User’s Manual

Version 3.0

Stop Attacks in Seconds.™

CounterStorm-1
User’s Manual
Release 3.0

CS1UM1106 • Revision 4

CounterStorm, Inc.
15 West 26th Street - 7th Floor
New York, NY 10010
USA
Telephone: (212) 206-1900
Fax: (212) 242-2975
Customer Support: (212) 206-1900
E-mail:info@CounterStorm.com

OWNERSHIP

Customer acknowledges that CounterStorm and its licensors own all right, title, and interest, including all patent, copyright, trade secret, trademark, moral rights, mask work rights, and other intellectual property rights (“***Intellectual Property Rights***”) in and to the User Equipment (including all components thereof), all software of CounterStorm provided or made accessible hereunder, any databases created by CounterStorm using data processed under this Agreement (including any data models, structures, or data contained therein), and that such items reflect CounterStorm’s selection, arrangement, coordination, and expression of such information and may contain confidential information, trade secrets, and/or patented technology. Customer shall not engage in any act or omission that would impair CounterStorm’s and/or its licensors’ Intellectual Property Rights in the any CounterStorm software, or User Equipment. CounterStorm reserves all rights in such items except the limited rights granted to Customer hereunder.

WARRANTIES

Representations and Warranties. Each Party represents and warrants to the other that the execution and performance of this Agreement and each Order Form does not and shall not violate any other contract, obligation, or instrument to which it is a party, or which is binding upon it, including terms relating to covenants not to compete and confidentiality obligations.

No Other Warranties. EXCEPT AS OTHERWISE EXPRESSLY WARRANTED IN THIS AGREEMENT, THE USER EQUIPMENT AND ANY OTHER MATERIALS, SOFTWARE, DATA AND/OR SERVICES PROVIDED BY COUNTERSTORM ARE PROVIDED “AS IS” AND “WITH ALL FAULTS,” AND COUNTERSTORM EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND OR NATURE, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF OPERABILITY, CONDITION, TITLE, NON-INFRINGEMENT, NON-INTERFERENCE, QUIET ENJOYMENT, VALUE, ACCURACY OF DATA, OR QUALITY, AS WELL AS ANY WARRANTIES OF MERCHANTABILITY, SYSTEM INTEGRATION, WORKMANSHIP, SUITABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THE ABSENCE OF ANY DEFECTS THEREIN, WHETHER LATENT OR PATENT.

LIMITATION OF LIABILITY

Limitations. Neither party shall have any liability or obligation to the other except as provided in this Agreement. IN NO EVENT SHALL COUNTERSTORM BE LIABLE TO CUSTOMER FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, EXEMPLARY OR INDIRECT DAMAGES, OR FOR ANY LOST PROFITS, EVEN IF ADVISED OF THE POSSIBILITY OF THE SAME, HOWEVER CAUSED AND REGARDLESS OF THEORY OF LIABILITY, WHETHER TORT, CONTRACT, OR STRICT LIABILITY. IN NO EVENT SHALL COUNTERSTORM BE LIABLE FOR DAMAGES RELATING TO PERSONAL INJURY CAUSED BY INSTALLATION OF THE USER EQUIPMENT. CounterStorm’s liability for any other damages asserted by Customer shall be limited to Customer’s actual damages and shall in no event exceed the amounts paid to CounterStorm by Customer under this Agreement as of the date of a claim by Customer. To the extent that any service, equipment, or facilities provided hereunder are provided by third parties pursuant to an arrangement with counterstorm, the disclaimers and limitations of CounterStorm’s liability, as stated in Sections 7 AND 8, shall extend fully to such third parties. The disclaimers and exclusions contained herein are independent of any exclusive remedy and shall apply notwithstanding the failure of such exclusive remedy. Some states do not allow the disclaimer or limitation of damages relating to personal injury, so the above disclaimer of, and limitation of liability.

ADDITIONAL LICENSES

This Product includes software developed by Apache Software Foundation. With respect to such software, the following terms apply: The Apache Software License, Version 2.0.

Copyright 2005 The Apache Software Foundation. All rights reserved.

Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994, The Regents of the University of California. All rights reserved.

This product includes libpcap and tcpdump software that is copyrighted by the Regents of the University of California. Copyright © 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement: “This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.'' Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED “AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

All brand or product names are trademarks or registered trademarks of their respective companies or organizations.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991
Copyright © 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-**1307** USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION.

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

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

   Whether that is true depends on what the Program does.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

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

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

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

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

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

END OF TERMS AND CONDITIONS

Contents

Chapter 1: About this Manual

Now that your Sensors and Command Center are physically installed, you need to perform some initial configuration (see “Initial Configuration” on page 3-1) in order to use this product to stop known, zero-day, and targeted attacks from spreading in real-time. This document describes the tasks required to configure and use the CounterStorm-1™ Command Center Interface.

In This Chapter

- Related Publications
- Intended Audience
- Conventions
- Getting Help

Related Publications

The CounterStorm-1 documentation set consists of:

- This User’s Manual
- Installation Manual

Intended Audience

This manual is intended for use by system and network administrators experienced with general networking hardware/ software architecture and basic TCP/IP.

Conventions

The following conventions are used in this manual.

Convention	Description
Bold	Actions you should take such as text or data to be typed exactly or items to click.
Italics	Arguments in which you must supply a value.
Bold Italics	Field or button names.

Getting Help

Helpful information is displayed on-screen in the Command Center Interface. A complete help system is available in the CounterStorm-1 interface by clicking the Help item in the upper-right corner of the interface.

If you need further assistance, please contact CounterStorm via e-mail at support@counterstorm.com. CounterStorm's URL is http://www.counterstorm.com. FAQs and support documents are available on the website. Phone support is available at 212-206-1900.

You also can send correspondence to:

CounterStorm, Inc.
15 West 26th Street - 7th Floor
New York, NY 10010

Chapter 2: Understanding the User Interface

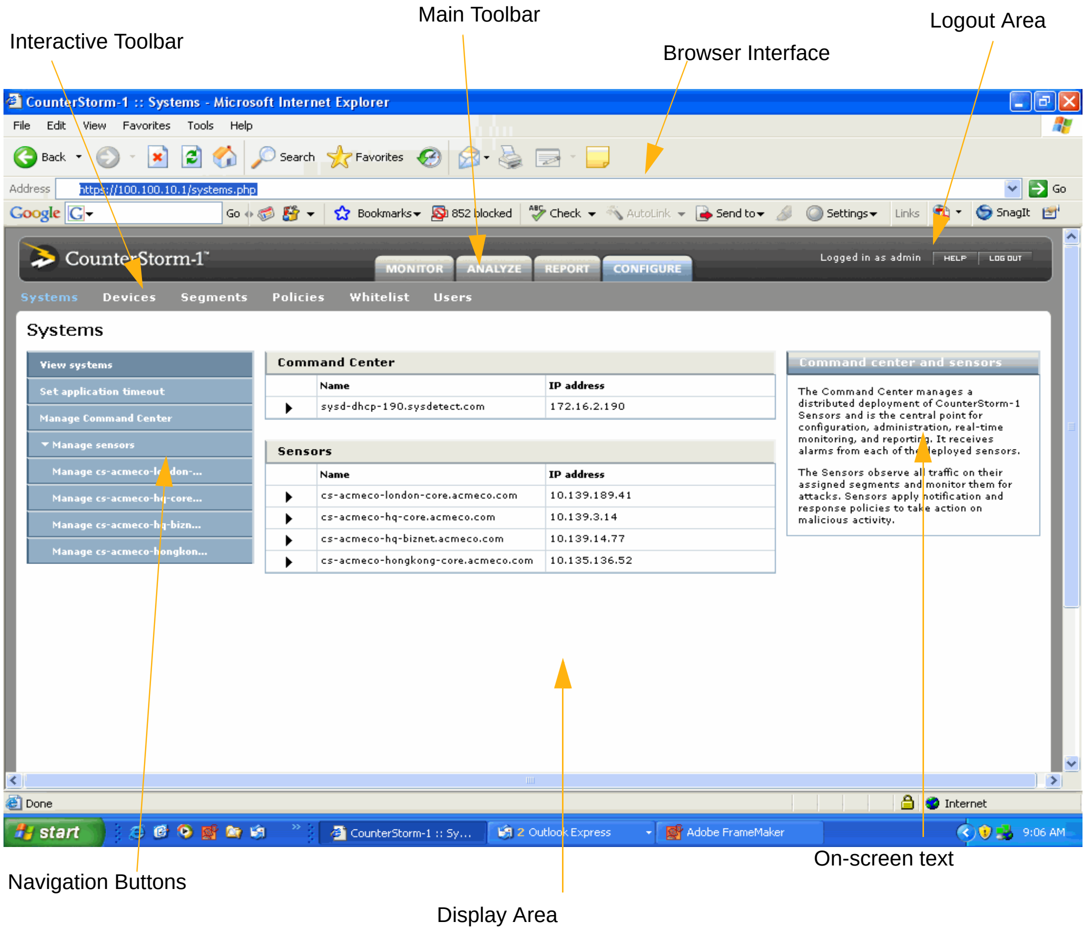
This section describes the CounterStorm-1 Command center Interface. This web-based interface allows you to monitor attacks, take appropriate action, and generate reports.

In This Chapter

- Basic layout
- Accessing the Interface
- CSV Files

Basic Layout

The following descriptions provide an explanation of the aspects of the interface. The segments screen below displays all elements of the interface. In some cases, such as the Monitor and Analyze screens, some interface elements have been removed to maximize the amount of information displayed.


Interactive Toolbar
Main Toolbar
Browser Interface
Logout Area
CounterStorm-1 :: Systems - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://100.100.10.1/systems.php Go
Google Go Bookmarks 852 blocked Check AutoLink Send to Settings Links SnagIt
CounterStorm-1™
MONITOR ANALYZE REPORT CONFIGURE
Logged in as admin HELP LOG OUT
Systems Devices Segments Policies Whitelist Users
Systems
View systems
Set application timeout
Manage Command Center
Manage sensors
Manage cs-acmeco-london-...
Manage cs-acmeco-hq-core...
Manage cs-acmeco-hq-bizn...
Manage cs-acmeco-hongkon...
Done Internet
start CounterStorm-1 :: Sy... 2 Outlook Express Adobe FrameMaker 9:06 AM
Navigation Buttons
Display Area
On-screen text

Command Center

	Name	IP address
▶	sysd-dhcp-190.sysdetect.com	172.16.2.190

Sensors

	Name	IP address
▶	cs-acmeco-london-core.acmeco.com	10.139.189.41
▶	cs-acmeco-hq-core.acmeco.com	10.139.3.14
▶	cs-acmeco-hq-biznet.acmeco.com	10.139.14.77
▶	cs-acmeco-hongkong-core.acmeco.com	10.135.136.52

Command center and sensors

The Command Center manages a distributed deployment of CounterStorm-1 Sensors and is the central point for configuration, administration, real-time monitoring, and reporting. It receives alarms from each of the deployed sensors.

The Sensors observe all traffic on their assigned segments and monitor them for attacks. Sensors apply notification and response policies to take action on malicious activity.

Help

An online help system is available by clicking the **Help** item in the Logout Area. This invokes an HTML-based help system. On-screen text is available on the right side of the Display Area for many topics.

Main Toolbar

The main toolbar contains high-level CounterStorm-1 items. Clicking a topic in the Main toolbar populates the interactive toolbar with items related to that topic and/or populates the Display Area. Clicking an item in the interactive toolbar populates the Display Area with the desired data.

Interactive Toolbar

The interactive toolbar contains items related to the topic selected in the Main toolbar. Clicking an item in the interactive toolbar populates the Display Area with the desired data.

Navigation Buttons

The left navigation buttons provide navigation within modules. These buttons change depending on what you have selected in the toolbars.

Logout Area

You may log out of the interface at anytime by clicking the **logout** item in the Logout Area. The Help link invokes the online help system. The user that is currently logged in is displayed.

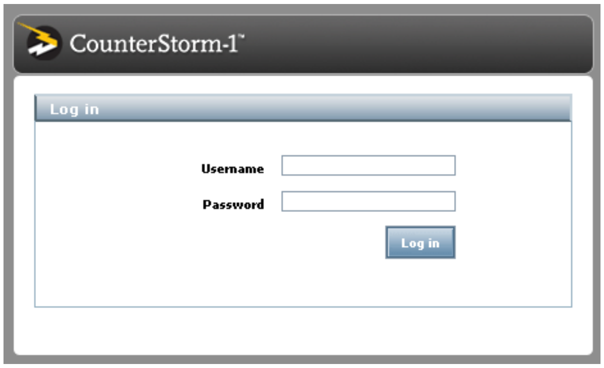
Accessing the Interface

The Interface may be accessed via any standard browser that has access to the Command Center via HTTPS and a valid login.

To access the Interface:

1. Go to a computer that has web access to your Command Center. Invoke a browser and use https to access the system via IP address. For example: https://10.10.10.1.

   The CounterStorm Login screen appears.



2. Log in to the web-based GUI.

   admin is the default login name and the password is whatever you set it to be during Command Center console configuration.

CSV Files

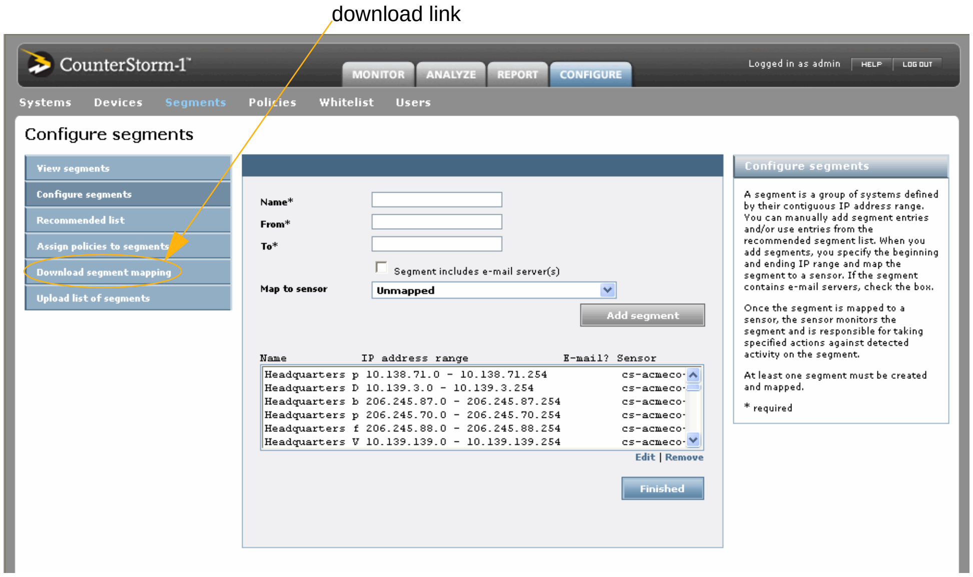
CounterStorm-1 allows you to upload and download comma separated values (CSV) files for table listings such as segment and whitelist entries.

You can download CSV files that already exist in CounterStorm-1 for use in other programs (such as Excel) or create your own CSV files for uploading.

To download CSV files:

1. Click any links with the word **Download**.

   These links appear throughout the interface. The segments selection is shown.



