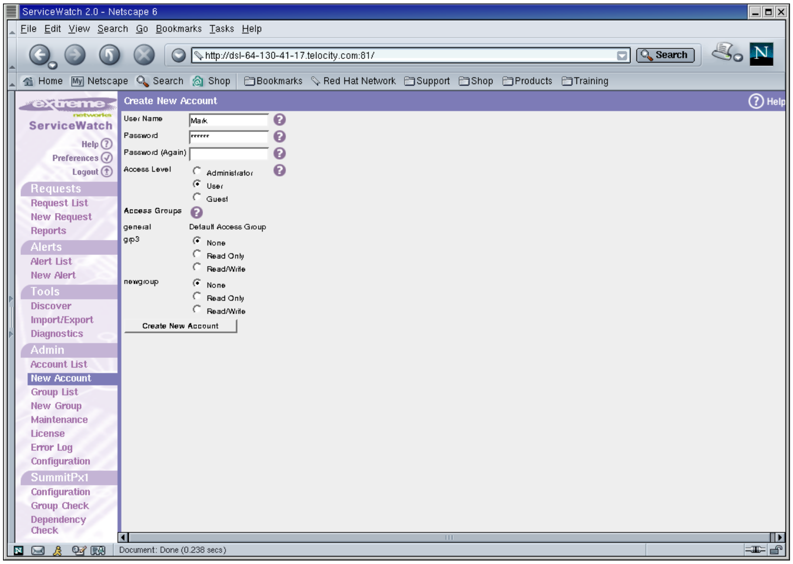
- — New Alert
- — Alert List
- — Discovery
- — Import/Export

Creating Accounts

When you are you are logged in as Admin, you can create new accounts.

To create a new account, follow these steps:

1 Click the **New Account** link on the ServiceWatch navigation pane. The Create New Account page appears, as shown in Figure 3-20.



Create New Account

User Name: Mark
Password: ••••••
Password (Again):
Access Level: ○ Administrator ● User ○ Guest
Access Groups
general: Default Access Group
grp3: ● None ○ Read Only ○ Read/Write
newgroup: ● None ○ Read Only ○ Read/Write

Figure 3-20: Create New Account page

2 Enter the following information for the account you want to create:

- — Username
- — Password
- — Password (Again)
- — Access Level

— Access Group

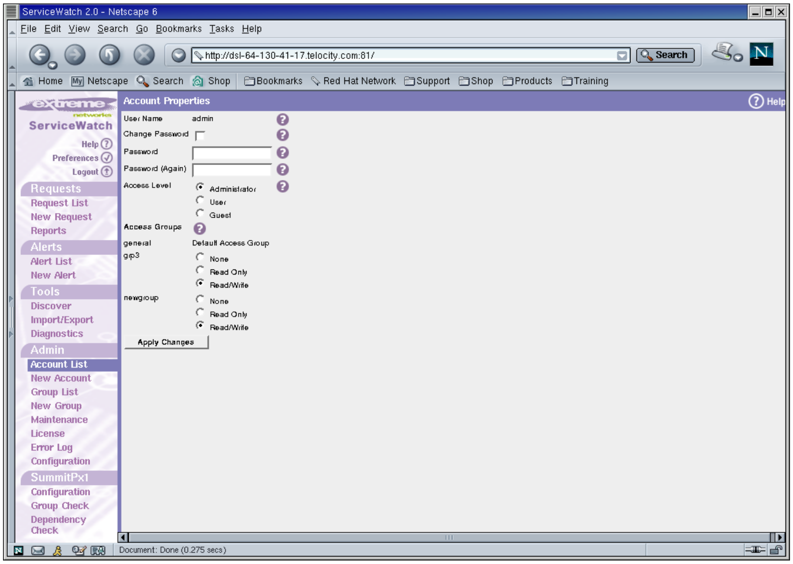
3 Click the **Create New Account** button to create the account.

Modifying Accounts

When you are logged in as Admin you can also modify accounts from the Account properties page.

To modify an account, follow these steps:

1 Click the name of the account you want to modify. The Account Properties page appears, as shown in Figure 3-21.



Account Properties

User Name admin

Change Password □

Password

Password (Again)

Access Level ● Administrator ○ User ○ Guest

Access Groups

general Default Access Group

grp3 ○ None ○ Read Only ● Read/Write

newgroup ○ None ○ Read Only ● Read/Write

Apply Changes

Figure 3-21: Account Properties page

2 Enter the information you want to change, and click the **Apply Changes** button.

To remove the account entirely, click the Remove **Account** button.

Removing Accounts

When you are logged in as Admin you can remove accounts from the Account List page.

To remove one or more accounts, follow these steps:

1 Click the check box next to the name of the account you want to remove.

To select all accounts, click the **Check All** button.

To clear the check boxes and start over, click the **Uncheck All** button.

2 After you make your selections, click the **Remove** button.

Groups

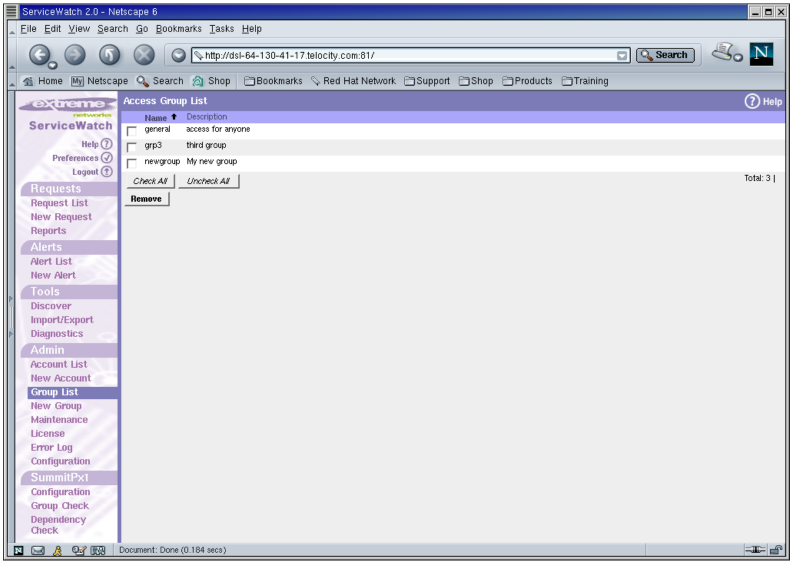
The General group is the default ServiceWatch group.

- The General group exists when the ServiceWatch software is installed.
- The General group cannot be removed.
- All users, by default, have access to the General group.
- An Admin user can move a user's access to the General group.

Remember the following when working with groups:

- All requests must belong to exactly one group.
- A user is shown requests only if the user has read access to the group the request is in.
- A user is allowed to modify requests only if the user has write access to the group the request is in.
- An alert also belongs to a group, and can only be used by requests within the same group.
- An alert belongs to the General group and can be used by all requests.

To manage groups, click the **Group List** link on the ServiceWatch navigation pane. The Group List appears, as shown in Figure 3-22, displaying a list of group names and roles.



	Name	Description
□	general	access for anyone
□	grp3	third group
□	newgroup	My new group

Total: 3 |

Document: Done (0.184 secs)

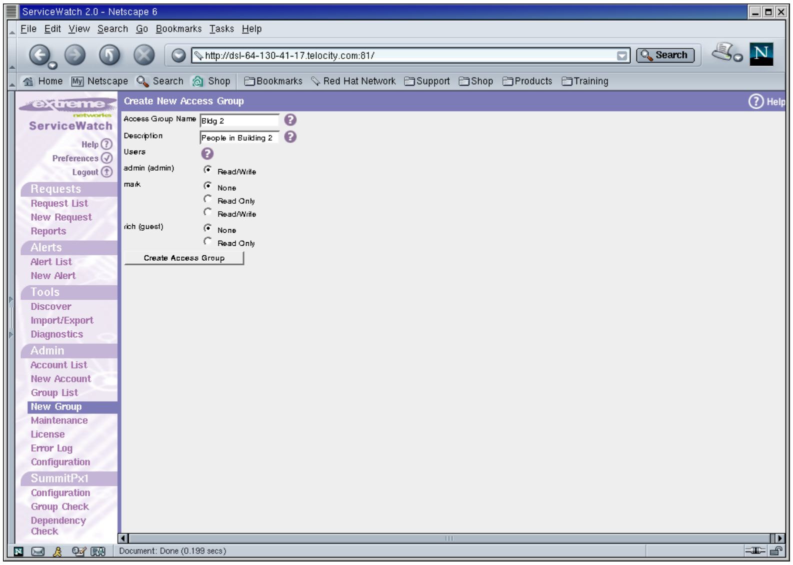
Figure 3-22: Group List

Creating Groups

When you are you are logged in as Admin, you can create new groups.

To create a new group, follow these steps:

1 Click the **New Group** link from the ServiceWatch navigation pane. The Create New Group page appears, as shown in Figure 3-23.



Create New Access Group

Access Group Name: Bldg 2

Description: People in Building 2

Users

admin (admin) ● Read/Write

mark ● None ○ Read Only ○ Read/Write

rich (guest) ● None ○ Read Only

Create Access Group

Figure 3-23: Create New Group page

2 Enter the following information for the group you want to create:

— Access Group Name

— Description

— User and type of access. Assign users the type of access they are allowed in each group. The types of access to groups are: Read only, Read/Write, or None (no access).

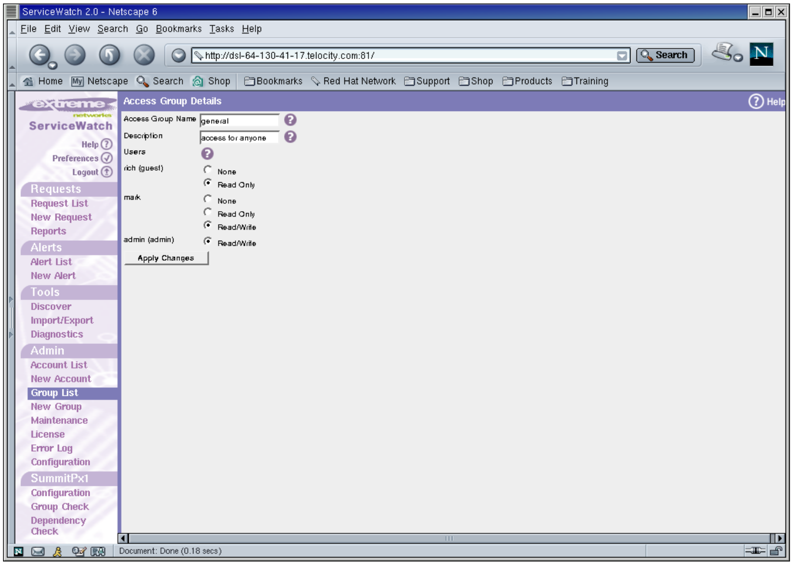
3 Click the **Create Access Group** button to create the group.

Modifying Groups

When you are logged in as Admin you can also modify groups from the Account Group Details page.

To modify a group, follow these steps:

1 Click the name of the group you want to modify. The Account Group Details page appears, as shown in Figure 3-24.



Access Group Details

Access Group Name: general

Description: access for anyone

Users

rich (guest) ○ None ● Read Only

mark ○ None ○ Read Only ● Read/Write

admin (admin) ● Read/Write

Apply Changes

Figure 3-24: Account Group Details page

2 Enter the information you want to change, and click the **Apply Changes** button.

To remove the group entirely, click the Remove **Access Group** button.

Removing Groups

When you are logged in as Admin or User, you can remove groups from the Group List.

To remove one or more groups, follow these steps:

1 Click the check box next to the name of the group you want to remove.

To select all groups, click the **Check All** button.

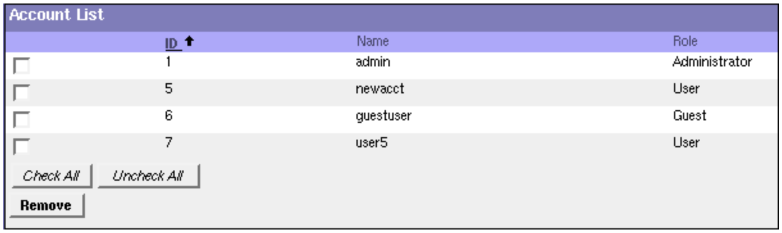
To clear the check boxes and start over, click the **Uncheck All** button.

2 After you make your selections, click the **Remove** button.

If an Admin user deletes a previously created group, any requests or alerts that belonged to that group are automatically assigned to the General group.

Examples of Accounts and Groups

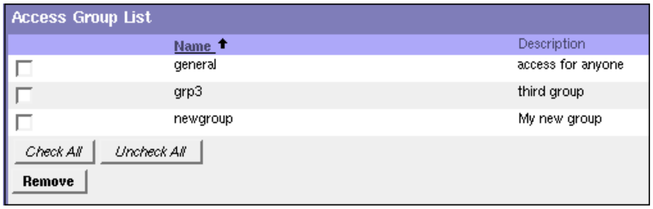
Figure 3-25 shows a sample Account List and Figure 3-26 shows a sample Group List.



Account List

	ID ↑	Name	Role
□	1	admin	Administrator
□	5	newacct	User
□	6	guestuser	Guest
□	7	user5	User

Figure 3-25: Sample Account List



Access Group List

	Name ↑	Description
□	general	access for anyone
□	grp3	third group
□	newgroup	My new group

Figure 3-26: Sample Group List

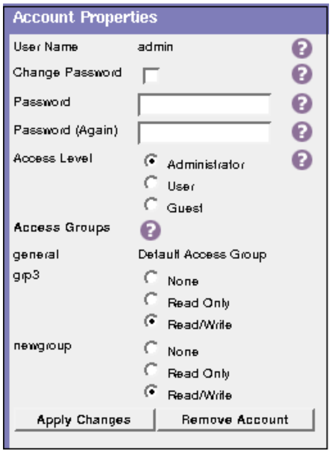
The samples show that there are four users and three groups.
The users are:

- Admin, with the Admin role
- newacct and user5 with the User role
- guestuser with the Guest role

The Groups are:

- General—always exists and cannot be removed
- newgroup
- grp3

Figure 3-27 shows more details on the Admin account, which always has read/write access to every group:



Account Properties

User Name admin

Change Password □

Password

Password (Again)

Access Level ● Administrator ○ User ○ Guest

Access Groups

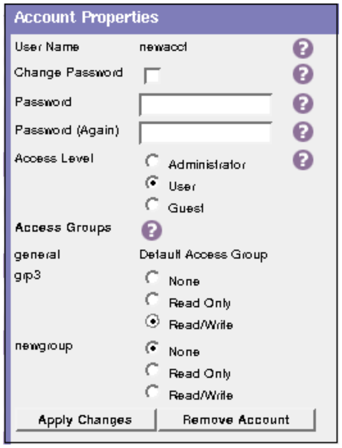
general Default Access Group

grp3 ○ None ○ Read Only ● Read/Write

newgroup ○ None ○ Read Only ● Read/Write

Figure 3-27: Admin Account Properties

Figure 3-28 shows more details on the newacct account.



Account Properties

User Name	newacct
Change Password	□
Password	
Password (Again)	
Access Level	○ Administrator ● User ○ Guest
Access Groups	
general	Default Access Group
grp3	○ None ○ Read Only ● Read/Write
newgroup	● None ○ Read Only ○ Read/Write

Figure 3-28: Newacct Account Properties

Figure 3-28 shows:

- The newacct account has the User role.
- The newacct account has read/write access to the groups newgroup and grp3 and has no access to the newgroup group.

Logging Out

To exit ServiceWatch, click the logout button.

Figure 3-29: ServiceWatch Logout button

4 Using ServiceWatch Effectively

This chapter describes:

- The set of network services you can monitor with the ServiceWatch software, including the method it uses to monitor each one.
- How to create reports and graphs in the ServiceWatch software, export data to spreadsheets, and how to use the built in relational database to improve reporting and analysis.
- How to use the ServiceWatch tools, such as the Discover function to discover machines and services, the ServiceWatch diagnostics, and Import and Export.
- ServiceWatch administration features, such as maintenance, licensing, the error log, configuration and user preferences.
- ServiceWatch maintenance features, such as database backup.

Definition of Network Services

The following sections define the types of network services that are monitored using the ServiceWatch software and the methods it uses to monitor them. The services listed in this section are in alphabetical order.

CIFS (Common Internet File System) Servers

The Common Internet File System (CIFS), as defined by Microsoft, is a file sharing system commonly used between Microsoft Windows computers and is based on the Server Message Block (SMB) protocol using a NetBIOS over TCP/IP transport layer.

The ServiceWatch CIFS implementation supports the following protocol levels:

- LANMAN1.0
- IBM PC Lan Manager version 1.0 Windows for Workgroups 3.1a
- Microsoft Windows for Workgroups PC networking LANMAN2.1
- IBM PC Lan Manager version 2.1 (OS/2, Windows 9X series) NT LM 0.12
- Windows NT Lan Manager Version 1

Specifically not supported are extended authentication and security extensions to NT Lan Manager 1, as well as the entire NT Lan Manager v. 2 protocol, which has appeared with the release of Microsoft Windows 2000 and Windows XP.

Only NetBIOS over TCP/IP is supported. NetBOUI, and NetBIOS over IPX/SPX are not supported at this time.

NetBIOS Name Resolution

ServiceWatch uses traditional methods such as DNS and hosts to retrieve network hostnames. Therefore, the hostname for a CIFS request must be resolvable by Internet applications such as ping and telnet. If the NetBIOS (Windows Networking) name of the machine differs from the DNS name, then it is entered in the **Calling** field. Similarly, if the ServiceWatch server's hostname differs from that of its NetBIOS name, the NetBIOS name is entered in the **Called** field.

The ServiceWatch CIFS fields are listed in Table 4-1.

Table 4-1: CIFS fields

User Name The user name of the account on the CIFS server. Depending on the system, this may or may not be case sensitive. If left blank, “guest” is used.

Password The password of the account specified in the User Name field.

Domain The Windows NT Domain or Workgroup used to access the share. If left blank, it is determined from the server's default domain listing. On some platforms the domain listing is not accurate, as it lists the server's local domain first, instead of its network domain.

Calling Name The Calling Name is the NetBIOS name of the ServiceWatch server. If left blank, it is determined by taking the host name of the server as reported by gethostname() and removing everything after and including the first period ('.'). For example, “file1.somecompany.com” would become “file1”.

Called Name The Called Name is the NetBIOS name of the server to be polled. If left blank, it is derived by taking the host name and removing everything after and including the first period ('.'). If the host name is an IP address, Called Name must be specified.

Share The name of the share to test on the CIFS server. For example, if you wanted to test “\\engineering\software”, the share would be “software”. This is not the same thing as a path. The CIFS poller does not test individual files, it only connects to the share.

CVS (Concurrent Versions System)

CVS is the Concurrent Versions System, an open-source network-transparent version control system.

The ServiceWatch CVS fields are listed in Table 4-2.

Table 4-2: CVS fields

Port	The port that is used to connect to the CVS server. Most CVS servers use port 2401.
Username	The username that is used to login to the CVS server.
Password	The password of the account specified in the Username field.
Path	The path of a directory under CVS control. You must set the correct path of a directory under CVS control. If the pathname is not a directory under CVS control, then ServiceWatch will not be able to log into the CVS server. The default path is /export/cvsroot.