Configure segments

Name*

From*

To*

☐ Segment includes e-mail server(s)

Map to sensor: Unmapped

```
Name          IP address range                 E-mail? Sensor
Headquarters p 10.138.71.0 - 10.138.71.254            cs-acmeco-
Headquarters D 10.139.3.0 - 10.139.3.254              cs-acmeco-
Headquarters b 206.245.87.0 - 206.245.87.254          cs-acmeco-
Headquarters p 206.245.70.0 - 206.245.70.254          cs-acmeco-
Headquarters f 206.245.88.0 - 206.245.88.254          cs-acmeco-
Headquarters V 10.139.139.0 - 10.139.139.254          cs-acmeco-
```

Configure segments

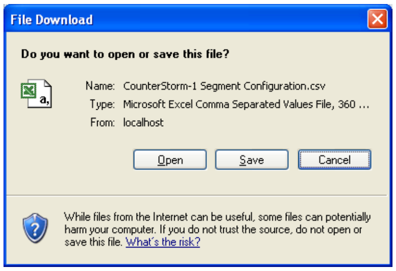
A segment is a group of systems defined by their contiguous IP address range. You can manually add segment entries and/or use entries from the recommended segment list. When you add segments, you specify the beginning and ending IP range and map the segment to a sensor. If the segment contains e-mail servers, check the box.

Once the segment is mapped to a sensor, the sensor monitors the segment and is responsible for taking specified actions against detected activity on the segment.

At least one segment must be created and mapped.

* required

   A save window appears.



Do you want to open or save this file?

Name: CounterStorm-1 Segment Configuration.csv

Type: Microsoft Excel Comma Separated Values File, 360 ...

From: localhost

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

2. Save the file to your desired location.
3. Open the file in any spreadsheet application such as Microsoft Excel.

   It is recommended that you use the existing CSV files in CounterStorm-1 as a template so that all formatting is correct.You must create at least one segment in order to create a default segment CSV file and one whitelist item in order to create a default whitelist CSV file. This is typically done during initial configuration. It is not recommended that you modify the Internet or Private segments.

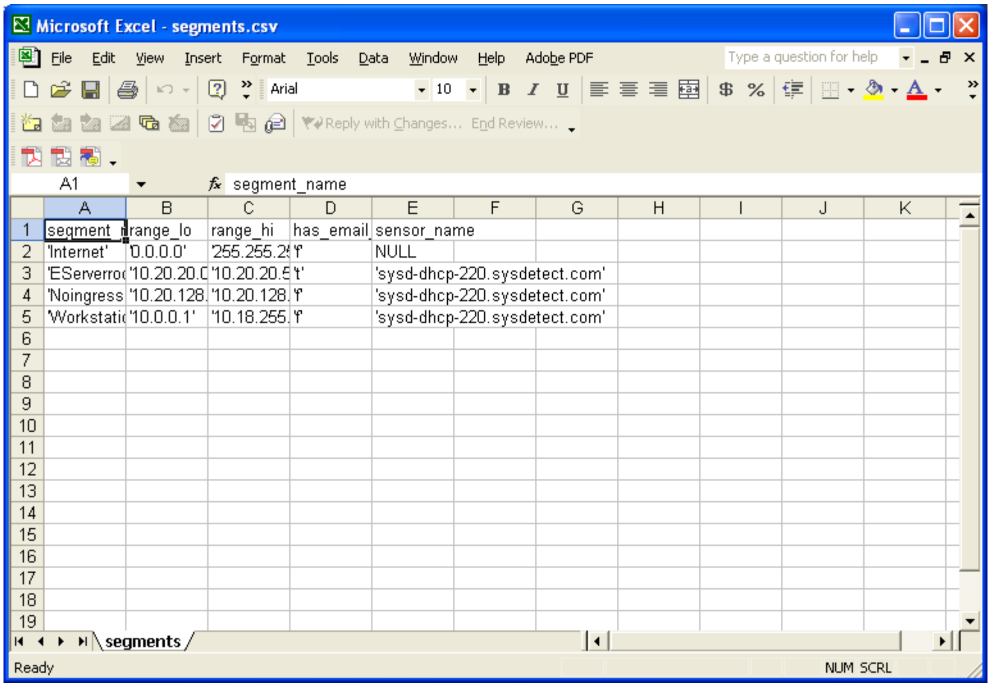
To create CSV files for use in CounterStorm-1:

1. Click the desired links with the word **Download** for the type of CSV file you wish to create.

   For example, if you wish to create a whitelist file, go to the Whitelist page and click the download link. See “Downloading the Whitelist to a CSV file” on page 12-8 for more information. A save window appears.

2. Save the file to your desired location.
3. Open the file in any spreadsheet application such as Microsoft Excel.

   A sample segments.csv file is shown opened in Microsoft Excel.


Microsoft Excel - segments.csv
File Edit View Insert Format Tools Data Window Help Adobe PDF
Type a question for help
Arial
10
Reply with Changes... End Review...
A1
segment_name
Ready
NUM SCRL

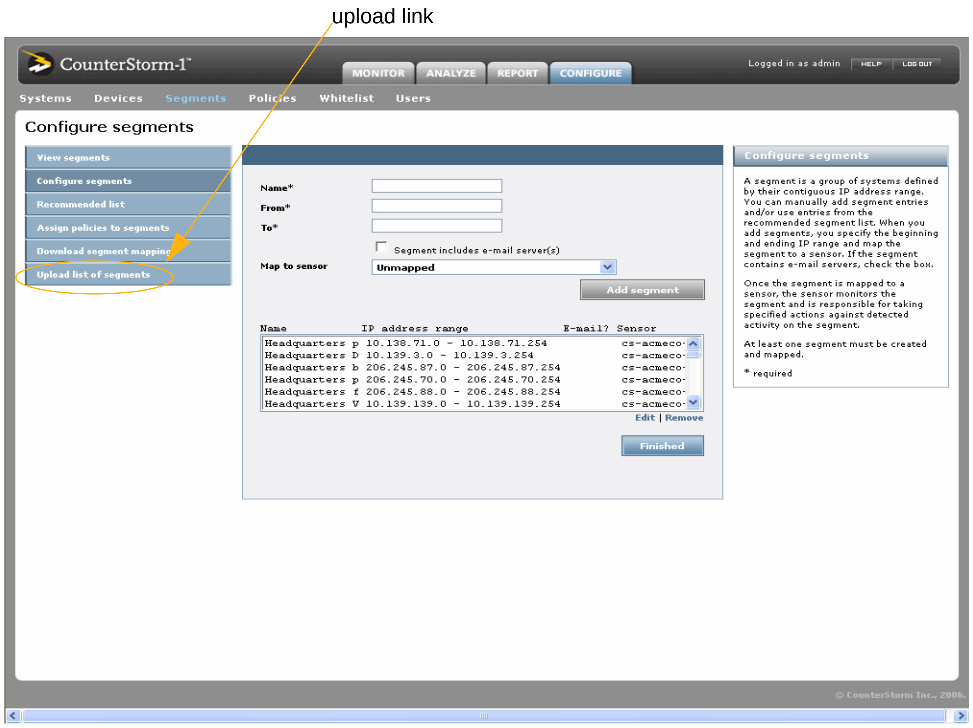
	A	B	C	D	E
1	segment_n	range_lo	range_hi	has_email	sensor_name
2	'Internet'	'0.0.0.0'	'255.255.2!	'f'	NULL
3	'EServerroo	'10.20.20.0	'10.20.20.5	't'	'sysd-dhcp-220.sysdetect.com'
4	'Noingress	'10.20.128.	'10.20.128.	'f'	'sysd-dhcp-220.sysdetect.com'
5	'Workstati	'10.0.0.1'	'10.18.255.	'f'	'sysd-dhcp-220.sysdetect.com'

4. Add entries as desired.

Note: You may add entries in this file. You cannot delete current data. Deletion must be performed through the interface. It may be easier to add new entries rather than modifying existing ones.

5. Save the file.
6. Use the Upload File options in CounterStorm-1 to upload the desired files.

The Segments upload link is shown.



upload link

Name*

From*

To*

□ Segment includes e-mail server(s)

Map to sensor: Unmapped

```
Name             IP address range                E-mail?  Sensor
Headquarters p 10.138.71.0 - 10.138.71.254               cs-acmeco-
Headquarters D 10.139.3.0 - 10.139.3.254                 cs-acmeco-
Headquarters b 206.245.87.0 - 206.245.87.254             cs-acmeco-
Headquarters p 206.245.70.0 - 206.245.70.254             cs-acmeco-
Headquarters f 206.245.88.0 - 206.245.88.254             cs-acmeco-
Headquarters V 10.139.139.0 - 10.139.139.254             cs-acmeco-
```

Configure segments

A segment is a group of systems defined by their contiguous IP address range. You can manually add segment entries and/or use entries from the recommended segment list. When you add segments, you specify the beginning and ending IP range and map the segment to a sensor. If the segment contains e-mail servers, check the box.

Once the segment is mapped to a sensor, the sensor monitors the segment and is responsible for taking specified actions against detected activity on the segment.

At least one segment must be created and mapped.

* required

© CounterStorm Inc., 2006.

This option is available for segments, switches, and whitelists.

Chapter 3: Initial Configuration

In This Chapter

- Accessing Initial Configuration
- Initial-Configuration Wizard

This section explains how to configure the Command Center for the first time via the initial configuration wizard. The Command Center and sensors must be physically installed and the console configured prior to invoking the initial-configuration wizard. See the *CounterStorm-1 Installation Manual* for detailed installation instructions. You will need the information you recorded during the Command Center installation to complete the initial-configuration wizard. These steps require a computer with web access to your Command Center appliance.

Before entering the initial configuration information, gather the following system configuration information about your network:

- Defined segments, or IP ranges, that CounterStorm-1 will monitor
- E-mail addresses, syslog server IP, and SNMP server IP for notifications
- Switch name, model, login username/password, enable username/password, and IP
- VPN Gateway information
- Items to whitelist

You will also need the data you recorded during console configuration.

After you complete the initial-configuration wizard, you may perform additional configuration or modification of configuration as described throughout this manual.

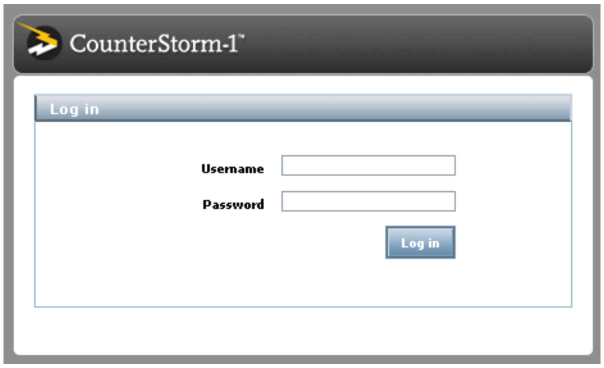
Accessing Initial Configuration

Once the Command Center and sensors are physically installed and commissioned, you can perform initial configuration on the Command Center.

To access the initial-configuration wizard:

1. Go to a computer that has web access to your Command Center. Invoke a browser and use https to access the system via IP address. For example: https://10.10.10.1.

The CounterStorm Login screen appears.



2. Log in to the web-based GUI.

   admin is the default login name and the password is whatever you set it to be during Command Center console configuration.

3. Follow the wizard to enter configuration as described in “Initial-Configuration Wizard” on page 3-2.

Initial-Configuration Wizard

Initial configuration is performed via a wizard. This wizard guides you through the initial configuration process. During this process, you create segments and map them to sensors, create notification policies, configure switch information, assign segments to policies, and create the whitelist.

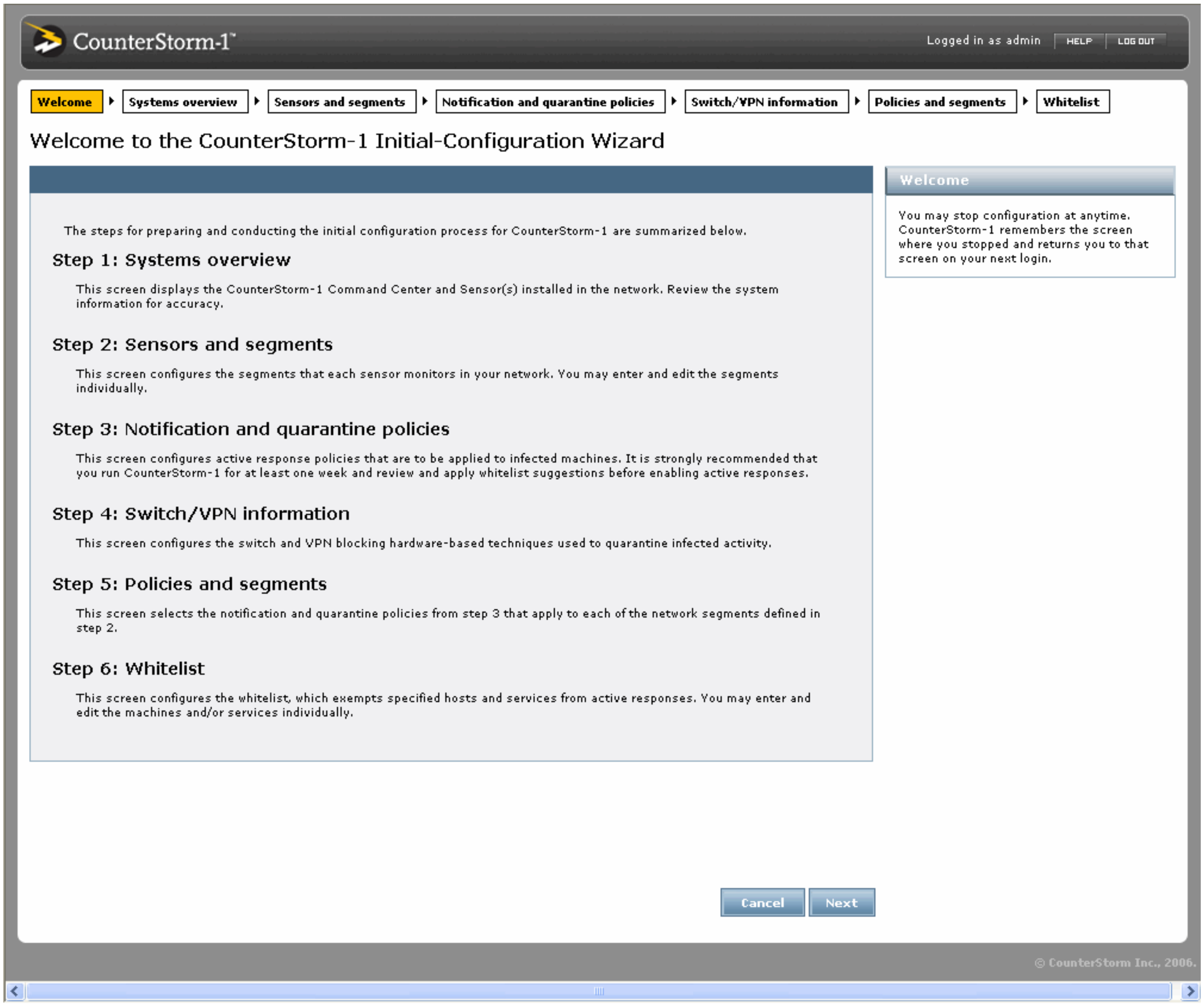
You can stop the configuration at any time. CounterStorm-1 remembers the screen you were on and returns you to it at the time of your next login.

The wizard combines the configuration screens that are available in the interface and presents them to you in a specific order. Each screen is described in detail within subsequent chapters of this manual, while its function is summarized here. Please see the referenced sections for detailed screen information.

To perform the initial configuration:

1. Access the GUI as described in “Accessing Initial Configuration” on page 3-1.

   The Initial-Configuration Wizard welcome screen appears.



Welcome to the CounterStorm-1 Initial-Configuration Wizard

The steps for preparing and conducting the initial configuration process for CounterStorm-1 are summarized below.

Step 1: Systems overview

This screen displays the CounterStorm-1 Command Center and Sensor(s) installed in the network. Review the system information for accuracy.

Step 2: Sensors and segments

This screen configures the segments that each sensor monitors in your network. You may enter and edit the segments individually.

Step 3: Notification and quarantine policies

This screen configures active response policies that are to be applied to infected machines. It is strongly recommended that you run CounterStorm-1 for at least one week and review and apply whitelist suggestions before enabling active responses.

Step 4: Switch/VPN information

This screen configures the switch and VPN blocking hardware-based techniques used to quarantine infected activity.

Step 5: Policies and segments

This screen selects the notification and quarantine policies from step 3 that apply to each of the network segments defined in step 2.

Step 6: Whitelist

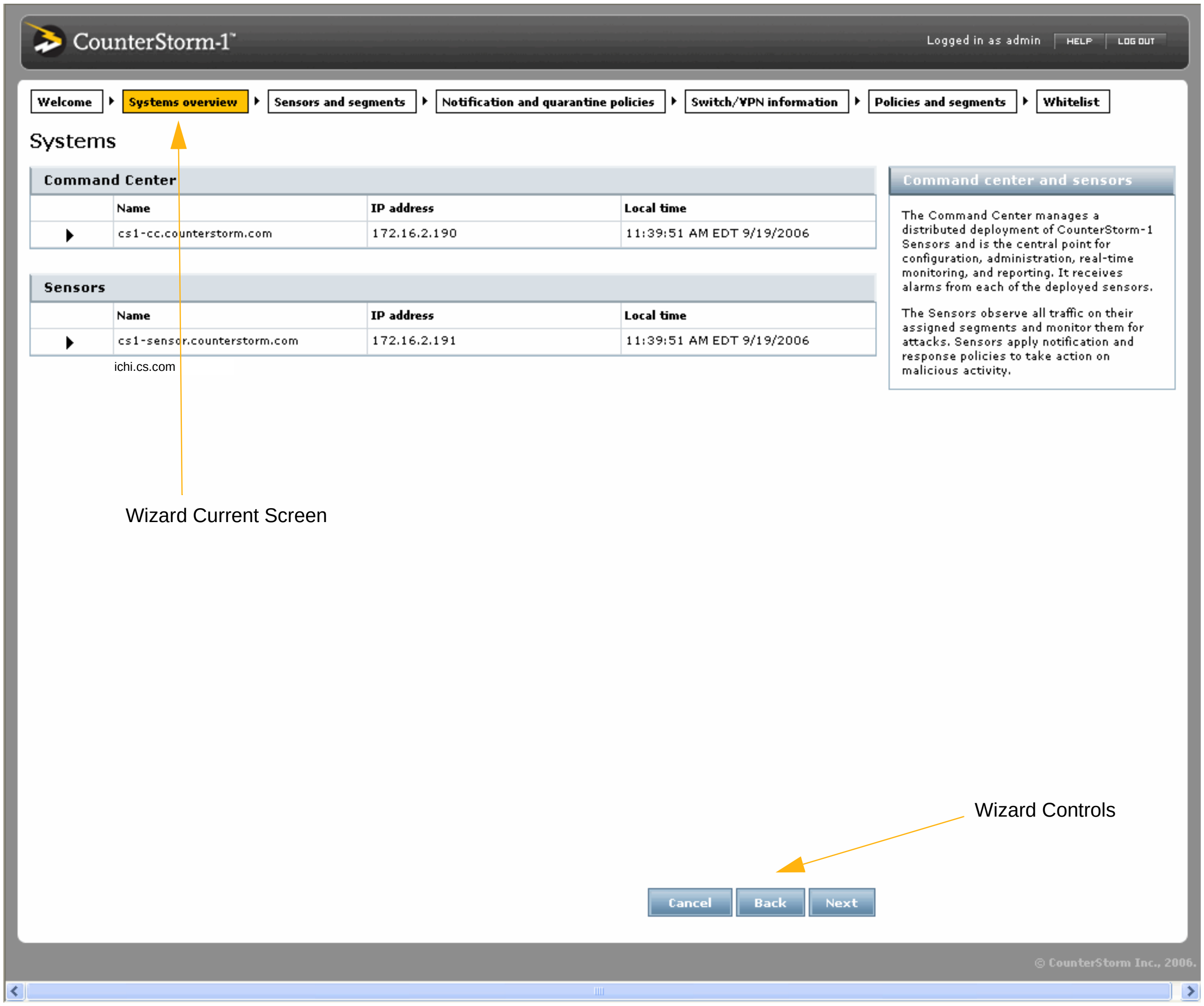
This screen configures the whitelist, which exempts specified hosts and services from active responses. You may enter and edit the machines and/or services individually.

Welcome

You may stop configuration at anytime. CounterStorm-1 remembers the screen where you stopped and returns you to that screen on your next login.

2. Click **Next** to proceed through the configuration steps.

The Systems overview screen appears.



Systems

Command Center

	Name	IP address	Local time
▸	cs1-cc.counterstorm.com	172.16.2.190	11:39:51 AM EDT 9/19/2006

Sensors

	Name	IP address	Local time
▸	cs1-sensor.counterstorm.com	172.16.2.191	11:39:51 AM EDT 9/19/2006

ichi.cs.com

Command center and sensors

The Command Center manages a distributed deployment of CounterStorm-1 Sensors and is the central point for configuration, administration, real-time monitoring, and reporting. It receives alarms from each of the deployed sensors.

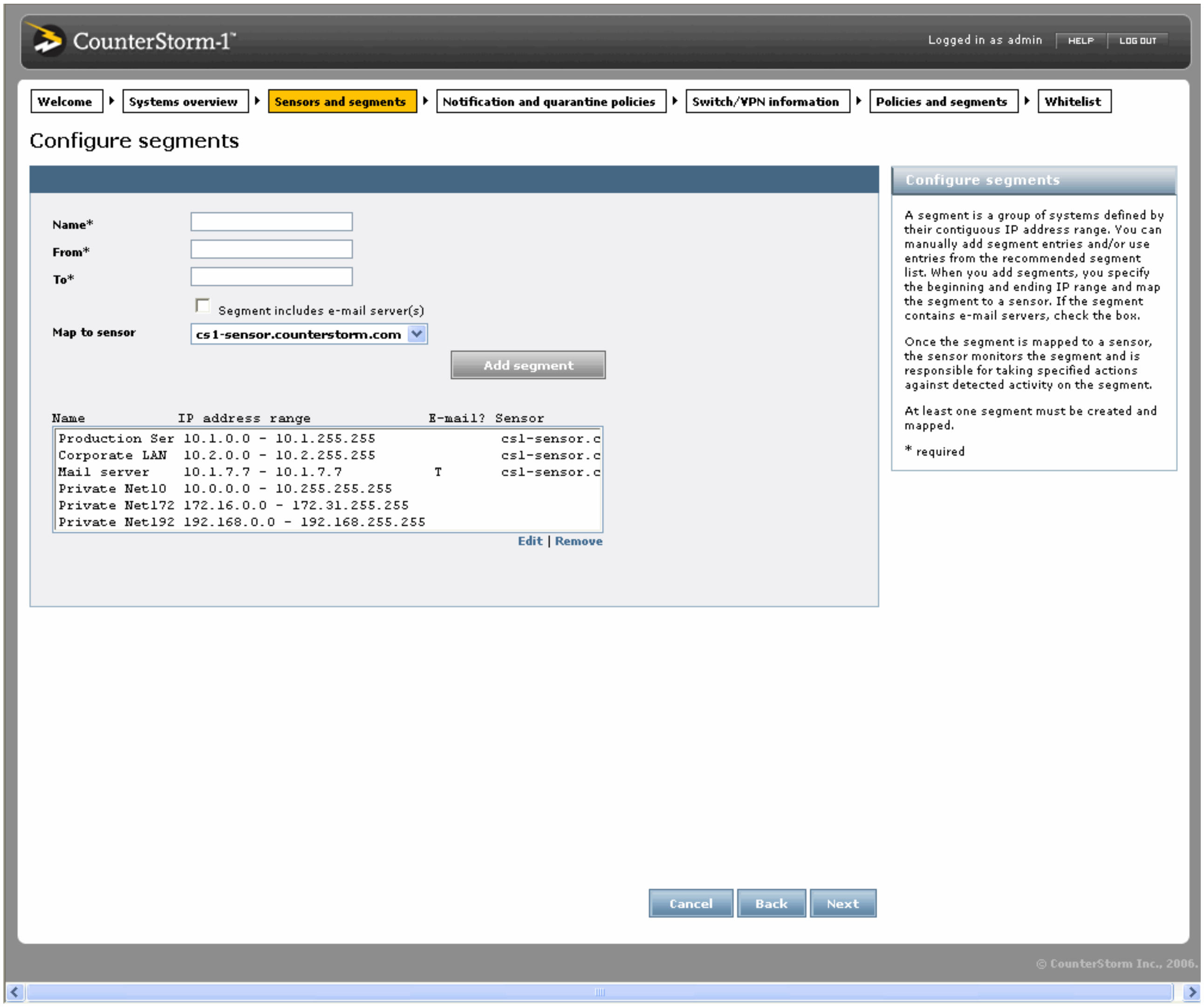
The Sensors observe all traffic on their assigned segments and monitor them for attacks. Sensors apply notification and response policies to take action on malicious activity.

© CounterStorm Inc., 2006.

3. Review the installed devices and click **Next**.

System overview displays the Command Center and sensor(s) that have been installed and registered. Sensors were registered with the Command Center during Console Configuration as each was installed. Click ▸ to display current configuration of the Command Center and Sensor(s). Make sure that all expected sensors appear and are registered. If a sensor is not registered, it will not appear. You must return to the sensor and register it. No configuration actions are required on this screen. See “Changing System Settings” on page 14-3 for screen details.

The Configure Segments screen appears.



Configure segments

Name*

From*

To*

□ Segment includes e-mail server(s)

Map to sensor: cs1-sensor.counterstorm.com

```
Name           IP address range                E-mail? Sensor
Production Ser 10.1.0.0 - 10.1.255.255                 csl-sensor.c
Corporate LAN  10.2.0.0 - 10.2.255.255                 csl-sensor.c
Mail server    10.1.7.7 - 10.1.7.7              T      csl-sensor.c
Private Net10  10.0.0.0 - 10.255.255.255
Private Net172 172.16.0.0 - 172.31.255.255
Private Net192 192.168.0.0 - 192.168.255.255
```

Configure segments

A segment is a group of systems defined by their contiguous IP address range. You can manually add segment entries and/or use entries from the recommended segment list. When you add segments, you specify the beginning and ending IP range and map the segment to a sensor. If the segment contains e-mail servers, check the box.

Once the segment is mapped to a sensor, the sensor monitors the segment and is responsible for taking specified actions against detected activity on the segment.

At least one segment must be created and mapped.

* required

4. Enter Segment to Sensor mapping information.

   Enter the desired segment and sensor information and click **Add Segment**. If the segment contains an e-mail server, make sure to check the **Segment includes e-mail server(s)** check box. Each mapping is listed in the table.

   At a minimum, one segment must be created.

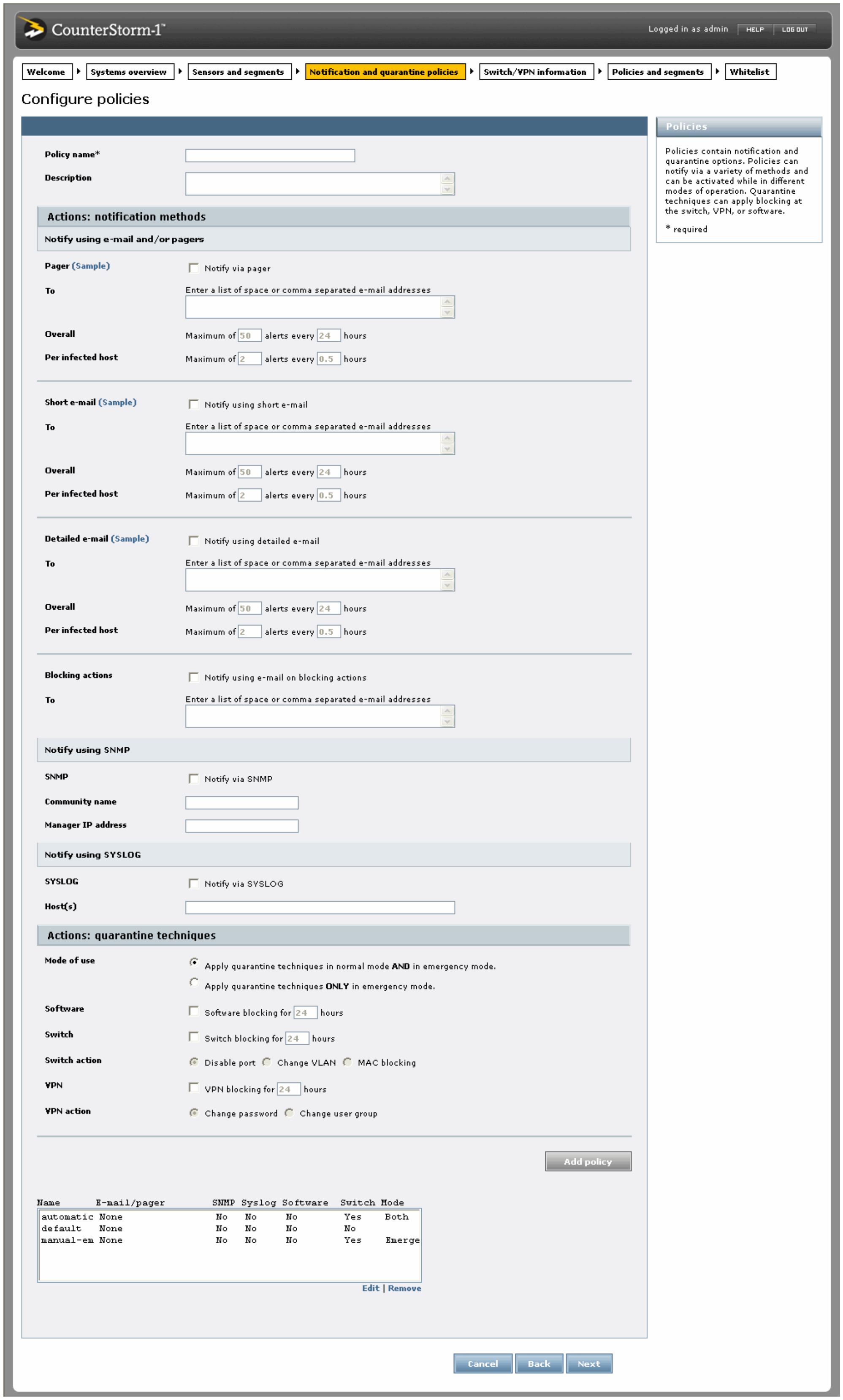
Note: The system supplies a few needed default segments. These are the Internet segment, private net10, private net172, and private net192. These segments are needed for system operation. You must still create at least one segment at this time.