DHCP (Dynamic Host Configuration Protocol) Servers

Dynamic Host Configuration Protocol (DHCP) is used to assign IP addresses to client machines upon boot up.

To monitor the availability of the DHCP network service, ServiceWatch software broadcasts a DHCP request for an IP address and waits for a DHCP server to respond with an IP address. Consequently, a DHCP server or relay server:

- Must be on the same physical network segment as the ServiceWatch software
- Must be configured to respond to (provide an IP address to) DHCP requests from the ServiceWatch machine

Since ServiceWatch software can monitor DHCP servers that respond on the ServiceWatch network, the hostname you enter is localhost. It does not look at the hostname to determine which DHCP server to monitor since it can monitor only DHCP servers that respond on the ServiceWatch network.

You should monitor only one DHCP server from a specific ServiceWatch host. If more than one DHCP request attempts to “bind” to port 68, the second attempt fails, reporting that the address is already in use. To monitor more than one DHCP server, set up each monitoring request on a different ServiceWatch host.

For Windows NT or Windows 2000 users: Do not attempt to monitor a DHCP server if the Windows NT or Windows 2000 system where the ServiceWatch software is installed has a dynamic IP address. The Windows NT or Windows 2000 system sometimes "forgets" its IP address after ServiceWatch sends out sample DHCP packets.

DNS (Domain Name System) Servers

The domain name system (DNS) service is used to convert hostnames into Internet addresses, or vice versa.

To monitor a DNS server, the ServiceWatch software contacts the server and requests that it resolve a hostname. It then parses the DNS server's response and checks for errors.

If you do not specify a hostname to resolve, the ServiceWatch software will select a hostname that the DNS server is likely to be able to resolve.

If you would like the DNS server to attempt to resolve a different hostname, use the **Hostname to Resolve** field.

Specifying TCP or UDP

Most network servers respond to *either* TCP or UDP, but not both. DNS is an exception to this. Typically, DNS servers can respond to queries via *both* UDP and TCP.

The DNS protocol is different, depending on whether the connection to DNS is UDP/IP or TCP/IP. ServiceWatch software can make "test" queries via UDP or TCP. By default, it communicates with DNS servers via TCP, since the its objective is to determine if a DNS server is up and reliable. If an unreliable protocol, such as UDP is used, it is more likely that an apparent failure of a DNS server is actually due to a dropped UDP packet.

However, you may find it useful to have the ServiceWatch software communicate with the DNS server via UDP. Even though UDP is an unreliable protocol, you may want to know how unreliable it is in your environment.

The ServiceWatch DNS fields are listed in Table 4-3.

Table 4-3: DNS fields

Port	The port that is used to connect to the DNS server. DNS servers respond to port 53.
Hostname to Resolve	The name of a host that you would like the DNS server to attempt to resolve. If this field is empty, ServiceWatch determines a hostname that the DNS server is likely able to resolve.
Protocol	The protocol that is used to communicate with the DNS server. This can be either TCP or UDP. Many DNS servers can communicate via either TCP or UDP, though UDP is more commonly used.

EPICenter Servers

EPICenter servers are used to manage Extreme Networks switches.

The ServiceWatch EPICenter fields are listed in Table 4-4.

Table 4-4: EPICenter fields

Port	The port that is used to connect to the EPICenter web server.
Username	The username that is used to login to the EPICenter web server.
Password	The password of the account specified in the Username field.

See the installation chapter appropriate for your operating system for information on configuring the ServiceWatch software to work with EPICenter servers.

FTP (File Transfer Protocol) Servers

FTP is used to transfer files between a client and server. By default, the Anonymous FTP user is used to monitor the FTP server. You may alternatively specify another FTP username and password in the Username and Password fields. If a filename to download is specified, it is requested from the FTP server.

The monitoring request is considered successful if the login process completes, or the file is downloaded, if that option was specified.

The ServiceWatch FTP fields are listed in Table 4-5.

Table 4-5: FTP fields

Port	The port that is used to connect to the FTP server. Most FTP servers use port 21.
Username (Optional)	The username that is used to login to the FTP server. If this field is empty, then the Anonymous FTP user is used.
Password	The password of the account specified in the Username field.
Filename to download	If a filename to download is specified it is requested from the FTP server. If this field is blank, then ServiceWatch attempts to log into the FTP server, but no file transfer is attempted.

HTTP (Web) Servers

Hyper Text Transfer Protocol (HTTP) is a client to web server protocol.

To monitor web servers, ServiceWatch sends an HTTP request to the specified web server, to retrieve either the default home page ("/") or a document you specify in the **Path** field. ServiceWatch then registers the time it takes for the page to be sent, and records this as the response time. If any errors occurred, such as the file was **Not found** on the web server, this information is also recorded.

Response Time and Web Servers

The ServiceWatch software records the time it takes for a web server to retrieve a specified page in the **Time** variable. Since some files stored on a web server are much larger than others, files of greater length return a longer response time. Keep this in mind when choosing which files ServiceWatch software requests.

If the specified filename does not exist, the web server responds with data that indicates an error, such as:

```
<HEAD><TITLE>404 Not Found</TITLE></HEAD>
<BODY><H1>404 Not Found</H1>
<P>The Requested URL /file.html was not found on this server.</P>
</BODY>
```

In this case, the ServiceWatch software reports the web server as down.

The information returned from the web server is the content only of the URL you specified. If the page at that URL contains links to other elements such as graphics files, those files are not requested from the web server by ServiceWatch software, as its purpose is to check for web server response time. If you want to download additional files, you can do so, by specifying specific filenames in additional queries.

The ServiceWatch HTTP fields are listed in Table 4-6.

Table 4-6: HTTP fields

Path	The path of the file to download from the HTTP server.
Port	The port that is used to connect to the HTTP server. The standard HTTP web server port is 80, though many other web ports are used also.
Username	The username that is sent for access to password protected web servers that use the basic HTTP authentication mechanism (where a pop-up window asks for UserID and Password). This field is not for web sites that require a username and password on the main browser page, which is then checked for validity by a back-end database. This field is used only for the basic HTTP authentication mechanism described in the HTTP standard documents.
Password	The password of the account specified in the Username field.
Search returned page for this string	If this field is not blank, then after the requested page is downloaded from the web server, it is searched for the string in this field. If the string is found in the page, then the web site is considered up. If the string is not found in the page, then the web site is considered down.
Search returned page for this regular expression	If this field is not blank, then after the requested page is downloaded from the web server, it is searched for the regular expression in this field. If the regular expression is found in the page, then the web site is considered up. Otherwise the web server is considered down.
Proxy Name	The name or IP address of a proxy server that is used to perform the HTTP request. Proxy servers might be used for a number of reasons: ■ In some enterprises, firewalls prevent users from directly accessing external web servers. In these cases, only proxy servers are allowed to make HTTP requests through a firewall. ■ You may want ServiceWatch to test the performance of proxy servers.
Proxy Port	The port number of the proxy server entered in the Proxy Name field.

Table 4-6: HTTP fields

Use Proxy Cache

If this box is checked, then the proxy server is allowed to send cached pages to ServiceWatch. Using the proxy cache can greatly improve response times, but does not necessarily show response time of the proxy-to-external-web-server communication. Rather, it is a measure of the proxy server performance itself.

If this box is not checked, then the proxy server's cache is not used. This tells the proxy server not to used a cached version of the requested page, but to have the proxy server re-retrieve the designated web page during each poll attempt.

Follow HTTP redirects?

Some web pages automatically redirect a user to another web site. If this box is checked, then ServiceWatch follows any redirect request from the web server, and download a web page from site it was redirected to.

In some cases, the second web server may redirect the user again.

If this box is not checked, then only one web page is attempted to download, even if there is a redirect request.

HTTPS (Secure Web) Servers

Hyper Text Transfer Protocol Secure (HTTPS) is a client to web server protocol. ServiceWatch software uses a Secure Sockets Layer (SSL) encrypted protocol to monitor secure web servers.

Due to U.S. export restrictions, this HTTPS/SSL monitoring feature is initially disabled. You can request this feature by filling out a form on the Extreme Networks web site.

To add support for HTTPS/SSL, fill out a form at the Extreme Networks web site `http://www.extremenetworks.com/go/SW20Encrypt.htm` If approved, you are told how to add HTTPS/SSL to ServiceWatch 2.0.

The ServiceWatch HTTPS fields are listed in Table 4-7.

Table 4-7: HTTPS fields

Path

The path of the file to download from the HTTPS server.

Port

The port that is used to connect to the HTTPS server. The standard HTTPS web server port is 443, though many other web ports are used also.

Table 4-7: HTTPS fields

Username

The username that is sent for access to password protected web servers that use the basic HTTPS authentication mechanism (where a pop-up window asks for UserID and Password).

This field is not for web sites that require a username and password on the main browser page, which is then checked for validity by a back-end database. This field is used only for the basic HTTPS authentication mechanism described in the HTTPS standard documents.

Password

The password of the account specified in the Username field.

Search returned page for this string

If this field is not blank, then after the requested page is downloaded from the web server, it is searched for the string in this field. If the string is found in the page, then the web site is considered up. If the string is not found in the page, then the web site is considered down.

Search returned page for this regular expression

If this field is not blank, then after the requested page is downloaded from the web server, it is searched for the regular expression in this field. If the regular expression is found in the page, then the web site is considered up. Otherwise the web server is considered down.

Proxy Name

The name or IP address of a proxy server that is used to perform the HTTPS request. Proxy servers might be used for a number of reasons:

- In some enterprises, firewalls prevent users from directly accessing external web servers. In these cases, only proxy servers are allowed to make HTTPS requests through a firewall.
- You may want ServiceWatch to test the performance of proxy servers.

Proxy Port

The port number of the proxy server entered in the Proxy Name field.

Use Proxy Cache

If this box is checked, then the proxy server is allowed to send cached pages to ServiceWatch. Using the proxy cache can greatly improve response times, but does not necessarily show response time of the proxy-to-external-web-server communication. Rather, it is a measure of the proxy server performance itself.

If this box is not checked, then the proxy server's cache is not used. This tells the proxy server not to use a cached version of the requested page, but to have the proxy server re-retrieve the designated web page during each poll attempt.

IMAP4 Mail Servers

IMAP4 mail servers are used to dynamically access mailboxes across a network. To monitor an IMAP4 server, the ServiceWatch software simply connects to the server. The request is considered successful if the server responds with a correct initial identification message.

The ServiceWatch IMAP 4 fields are listed in Table 4-8.

Table 4-8: IMAP 4 fields

Port	The port that is used to connect to the IMAP server. Most IMAP servers use port 143.
Username (Optional)	The username that is used to access the IMAP server. If this field is empty, then the IMAP server is contacted and checked for returning correct information, but no username is used.
Password	The password of the account specified in the Username field.

LDAP (Lightweight Directory Access Protocol) Servers

Lightweight Directory Access Protocol (LDAP) is used to access online directory services.

LDAP servers are used for accessing online directory services. By default, the ServiceWatch software does a generic search that returns top-level information about the directory.

You can also specify custom searches by entering a search filter in the **Search Filter** field.

The ServiceWatch LDAP fields are listed in Table 4-9.

Table 4-9: LDAP fields

Port	The port that is used to connect to the LDAP server. Most LDAP servers use port 389.
Search Filter	The filter that is used to search the LDAP directory. By default, this is: objectclass=*. Another example for a search filter is: cn=smith

NFS (Network File System)

Network File System (NFS) is used to share directories and files on one machine with others via the network. Using NFS, users and programs can access files on remote systems as if they were local files.

The ServiceWatch NFS fields are listed in Table 4-10.

Table 4-10: NFS fields

Port	The port that is used to connect to the NFS server. Most NFS servers use port 111.
Transport	The transport protocol that is used to communicate with the NFS server (UDP or TCP).
Path	The path of a directory that is mounted from the NFS servers.

News (NNTP) Servers

Network News Transfer Protocol (NNTP) is used to send and receive Usenet news articles. That the NNTP/news server must be configured to allow delivery of news to the ServiceWatch machine in order for the ServiceWatch software to accurately report its status.

The ServiceWatch NNTP fields are listed in Table 4-11.

Table 4-11: NNTP fields

Port	The port that is used to connect to the NNTP server. Most NNTP servers use port 119.
Username	The username that is used to access the NNTP server. If this field is empty, then the NNTP server is contacted and checked for returning correct information, but no username is used.
Password	The password of the account specified in the Username field.

ODBC

ODBC is used to access ODBC compatible databases. ServiceWatch software uses the driver connection with the connection string entered in Use connection string for connection, or the string DSN=DSN name;UID=User Name;PWD=Password for connection. The ODBC managers are Windows ODBC manager (preinstalled in Windows) and iODBC manager (for UNIX systems).

- For ODBC access, you can use the DSN name or the FileDSN name. Monitoring a database with ServiceWatch software requires using the DSN name. When using the DSN name, make sure that the DSN name was created under the System DSN, not the User DSN, since the ServiceWatch software in Windows (NT and Windows 2000) is run as a service.
- In the connection string or the setup in the ODBC manager you need to make sure that AutoStart = No and AutoStop = No. Otherwise, the former always makes the checking successful, and the latter probably interferes with the server that is being polled.
- The database server needs to make sure that the TCP/IP connection is enabled.

Example Connection Strings

In Windows, if there is DSN filename named `FooFile` that looks like this:

```
[ODBC]
        DRIVER=Adaptive Server Anywhere 7.0
        UID=DBA
        PWD=SQL
        CommLinks=TCPIP{ip=zlu-c}
        EngineName=foo
```

Then the connection string (the DSN string) is “`FileDSN=FooFile`”. Make sure this file is accessible to any Windows users.

In Windows, use the ODBC manager to set up a system DSN, then use the connection string:

```
DSN=dsn name;UID=DBA;PWD=SQL
```

In UNIX and Windows, a connection string looks like:

```
Driver=/opt/swatch2/Sybase/dbodbc7_r.so.1;UID=guest;PWD=swatch;
ENG=ServiceWatch;
```

The ServiceWatch ODBC fields are listed in Table 4-12.

Table 4-12: ODBC fields

DSN Name	The ODBC Data Source Name.
Username	The username that is used to access the database server.
Password	The password of the account specified in the Username field.
Use Connection String	The connection string that users prefer to use to connect to the database. See “Example Connection Strings” on page 4-13.
SQL statement	The SQL statement that is used in the status monitoring. For example, you might want ServiceWatch to request a particular table to be searched.

Ping Protocol

The ICMP Ping protocol is used to determine whether or not a host is responding on its network connection.

Virtually all machines that communicate via TCP/IP can respond to ping requests. You can use a Ping request to determine whether a system is up or down.

To determine whether a machine is up, ServiceWatch software sends a ping packet (an ICMP echo request packet) to a target machine. The target machine, if up, responds with a ping reply. If the machine is down, the ping eventually returns with an error. However, depending on the value you set for **Maximum Wait**, the request may exceed the response-time threshold and the ServiceWatch software considers the host down without waiting for the request to complete.

Pop3 Servers

Post Office Protocol (POP3) POP allows users to dynamically access their mailboxes from across a network.

To monitor a POP3 server, ServiceWatch software simply connects to the server. The request is considered successful if the server responds with a correct initial identification message.

The ServiceWatch POP3 fields are listed in Table 4-13.

Table 4-13: POP3 fields

Port	The port that is used to connect to the POP server. Most POP servers use port 110.
Username (Optional)	The username that is used to access the POP server. If this field is empty, then the POP server is contacted and checked for returning correct information, but no username is used.
Password	The password of the account specified in the Username field.

RADIUS Servers

The Remote Authentication Dial In User Service (RADIUS) is used for remote authentication primarily for dial-up centers.

The ServiceWatch RADIUS fields are listed in Table 4-14.

Table 4-14: RADIUS fields

Port	The UDP port to connect to on the RADIUS server. Note from RFC 2138: There has been some confusion in the assignment of port numbers for this protocol. The early deployment of RADIUS was done using the erroneously chosen port number 1645, which conflicts with the “datametrics” service. The officially assigned port number for RADIUS is 1812.
Username	The username of the login account used in verifying the server.
Password	The password of the account specified in the Username field.
Trust Key/Secret	The Trust (Secret) key for ServiceWatch Server used when communicating with the RADIUS server.

RPing Servers

Remote Ping (RPing) is used to specify a switch that should attempt to ping another host.

For example, ServiceWatch software requests switch A to ping switch B. If the ping to switch B responds, then you know that the path between switch A and switch B is up.

For RPing polling to work, the hostname field must be the name of a switch that supports the PING MIB (RFC 2925) and the remote ping facility must be enabled on the switch.

The ServiceWatch RPing fields are listed in Table 4-15.

Table 4-15: RPing fields

Write Community String	The write community string of the switch that performs the ping. The default write community string is private.
Target address for switch to ping	The IP address (not hostname) of a second switch that the first switch attempts to ping.

SMTP Mail Servers

Simple Mail Transfer Protocol (SMTP) is used to deliver email messages.

To monitor an SMTP server, ServiceWatch software simply connects to the server. The request is considered successful if the server responds with a correct initial identification message.

The ServiceWatch SMTP fields are listed in Table 4-16.

Table 4-16: SMTP fields

Port	The port that is used to connect to the SMTP server. Most SMTP servers use port 25

SNMP Agents

Simple Network Management Protocol (SNMP) is used to manage nodes (servers, workstations, routers, switches, hubs, and so forth).

The ServiceWatch software attempts to retrieve the value of the specified MIB-II variable from the SNMP agent only once. It does not perform any retries. SNMP version 1 is used in the GET request.

The ServiceWatch SNMP fields are listed in Table 4-17.

Table 4-17: SNMP fields

Port	The port that is used to connect to the SNMP server. Most SNMP servers use port 161.
Read Community String	The read community string of the SNMP agent being contacted. The default read community string is public.
MIB-II variable name	The MIB-II variable that is retrieved from the SNMP agent. ServiceWatch attempts to retrieve the value of the specified MIB-II variable from the SNMP agent only once. SNMP version 1 is used in the GET request. The default variable retrieved is: `sysDescr.0` If the MIB-II variable can be retrieved, its value is placed in the Response Reason field.
SNMP value greater than this value	The SNMP variable's returned value must be greater than this parameter or the service is considered down.
SNMP value less than this value	The SNMP variable's returned value must be less than this parameter or the service is considered down.
SNMP value equal to this value	The SNMP variable's returned value must be the same as this parameter or the service is considered down.
SNMP value contains this value	The SNMP variable's returned value must contain this string or the service is considered down.

TCP Layer 4

TCP Layer 4 is used to connect to a server listening on a TCP port. Optionally, the ServiceWatch software can attempt to read data from the TCP server and search for a specified string.

The ServiceWatch TCP Layer 4 fields are listed in Table 4-18.

Table 4-18: TCP layer 4 fields

Port	The TCP layer 4 port that is used to attempt to connect to a TCP server.
Check for this string after connection (Optional)	If this field is not blank, then data is attempted to be read from the server. Then the data read is searched for the string in this field. If the string is found, then the TCP server is considered up. If the string is not found, the TCP server is considered down.

Telnet Servers

Telnet is a virtual terminal service used for logging into a remote machine.

To monitor a telnet server, ServiceWatch software simply connects to the server. It does not attempt to log in, so a username and password are not needed. The request is considered successful if the server responds appropriately to the connection and telnet configuration request.

The ServiceWatch telnet fields are listed in Table 4-19.

Table 4-19: Telnet fields

Port	The port that is used to connect to the telnet server. Most telnet servers use port 23.

TFTP

Trivial File Transfer Protocol (TFTP) is used to transfer files between a client and server over the unreliable UDP protocol.

The ServiceWatch TFTP fields are listed in Table 4-20.

Table 4-20: TFTP fields

Filename to download	The name of the file to download from the TFTP server.

Reports

ServiceWatch reports let you graph and report data on requests that are present in your Request List.

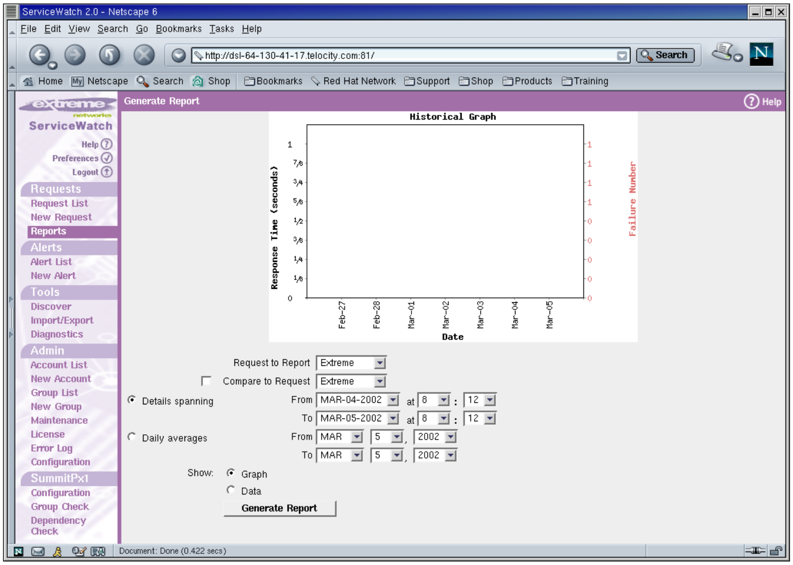
Overview of ServiceWatch Reports

You can display the following types of reports from the ServiceWatch software:

- Response time of one request
- Response times of two requests, compared and displayed together
- Daily average response time of one request
- Daily average response times of two requests, compared and displayed together

To use the reports feature, follow these steps:

1 Click the **Reports** link on the ServiceWatch navigation pane. The Generate Report page appears, as shown in Figure 4-1.



Request to Report: Extreme

□ Compare to Request: Extreme

● Details spanning From MAR-04-2002 at 8 : 12

To MAR-05-2002 at 8 : 12

○ Daily averages From MAR 5, 2002

To MAR 5, 2002

Show: ● Graph ○ Data

Generate Report

Document: Done (0.422 secs)

Figure 4-1: Generate Report page

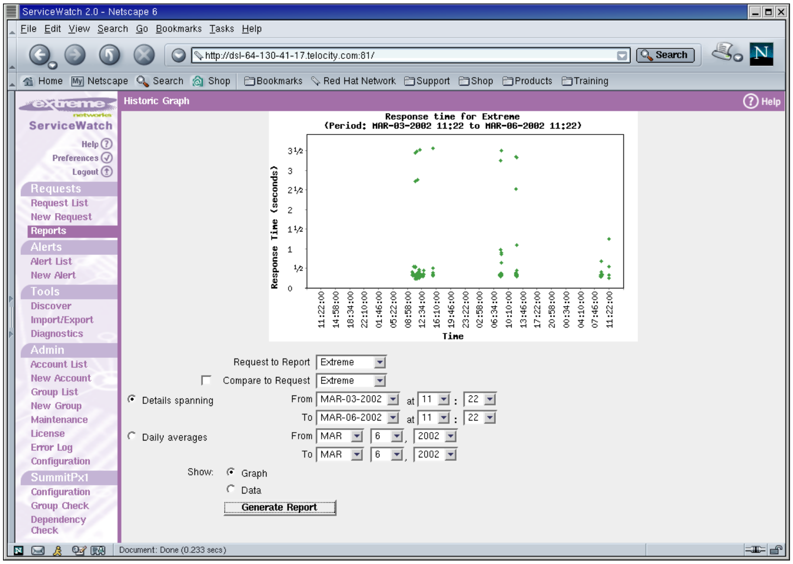
After you select the time range for your report, you can chose either Graph or Data from the show options, to have your report displayed as a graph or as a table of data.

- For the response time reports, you can select any time span from the present to six days ago.
- For the daily averages reports, you can select any time span from today to January 1, 2001.

Request Response Time Reports

To create a request response time report, follow these steps:

1. From the **Request to Report** drop list, select the request you want to generate a report for.
2. Select the **Details Spanning** option, if not already selected.
3. In the **From** drop lists, select a date and time.
4. In the **To** drop lists, select a date and time.
5. From the **Show** options, select **Graph** to display a graphical report or **Data** to display a tabular data report.
6. Click **Generate Report**. Your report appears as shown in Figure 4-2 or Figure 4-3.



Request to Report: Extreme

□ Compare to Request: Extreme

● Details spanning

From MAR-03-2002 at 11 : 22

To MAR-06-2002 at 11 : 22

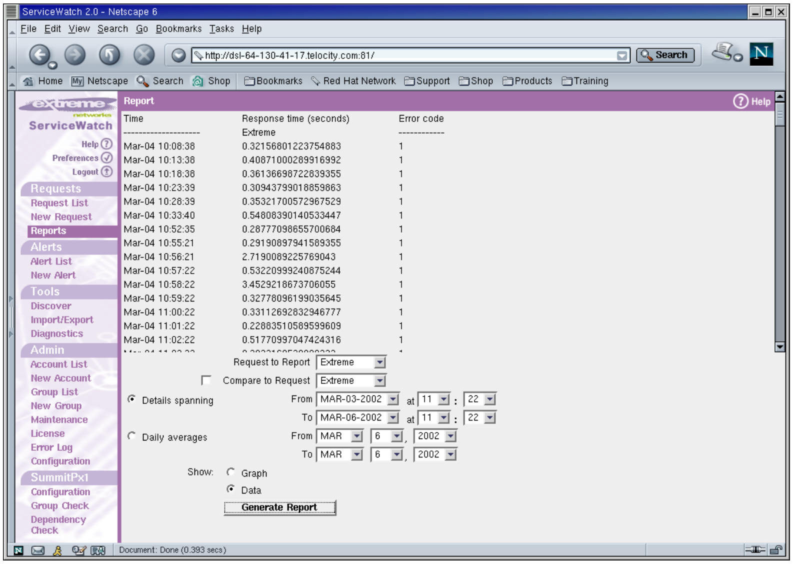
○ Daily averages

From MAR 6, 2002

To MAR 6, 2002

Show: ● Graph ○ Data

Figure 4-2: Request Response Time graph report



```
Time                  Response time (seconds)    Error code
--------------------  Extreme                    ------------
Mar-04 10:08:38       0.32156801223754883        1
Mar-04 10:13:38       0.40871000289916992        1
Mar-04 10:18:38       0.36136698722839355        1
Mar-04 10:23:39       0.30943799018859863        1
Mar-04 10:28:39       0.35321700572967529        1
Mar-04 10:33:40       0.54808390140533447        1
Mar-04 10:52:35       0.28777098655700684        1
Mar-04 10:55:21       0.29190897941589355        1
Mar-04 10:56:21       2.7190089225769043         1
Mar-04 10:57:22       0.53220999240875244        1
Mar-04 10:58:22       3.4529218673706055         1
Mar-04 10:59:22       0.32778096199035645        1
Mar-04 11:00:22       0.33112692832946777        1
Mar-04 11:01:22       0.22883510589599609        1
Mar-04 11:02:22       0.51770997047424316        1
```

Request to Report: Extreme

□ Compare to Request: Extreme

● Details spanning — From MAR-03-2002 at 11 : 22 — To MAR-06-2002 at 11 : 22

○ Daily averages — From MAR 6, 2002 — To MAR 6, 2002

Show: ○ Graph ● Data

Generate Report

Document: Done (0.393 secs)

Figure 4-3: Request Response Time data report

Request Response Time Comparison Reports

To create a request response time report comparing two requests, follow these steps:

1 From the **Request to Report** drop list, select the first request you want to generate a report for.

2 Check the **Compare to Request** check box, and from the drop list, select the second request you want to generate a report for.

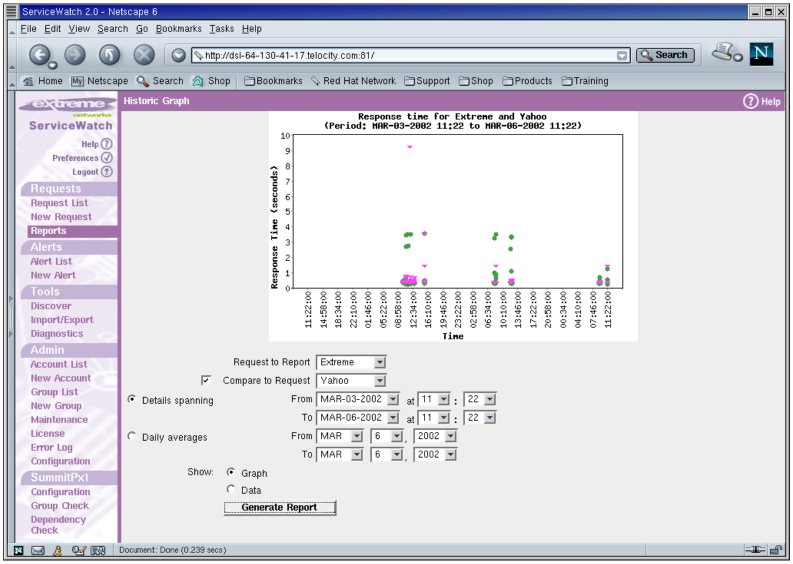
3 Select the **Details Spanning** option, if not already selected.

4 In the **From** drop lists, select a date and time.

5 In the **To** drop lists, select a date and time.

6 From the **Show** options, select **Graph** to display a graphical report or **Data** to display a tabular data report.

7 Click **Generate Report**. Your report appears as shown in Figure 4-4 or Figure 4-5.



Request to Report: Extreme

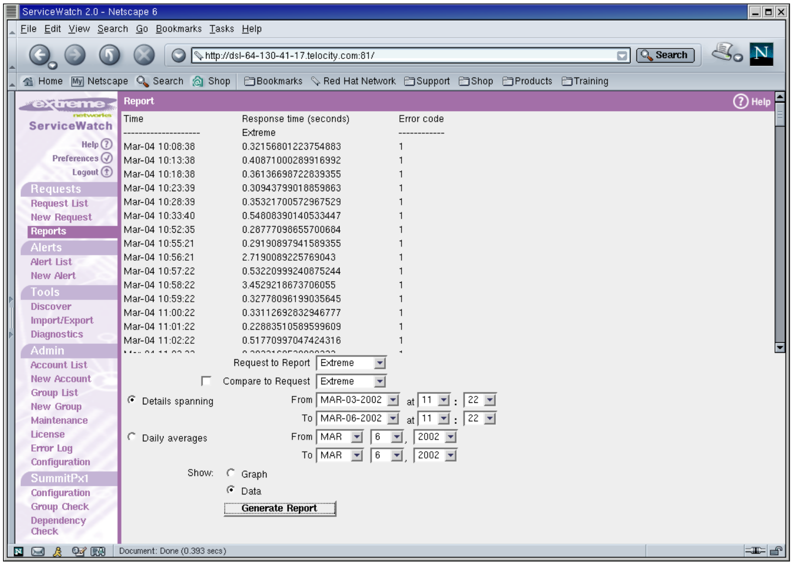
☑ Compare to Request: Yahoo

● Details spanning From MAR-03-2002 at 11 : 22
To MAR-06-2002 at 11 : 22

○ Daily averages From MAR 6, 2002
To MAR 6, 2002

Show: ● Graph
○ Data

Figure 4-4: Request Response Time Comparison graph report



```
Time                    Response time (seconds)    Error code
--------------------    Extreme                    ------------
Mar-04 10:08:38         0.32156801223754883        1
Mar-04 10:13:38         0.40871000289916992        1
Mar-04 10:18:38         0.36136698722839355        1
Mar-04 10:23:39         0.30943799018859863        1
Mar-04 10:28:39         0.35321700572967529        1
Mar-04 10:33:40         0.54808390140533447        1
Mar-04 10:52:35         0.28777098655700684        1
Mar-04 10:55:21         0.29190897941589355        1
Mar-04 10:56:21         2.7190089225769043         1
Mar-04 10:57:22         0.53220999240875244        1
Mar-04 10:58:22         3.4529218673706055         1
Mar-04 10:59:22         0.32778096199035645        1
Mar-04 11:00:22         0.33112692832946777        1
Mar-04 11:01:22         0.22883510589599609        1
Mar-04 11:02:22         0.51770997047424316        1
```

Request to Report: Extreme

□ Compare to Request: Extreme

● Details spanning From MAR-03-2002 at 11 : 22
To MAR-06-2002 at 11 : 22

○ Daily averages From MAR 6, 2002
To MAR 6, 2002

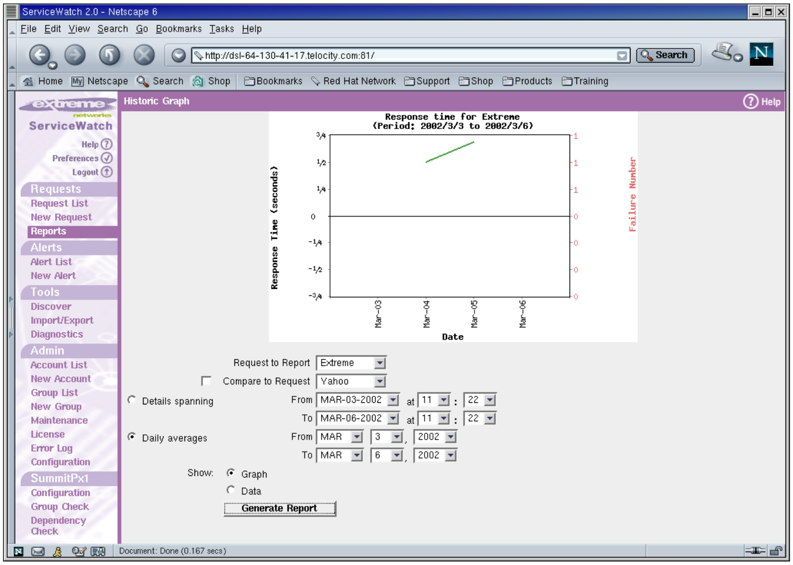
Show: ○ Graph
● Data

Figure 4-5: Request Response Time Comparison data report

Daily Averages Response Time Reports

To create a daily averages request response time report, follow these steps:

1. From the **Request to Report** drop list, select the request you want to generate a report for.
2. Select the **Daily Averages** option, if not already selected.
3. In the **From** drop list, select a date and time.
4. In the **To** drop list, select a date and time.
5. From the **Show** options, select **Graph** to display a graphical report or **Data** to display a tabular data report.
6. Click **Generate Report**. Your report appears as shown in Figure 4-6 or Figure 4-7.



Request to Report: Extreme

□ Compare to Request: Yahoo

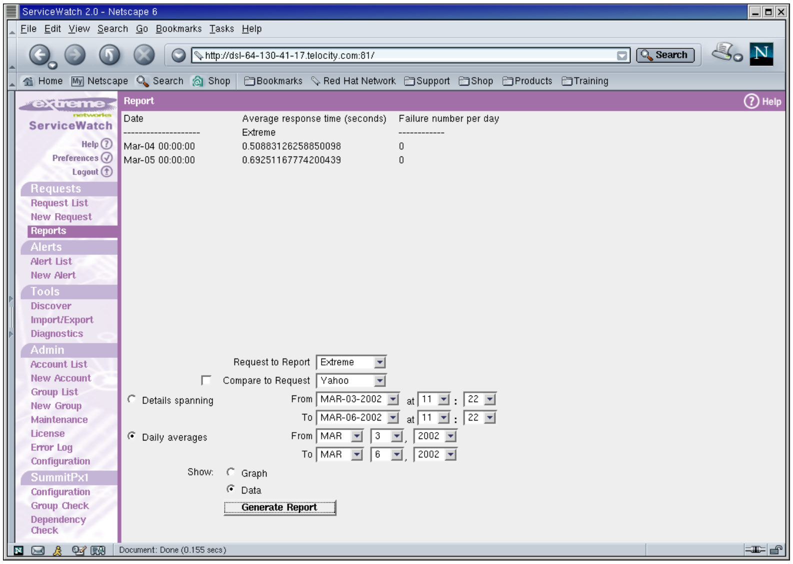
○ Details spanning From MAR-03-2002 at 11 : 22
To MAR-06-2002 at 11 : 22

● Daily averages From MAR 3, 2002
To MAR 6, 2002

Show: ● Graph
○ Data

Generate Report

Figure 4-6: Daily Averages Response Time graph report



```
Date                    Average response time (seconds)   Failure number per day
--------------------    Extreme                           ------------
Mar-04 00:00:00         0.50883126258850098               0
Mar-05 00:00:00         0.69251167774200439               0
```

Request to Report: Extreme

□ Compare to Request: Yahoo

○ Details spanning — From: MAR-03-2002 at 11 : 22 — To: MAR-06-2002 at 11 : 22

● Daily averages — From: MAR 3, 2002 — To: MAR 6, 2002

Show: ○ Graph ● Data

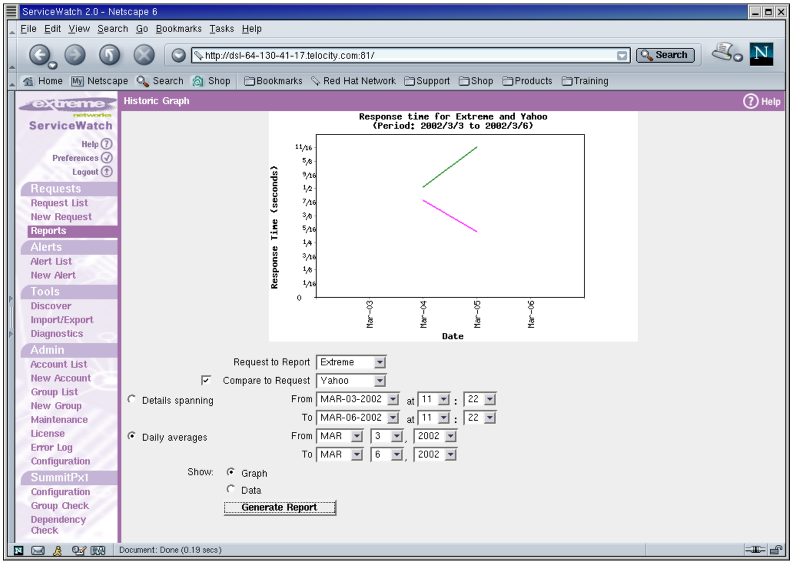
Generate Report

Figure 4-7: Daily Averages Response Time data report

Daily Averages Request Response Time Comparison Reports

To create a daily averages request response time report comparing two requests, follow these steps:

1. From the **Request to Report** drop list, select the first request you want to generate a report for.
2. Check the **Compare to Request** check box, and from the drop list, select the second request you want to generate a report for.
3. Select the **Daily Averages** option, if not already selected.
4. In the **From** drop lists, select a date and time.
5. In the **To** drop lists, select a date and time.
6. From the **Show** options, select **Graph** to display a graphical report, or **Data** to display a tabular data report.
7. Click **Generate Report**. Your report appears as shown in Figure 4-8 or Figure 4-9.