Recommended segments are automatically added to your segment table during initial configuration. See "Recommended Segment List" on page 9-4 for more information.

Read "Segment to sensor mapping allows you to create segments and to configure which sensors monitor which segments. Each segment in the network can be mapped, or assigned, to a specified CounterStorm-1 sensor. Segments may also be created, while remaining unmapped. See "Mapping the sensor" on page 9-8 for information on mapped and unmapped segments." on page 9-6 for important information on creating segments. Segment definition is crucial to proper CounterStorm-1 operation.

5. When all mappings have been added, click **Next**.

The Policies screen appears.



CounterStorm-1™

Logged in as admin | HELP | LOG OUT

Welcome ▸ Systems overview ▸ Sensors and segments ▸ **Notification and quarantine policies** ▸ Switch/VPN information ▸ Policies and segments ▸ Whitelist

Configure policies

Policy name*

Description

Actions: notification methods

Notify using e-mail and/or pagers

Pager (Sample) □ Notify via pager

To Enter a list of space or comma separated e-mail addresses

Overall Maximum of 50 alerts every 24 hours

Per infected host Maximum of 2 alerts every 0.5 hours

Short e-mail (Sample) □ Notify using short e-mail

To Enter a list of space or comma separated e-mail addresses

Overall Maximum of 50 alerts every 24 hours

Per infected host Maximum of 2 alerts every 0.5 hours

Detailed e-mail (Sample) □ Notify using detailed e-mail

To Enter a list of space or comma separated e-mail addresses

Overall Maximum of 50 alerts every 24 hours

Per infected host Maximum of 2 alerts every 0.5 hours

Blocking actions □ Notify using e-mail on blocking actions

To Enter a list of space or comma separated e-mail addresses

Notify using SNMP

SNMP □ Notify via SNMP

Community name

Manager IP address

Notify using SYSLOG

SYSLOG □ Notify via SYSLOG

Host(s)

Actions: quarantine techniques

Mode of use
● Apply quarantine techniques in normal mode **AND** in emergency mode.
○ Apply quarantine techniques **ONLY** in emergency mode.

Software □ Software blocking for 24 hours

Switch □ Switch blocking for 24 hours

Switch action ● Disable port ○ Change VLAN ○ MAC blocking

VPN □ VPN blocking for 24 hours

VPN action ● Change password ○ Change user group

Add policy

```
Name       E-mail/pager          SNMP  Syslog  Software  Switch  Mode
automatic  None                  No    No      No        Yes     Both
default    None                  No    No      No        No
manual-em  None                  No    No      No        Yes     Emerge
```

Edit | Remove

Cancel | Back | Next

Policies

Policies contain notification and quarantine options. Policies can notify via a variety of methods and can be activated while in different modes of operation. Quarantine techniques can apply blocking at the switch, VPN, or software.

* required

6. Configure the policies.

   You may modify the default policy or add new policies to apply appropriate defense strategies to the different segments in the network. Policies contain notification and quarantine settings which can automatically stop attacks and alert administrators.

Note: It is recommended that active responses not be activated until after the first week of CounterStorm-1's operation so that you don't block any activity that should be whitelisted. However, you can configure active response policies during the initial installation and activate them at a later time.

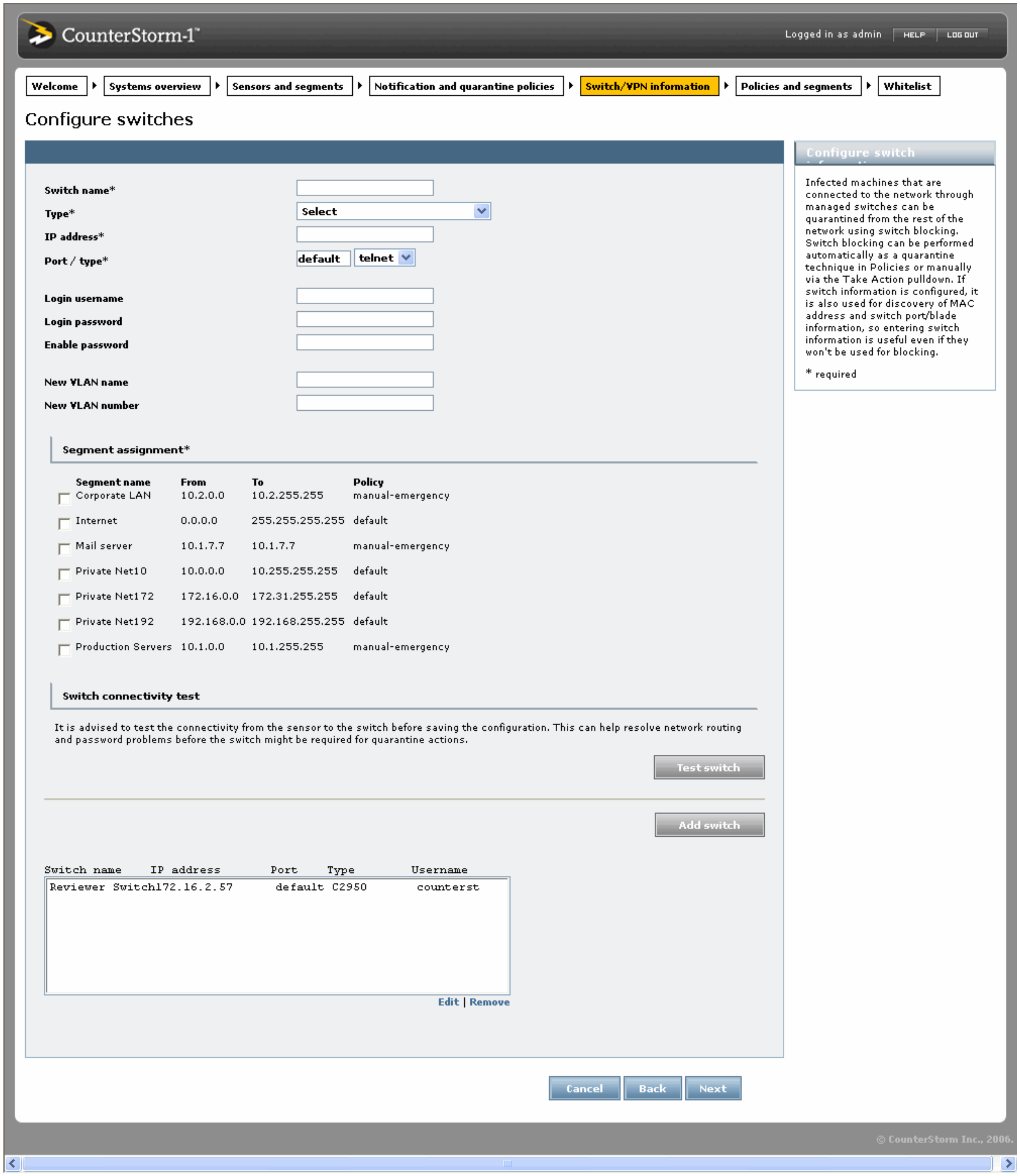
Note: Enabling switch blocking for a segment requires two steps. First, you must select switch blocking as the active response for the specified segment. Second, you must also configure the switches for that segment on the Switch Information screen. If a host becomes infected and both of these items are not configured properly, then the system cannot implement a switch-based quarantine. If active responses have not been activated, you can take action manually as described in "Taking Action On Attacks" on page 6-7.

Note: Enabling VPN blocking for a segment also requires that you select blocking as the active response for the specified segment and that you configure the VPNs for that segment on the VPN configuration screen. If a host becomes infected and both of these items are not configured properly, then the system cannot implement a VPN-based quarantine. If active responses have not been activated, you can take action manually as described in "Taking Action On Attacks" on page 6-7.

See "Configuring Policies" on page 10-2 for screen details. Make sure you click **Add Policy** for each new policy added.

7. Click **Next**.

The Configure Switch Information screen appears.



Configure switches

Switch name*	
Type*	Select
IP address*	
Port / type*	default telnet
Login username	
Login password	
Enable password	
New VLAN name	
New VLAN number	

Segment assignment*

	Segment name	From	To	Policy
□	Corporate LAN	10.2.0.0	10.2.255.255	manual-emergency
□	Internet	0.0.0.0	255.255.255.255	default
□	Mail server	10.1.7.7	10.1.7.7	manual-emergency
□	Private Net10	10.0.0.0	10.255.255.255	default
□	Private Net172	172.16.0.0	172.31.255.255	default
□	Private Net192	192.168.0.0	192.168.255.255	default
□	Production Servers	10.1.0.0	10.1.255.255	manual-emergency

Switch connectivity test

It is advised to test the connectivity from the sensor to the switch before saving the configuration. This can help resolve network routing and password problems before the switch might be required for quarantine actions.

```
Switch name    IP address        Port     Type          Username
Reviewer Switch172.16.2.57        default  C2950         counterst
```

Configure switch information

Infected machines that are connected to the network through managed switches can be quarantined from the rest of the network using switch blocking. Switch blocking can be performed automatically as a quarantine technique in Policies or manually via the Take Action pulldown. If switch information is configured, it is also used for discovery of MAC address and switch port/blade information, so entering switch information is useful even if they won't be used for blocking.

* required

8. Configure the switches.

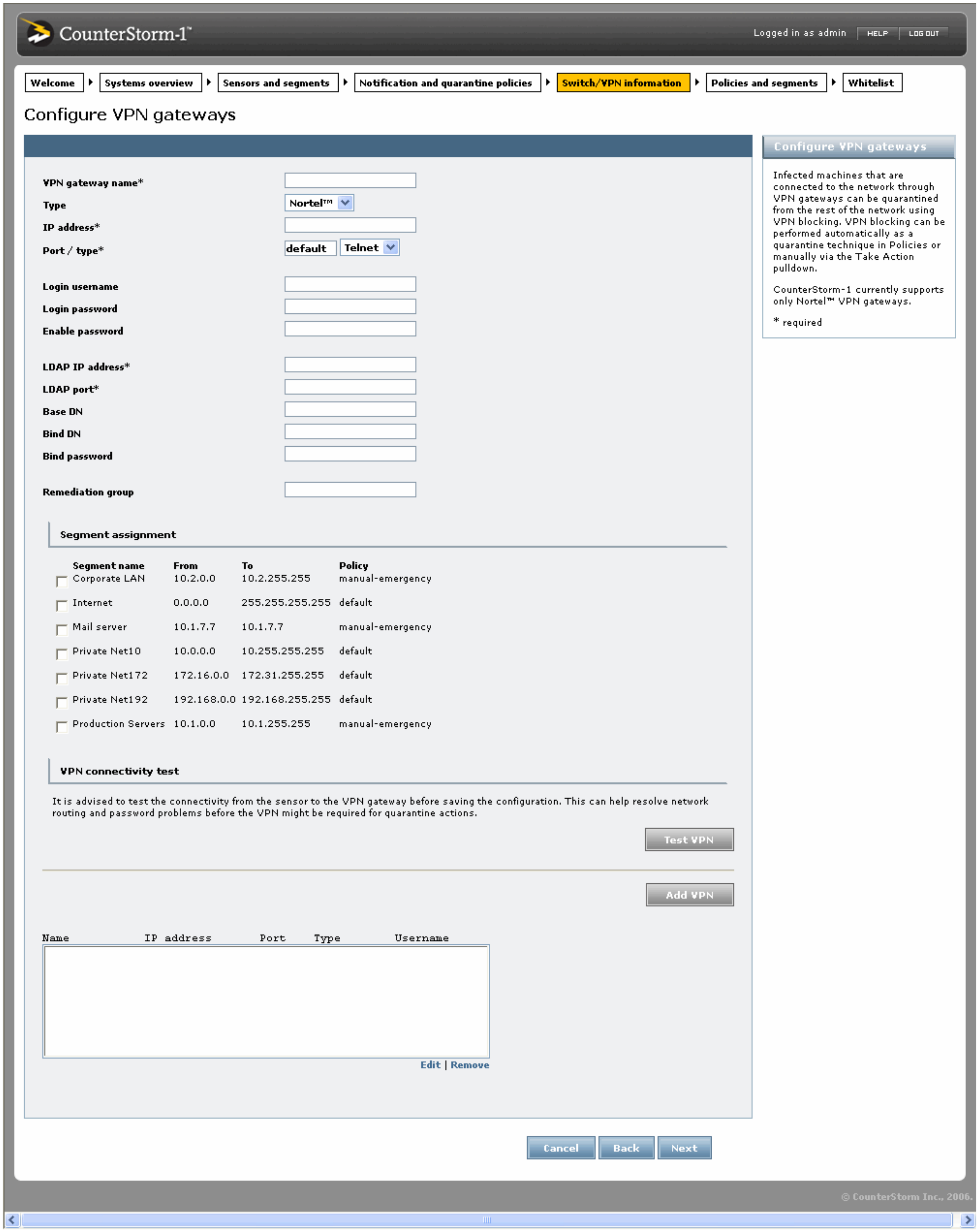
Switch blocking is used in CounterStorm-1 to quarantine attacks. Switch information is also used for the discovery of MAC address and switch port/blade information. Even if you don’t intend to use your switches for blocking, it is recommended that you add them to the list.

Note: It is recommended that you configure the switch used for blocking even if you do not intend to activate the automatic active responses in case you need to manually activate blocking.

If switch information is not available, click **Next**. You can configure the switches later. See “Configuring Switch Information” on page 11-3 for screen details.

9. Click **Next**.

The Configure VPN screen appears.



Configure VPN gateways

VPN gateway name*	
Type	Nortel™
IP address*	
Port / type*	default · Telnet
Login username	
Login password	
Enable password	
LDAP IP address*	
LDAP port*	
Base DN	
Bind DN	
Bind password	
Remediation group	

Segment assignment

	Segment name	From	To	Policy
□	Corporate LAN	10.2.0.0	10.2.255.255	manual-emergency
□	Internet	0.0.0.0	255.255.255.255	default
□	Mail server	10.1.7.7	10.1.7.7	manual-emergency
□	Private Net10	10.0.0.0	10.255.255.255	default
□	Private Net172	172.16.0.0	172.31.255.255	default
□	Private Net192	192.168.0.0	192.168.255.255	default
□	Production Servers	10.1.0.0	10.1.255.255	manual-emergency

VPN connectivity test

It is advised to test the connectivity from the sensor to the VPN gateway before saving the configuration. This can help resolve network routing and password problems before the VPN might be required for quarantine actions.

Name	IP address	Port	Type	Username

Configure VPN gateways

Infected machines that are connected to the network through VPN gateways can be quarantined from the rest of the network using VPN blocking. VPN blocking can be performed automatically as a quarantine technique in Policies or manually via the Take Action pulldown.

CounterStorm-1 currently supports only Nortel™ VPN gateways.

* required

© CounterStorm Inc., 2006.

10. Configure VPN gateways.

    VPN blocking is used in CounterStorm-1 to quarantine attacks. Even if you don’t intend to use your VPN gateways for blocking, it is recommended that you add them to the list.