ServiceWatch 2.0 - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
http://dsl-64-130-41-17.telocity.com:81/
Search
Home My Netscape Search Shop Bookmarks Red Hat Network Support Shop Products Training
ServiceWatch
Help Preferences Logout
Requests Request List New Request Reports
Alerts Alert List New Alert
Tools Discover Import/Export Diagnostics
Admin Account List New Account Group List New Group Maintenance License Error Log Configuration
SummitPx1 Configuration Group Check Dependency Check
Historic Graph
Help
Response time for Extreme and Yahoo
(Period: 2002/3/3 to 2002/3/6)
Response Time (seconds)
11/16
5/8
9/16
1/2
7/16
3/8
5/16
1/4
3/16
1/8
1/16
0
Mar-03
Mar-04
Mar-05
Mar-06
Date
Generate Report
Document: Done (0.19 secs)

Request to Report: Extreme

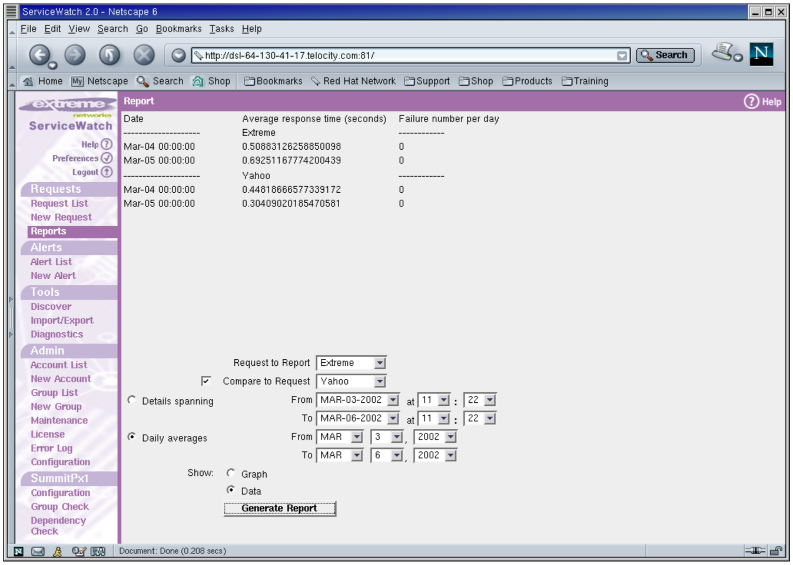
☑ Compare to Request: Yahoo

○ Details spanning From MAR-03-2002 at 11 : 22 To MAR-06-2002 at 11 : 22

● Daily averages From MAR 3, 2002 To MAR 6, 2002

Show: ● Graph ○ Data

Figure 4-8: Daily Averages Request Response Time Comparison graph report


ServiceWatch 2.0 - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
http://dsl-64-130-41-17.telocity.com:81/
Search
Home My Netscape Search Shop Bookmarks Red Hat Network Support Shop Products Training
ServiceWatch
Help Preferences Logout
Requests Request List New Request Reports
Alerts Alert List New Alert
Tools Discover Import/Export Diagnostics
Admin Account List New Account Group List New Group Maintenance License Error Log Configuration
SummitPx1 Configuration Group Check Dependency Check
Report
Help
Generate Report
Document: Done (0.208 secs)

```
Date                    Average response time (seconds)   Failure number per day
--------------------    Extreme                           ------------
Mar-04 00:00:00         0.50883126258850098               0
Mar-05 00:00:00         0.69251167774200439               0
--------------------    Yahoo                             ------------
Mar-04 00:00:00         0.44818666577339172               0
Mar-05 00:00:00         0.30409020185470581               0
```

Request to Report: Extreme

☑ Compare to Request: Yahoo

○ Details spanning From MAR-03-2002 at 11 : 22 To MAR-06-2002 at 11 : 22

● Daily averages From MAR 3, 2002 To MAR 6, 2002

Show: ○ Graph ● Data

Figure 4-9: Daily Averages Request Response Time Comparison data report

Tools

ServiceWatch Tools gives you options for the Discover, Import/Export, and Diagnostics features.

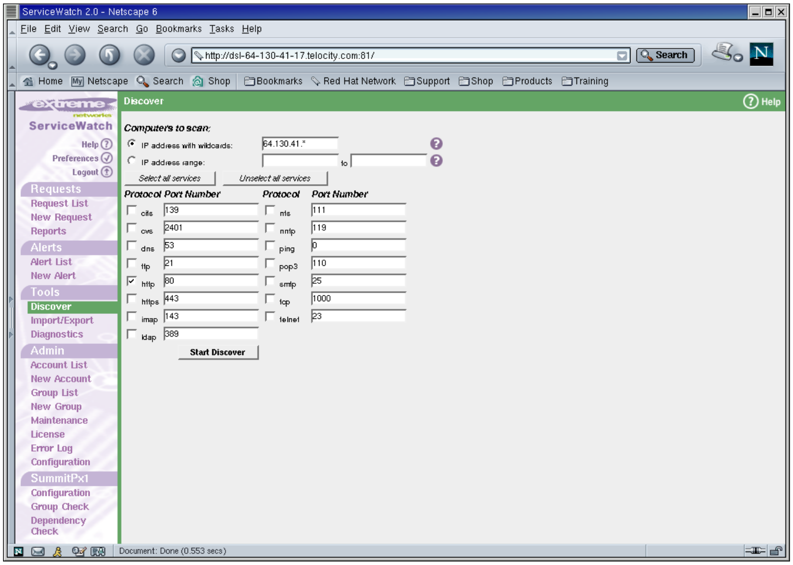
Discover

The ServiceWatch Discover feature allows it to find the various services running on a network.

First you specify what IP address range are searched and what kinds of services to search for. Then the ServiceWatch software discovers the services on the network. After the discovery is finished, it displays all the services it found and lets you choose which of these services you would like monitored.

To use the Discover feature, follow these steps:

1 Click the **Discover** link on the ServiceWatch navigation pane. The Discover page appears, as shown in Figure 4-10.



Computers to scan:

● IP address with wildcards: 64.130.41.*

○ IP address range: ______ to ______

Protocol	Port Number	Protocol	Port Number
☐ cifs	139	☐ nfs	111
☐ cvs	2401	☐ nntp	119
☐ dns	53	☐ ping	0
☐ ftp	21	☐ pop3	110
☑ http	80	☐ smtp	25
☐ https	443	☐ tcp	1000
☐ imap	143	☐ telnet	23
☐ ldap	389		

Figure 4-10: ServiceWatch Discover page

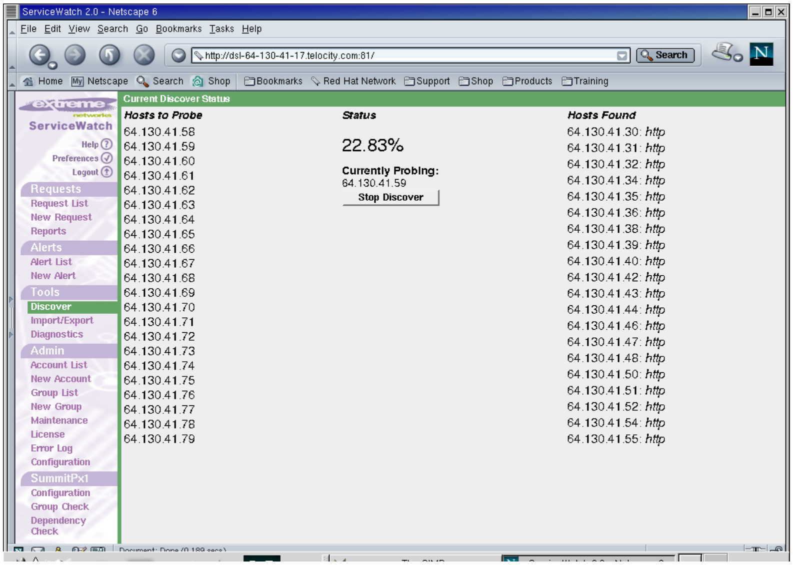
2 Select either an IP address with wildcards, or an IP address range.

— Wild Card Specification: You can specify the IP address range with a wildcard ("*") instead of a number. For example you could enter: 192.168.12.* or 192.168.*.254.

— IP Range Specification: You can choose the IP address range by entering a starting and stopping address range such as: 192.168.12.5 to 192.168.12.254

3 Select protocols and port numbers.

4 Click the **Start Discovery** button. The Current Discover Status page appears, as shown in Figure 4-11, while ServiceWatch is probing hosts.



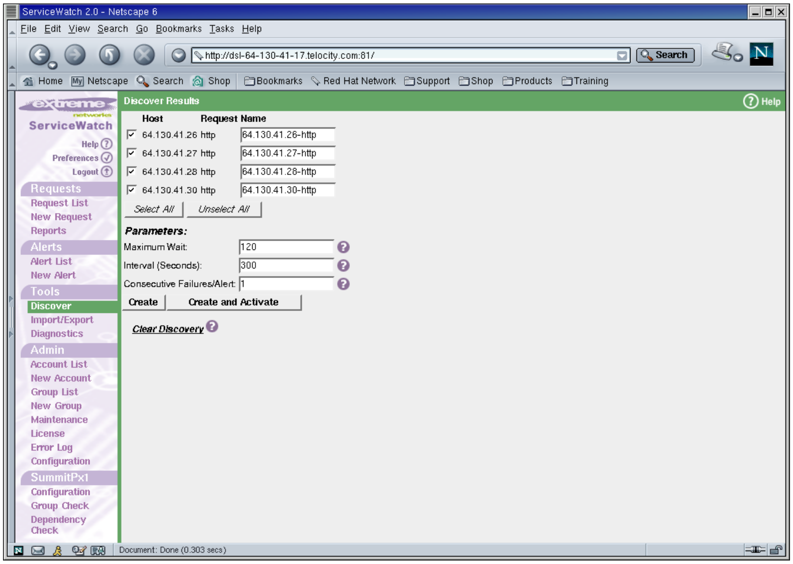
Current Discover Status

Hosts to Probe	Status	Hosts Found
64.130.41.58	22.83%	64.130.41.30: *http*
64.130.41.59	Currently Probing: 64.130.41.59	64.130.41.31: *http*
64.130.41.60		64.130.41.32: *http*
64.130.41.61		64.130.41.34: *http*
64.130.41.62		64.130.41.35: *http*
64.130.41.63		64.130.41.36: *http*
64.130.41.64		64.130.41.38: *http*
64.130.41.65		64.130.41.39: *http*
64.130.41.66		64.130.41.40: *http*
64.130.41.67		64.130.41.42: *http*
64.130.41.68		64.130.41.43: *http*
64.130.41.69		64.130.41.44: *http*
64.130.41.70		64.130.41.46: *http*
64.130.41.71		64.130.41.47: *http*
64.130.41.72		64.130.41.48: *http*
64.130.41.73		64.130.41.50: *http*
64.130.41.74		64.130.41.51: *http*
64.130.41.75		64.130.41.52: *http*
64.130.41.76		64.130.41.54: *http*
64.130.41.77		64.130.41.55: *http*
64.130.41.78		
64.130.41.79		

Document: Done (0.189 secs)

Figure 4-11: Current Discover Status page

When the ServiceWatch software is done probing for hosts, the Discover Results page appears, as shown in Figure 4-12.



Discover Results

	Host	Request Name
☑	64.130.41.26 http	64.130.41.26-http
☑	64.130.41.27 http	64.130.41.27-http
☑	64.130.41.28 http	64.130.41.28-http
☑	64.130.41.30 http	64.130.41.30-http

Select All | Unselect All

Parameters:

Maximum Wait:	120
Interval (Seconds):	300
Consecutive Failures/Alert:	1

Create | Create and Activate

Clear Discovery

Document: Done (0.303 secs)

Figure 4-12: Discover Results page

Discover Results

The Discover Results page displays the services that were found during the discovery.

Any discovered service is shown in its own row. The host, protocol, and suggested request names are listed.

To add any of the discovered services to your request list, follow these steps:

1 Check the check box to the left of each protocol you want to add.

2 In the **Parameters** section, enter the appropriate parameters for your new requests.

3 Click the **Create** button to create a new request from this discovered service, or click the **Create and Activate** button to create the new request and activate it.

To clear the Discover Results page and start a new discovery, follow these steps:

1 Click the **Clear Discover** Button.

2 The Discover Results are cleared and you return to the Discover page.

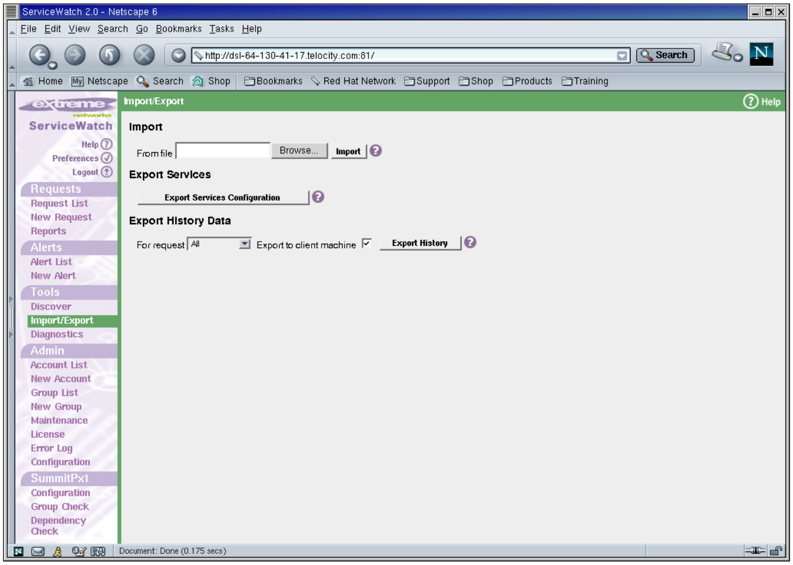
Import/Export

The ServiceWatch Import/Export feature allows you to:

- Import requests from a file.
- Export requests to a file.
- Export poller history data in a format that can be easily parsed and analyzed by spreadsheets or other programs.

To use the Import/Export features, follow these steps:

1 Click the **Import/Export** link under the Tools tab on the ServiceWatch navigation pane. The Import/Export page appears, as shown in Figure 4-13.



From file

For request All

Export to client machine ☑

Figure 4-13: ServiceWatch Import/Export page

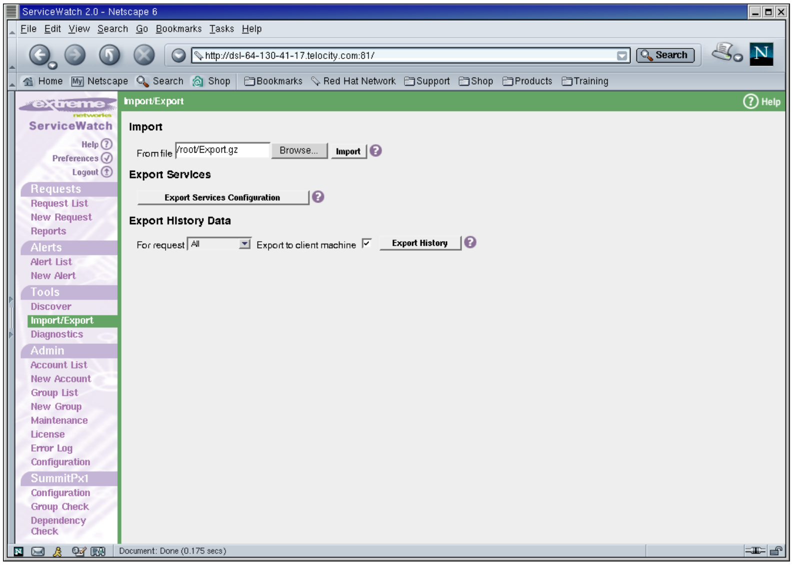
2 Choose from the following features described in the next sections and enter the appropriate parameters.

Import

The Import feature allows you to import a set of requests from a file.

To import a list of requests, follow these steps:

1 In the **Import** section of the page, as shown in Figure 4-14, enter the filename, or click the **Browse** button and navigate to the file you want to import. You can import text files or gz compressed files.



Import

From file /root/Export.gz

Export Services

Export History Data

For request All Export to client machine ☑

Figure 4-14: Importing a file into ServiceWatch

2 After the file is specified, click the **Import** button for the requests to be imported.

3 Requests are automatically added to the Request List, but not activated.

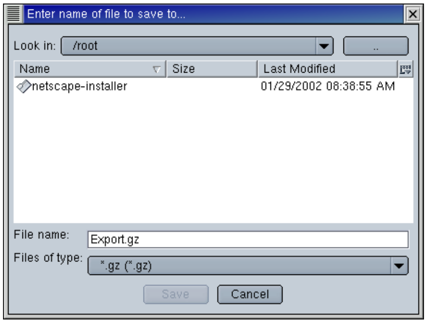
If you import requests with the same name as requests already present in your Request List, the ServiceWatch software will append a number to the names of the existing requests to make their names unique.

Export Services

This feature allows you to export all of your requests and alerts to a file. This is useful if you want to import the same set of requests on another machine running ServiceWatch software, or if you want to make sure you have a backup of the ServiceWatch requests.

To export your requests and alerts, follow these steps:

1 In the **Export Services** section of the page, click the **Export Services Configuration** button. A dialog box appears, as shown in Figure 4-15, letting you specify where to save the exported requests. The file is saved in a compressed (gzip) XML format.



Look in: /root

Name	Size	Last Modified
netscape-installer		01/29/2002 08:38:55 AM

File name: Export.gz

Files of type: *.gz (*.gz)

Figure 4-15: Export File dialog box for Netscape 6.2

2 Enter a file name, and click **Save**.

Export History Data

This feature allows you to have the poller history data exported in a format that can be parsed and analyzed by spreadsheets and other programs. The format of the file is tab-delimited and compressed in gzip format.

To export your history data, follow these steps:

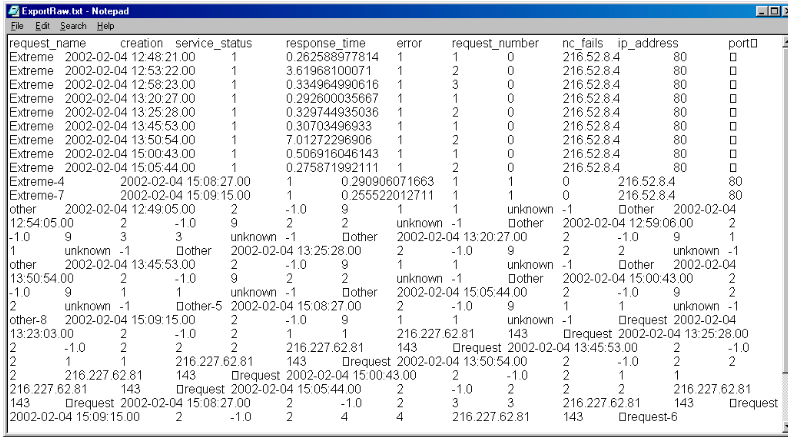
1 In the **Export History Data** section of the page, select the request you want to export data for from the **For Request** drop list, or select **All**.

2 If you want, check the **Export to client machine** check box.

When the **Export to client machine** check box is checked, the history file is saved on your machine. The file is sent to your browser, and your browser asks you where you want the file saved. If the check box isn't checked, then the file is saved on the ServiceWatch server machine in the ServiceWatch Log directory. You are told the filename and location after the export completes.

3 Click the **Export History** button. Your history data is exported in gzip format.

A sample history data file is shown in Figure 4-16.



```
request_name        creation    service_status          response_time       error       request_number      nc_fails    ip_address          port□
Extreme     2002-02-04 12:48:21.00      1           0.262588977814      1           1           0           216.52.8.4          80          □
Extreme     2002-02-04 12:53:22.00      1           3.61968100071       1           2           0           216.52.8.4          80          □
Extreme     2002-02-04 12:58:23.00      1           0.334964990616      1           3           0           216.52.8.4          80          □
Extreme     2002-02-04 13:20:27.00      1           0.292600035667      1           1           0           216.52.8.4          80          □
Extreme     2002-02-04 13:25:28.00      1           0.329744935036      1           2           0           216.52.8.4          80          □
Extreme     2002-02-04 13:45:53.00      1           0.30703496933       1           1           0           216.52.8.4          80          □
Extreme     2002-02-04 13:50:54.00      1           7.01272296906       1           2           0           216.52.8.4          80          □
Extreme     2002-02-04 15:00:43.00      1           0.506916046143      1           1           0           216.52.8.4          80          □
Extreme     2002-02-04 15:05:44.00      1           0.275871992111      1           2           0           216.52.8.4          80          □
Extreme-4               2002-02-04 15:08:27.00      1           0.290906071663      1           1           0           216.52.8.4          80
Extreme-7               2002-02-04 15:09:15.00      1           0.255522012711      1           1           0           216.52.8.4          80
other       2002-02-04 12:49:05.00      2           -1.0        9           1           1           unknown     -1          □other      2002-02-04
12:54:05.00             2           -1.0        9           2           2           unknown     -1          □other      2002-02-04 12:59:06.00      2
-1.0        9           3           3           unknown     -1          □other      2002-02-04 13:20:27.00      2           -1.0        9           1
1           unknown     -1          □other      2002-02-04 13:25:28.00      2           -1.0        9           2           2           unknown     -1
other       2002-02-04 13:45:53.00      2           -1.0        9           1           1           unknown     -1          □other      2002-02-04
13:50:54.00             2           -1.0        9           2           2           unknown     -1          □other      2002-02-04 15:00:43.00      2
-1.0        9           1           1           unknown     -1          □other      2002-02-04 15:05:44.00      2           -1.0        9           2
2           unknown     -1          □other-5    2002-02-04 15:08:27.00      2           -1.0        9           1           1           unknown     -1
other-8     2002-02-04 15:09:15.00      2           -1.0        9           1           1           unknown     -1          □request    2002-02-04
13:23:03.00             2           -1.0        2           1           1           216.227.62.81           143         □request    2002-02-04 13:25:28.00
2           -1.0        2           2           2           216.227.62.81           143         □request    2002-02-04 13:45:53.00      2           -1.0
2           1           1           216.227.62.81           143         □request    2002-02-04 13:50:54.00      2           -1.0        2           2
2           216.227.62.81           143         □request    2002-02-04 15:00:43.00      2           -1.0        2           1           1
216.227.62.81           143         □request    2002-02-04 15:05:44.00      2           -1.0        2           2           2           216.227.62.81
143         □request    2002-02-04 15:08:27.00      2           -1.0        2           3           3           216.227.62.81           143         □request
2002-02-04 15:09:15.00              2           -1.0        2           4           4           216.227.62.81           143         □request-6
```

Figure 4-16: Sample history data file

Exporting Data to Excel Spreadsheets

To export data to Excel in Windows NT and Windows 2000, follow these steps:

1 Start the ServiceWatch software.

2 Setup an ODBC Data Source Name:

- **a** Start the Windows ODBC Manager from Control Panel Data Sources, select the System DSN tab, and click the **Add** button.
- **b** In the pop-up dialog box, select **ServiceWatch ASA** driver, and click **Finish**.
- **c** In the second pop-up dialog box, select the ODBC tab and enter your choice of name in the Data Source Name box, for example, *Ext Access ServiceWatch*.
- **d** Select the Login tab, enter `guest` in the UserID box, and `swatch` in the password box.
- **e** Select the Database tab and enter `ServiceWatch` in the Server Name box.
- **f** Uncheck the **Automatically shut down database after last disconnect** check box.
- **g** Select the ODBC tab again and you should be able to test the database connection by clicking the **Test Connection** button. It should succeed.

3 Start Excel and select Data, then Get External Data, then Run Database Query.

4 Select one of the following query files from the ServiceWatch 2.0 installation directory (change the “DSN=” line to the DSN you just created):

— SelectAlertHistory.dqy

— SelectRequest.dqy

— SelectResponseData.dqy

5 Your ServiceWatch data is exported to Excel.

Exporting Data via SQL

If you have a large number of requests, exporting the configuration can take a long time to be sent to the browser. In this case, you may want to speed up the export by running an SQL script that exports data from the database.

To export data from the SQL database for use in external applications, follow these steps:

For all operating systems:

1 Start your ServiceWatch server.

2 Change directories to your python directory by typing:

```
python ../DataEngine/GetSwatchData.pyc
"../Examples/export_data_scripts/SelectRequest.sql" output.txt
```

3 The output of the SQL statement in the SelectRequest.sql is exported to the `output.txt` file.

4 Change the SQL statement to fit your needs, and continue with step 3 below.

For Windows systems, follow the steps here to export data into Excel directly:

1 Start your ServiceWatch server.

2 Setup an ODBC Data Source Name:

a Start the Windows ODBC Manager from Control Panel Data Sources, select the System DSN tab, and click the **Add** button.

b In the pop-up dialog box, select **ServiceWatch ASA** driver, and click **Finish**.

c In the second pop-up dialog box, select the ODBC tab and enter your choice of name in the Data Source Name box, for example, *Ext Access ServiceWatch.*

d Select the Login tab, enter `guest` in the UserID box, and `swatch` in the password box.

e Select the Database tab and enter `ServiceWatch` in the Server Name box.

f Uncheck the **Automatically shut down database after last disconnect** check box.

g. Select the ODBC tab again and you should be able to test the database connection by clicking the **Test Connection** button. It should succeed.

3. Go to the Examples/export data scripts directory, select any of the .dqy files, and change the DSN= line to the DSN name you created in step (2c), for example, *Ext Access ServiceWatch*. Change the SQL statements as necessary.
4. Start Excel, select Data/Get External Data/Run Database Query, then select the .dqy file you just changed in the Examples/export_data_scripts directory. It then imports the data to your Excel spreadsheet.

Diagnostics

The ServiceWatch Diagnostics feature lets you perform diagnostics on a host. You can use such diagnostics as ping, trace route, or telnet to gather important quality of service information about a particular host.

To use the Diagnostics feature, follow these steps:

1. Click the **Diagnostics** link under the **Tools** tab on the ServiceWatch navigation pane. The ServiceWatch Diagnostics page appears, as shown in Figure 4-17.

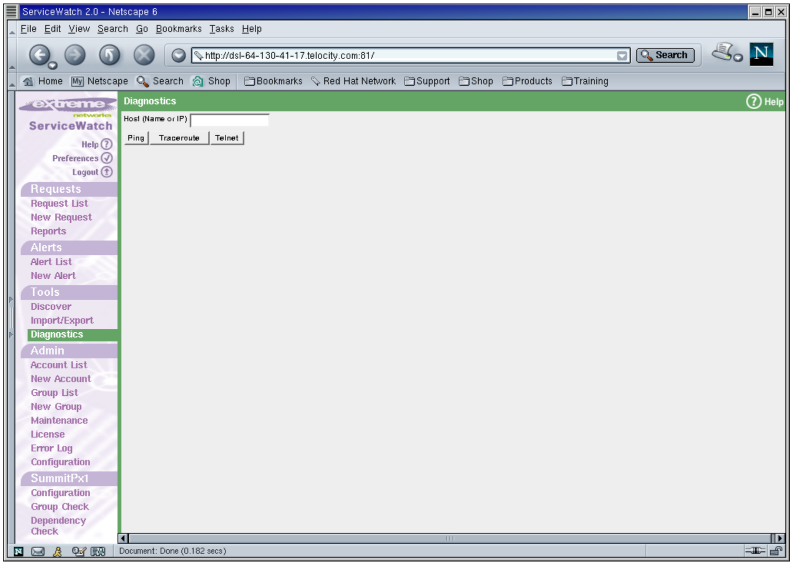
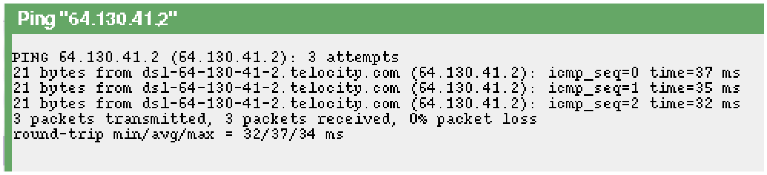


Figure 4-17: ServiceWatch Diagnostics page

2 Enter a hostname or IP address in the **Host (Name or IP)** box.

3 Click one of the **Ping**, **Trace Route,** or **Telnet** buttons.

4 ServiceWatch software attempts to ping, trace route, or telnet to the host, as shown in Figure 4-18.



```
PING 64.130.41.2 (64.130.41.2): 3 attempts
21 bytes from dsl-64-130-41-2.telocity.com (64.130.41.2): icmp_seq=0 time=37 ms
21 bytes from dsl-64-130-41-2.telocity.com (64.130.41.2): icmp_seq=1 time=35 ms
21 bytes from dsl-64-130-41-2.telocity.com (64.130.41.2): icmp_seq=2 time=32 ms
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 32/37/34 ms
```

Figure 4-18: ServiceWatch Ping diagnostic

Ping and trace route may take up to a minute to complete.

ServiceWatch Admin Features

Besides the creation and maintenance of accounts and groups discussed in the last chapter, there are other features on the **Admin** tab, such as **License**, **Error Log**, and **Configuration**.

You must be logged in as Admin to use these features.

Maintenance

The Maintenance feature allows you to perform maintenance on the ServiceWatch server.

Shutdown ServiceWatch

This feature allows you to shutdown ServiceWatch.

This feature is only available when running ServiceWatch under Linux or Solaris.

Clean Database

This feature allows you to clean the database. Running this will reduce the amount of disk space used.

You should clean the database periodically. The frequency depends on how much data you are collecting. No more than once a month is recommended for less than 100 requests polling at 5 minute intervals. For significantly higher polling demands, no more than weekly database cleaning is required.

To use the ServiceWatch Maintenance feature to clean the database, follow these steps:

1 Deactivate all requests.

2 Click the **Maintenance** link under **Admin** tab on the ServiceWatch navigation pane. The ServiceWatch Maintenance page appears, as shown in Figure 4-22

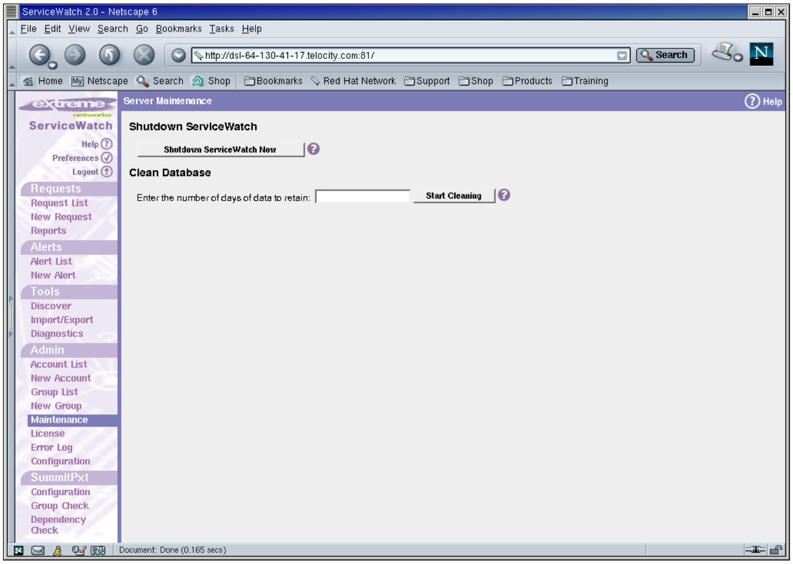


Figure 4-19: ServiceWatch maintenance page

1 In the **Clean Database** section of the page, enter the number of days to retain files in the database. Files older than that will be deleted.

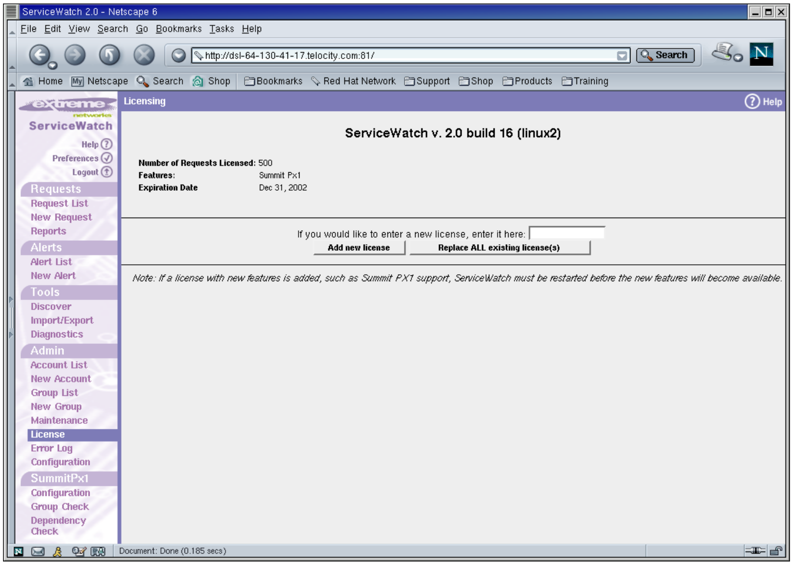
2 Click the **Start Cleaning** button.

License

The License feature allows you to add licenses to your ServiceWatch installation. If you downloaded a free evaluation version of the ServiceWatch software from the Extreme Networks website, it runs with a limited number of simultaneous requests. In order to obtain a permanent license and to allow more requests to run simultaneously or to add other features, such as support for the Summit Px1, a license must be added.

To use the ServiceWatch License feature, follow these steps:

1 Click the **License** link under the **Admin** tab on the ServiceWatch navigation pane. The ServiceWatch License page appears, as shown in Figure 4-20.



ServiceWatch v. 2.0 build 16 (linux2)

Number of Requests Licensed: 500
Features: Summit Px1
Expiration Date Dec 31, 2002

If you would like to enter a new license, enter it here:

Note: If a license with new features is added, such as Summit PX1 support, ServiceWatch must be restarted before the new features will become available.

Figure 4-20: ServiceWatch License page

2 Enter your license key into the text box.

3 Click the **Add new license** button to add a new license. Click the **Replace ALL existing license(s)** button to replace the existing license.

The license is stored in the `license.txt` file at the top level of the ServiceWatch installation directory.

Replacing Licenses

For example, you may have the evaluation version of the ServiceWatch software, and sometime after purchase a license for 500 requests that expires March 1. After it expires, you then buy a 500-pack. You would then use the **Replace ALL existing licenses** option. That removes the license that expired and places the 500-pack license there.

Adding Licenses

For example, you may have bought a 5-pack, allowing you to monitor 5 requests simultaneously. After that you realize you need to monitor 20 *additional* services, so you buy a 20-pack. You would then use the **Add new license** option.

Obtaining a ServiceWatch License

The downloadable version of ServiceWatch allows you to monitor five services without a license, however, it does not include technical support.

To purchase ServiceWatch software:

- Call (888) 257-3000, or +1 (408) 479-2800, or
- Email `sales@extremenetworks.com`, or
- Contact your Extreme Networks distributor

Have the following information available:

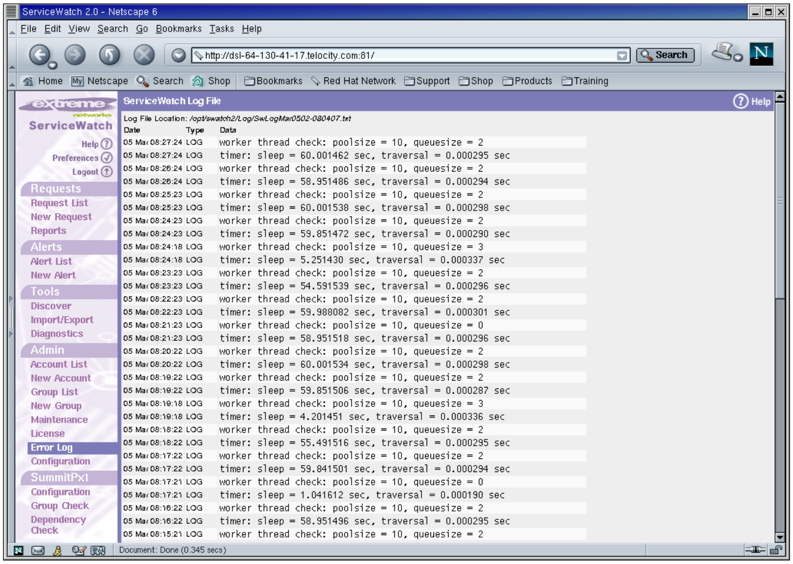
- Your name, company name, contact information, and email address where the license key should be sent.
- The number of ServiceWatch licenses you would like to purchase:

  ServiceWatch software pricing is based on the number of simultaneous network services you would like to monitor. For example, if you were monitoring two web servers, one DNS server, one mail server and one ftp server, that would be a total of five network services and a 5-pack would be needed. ServiceWatch software is sold in 5-packs, 10-packs, 50-packs, 100-packs, etc.
- Any other features you would like to purchase, such as support for the Summit Px1.