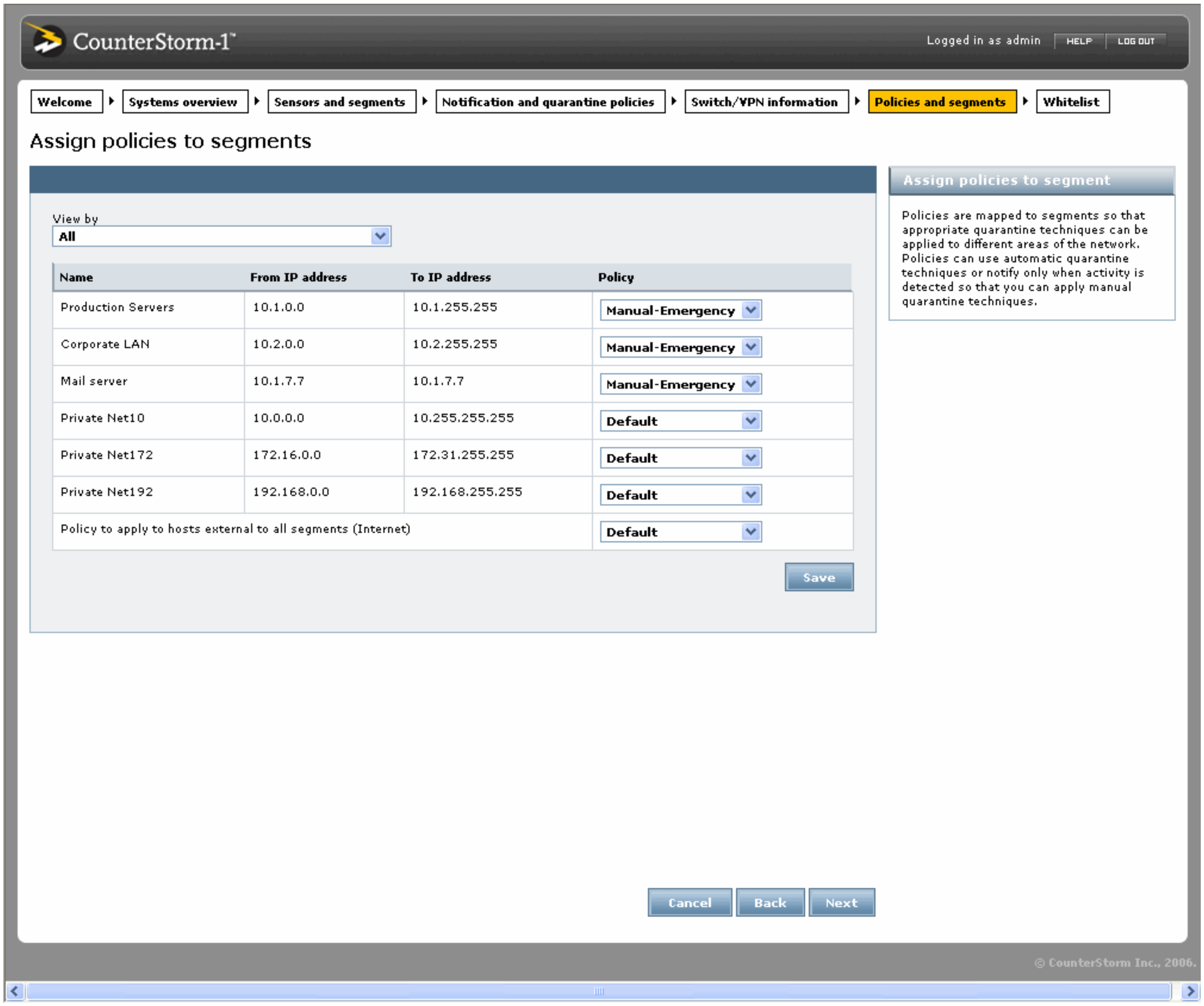
Note: It is recommended that you configure the VPN gateway used for blocking even if you do not intend to activate the automatic active responses in case you need to manually activate blocking.

If VPN information is not available, click **Next**. You can configure the gateway later. See“VPN Gateways” on page 11-6 for screen details.

Note: VPNs need to be deployed at the same segment as the VPN termination device.

11. Click **Next**.

    The Assign Policy to segment mapping screen appears.



Assign policies to segments

View by: All

Name	From IP address	To IP address	Policy
Production Servers	10.1.0.0	10.1.255.255	Manual-Emergency
Corporate LAN	10.2.0.0	10.2.255.255	Manual-Emergency
Mail server	10.1.7.7	10.1.7.7	Manual-Emergency
Private Net10	10.0.0.0	10.255.255.255	Default
Private Net172	172.16.0.0	172.31.255.255	Default
Private Net192	192.168.0.0	192.168.255.255	Default
Policy to apply to hosts external to all segments (Internet)			Default

Assign policies to segment

Policies are mapped to segments so that appropriate quarantine techniques can be applied to different areas of the network. Policies can use automatic quarantine techniques or notify only when activity is detected so that you can apply manual quarantine techniques.

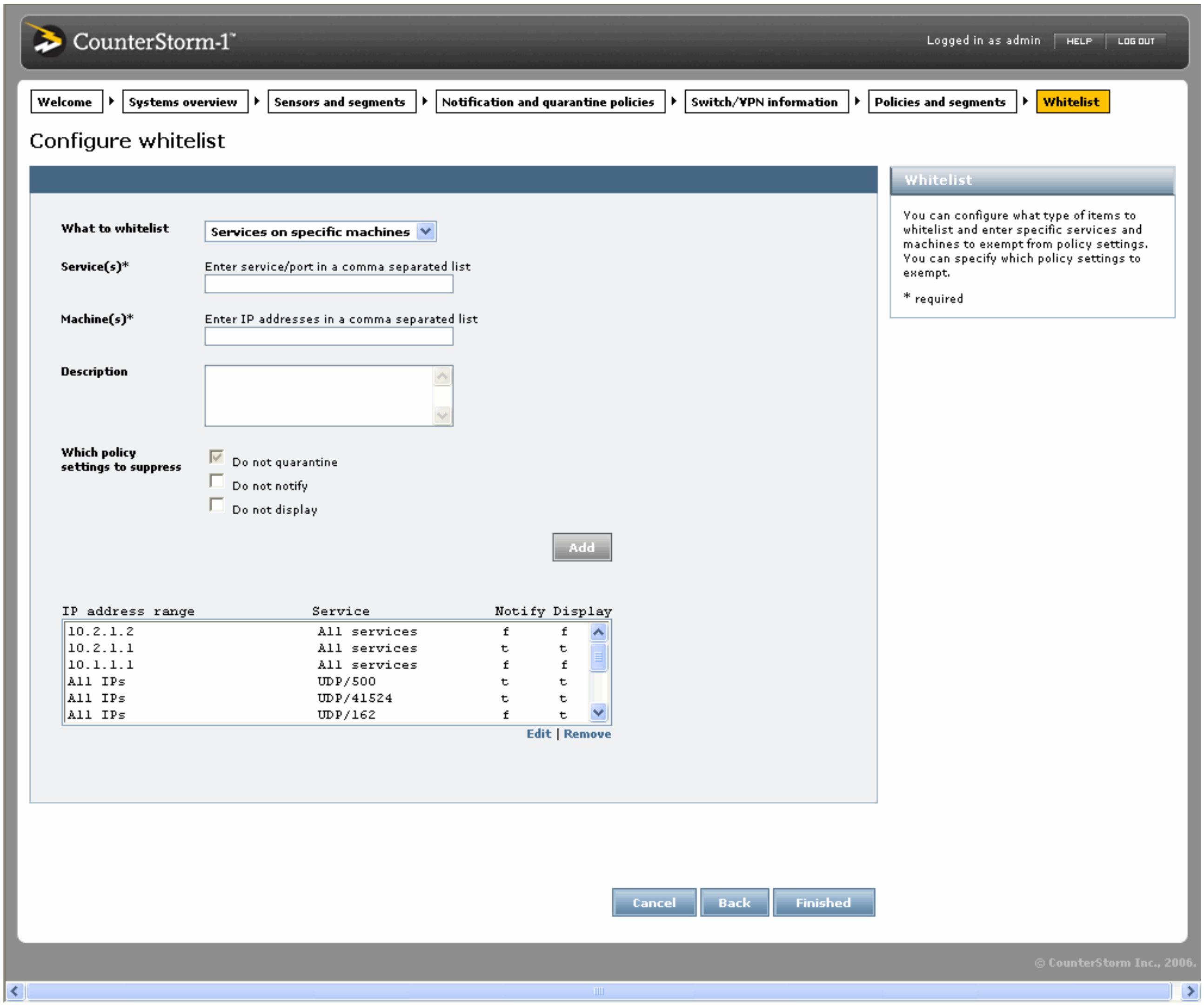
Assign the active response policies that you created in step 3 to specific segments.

Policies are mapped to individual segments so that an appropriate defense strategy can be applied to different areas of the network. If there is a segment for which blocking is not optimal, it is advised to implement a notification-only policy. Alternatively, in a segment with critical assets, an aggressive blocking policy may be the best way to mitigate attack propagation.

See “Assigning Policies to Segments” on page 9-8 for screen details. Make sure you click the **Save** button after assigning policies.

12. Click **Next**.

The Configure whitelist screen appears.



Configure whitelist

What to whitelist: Services on specific machines

Service(s)*: Enter service/port in a comma separated list

Machine(s)*: Enter IP addresses in a comma separated list

Description

Which policy settings to suppress
☑ Do not quarantine
☐ Do not notify
☐ Do not display

IP address range	Service	Notify	Display
10.2.1.2	All services	f	f
10.2.1.1	All services	t	t
10.1.1.1	All services	f	f
All IPs	UDP/500	t	t
All IPs	UDP/41524	t	t
All IPs	UDP/162	f	t

Whitelist

You can configure what type of items to whitelist and enter specific services and machines to exempt from policy settings. You can specify which policy settings to exempt.

* required

13. Configure the whitelist.

The whitelist configures the machines and services that are exempted from the active response policies.

When you add a whitelist entry, it will always suppress blocking of the machine or service (quarantine). Additionally, if you elect not to display activity, notifications are also suppressed (i.e. each checkbox includes the ones above it implicitly).

You can configure CounterStorm-1 to:

- Not block the traffic from a whitelisted machine or service
- Not notify administrators about activity from a whitelisted machine or service
- Not display activity in the user interface from a whitelisted machine or service

Auto-whitelisted entries have been added to the whitelist during sensor registration; these are the entries that are already present. While you won't know what sorts of traffic will need to be whitelisted at this time, there are some particular types of whitelist entries that are commonly entered after validating specific network traffic:

Service/Port	Description
TCP/25	This is the Simple Mail Transfer Protocol (SMTP) service. You should add whitelist entries for any mail server or gateway that performs external delivery (i.e. that sends mail directly to recipients on the Internet). Note that rather than adding a specific TCP/25 whitelist entry for the mail server(s), you may want to whitelist e-mail worms; this will prevent alarms due to the quantity or volume of e-mail, as well as for attempts to deliver to unreachable mail servers on the Internet. Whitelisting e-mail worms is especially important for any mail servers that are also hosting mailing lists or other types of mail exploders. Microsoft Exchange servers are typically also SMTP relays or servers.
UDP/53	This is the Domain Name System (DNS) service; CounterStorm-1 will auto-whitelist any servers that it knows about. You should add whitelist entries for any DNS server that will perform recursive queries (i.e. that it will query for information on behalf of another machine). Almost all DNS servers are set up to support recursive queries. Microsoft Active Directory and Domain Controllers will typically be DNS servers as well.
UDP/67	This is the Dynamic Host Configuration Protocol (DHCP) server port; CounterStorm-1 will generate an auto-whitelist entry for all machines on this service, as well as for UDP/68, the DHCP client port. These are broader whitelists than are actually needed, and you should consider replacing the all-machines whitelist entry (especially for UDP/68) with separate entries for each DHCP server or relay (DHCP relays in particular need whitelisting for UDP/68). DHCP servers frequently check for expired/inactive leases using ICMP, so you may want or need to whitelist them for ICMP as well. Microsoft Active Directory servers or Domain Controllers might be in this category.
TCP/80	This is the HyperText Transfer Protocol (HTTP) service used for web access. You should add whitelist entries for any HTTP proxies that will forward web requests from other machines. If these proxies support other web-related services, like TCP/21 (FTP) or TCP/443 (HTTPS), you should consider adding whitelist entries for those services as well. Note that there is no need to whitelist ordinary web servers for this port; unlike the other services on this list, web servers are not typically web clients as well, and whitelisting is based on client-side behaviors, not server status. In fact, you should avoid whitelisting web servers for TCP/80, because if they are infected by an HTTP exploit, they are most likely to spread the infection using this service.
TCP/113	This is the Ident (or Auth) service, which is used by some other servers (mostly IRC chat and anonymous FTP servers, but occasionally SMTP mail relays and others) to attempt to identify a user name for a particular connection. Since very few client machines support Ident, the failed reverse Ident connections will cause false alarms. You should add whitelist entries for any servers that use Ident.

Service/Port	Description
UDP/123	This is the Network Time Protocol (NTP) service; if you have manually configured NTP servers by IP address (not hostname) for the Command Center or sensors during the initial console configuration, CounterStorm-1 will auto-whitelist those servers. You should also add whitelist entries for any NTP servers that are not already auto-whitelisted. While NTP servers that are only configured with two or three peer servers are not likely to cause false alarms, it is always better to enter them just in case. Microsoft Domain Controllers may also be NTP servers.
UDP/161	This is the Simple Network Management Protocol (SNMP) service. You should add whitelist entries for any network management stations that perform periodic monitoring of network devices via SNMP. Very often, these management stations also perform ICMP scanning of local networks, and should be whitelisted for ICMP as well.
UDP/1645 UDP/1812	These are the preliminary and official RADIUS (Remote Authentication Dial In User Service) ports, which may be used for authenticating dial-in, VPN, or Wireless LAN users. You should add whitelist entries with the appropriate port for any RADIUS servers that will be acting as RADIUS proxies (i.e. acting as clients as well as servers).
Active Directory or Domain Controllers	Certain Microsoft systems perform monitoring of the other servers in a way that is likely to appear as scanning. You may wish to whitelist these for certain services (ICMP, UDP/137) or simply whitelist the entire machine. It is probably best to wait before doing this and see what the whitelist suggestions screen recommends.
Network Management	Certain types of network management systems, like vulnerability assessment and asset management tools, will perform scanning activity as part of their normal operations. These machines should be whitelisted for the entire machine. Examples of these might include Tivoli or SolarWinds.
Mission-critical	This is for mission-critical machines that you do not want to quarantine, even if they are infected with a worm and might spread it to other machines. In most cases, it is preferable to define a special segment that contains these mission-critical machines and assign it a policy that does not use any quarantine technique (blocking), but if that is not practical (for example, defining a segment for the default router on each subnet), you may want to simply add an entire-machine whitelist entry for each of these mission-critical machines (e.g. default routers). When adding these entire-machine whitelist entries, you should leave notification and display enabled (leave the “Do not notify” and “Do not display” boxes unchecked) so that the whitelist merely prevents quarantine techniques.

After adding whitelist entries for the above cases, you will still need to add more, but until the system has been running for a while, you won't know which ones. You can add whitelist entries using the **Take Action** pull-down menu on the **Analyze** screen when you receive alarms for systems that are not infected, but in most cases it is easier to wait a few days as alarms are generated and then use the **Recommended list** button on the **Whitelist** screen of the Configure tab to generate a complete set of whitelist entries for your site.