Error Log

A running error log is kept, as shown in Figure 4-21, which contains error messages and warning messages. If something appears to be not functioning as you expect with the ServiceWatch software, checking the error log sometimes can explain the problem that occurred. There are also additional log files under:

```
<servicewatch-install-directory>/Log
```



ServiceWatch Log File

Log File Location: */opt/swatch2/Log/SwLogMar0502-080407.txt*

```
Date            Type  Data
05 Mar 08:27:24 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:27:24 LOG   timer: sleep = 60.001462 sec, traversal = 0.000295 sec
05 Mar 08:26:24 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:26:24 LOG   timer: sleep = 58.951486 sec, traversal = 0.000294 sec
05 Mar 08:25:23 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:25:23 LOG   timer: sleep = 60.001538 sec, traversal = 0.000298 sec
05 Mar 08:24:23 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:24:23 LOG   timer: sleep = 59.851472 sec, traversal = 0.000290 sec
05 Mar 08:24:18 LOG   worker thread check: poolsize = 10, queuesize = 3
05 Mar 08:24:18 LOG   timer: sleep = 5.251430 sec, traversal = 0.000337 sec
05 Mar 08:23:23 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:23:23 LOG   timer: sleep = 54.591539 sec, traversal = 0.000296 sec
05 Mar 08:22:23 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:22:23 LOG   timer: sleep = 59.988082 sec, traversal = 0.000301 sec
05 Mar 08:21:23 LOG   worker thread check: poolsize = 10, queuesize = 0
05 Mar 08:21:23 LOG   timer: sleep = 58.951518 sec, traversal = 0.000296 sec
05 Mar 08:20:22 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:20:22 LOG   timer: sleep = 60.001534 sec, traversal = 0.000298 sec
05 Mar 08:19:22 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:19:22 LOG   timer: sleep = 59.851506 sec, traversal = 0.000287 sec
05 Mar 08:19:18 LOG   worker thread check: poolsize = 10, queuesize = 3
05 Mar 08:19:18 LOG   timer: sleep = 4.201451 sec, traversal = 0.000336 sec
05 Mar 08:18:22 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:18:22 LOG   timer: sleep = 55.491516 sec, traversal = 0.000295 sec
05 Mar 08:17:22 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:17:22 LOG   timer: sleep = 59.841501 sec, traversal = 0.000294 sec
05 Mar 08:17:21 LOG   worker thread check: poolsize = 10, queuesize = 0
05 Mar 08:17:21 LOG   timer: sleep = 1.041612 sec, traversal = 0.000190 sec
05 Mar 08:16:22 LOG   worker thread check: poolsize = 10, queuesize = 2
05 Mar 08:16:22 LOG   timer: sleep = 58.951496 sec, traversal = 0.000295 sec
05 Mar 08:15:21 LOG   worker thread check: poolsize = 10, queuesize = 2
```

Figure 4-21: ServiceWatch error log

The error log displays the most recent errors first (reverse chronological order).

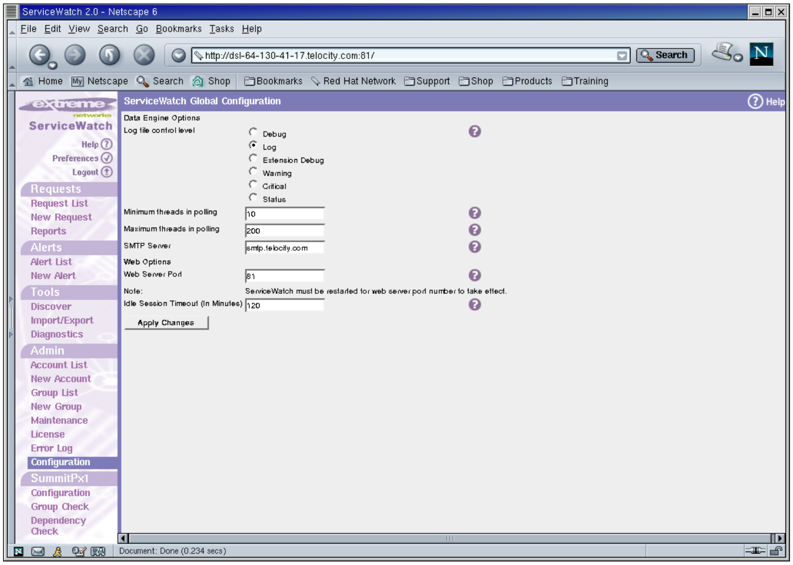
Configuration

The ServiceWatch Configuration feature allows you to change the global configuration for the ServiceWatch software. These configuration variables are stored in:

```
swatch2-install-directory/swatch.ini
```

To use the ServiceWatch Configuration feature, follow these steps:

1 Click the **Configuration** link under **Admin** tab on the ServiceWatch navigation pane. The ServiceWatch Configuration page appears, as shown in Figure 4-22.



ServiceWatch Global Configuration

Data Engine Options

Log file control level: ○ Debug ● Log ○ Extension Debug ○ Warning ○ Critical ○ Status

Minimum threads in polling: 10

Maximum threads in polling: 200

SMTP Server: smtp.telocity.com

Web Options

Web Server Port: 81

Note: ServiceWatch must be restarted for web server port number to take effect.

Idle Session Timeout (In Minutes): 120

Apply Changes

Figure 4-22: ServiceWatch Configuration page

2 Select from the following options and enter the appropriate parameters:

Log file control level

This option specifies how much information is logged to the error log. If you want to see only critical errors that can cause ServiceWatch software to operate improperly, select **Critical**. If you want more information, in addition to critical errors, then you could select **Warning**, for example.

Minimum threads in polling

This option specifies the minimum number of simultaneous threads that are started when polling begins.

Generally you should not change this value as it could adversely effect the ability of ServiceWatch software to perform monitoring requests.

Maximum threads in polling

This option specifies the maximum number of simultaneous threads that can ever be started. For slower machines with less memory than normal, you may want a lower maximum. You generally would not want to increase the maximum, since the default number of simultaneous threads is usually more than enough to process all polling requests in a timely manner.

Generally you should not change this value as it could adversely effect the ability of ServiceWatch software to perform monitoring requests.

SMTP Server

This option specifies the SMTP (Simple Mail Transfer Protocol) mail server where email is sent when sending email or epager alerts.

Web Server Port

This option specifies the web server port where the ServiceWatch software answers browser requests. This does not take effect until the ServiceWatch software is stopped and restarted.

Idle Session Timeout (in Minutes)

After the session is idle for this amount of time, you are logged out of ServiceWatch and need to log back in.

3 Click the **Apply Changes** button to save your changes in ServiceWatch configuration.

Setting User Preferences

The ServiceWatch User Preferences feature allows you to change user settings in the ServiceWatch software, such as the Admin password.

To use the ServiceWatch User Preferences feature, follow these steps:

1 Click the **ServiceWatch User Preferences** button, as shown in Figure 4-23, on the ServiceWatch navigation pane. The ServiceWatch User Preferences page appears, as shown in Figure 4-24.

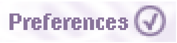
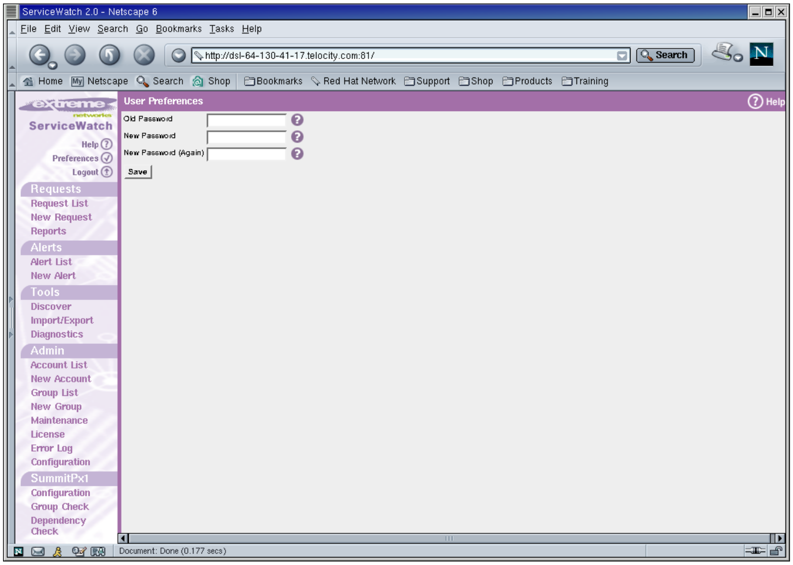


Figure 4-23: ServiceWatch User Preferences button



http://dsl-64-130-41-17.telocity.com:81/

User Preferences

Old Password

New Password

New Password (Again)

Save

Document: Done (0.177 secs)

Figure 4-24: ServiceWatch User Preferences page

2 To change the Admin password, enter your current password in the **Old Password** box.

3 Enter your new password in both the **New Password** and **New Password (Again)** boxes.

4 Click **Save**.

ServiceWatch Maintenance

Occasionally log and data files maintained by ServiceWatch software may grow large over time. You may need to truncate or delete some of these files to save disk space. The various files you need to manage are:

Web server log files (all platforms):

```
<install-directory>/Log/http-access.log
```

Error log files (all platforms):

```
<install-directory>/Log/SwLog<date+time>
```

5 Summit Px1 Support

ServiceWatch software includes optional features that support the Summit Px1 switch. These features are available only with a license that includes the Summit Px1 features.

If you purchased a license to use the Summit Px1 features, install it following the procedures in “License” on page 4-37.

The Summit Px1 must be running version 1.1.0 or later. To determine which version the Summit Px1 is running, login to the Summit Px1 and type `show version`*. The image line will show you the version number.*

Overview of the Summit Px1 Features

Before configuring ServiceWatch for Summit Px1 support, it is recommended that you first read the *Summit Px1 Application Switch Installation and Configuration Guide*.

The ServiceWatch Summit Px1 tab provides the following features:

- A Configuration page, which allows you to:
  - — Display configuration.
  - — Manage servers.
  - — Manage groups.
  - — Add L4 services.
  - — Add L7 services.

- A Group Check page, which allows you to create a monitoring request for every server in a Summit Px1 group.
- A Dependency Check page, which allows you to monitor one server that has an important service running on it that other servers depend on.

Configuration

ServiceWatch software allows you to configure one or more Summit Px1 switches from ServiceWatch using the Add/Remove link.

To display the Summit Px1 configuration page, click the **Configure** link under the **Summit Px1** tab on the ServiceWatch navigation pane. The Summit Px1 Configuration page appears, as shown in Figure 5-1.

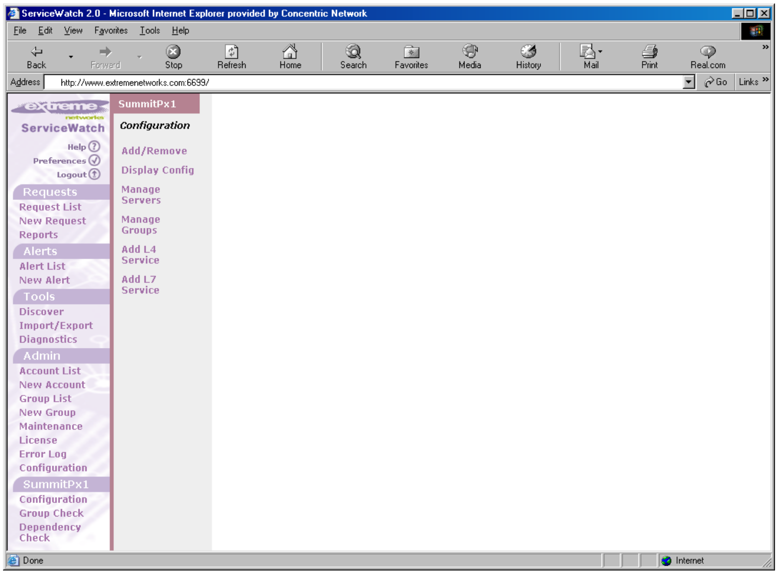
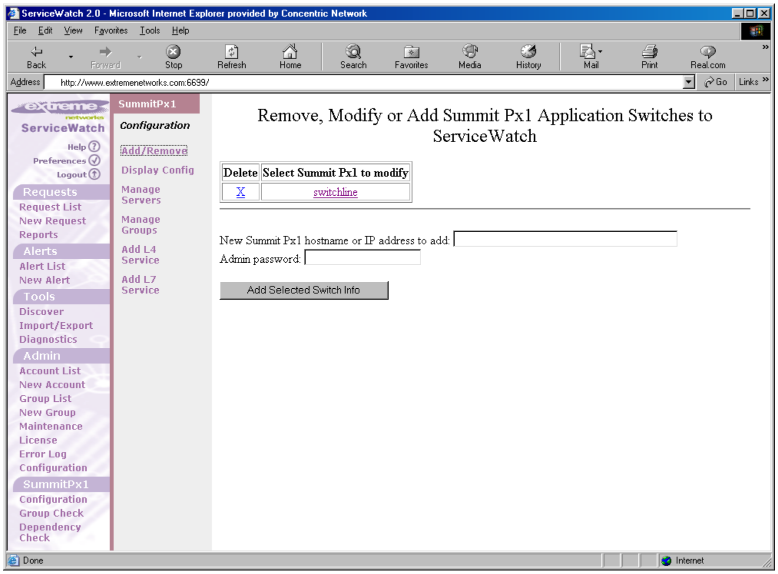


Figure 5-1: Summit Px1 Configuration page

Adding, Modifying, and Removing Summit Px1 Switches

You can add, modify, and remove Summit Px1 switches from the Remove, Modify or Add Summit Px1 Application Switches to ServiceWatch page.

Click the **Add/Remove** link. The Remove, Modify or Add Summit Px1 Application Switches to ServiceWatch page appears, as shown in Figure 5-2.



Remove, Modify or Add Summit Px1 Application Switches to ServiceWatch

Delete	Select Summit Px1 to modify
X	switchline

New Summit Px1 hostname or IP address to add:

Admin password:

Figure 5-2: Summit Px1 Add/Remove page

To add Summit Px1 switches to ServiceWatch, follow these steps:

1. Enter the hostname or IP address of the Summit Px1 you want to add.
2. Enter the Admin password. This is the password that you set for the Summit Px1.

Click the **Add Selected Switch Info** button.

To modify a Summit Px1, follow these steps:

1. Click the name of the Summit Px1 you want to modify.
2. Enter a new hostname or IP address.
3. Enter the Admin password. This is the password that you set for the Summit Px1.

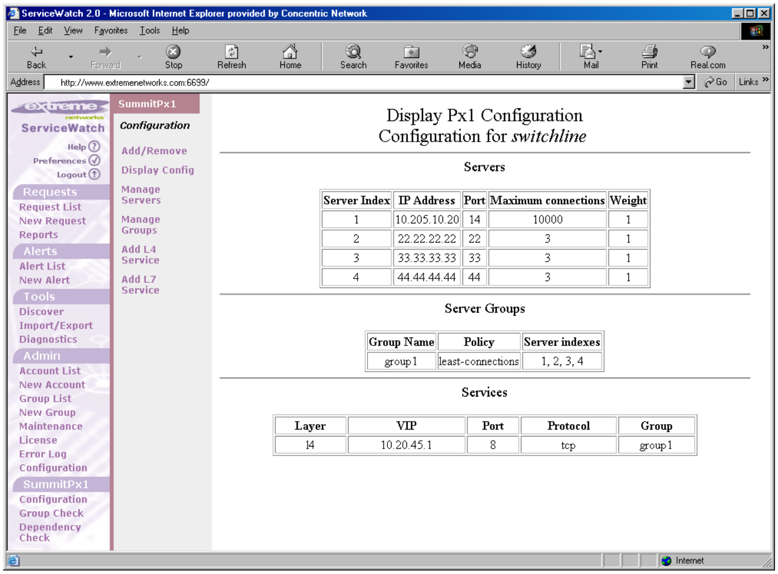
4 Click the **Modify Summit Px1 info** button.

To remove a Summit Px1, click the **X** in the Delete column next to the name of the Summit Px1 you want to remove.

Displaying Configuration

After you have added Summit Px1 switches to the ServiceWatch software, you can use the Display Config feature, which displays the current configuration of the Summit Px1, such as the servers, groups, layer 4 services, and layer 7 services that are defined on the Summit Px1.

To display your configuration, click the **Display Config** link. The Display Px1 Configuration Page appears, as shown in Figure 5-3.



Display Px1 Configuration
Configuration for *switchline*

Servers

Server Index	IP Address	Port	Maximum connections	Weight
1	10.205.10.20	14	10000	1
2	22.22.22.22	22	3	1
3	33.33.33.33	33	3	1
4	44.44.44.44	44	3	1

Server Groups

Group Name	Policy	Server indexes
group1	least-connections	1, 2, 3, 4

Services

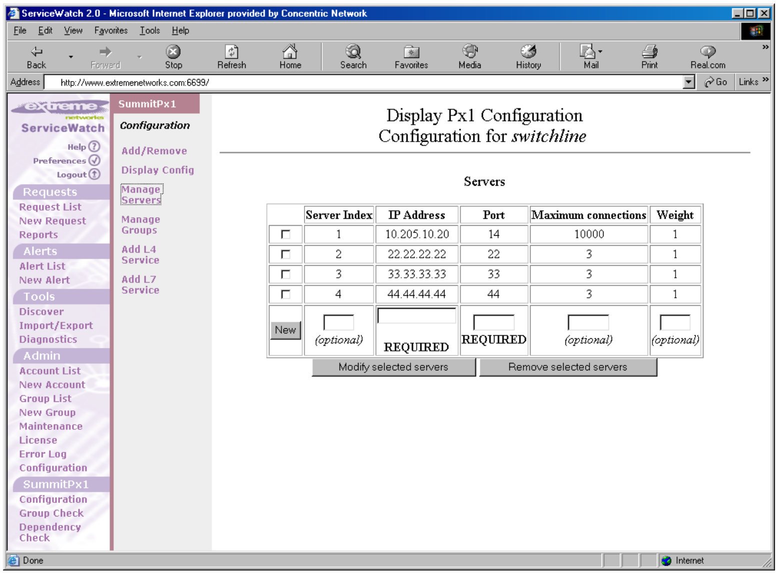
Layer	VIP	Port	Protocol	Group
l4	10.20.45.1	8	tcp	group1

Figure 5-3: Display Px1 Configuration page

Managing Servers

You can add, remove, and modify servers in a Summit Px1 through the Manage Servers page.

To manage your servers, click the **Manage Servers** link. The Display Px1 Configuration Page appears, as shown in Figure 5-4.



Address: http://www.extremenetworks.com:6699/

Display Px1 Configuration
Configuration for *switchline*

Servers

	Server Index	IP Address	Port	Maximum connections	Weight
□	1	10.205.10.20	14	10000	1
□	2	22.22.22.22	22	3	1
□	3	33.33.33.33	33	3	1
□	4	44.44.44.44	44	3	1
New	(optional)	REQUIRED	REQUIRED	(optional)	(optional)

Figure 5-4: Display Px1 Configuration page

To remove servers, check the check box next to the server in the Server Index list, then click the **Remove selected servers** button.

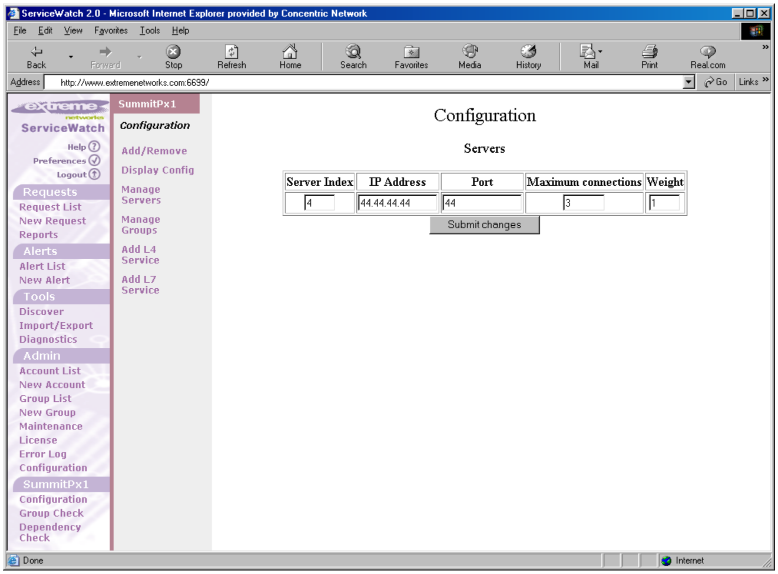
To add a server, enter the appropriate values into the required and optional fields, then click the **New** button. If you do not enter one of the optional fields (such as server index, maximum connections or weight), then ServiceWatch determines these values from:

- Server index: the first available index
- Maximum connections and weight: the defaults as configured in the Px1

To modify servers, follow these steps:

1 Check the check box next to the number of the server in the Server Index list,.

2 Click the **Modify selected servers** button. The Configuration page appears, as shown in Figure 5-5.



Configuration

Servers

Server Index	IP Address	Port	Maximum connections	Weight
4	44.44.44.44	44	3	1

Figure 5-5: Configuration page

3 Change any of the server information you want.

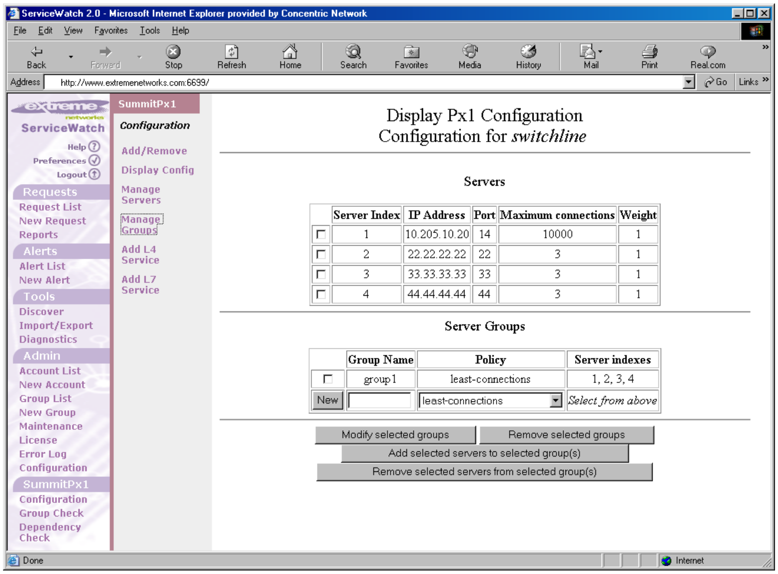
4 Click the **Submit changes** button.

Managing Groups

The Manage Groups page allows you to:

- Create new groups.
- Remove groups.
- Modify groups.
- Add servers to a group.
- Remove servers from a group.

To manage your groups, click the **Manage Groups** link. The Display Px1 Configuration Page appears, as shown in Figure 5-6.



Display Px1 Configuration
Configuration for *switchline*

Servers

	Server Index	IP Address	Port	Maximum connections	Weight
□	1	10.205.10.20	14	10000	1
□	2	22.22.22.22	22	3	1
□	3	33.33.33.33	33	3	1
□	4	44.44.44.44	44	3	1

Server Groups

	Group Name	Policy	Server indexes
□	group1	least-connections	1, 2, 3, 4
New		least-connections	*Select from above*

Modify selected groups
Remove selected groups
Add selected servers to selected group(s)
Remove selected servers from selected group(s)

Figure 5-6: Display Px1 Configuration page

To create new groups, follow these steps:

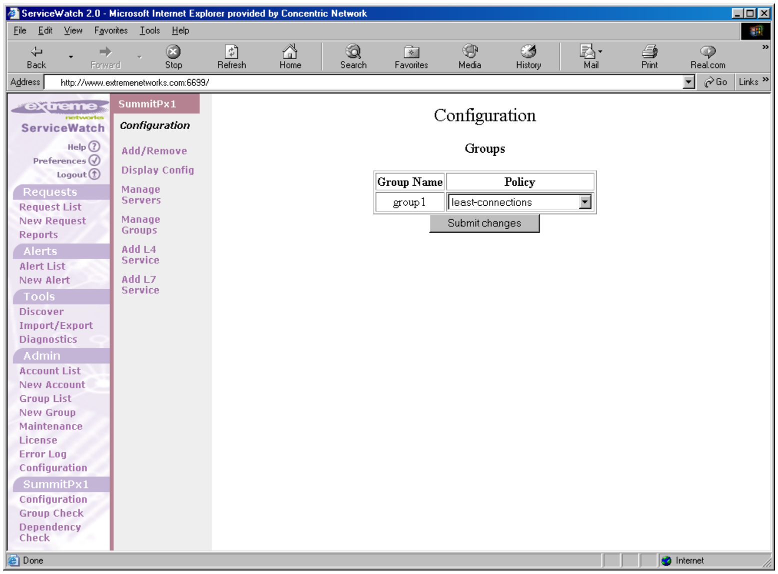
1. Enter a name for the new group in the Group Name box.
2. Select a policy to use for the new group from the Policy drop list.
3. Click the **New** button.

To remove groups, follow these steps:

1. Check the check box for the groups you want to remove.
2. Click the **Remove selected groups** button.

To modify groups, follow these steps:

1. Check the check box for the groups you want to modify.
2. Click the **Modify selected groups** button. The Configuration page appears, as shown in Figure 5-7.



Configuration

Groups

Group Name	Policy
group1	least-connections

Submit changes

Figure 5-7: Configuration page

3 Change the group to use the policy your prefer.

4 Click the **Submit changes** button.

To add servers to one or more groups, follow these steps:

1 Check the check box for the servers you want to add.

2 Check the check box for the groups you want to add them to.

3 Click the **Add selected servers to selected groups** button.

To remove servers from one or more groups, follow these steps:

1 Check the check box for the groups you want to remove.

2 Click the **Remove selected servers from selected groups** button.

Access Control Example

In the example shown in figure Figure 5-8, the arrows show the direction of access allowed. For example, Bob (Guest) can only read, but not change requests in the Customers access group. David, having Admin access, can read and write all requests in all access groups.

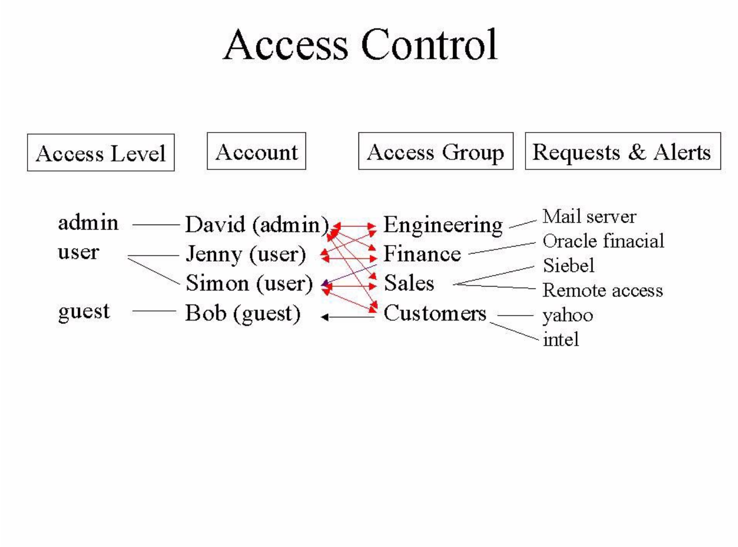
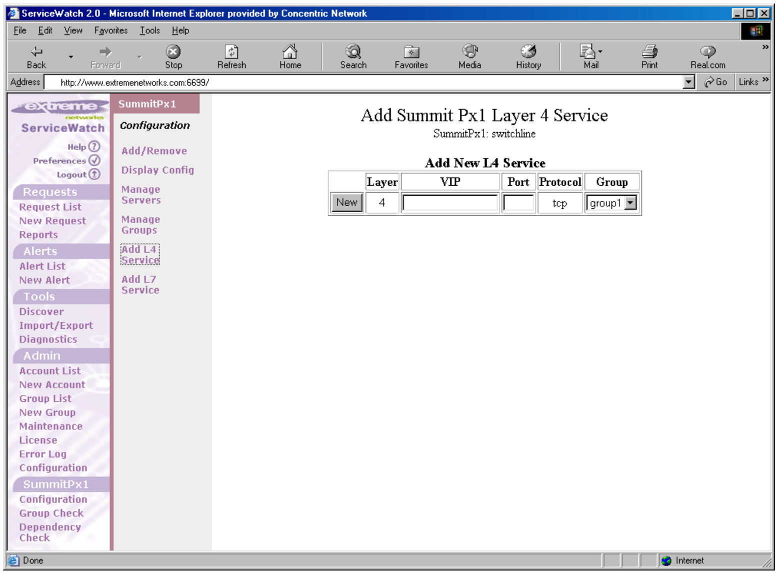


Figure 5-8: Access control example

Adding Layer 4 Services

To add a layer 4 service, follow these steps:

1 Click the **Add L4 Service** link. The Add Summit Px1 Layer 4 Service page appears, as shown in Figure 5-9.



Add Summit Px1 Layer 4 Service

SummitPx1: switchline

Add New L4 Service

	Layer	VIP	Port	Protocol	Group
New	4			tcp	group1

Figure 5-9: Add Summit Px1 Layer 4 Service page

2 Enter a Virtual IP address in the VIP box.

3 Enter a port number for the VIP in the Port box.

4 Select a group to which the Layer 4 service should use from the Group drop list.

5 Click the **New** button.

Adding Layer 7 Services

ServiceWatch allows you to configure Layer 7 services with Domain Name Switching. The Summit Px1 can use a single VIP to service one or more domains. This type of configuration is called *Domain Name Switching*.

Assume you would like the Summit Px1 to have the following HTTP service:

vip 10.65.31.202 at port 808 for class http

and the above VIP would service the domains and Px1 groups:

- www.buystuff.com - use “group1”
- www.speakyourmind.com - use “group2”
- all other domains: - use “mainpage” group

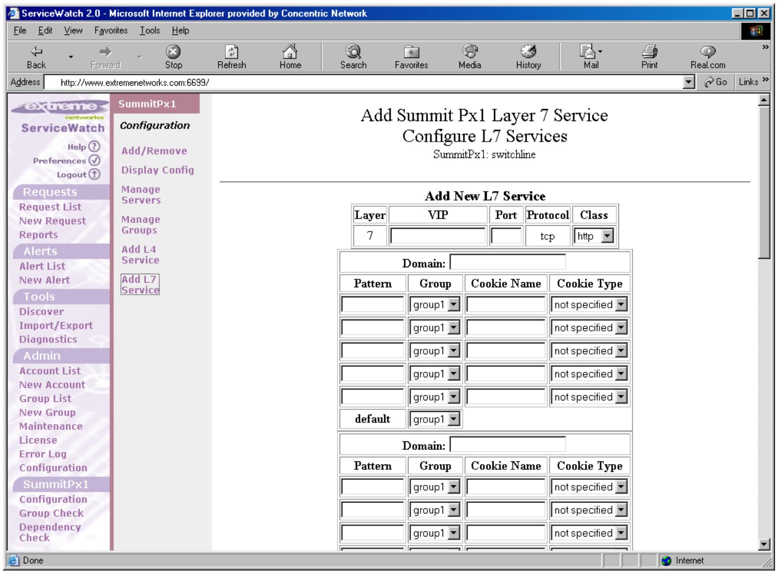
You could login to the Summit Px1 and type this:

```
config service vip 77.77.77.77 port 77 protocol tcp l7 class http
config domain name www.buystuff.com
config pattern-rule "default" server-group-name group1

config domain name www.speakyourmind.com
config pattern-rule "default" server-group-name group2

config domain name default
config pattern-rule "default" server-group-name mainpage
```

Alternatively, ServiceWatch allows you to do the above with much less typing and a few mouse clicks.

To configure a Px1 with Domain Name Switching, follow these steps:

1 Click **Add L7 Service**. The Add Summit Px1 Layer 7 Service page appears, as shown in Figure 5-10.



Add Summit Px1 Layer 7 Service
Configure L7 Services
SummitPx1: switchline

Add New L7 Service

Layer	VIP	Port	Protocol	Class
7			tcp	http

Domain:

Pattern	Group	Cookie Name	Cookie Type
	group1		not specified
	group1		not specified
	group1		not specified
	group1		not specified
	group1		not specified
default	group1		

Domain:

Pattern	Group	Cookie Name	Cookie Type
	group1		not specified
	group1		not specified
	group1		not specified

Figure 5-10: Add Summit Px1 Layer 7 Service page

2 In the first row, enter the VIP, port and the class (HTTP or HTTPS)

The next 5 tables begin with the heading Domain. After Domain in each of these sections, you enter the domains that the single VIP should be used to service.

3 Enter the following:

```
VIP: 10.65.31.202
Port: 808
Class: http
```

4 Then after the first Domain cell headings, enter:

```
www.buystuff.com
```

5 About 6 rows down, under Pattern, you see the default section. To the right of default, select the group for this domain to use. First, you would of course have to have created the groups “group1”, “group2” and “mainpage”.

6 Similarly, after the next Domain heading, enter:

```
www.speakyourmind.com
```

and after default about 5 rows down, select the group2 group.

7 Since you aren't configuring any more domains for this VIP, you can then skip/scroll all the way down to the last Domain table, labeled Domain: default. On the very last row, next to default, select the group you want: mainpage.

8 Click the **Add New L7 Service** button. The above config commands are all sent to the Summit Px1 to configure the service.

ServiceWatch also allows you to configure a layer 7 service with URL switching. The Summit Px1 allows you to take the concept of domain name switching one step further by looking deeper into the request. The SummitPx1 examines the entire requested URL. The URL is matched against a list of pattern rules. Each of the pattern rules has its own associated server group.

To configure a layer 7 service using patterns, you simply enter the patterns into the tables under the Pattern column. For example, you could have all requests with *.gif in the URL be sent to the images group, all *.mov URLs be sent to the media group, etc.

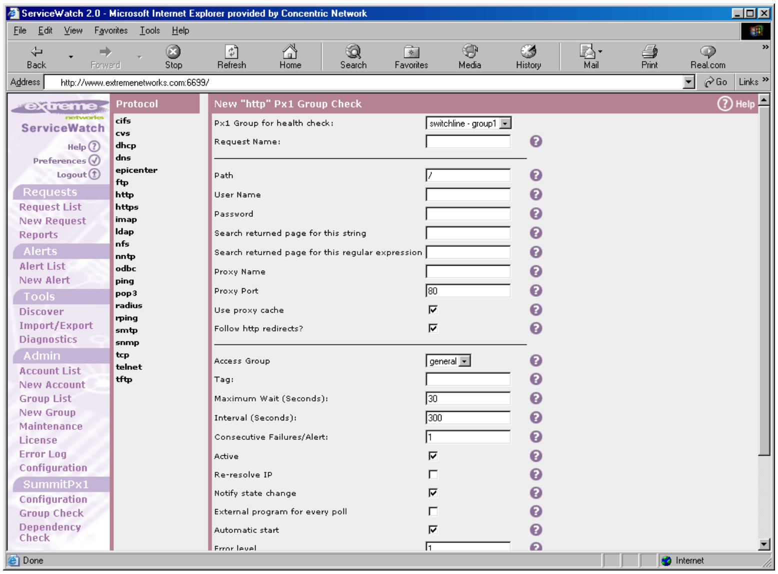
Group Check

The Group Check feature allows you to configure ServiceWatch to:

- Start a monitoring request for every server in a Summit Px1 group.
- If any of the servers in the Summit Px1 group is considered down, then automatically remove that server from the Summit Px1 group. Then if that server comes up again, add it back to the Summit px1 group.

To use the Group Check feature, follow these steps:

1 Click the **Group Check** link under the **Summit Px1** tab in the ServiceWatch navigation pane. The New Px1 Group Check page appears, as shown in Figure 5-11.



New "http" Px1 Group Check

Px1 Group for health check:	switchline - group1
Request Name:	
Path	/
User Name	
Password	
Search returned page for this string	
Search returned page for this regular expression	
Proxy Name	
Proxy Port	80
Use proxy cache	☑
Follow http redirects?	☑
Access Group	general
Tag:	
Maximum Wait (Seconds):	30
Interval (Seconds):	300
Consecutive Failures/Alert:	1
Active	☑
Re-resolve IP	□
Notify state change	☑
External program for every poll	□
Automatic start	☑
Error level	1

Figure 5-11: New Px1 Group Check page

2 Select the type of service that the servers in a group are running. You see a new field at the very top of the main web frame: Px1 Group for health check:

The menu to the right of the field lists all groups on all switches. The menu field is in the format: “px1name - groupname”. For example if you have a switch named “switchline” and there are five groups on that switch, the menu items are:

— switchline - group1

- switchline - group2
- switchline - group3
- switchline - group4
- switchline - group5

3 Select a group from this list.

4 Fill in any fields as in a normal request, such as the maximum wait, interval, etc. When you click the button to start the request, you see that one request is started for every server that is in that Summit Px1 group.

Additionally, if you look at the Request Details for any of these new requests, they are automatically configured to use the px1_group_check alert. This alert is programmed to automatically remove a server from a Summit Px1 if the service is down and to add a server back to a Summit Px1 if a server comes back up.

Note that the port field will not be listed. This is because the port used for each request is taken from each server in the server group.

Dependency Check

The Dependency Check feature allows you to configure the ServiceWatch software to:

- Start monitoring one server that has an important service running on it that other servers depend on. If the monitored server is down, the ServiceWatch software automatically removes servers from a Summit Px1 group if these servers are dependent on that server that is down.
- Conversely, if the monitored server comes back up, the dependent servers are added back to the correct Summit Px1 groups.

Example

As an example of how this would be used, assume:

- Your company has a web service that allows a user to use their browser to login and view their portfolio, etc.
- The user logs in to the web site, and displays their portfolio information.

And assume the following overall type of architecture is used to support the above:

- A Summit Px1 is used as a “front-end” to the web servers.
- Two database servers have duplicate user portfolio data in case one of the database servers goes down.
- Some of the web servers use “database1” as the back-end and some of the web servers use the duplicate “database2” on a different server.