If whitelist information is not available, click **Next**. You can configure the whitelist later. See “Creating the Whitelist” on page 12-4 for additional details. Make sure you click the **Add** button after each whitelist entry.

14. Click **Finish**.

    After a short time and some processing messages, you are placed in the CounterStorm-1 Monitor screen.

Chapter 4: User Configuration

In This Chapter

You can add, delete, and modify users and user roles. The default login account is the admin account. For this account, the admin password, which was assigned during the Command Center console configuration, is required to ensure the security of the CounterStorm-1 system and data.

Three default roles exist: administrator, analyst, and guest. The administrator must assign a password to the guest and analyst accounts. Guests and Analysts cannot change their own password.

Viewing Users And Roles

When you access the Users page, all users and roles are shown. You can return to this list at any time.

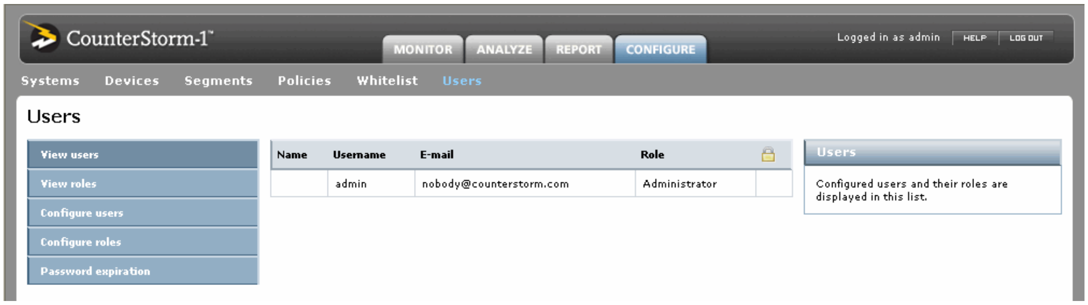
To view users and roles:

1. Select **Configure** from the Main Toolbar and **Users** from the Interactive Toolbar.

   The Users screen is displayed.

2. Click **View users**.

   A list of users is displayed. You can view or modify the configuration for items in the list by clicking on the desired user name.



Name	Username	E-mail	Role
	admin	nobody@counterstorm.com	Administrator

Configured users and their roles are displayed in this list.

Configuring Users

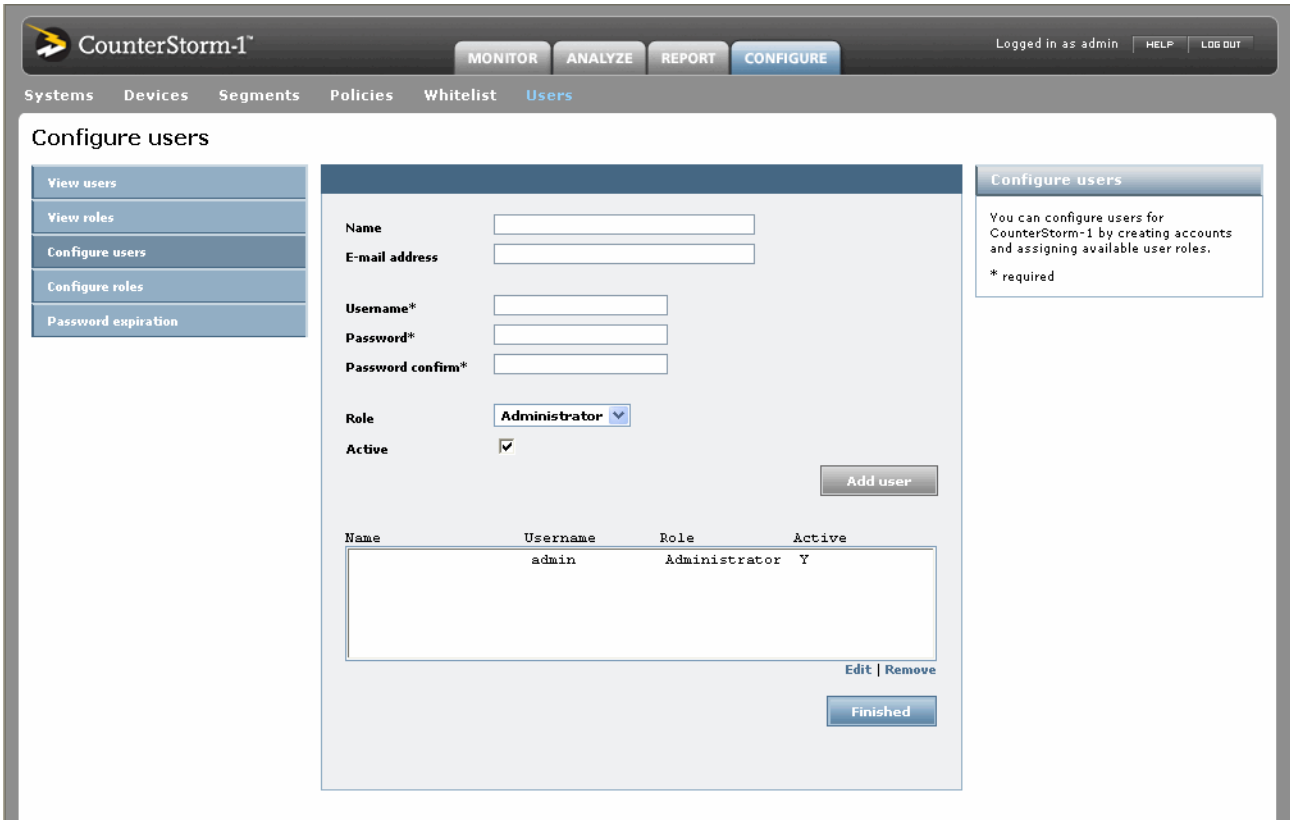
Every user of CounterStorm-1 must have an account. The administrator's account is the account used for first login and was created during console configuration. Only the administrator can create additional users.

To create users:

1. Select **Configure** from the Main Toolbar and **Users** from the Interactive Toolbar.

   The Users screen is displayed.
2. Click **Configure user**.

   The Configure user screen is displayed.



Configure users

You can configure users for CounterStorm-1 by creating accounts and assigning available user roles.

* required

Name	
E-mail address	
Username*	
Password*	
Password confirm*	
Role	Administrator
Active	☑

Name	Username	Role	Active
	admin	Administrator	Y

3. Enter the desired information.

   Enter the ***Name*** and ***E-mail Address*** for the user as well as a ***Password***. Select the ***Role*** for the user. To create new roles see "Configuring Roles" on page 4-3. Check the ***Active*** box to enable this user account.
4. Click **Add User**.

   You may add many accounts before clicking Finished.
5. Click **Finished** when all users are added.

   You may delete a user by highlighting the desired user name in the user table and clicking the **Remove** link. You may modify a user by highlighting the desired user name in the user table and clicking the **Edit** link.

Configuring Roles

Three default roles are provided with CounterStorm-1. These are: the administrator, who has superuser permissions, the network analyst, who has many permissions, and the guest ,who has limited permissions. These three roles cannot be changed; however, you may create additional roles. You can view existing roles by clicking **View Roles**.

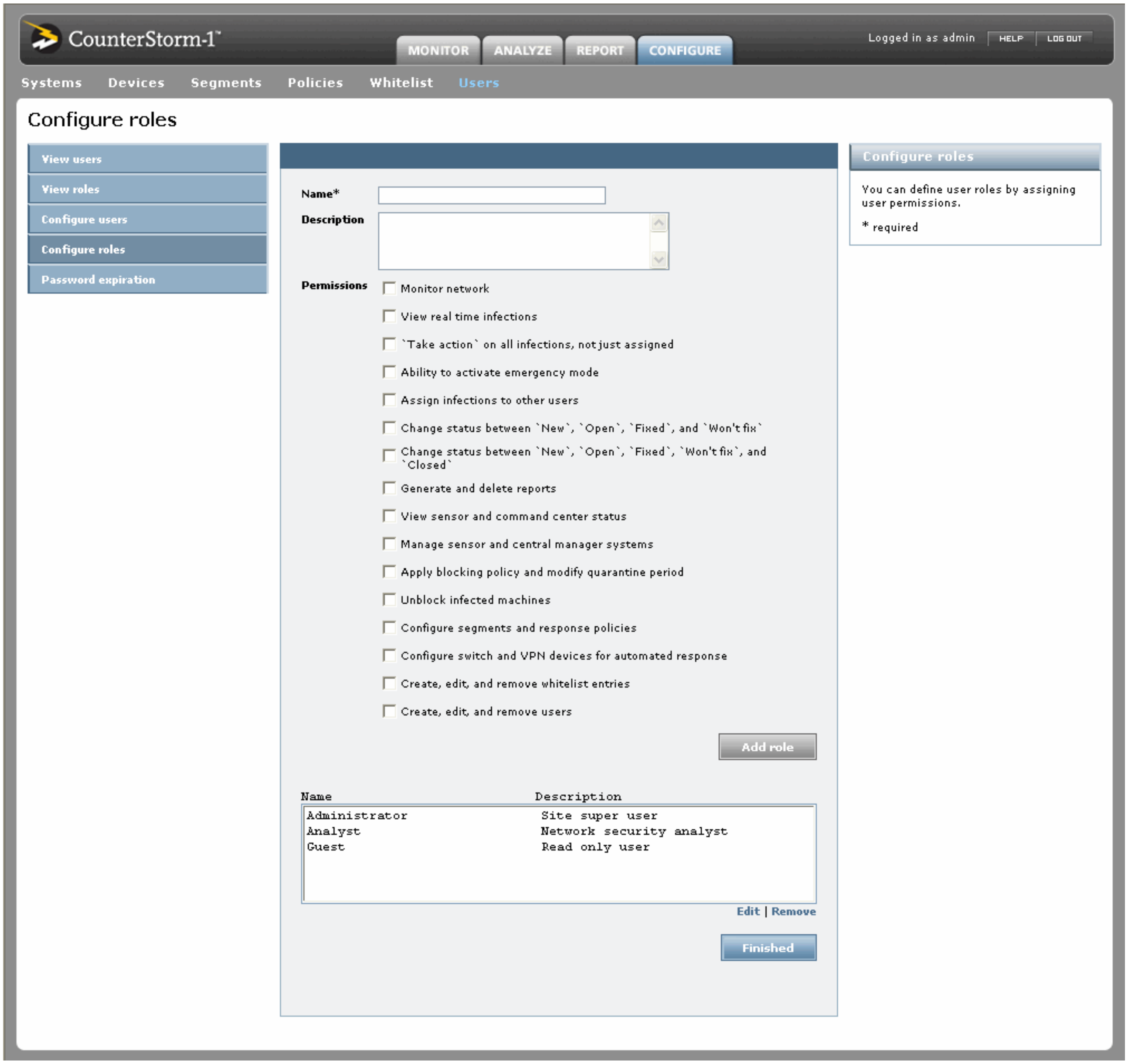
To create roles:

1. Select **Configure** from the Main Toolbar and **Users** from the Interactive Toolbar.

   The Users screen is displayed.

2. Click **Configure roles**.

   The Configure roles screen is displayed.



Configure roles

Name*

Description

Permissions

☐ Monitor network
☐ View real time infections
☐ `Take action` on all infections, not just assigned
☐ Ability to activate emergency mode
☐ Assign infections to other users
☐ Change status between `New`, `Open`, `Fixed`, and `Won't fix`
☐ Change status between `New`, `Open`, `Fixed`, `Won't fix`, and `Closed`
☐ Generate and delete reports
☐ View sensor and command center status
☐ Manage sensor and central manager systems
☐ Apply blocking policy and modify quarantine period
☐ Unblock infected machines
☐ Configure segments and response policies
☐ Configure switch and VPN devices for automated response
☐ Create, edit, and remove whitelist entries
☐ Create, edit, and remove users

Name	Description
Administrator	Site super user
Analyst	Network security analyst
Guest	Read only user

Configure roles

You can define user roles by assigning user permissions.

* required

3. Enter the ***Name*** and ***Description*** for the role and check the desired permissions.

   The following table describes the role when the box is checked. When the box is not checked, the user cannot perform the action.

Role	Description
Monitor network	Users are able to view the Monitor screen. If not checked, user is placed in the Analyze screen.
View real time infections	Users are able to view the screens that have auto-refresh capability automatically refresh.
Take action on all infections, not just assigned	Users are able to use the Take Action pulldown options on all infection. Can be used in Analyze or Investigate screens.
Ability to activate emergency mode	Users are able to change all modes including activate or deactivate, emergency blocking, and non-blocking modes.
Assign infections to other users	Users are able to use the Assign To drop down to give the case to someone else.
Change status between "New," "Open," "Fixed," and "Won't fix"	Users are able to change status between the non-closed states.
Change status between "New," "Open," "Fixed," "Won't fix," and "Closed"	Users are able to change status to "Closed". Checking this option also checks the above option.
Generate and delete reports	Users can always view reports, but this allows users to modify the existing ones.
View sensor and command center status	Users are able to view the Systems screen.
Manage sensor and Command Center systems	Users have access to the Systems screen.
Apply blocking policy and modify quarantine period	Users can choose Take action->Block and modify the time period for blocking.
Unblock infected machines	Users can choose Take action->Unblock on machines.
Configure segments and response policies	Users have access to the Segments and Policies configuration screens.
Configure switch and VPN devices for automated response	Users have access to the Devices configuration screen.
Create, edit, and remove whitelist entries	Users have access to the Whitelist configuration screen and to the Take action->Whitelist options.
Create, edit, and remove users	Users have access to the Users screen.

4. Click **Add Roles**.
5. Click **Finished** when all roles are added.

   You may delete a role by highlighting the desired role in the role table and clicking the **Remove** link. You may modify a role by highlighting the desired role in the role table and clicking the **Edit** link.

Password Expiration

You can configure web login user passwords to expire after a certain number of days, from 3 to 99999 (the latter value effectively disables expiration). This may be necessary to comply with a password security policy. You may also configure the number of most recently used passwords that are blocked from use as the new password. This action applies to all user accounts.

This screen pertains to web login user account passwords. You can also change the root password for appliance access via "Change Root Password" on page 14-31.

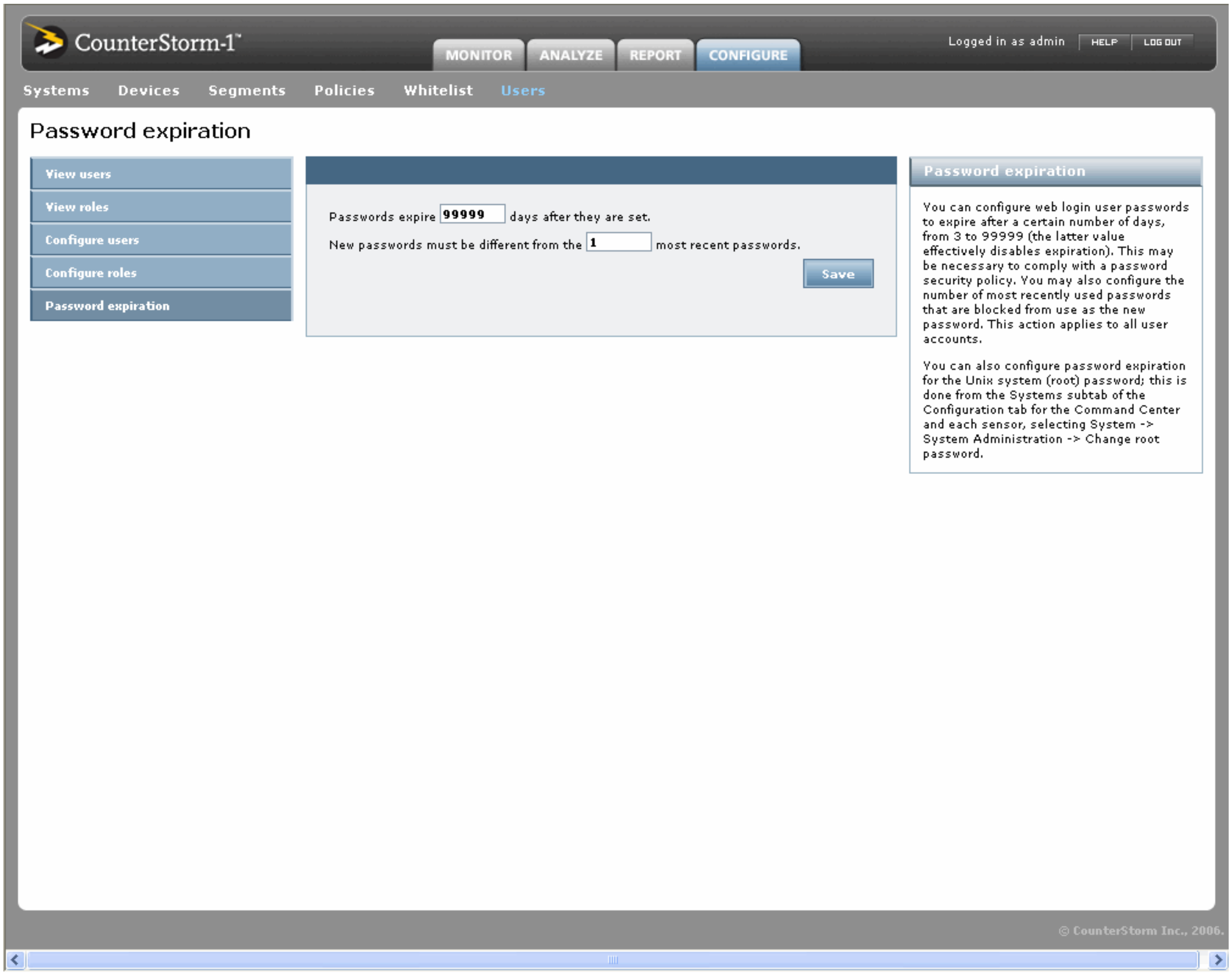
To change the web login user password expiration:

1. Select **Configure** from the Main Toolbar and **Users** from the Interactive Toolbar.

   The Users screen is displayed

2. Click **Password expiration**.

   The Password expiration screen is displayed.



Password expiration

Passwords expire 99999 days after they are set.

New passwords must be different from the 1 most recent passwords.

Password expiration

You can configure web login user passwords to expire after a certain number of days, from 3 to 99999 (the latter value effectively disables expiration). This may be necessary to comply with a password security policy. You may also configure the number of most recently used passwords that are blocked from use as the new password. This action applies to all user accounts.

You can also configure password expiration for the Unix system (root) password; this is done from the Systems subtab of the Configuration tab for the Command Center and each sensor, selecting System -> System Administration -> Change root password.

3. Enter the number of days after which the password will expire.

   This value can be 3 to 99999. 99999 indicates no expiration.

4. Enter how many passwords can be entered before the current password can be repeated.
5. Click **Save**.

Chapter 5: Monitoring Current Activity

This section explains how to use CounterStorm-1's monitoring graphs to review status about your network.

The Monitor screen provides a pictorial overview of the network status, enabling you to quickly check the status of the network and CounterStorm-1. The Monitor screen is always displayed upon initial login, unless you have entered the application via a link in an alert e-mail. You can return to this screen at any time to get a global view of your network status.

In This Chapter

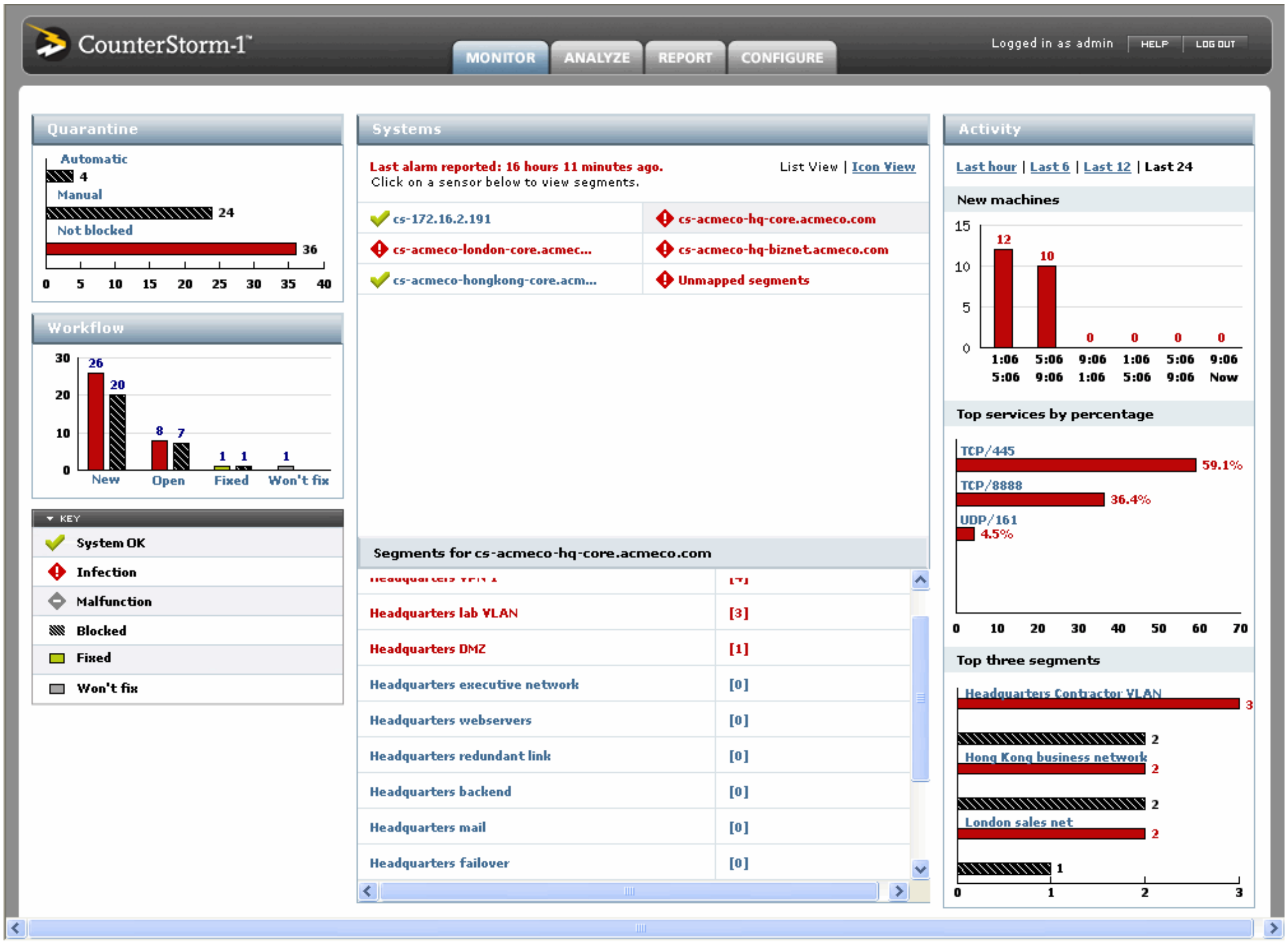
To access the Monitor screen:

1. Click the **Monitor** tab on the main toolbar.

   The Monitor screen displays four graphs:

   - Quarantine
   - Workflow
   - Systems
   - Activity
2. View the status of the system and its activity.
3. If desired, click on a sensor to view its segments.
4. If desired, click a on a segment to be placed in the Activity window for further details.

5. If desired, click on any graphical item to be placed in the Activity window for further details.



Last alarm reported: 16 hours 11 minutes ago.
Click on a sensor below to view segments.

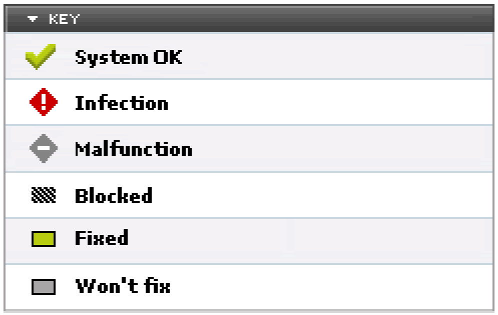
✓ cs-172.16.2.191	◆ cs-acmeco-hq-core.acmeco.com
◆ cs-acmeco-london-core.acmec...	◆ cs-acmeco-hq-biznet.acmeco.com
✓ cs-acmeco-hongkong-core.acm...	◆ Unmapped segments

Segments for cs-acmeco-hq-core.acmeco.com

Headquarters VPN 1	[4]
Headquarters lab VLAN	[3]
Headquarters DMZ	[1]
Headquarters executive network	[0]
Headquarters webservers	[0]
Headquarters redundant link	[0]
Headquarters backend	[0]
Headquarters mail	[0]
Headquarters failover	[0]

Key

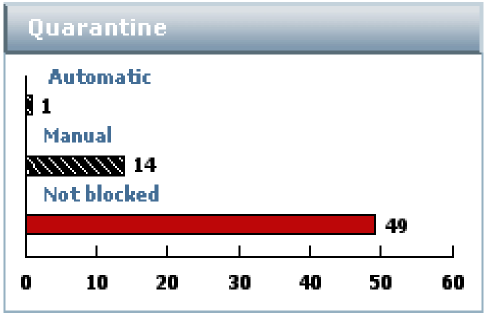
The key describes the icons and color code for all graphs.


KEY

✓	System OK
◆	Infection
◆	Malfunction
▨	Blocked
🟨	Fixed
▭	Won't fix

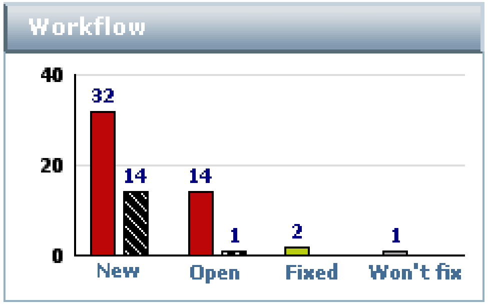
Quarantine

The Quarantine graph shows the number of currently blocked infections. It separates those that have been blocked manually from those that have been blocked automatically. It also displays infections that have not been blocked.



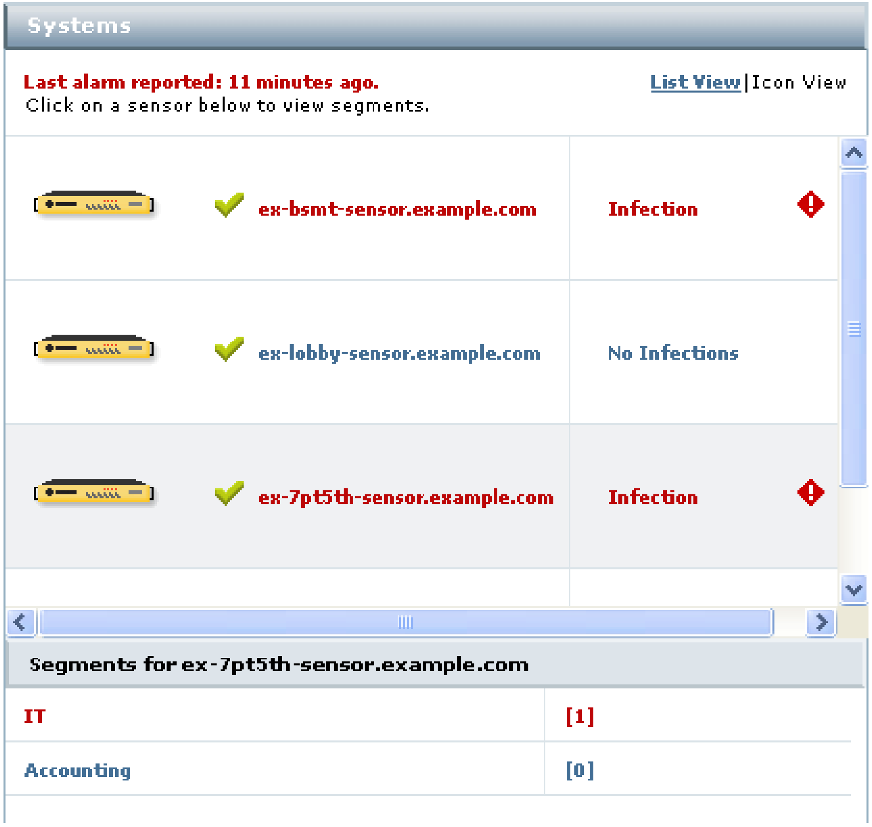
Workflow

The Workflow graph displays all infections that have been assigned a workflow. It displays infections that are New, Open, Fixed, or that have been labelled Won't Fix. Clicking on a bar in the graph takes you to the Analyze Activity table and displays the infections for that bar.



Systems

The Systems graph displays all sensors monitored by this Command Center. Clicking on a System displays its segments below. The segments are listed by name and the number of machines within which the segment is listed. Clicking on a segment takes you to the Analyze Activity table and displays the infections for that segment.



Systems

Last alarm reported: 11 minutes ago.
Click on a sensor below to view segments.

✓	ex-bsmt-sensor.example.com	Infection
✓	ex-lobby-sensor.example.com	No Infections
✓	ex-7pt5th-sensor.example.com	Infection

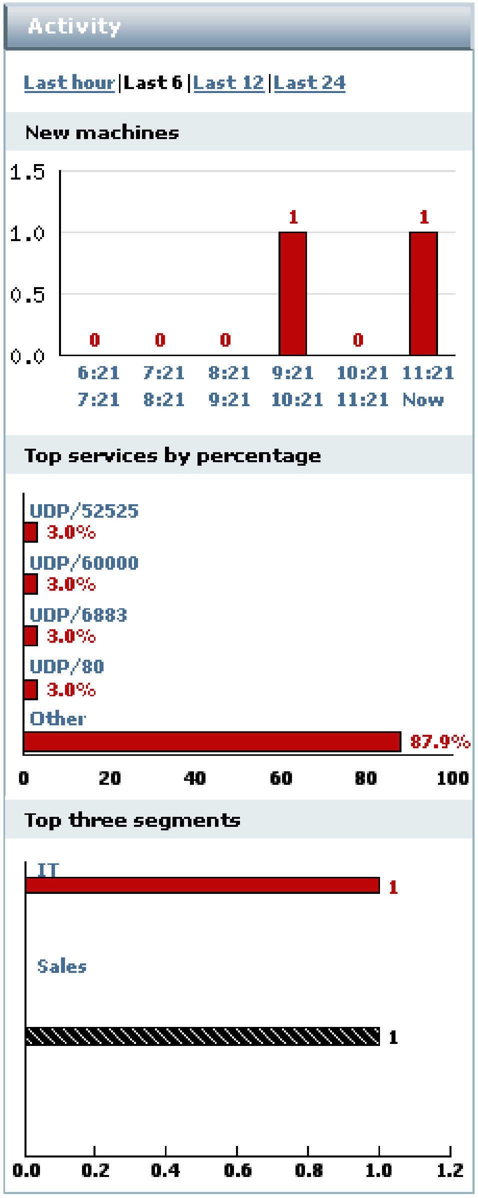
Segments for ex-7pt5th-sensor.example.com

IT	[1]
Accounting	[0]

You can view the sensors in List View or Icon View. List view displays the sensors in a list and Icon view places icons on the screen. Icon View is recommended for four or fewer than four sensors. For systems with a lot of sensors, List View is recommended. It places more sensors on the screen.