Assume 10 web servers are used to support the application, with the first five using database1, and the last five using database2:

1 192.168.12.1 - uses database1

2 .192.168.12.2 - uses database1

3 192.168.12.3 - uses database1

4 192.168.12.4 - uses database1

5 192.168.12.5 - uses database1

6 192.168.12.6 - uses database2

7 192.168.12.7 - uses database2

8 192.168.12.8 - uses database2

9 192.168.12.9 - uses database2

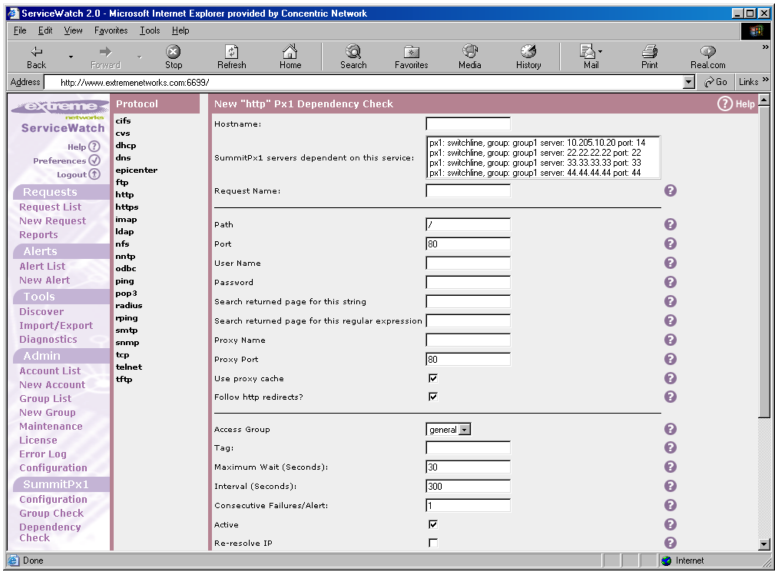
10 192.168.12.10 - uses database2

You can configure ServiceWatch software, using Dependency Check to:

- Monitor database1.
- If database1 is down, automatically take the five servers that depend on it out of the Summit Px1 web server group.
- If database1 comes back up, automatically place the five servers that depend on it back into the Summit Px1 web server group.

To configure ServiceWatch software to do these tasks, follow these steps:

1 Click the **Dependency Check** link under the **Summit Px1** tab on the ServiceWatch navigation pane. The New Px1 Dependency Check page appears, as shown in Figure 5-12.



http://www.extremenetworks.com:6699/

New "http" Px1 Dependency Check

Hostname:	
SummitPx1 servers dependent on this service:	px1: switchline, group: group1 server: 10.205.10.20 port: 14 px1: switchline, group: group1 server: 22.22.22.22 port: 22 px1: switchline, group: group1 server: 33.33.33.33 port: 33 px1: switchline, group: group1 server: 44.44.44.44 port: 44
Request Name:	
Path	/
Port	80
User Name	
Password	
Search returned page for this string	
Search returned page for this regular expression	
Proxy Name	
Proxy Port	80
Use proxy cache	☑
Follow http redirects?	☑
Access Group	general
Tag:	
Maximum Wait (Seconds):	30
Interval (Seconds):	300
Consecutive Failures/Alert:	1
Active	☑
Re-resolve IP	□

Figure 5-12: New Px1 Dependency Check page

2 Click the protocol that you want to use to monitor database1 (such as ODBC).

3 A list of all servers in all Summit Px1 servers and server groups appears.

4 Select the servers that depend on database1.

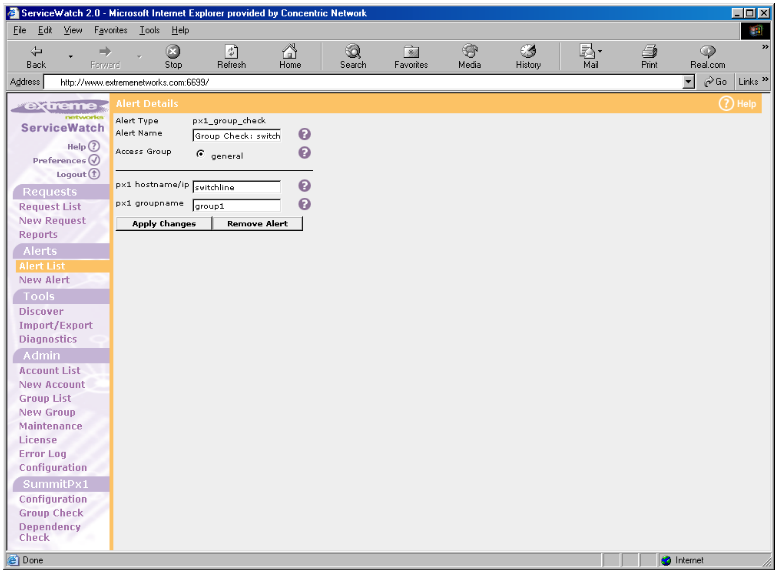
5 Enter the appropriate fields for the form, such as Max Wait, Interval, etc.

6 Start the request.

Summit Px1 Alerts

After you have done a Group Check or Dependency Check, you may notice you have two new alerts that appear in the Alert List or Request Details pages. They are:

- The px1_group_check alert, as shown in Figure 5-13
- The px1_depend_check alert, as shown in Figure 5-14



http://www.extremenetworks.com:6699/

Alert Details

Alert Type px1_group_check

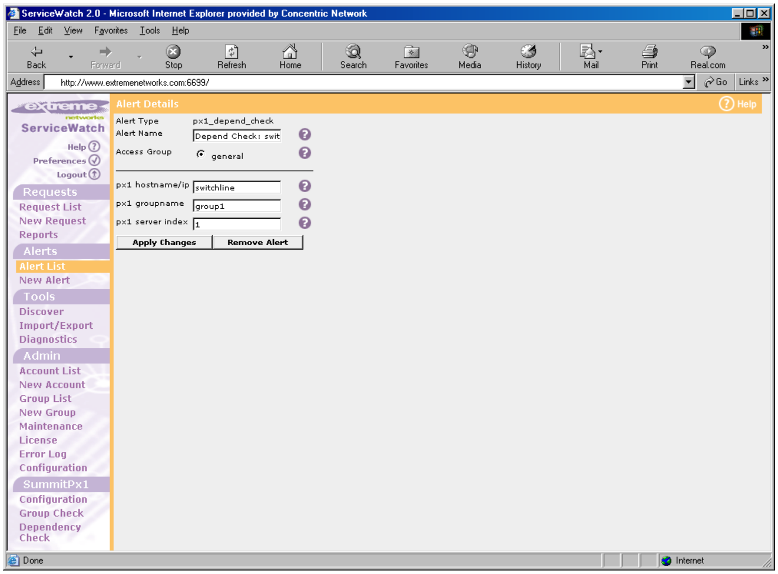
Alert Name Group Check: switch

Access Group ● general

px1 hostname/ip switchline

px1 groupname group1

Figure 5-13: Summit px1_group_check alert



Alert Details

Alert Type	px1_depend_check
Alert Name	Depend Check: swit
Access Group	● general
px1 hostname/ip	switchline
px1 groupname	group1
px1 server index	1

Figure 5-14: Summit px1_depend_check alert

Generally, you should not modify these alerts, as they are automatically created by the Group Check and Dependency Check features. Modifying these alerts could likely result in the wrong servers being added or removed from a Px1 group.

6 Extending ServiceWatch via the API

The ServiceWatch software provides an application programming interface (API) that allows the development of custom monitoring scripts or programs to monitor additional network services, hardware, databases, and so forth.

ServiceWatch software can call an external poller program if the program is set up according to its specification. An example of an external program can be found in:

```
Examples/ExternalPoller/heat
```

under the top level ServiceWatch directory.

To get a quick idea of how things work, follow these steps:

1. Copy the whole heat directory into the API directory.
2. Restart the ServiceWatch server.
3. Click **New Request**. The new heat service appears in the protocol list.
4. Click **heat** to create a new request, and enter the required parameters.
5. Click **Create Request**.
6. Click **Request List**. The new heat service appears in the Request List.
7. Click the heat request to display the request details.

The request details should show some random results that originated from the new poller. The ServiceWatch software communicates with the poller program by writing data to a flat file.

Creating and Integrating a New Poller

To create a new poller and integrate it into the ServiceWatch software, follow these steps:

1. Create a new directory under the api directory for your new external poller.
2. Create an `__init__.py` file inside this new directory.
3. Customize `__init__.py` to reflect the poller-specific parameters, the port used by the service, how to call the poller program/script, and which additional arguments to call the poller/program script with.
4. Write a program or script that monitors the new service and returns the status from the poll.

The __init__.py File

The `__init__.py` file contains the glue that connects your external program to the ServiceWatch software.

In particular, the `__init__.py` specifies:

- Any poller-specific parameters used
- The port used by the service
- How to call the poller program/script
- Which additional arguments ServiceWatch software calls the poller/program script with

This program can be written in Python, which is a high-level scripting language. You can start with the sample `__init__.py` script and easily customize it for your poller without even knowing Python.

Start by copying the `__init__.py` file from the `Examples/ExtendPoller/heat` directory to a new directory that will contain your new poller. Create the following directory in the top-level ServiceWatch directory:

```
api/heat
```

This directory on an NT system might be:

```
C:/Program Files/Extreme Networks/ServiceWatch20/api/heat
```

On a Linux system it might be:

```
/opt/swatch2/api/heat
```

Note that in Python, you need to indent lines correctly. Each line within a basic code block must be indented using the same number of spaces or tabs.

Before running your external poller program, the current directory is set to the ServiceWatch 2.0 top-level directory.

Four function calls are required in the `__init__.py` file:

- **GetComponentInfo()**
- **GetPortInfo()**
- **GetCommandLine()**
- **GetCommandLineArgument()**

These four functions are described below.

GetComponentInfo()

This function describes to the ServiceWatch software what poller-specific parameters are required by this poller. The example poller, heat, requires three poller-specific parameters:

1. Username—a string
2. Password—a string
3. Coffee—a check box the user can check if they want a cup of coffee

ServiceWatch software calls your **GetComponentInfo** function to determine what "poller specific" parameters are required from the user when the user is creating a new request using this poller. You provide one ComponentParameterInfo structure for each parameter.

For example, the first parameter for the heat example has the following properties:

- Parameter name: username
- Parameter type: string
- Parameter precision: up to 123 bytes

- Parameter description: User Name
- Parameter help text: for password-protected nuclear power plant heat monitor
- Parameter choices: none (For the heat example, this parameter is a string, not a menu of choices, it is empty: [])
- Parameter default value: no default value

This is how the above parameter information would be encoded in the `__init__.py` file:

```
param1 = ComponentParameterInfo(
  'username',                      # param name, can't have space
  ComponentDataType.string,        # data type
  123,                             # precision
  'User name',                     # description, facing users
  'for password-protected nuclear power plant heat monitor', # help text
  [],                              # choice list
  ''                               # default
  )
```

In the above case, the parameter was a string. The list of choices is:

- **ComponentDataType.string**
- **ComponentDataType.password**
- **ComponentDataType.integer**
- **ComponentDataType.float**
- **ComponentDataType.bool**

The format of the help tag is three fields separated by a “.”:

```
directory.file.anchor
```

For example, the “Tag for file with help text” for the poller name heat, the username parameter has the following help tag:

```
'pollers.heat.username'
```

The “directory.file.anchor” fields are:

- directory: The main directory under the Help directory where the help text (under the ServiceWatch “Help” directory) is located for this module. For example, “heat” is a new poller type so it would be described in the “Help/pollers” directory.

- file: the filename where this parameter is documented, excluding the ".html" extension. For the "heat" example, the filename where this is documented would be "Help/pollers/heat.html".
- anchor: the name of the HTML anchor where this parameter is documented. For the "heat" example, parameter #1 is "username", and its anchor is also "username".

Below is an example of how to define the three parameters (username, password, coffee check box) required for the heat poller:

```
def GetComponentInfo():
  param1 = ComponentParameterInfo(
    'username',                     # param name, can't have space
    ComponentDataType.string,       # data type
    123,                            # precision
    'User name',                    # description, facing users
    'pollers.heat.username', # Tag for file with help text
    [],                             # choice list
    ''                              # default
    )
  param2 = ComponentParameterInfo(
    ‘password',                     # param name, can't have space
    ComponentDataType.string,       # data type
    123,                            # precision
    'Password',                    # description, facing users
    'pollers.heat.password', # Tag for file with help text
    [],                             # choice list
    ''                              # default, nothing here
    )
  param3 = ComponentParameterInfo(
    'coffee',                       # param name, can't have space
    ComponentDataType.bool,         # data type
    1,                              # precision
    'Coffee',                       # description, facing users
    'pollers.heat.coffee', # Tag for file with help text
    [1,0],                          # choice list
    ''                              # default, nothing here

  # The 3 parameters are defined above.
  # Below is where the parameters are returned to ServiceWatch

  return ComponentInfo(
    'heat',                         # program name
    'heat',                         # program description, facing users
```

```
      'a sample demo program',        # Help text
      1,                              # reserved
      param1, param2, param3]        # ComponentParameterInfo objects
      )
```

ServiceWatch software automatically makes sure data entered on the "new request" form, etc. is of the correct type (an integer can not have the letter 'z' or other noninteger characters in it, etc.)

GetPortInfo() Function

You can optionally include the type of port (tcp or udp) and the port number the service is running on in the **GetPortInfo()** function. If you include this information in this function, and it is tcp, then the service will be included in the Discovery page. If you do not include any information in the **GetPortInfo()** function, then the service will not show up in the Discovery page.

```
def GetPortInfo():
  '''This function returns a dictionary of {protocal:port}'''
  return {'tcp': 8000}
```

This example returns nothing:

```
def GetPortInfo():
  return
```

GetCommandLine() Function

This is the function that the ServiceWatch software calls to find out how to call your external program. The function returns:

- The name of a program needed to run the external poller (if any)
- The name of the external poller script or program.

For example, if your poller is written in perl and called heat.pl, and you want your program called by:

```
        perl.exe c:/Program Files/UserDir/heat.pl
```

The GetCommandLine() function would look like this on NT or Windows 2000:

```
def GetCommandLine():return ['perl', 'c:/Program Files/UserDir/heat.pl']
```

For Linux and Solaris, you need to specify the full path to perl, so the GetCommandLine() function would look like this:

```
def GetCommandLine(): return
['/usr/bin/perl','/opt/swatch2/api/heat/heat.pl']
```

On all platforms, Perl must be installed on the system for this heat poller example to work.

Linux and Solaris note:

- If calling a scripting language, such as perl, you need to specify an absolute pathname of perl. for example, do not specify just 'perl', but '/usr/bin/perl':

NT and Windows 2000 notes:

- The path to perl must be set in the system
- If you just installed perl, you must restart the machine in order for the system to recognize the path to perl.

If you put your program under the api/heat in the ServiceWatch directory, and want ServiceWatch software to call it using that directory, the function should look like this:

def GetCommandLine(): ''' Use '^' for ServiceWatch to add the script path to your command line, or you can hard code it yourself. ''' return ['perl', '^heat.pl']

ServiceWatch will replace the '^' (caret) with the full path to your external program heat.pl, which could be the following under Windows 2000:

```
c:/Program Files/Extreme Networks/ServiceWatch20/api/heat/heat.pl
```

If the poller program can be executed without calling an interpreter such as perl or Python, the return will have only one argument:

```
def GetCommandLine():
  return ['c:/Program Files/UserDir/heat.exe']
```

The GetCommandLine() function does not include any arguments that the ServiceWatch software should call it with.

ServiceWatch software will call the program or script with the following arguments:

1 The first argument is always the name of the “communication” file name that contains all the information about the request.

2 Any additional arguments, as specified by the **GetCommandLineArgument()** function, described next.

In the Windows environment, the program or script can not be a batch file.

GetCommandLineArgument() Function

ServiceWatch software always calls the program or script with the first argument being the “communication filename”. The **GetCommandLineArgument()** function defines which arguments in addition to the communication filename it should call the program or script with.

For example, assume your poller program is a perl script that is run this way:

```
perl.exe heat.pl <FileName> debug -z
```

The <FileName> argument shown above would be replaced by the filename that contains all of the details of the request in XML format.

You would then define your **GetCommandLineArgument()** function as having two additional arguments: `debug -z` as shown below:

```
def GetCommandLineArgument():
  return [ 'debug', '-z' ]
```

In addition to these static arguments, you can have ServiceWatch software call the program or script with dynamic arguments that could differ for each request. For example, if you want it to call the program or script with the request name and maximum wait that the user entered, you would define **GetCommandLineArgument()** as follows:

```
def GetCommandLineArgument():
  return [ 'debug', '-z', 'request_name', 'maxwait' ]
```

The ServiceWatch software would then call the program/script like this:

```
perl.exe heat.pl <FileName> debug -z <request_name> <maxwait>
```

where the <FileName> is the dynamically generated filename for communication, <request_name> is the RequestName that was entered by the user when creating this request, and <maxwait> is the maximum waiting period for the poller when creating this request.

ServiceWatch keywords are shown in Table 6-1.

Table 6-1: ServiceWatch Keywords

Keyword	Meaning
hostname	Name of the host
request_name	Name of the request
maxwait	Maximum wait period value
gatehost	Gateway request value
keyword defined in the GetComponentInfo() function	The value as entered by the user for the request

In addition, the last row in the above table mentions the fact that poller-specific parameters can be added to the command-line, too. For example, the heat example has parameters named username and password. The next example shows uses these too:

```
def GetCommandLineArgument():
  return ['request_name', 'hostname', 'maxwait' 'interval', 'username',
  'password']
```

Returning Polling Results Back to ServiceWatch

The polling program sends the polling results back to the ServiceWatch software in the filename passed in argument 1. The format is in XML, as shown in the following example:

```
<sw>
<bytes_read>1234</bytes_read>
<data>some monitored data: <news>embedding something</news></data>
<error>1</error>
<ip_address>123.123.123.0</ip_address>
<port>80</port>
<response_reason>OK</response_reason>
<response_time>6</response_time>
<response_type>401</response_type>
```

```
<service_status>1</service_status>
</sw>
```

The ServiceWatch results keywords are shown in Table 6-2.

Table 6-2: ServiceWatch results keywords

Keyword	Data type
bytes_read	integer
data	string
port	integer
response_reason	string
response_time	integer
response_type	integer
service_status	integer 1 = up, 2 = down

error	integer:
	None = 1
	ConnectionTimeOut = 2
	SendingTimeOut = 3
	RecevingTimeOut = 4
	GeneralTimeOut = 5
	ConnectToServerFailed = 6
	SendingToServerFailed = 7
	ReceivingFromServerFailed = 8
	HostNameInURLNotFoundViaNameService = 9
	SocketError = 10
	BadProtocolType = 11
	UnknownFailure = 12
	CouldNotExecuteExtensibleProgram = 13
	ExtensionProgramSendNoResult = 14
	InvalidServerResponse = 17
	ProtocolSpecificError = 18
	GateHostDown = 19
	SqlQueryFailed = 20

Creating a large number of simultaneous ServiceWatch requests that call an external program in the ServiceWatch software is not recommended.
Some operating systems (such as NT) limit the maximum number of files allowed under one directory. Disk access could be slow if there are a large number of files being opened and closed on a system.

Index