Activity

The Activity graph displays the infection activity for all segments. You can isolate the activity by displaying the last hour, last six hours, last twelve hours, or last twenty-four hours. The graph shows: new machines that have been infected, top affected services by percentage, and the top three most affected segments. Clicking on a bar in the graph takes you to the Analyze Activity table and displays the infections for that bar.



Chapter 6: Analyzing Attack Activity

This section explains how to use CounterStorm-1's Analyze screen. This screen can be accessed via the Analyze item on the Main toolbar or by clicking on items on the Monitor page graphs. The Analyze screen displays detailed information about infected hosts and services.

In This Chapter

Viewing Attack Activity

You can view information about infected machines on the Analyze screen.

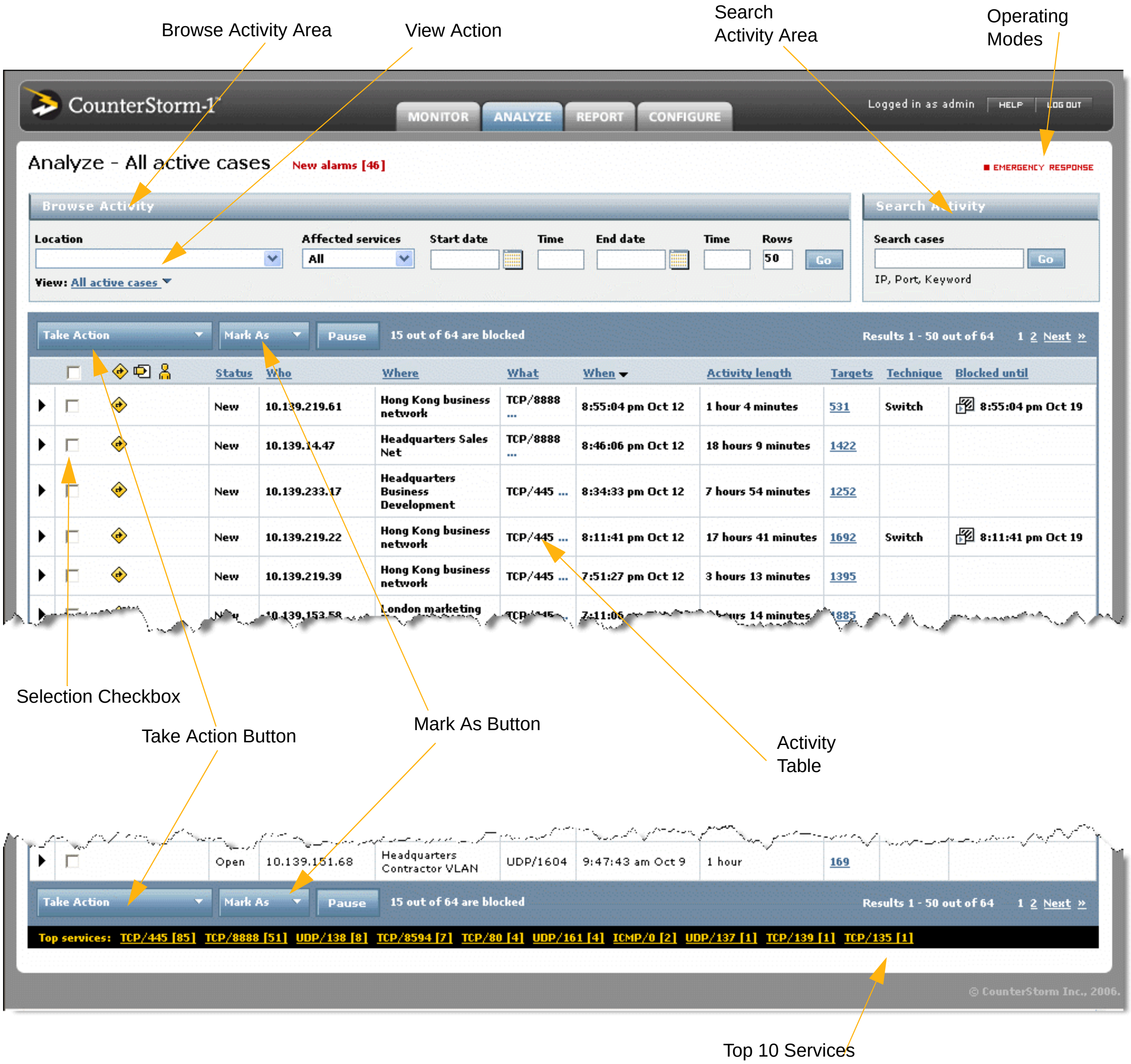
The Analyze screen displays a table that lists all machines on which attack activity has been observed by CounterStorm-1's sensors. The Analyze screen provides a descriptive view of the machine status, enabling you to drill-down into infected machines, implement active responses, and filter activity by location and/or by affected services.

To access the Analyze screen:

1. Select **Analyze** from the Main Toolbar.

   The Analyze screen is displayed.

Analyzing Attack Activity



Analyze - All active cases New alarms [46]

Browse Activity

Location: (empty) Affected services: All Start date: (empty) Time: (empty) End date: (empty) Time: (empty) Rows: 50 Go

View: All active cases

Search Activity

Search cases: (empty) Go

IP, Port, Keyword

Take Action | Mark As | Pause | 15 out of 64 are blocked | Results 1 - 50 out of 64 | 1 2 Next »

	□		Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
▶	□	◈	New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19
▶	□	◈	New	10.139.14.47	Headquarters Sales Net	TCP/8888 ...	8:46:06 pm Oct 12	18 hours 9 minutes	1422		
▶	□	◈	New	10.139.233.17	Headquarters Business Development	TCP/445 ...	8:34:33 pm Oct 12	7 hours 54 minutes	1252		
▶	□	◈	New	10.139.219.22	Hong Kong business network	TCP/445 ...	8:11:41 pm Oct 12	17 hours 41 minutes	1692	Switch	8:11:41 pm Oct 19
▶	□	◈	New	10.139.219.39	Hong Kong business network	TCP/445 ...	7:51:27 pm Oct 12	3 hours 13 minutes	1395		
▶	□		New	10.139.153.58	London marketing	TCP/445 ...	7:11:06	hours 14 minutes	1885		
▶	□		Open	10.139.151.68	Headquarters Contractor VLAN	UDP/1604	9:47:43 am Oct 9	1 hour	169		

Take Action | Mark As | Pause | 15 out of 64 are blocked | Results 1 - 50 out of 64 | 1 2 Next »

Top services: TCP/445 [85] TCP/8888 [51] UDP/138 [8] TCP/8594 [7] TCP/80 [4] UDP/161 [4] ICMP/0 [2] UDP/137 [1] TCP/139 [1] TCP/135 [1]

The screen provides areas for you to browse activity, sort activity, and search for activity.

The Activity table displays all machines on which attack activity has been observed in real-time. The column fields in the Activity table provide descriptive information about the machine and the observed incident.

Column Heading	Description
▸ icon	Expansion button which, when clicked, displays a detailed view table about the observed attack activity. See “Drilling-down” on page 6-6 for the expanded view.
Take Action check box	Clicking this box selects this machine. Actions taken are applied to selected machines.
Icon bar	Realarm - indicates this is not the first alarm for this infection. Clicking the icon in the row invokes the Activity History screen. Notes - indicates notes have been recorded. Clicking the note icon in the row invokes the Infection Details screen. Assigned to - displays the name of the person to which the activity has been assigned. Clicking the icon in the row invokes the Infection Details screen.
Who	IP address of the flagged machine. Whitelisted - indicates this IP has been whitelisted.
Where	Segment in which the flagged machine is located.
What	Service or port that was affected by the attack. It may also contain a whitelisted icon, if the service was whitelisted.
When	Time when activity was last observed. The time it was first observed is recorded in the details.
Activity length	The difference in time between the first and last activity noticed.
Targets	The number of machines the infection is targeting. Clicking the number takes you to the Destination IP list. See “Destination IP List” on page 7-2.
Technique	If known, the technique used to quarantine the machine.
Blocked until	Time when the blocking, or quarantine, active response expires.

You can click the **Pause** button to stop the flow of real-time data. You must click this button again to restart real-time data flow.

2. Review (drill-down) the information as desired.

You can view Activity History for a specific infection by clicking the **Activity History** button. This takes you to the Investigate screen with Activity History selected. See “Activity History” on page 7-3. You can access detailed information for this activity by selecting the **Investigate** button. See “Investigating Attack Activity” on page 7-1 for a detailed explanation of investigations.

Browsing Attack Activity

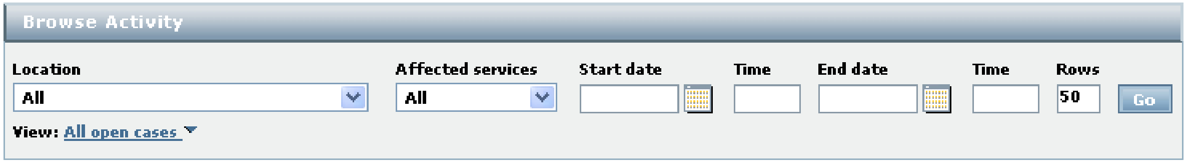
You can display the rows in the Activity table by location or by affected services. You can also specify how many rows to display and select a variety of items to view.

To custom display attack activity:

1. Select **Analyze** from the Main Toolbar.

   The Analyze screen is displayed.

2. Enter the desired search criteria in the Browse Activity area.

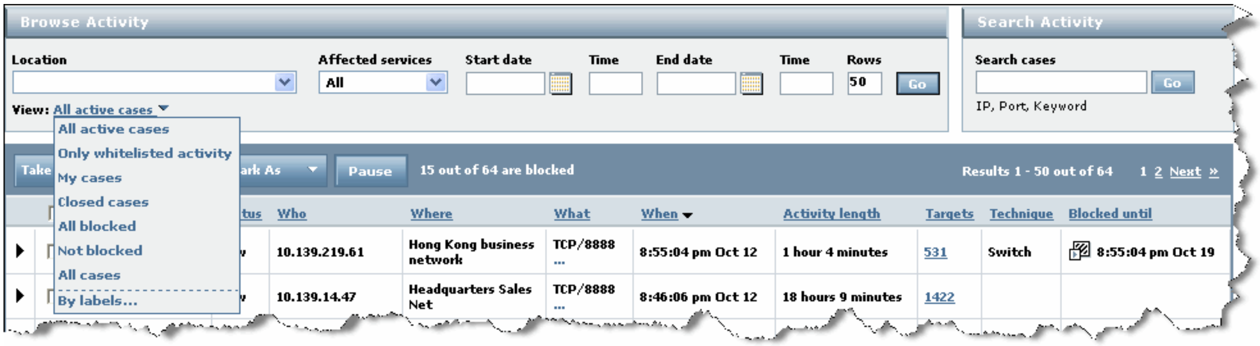


Browse Activity

Location: All
Affected services: All
Start date:
Time:
End date:
Time:
Rows: 50

View: All open cases

You can sort by the location of the segment or by the affected services. You can also specify how many rows to display and whether whitelisted activity is displayed. Dates can be manually entered in the format mm/dd/yyyy, or you can click the built-in calendar to select a date. You can also view specific activity groups by selecting an item under View. For example, you can view all activity that has been marked "Open" by selecting **View** and then **Open Cases**. My cases are those specific items that have been assigned to you via the Assign to functionality. Labels must exist to view by labels.



Browse Activity

Location:
Affected services: All
Start date:
Time:
End date:
Time:
Rows: 50

View: All active cases

Search Activity

Search cases:
IP, Port, Keyword

15 out of 64 are blocked

Results 1 - 50 out of 64

tus	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
v	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19
v	10.139.14.47	Headquarters Sales Net	TCP/8888 ...	8:46:06 pm Oct 12	18 hours 9 minutes	1422		

3. Click **GO**.

Marking Activity

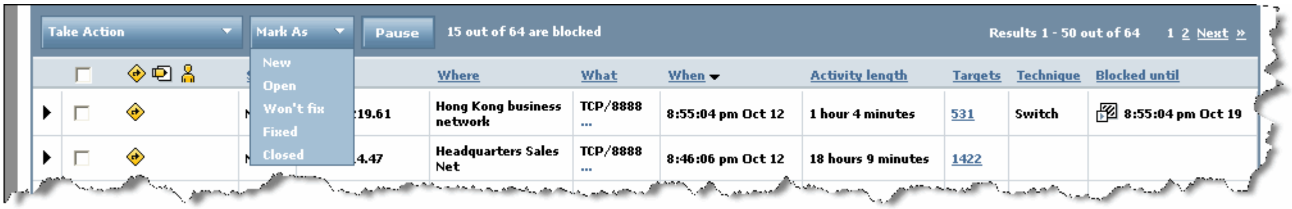
You can mark the activity New, Open, Fixed, Closed, Resolved, or Won't Fix. This workflow is optional. Items marked "Closed" are removed from the activity listing, but can still be searched and displayed. Closed items can be selected in the View pulldown menu. It is helpful to close items in order to unclutter your Activity table display. This feature is also available from the Investigate screens.

1. Select **Analyze** from the Main Toolbar.

   The Analyze screen is displayed.

2. Check the desired activity(s).

3. Click the **Mark As** button and select the desired item.



15 out of 64 are blocked

Results 1 - 50 out of 64 1 2 Next »

□		Where	What	When ▾	Activity length	Targets	Technique	Blocked until
□	:19.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19
□	4.47	Headquarters Sales Net	TCP/8888 ...	8:46:06 pm Oct 12	18 hours 9 minutes	1422		

A confirmation window appears.

4. Click **Mark**.

The window refreshes and the item(s) are marked.

Sorting Activity

You can sort activity by selecting the clickable column headers. The table refreshes and display rows sorted according to their priority to the selected header. The following columns may be used to sort: Status, Who, When, What, Activity Length, Target, and Blocked Until.

Searching Activity

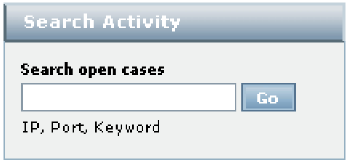
You can search for activity based on IP, Port, and keyword.

To search attack activity:

1. Select **Analyze** from the Main Toolbar.

   The Analyze screen is displayed.

2. Enter the desired search criteria in the Search area.



Search terms are AND'ed together in boolean terms. Results include all terms, not partial matches. A minus (-) sign indicates a NOT operator. For example, "TCP-foo" returns all items with TCP/80 but no items with foo.

3. Click **GO**.

Drilling-down

You can drill-down into the details of each row displayed in the Activity table. This allows you to see detailed information about the attack and review its history as well as to further investigate the attack.

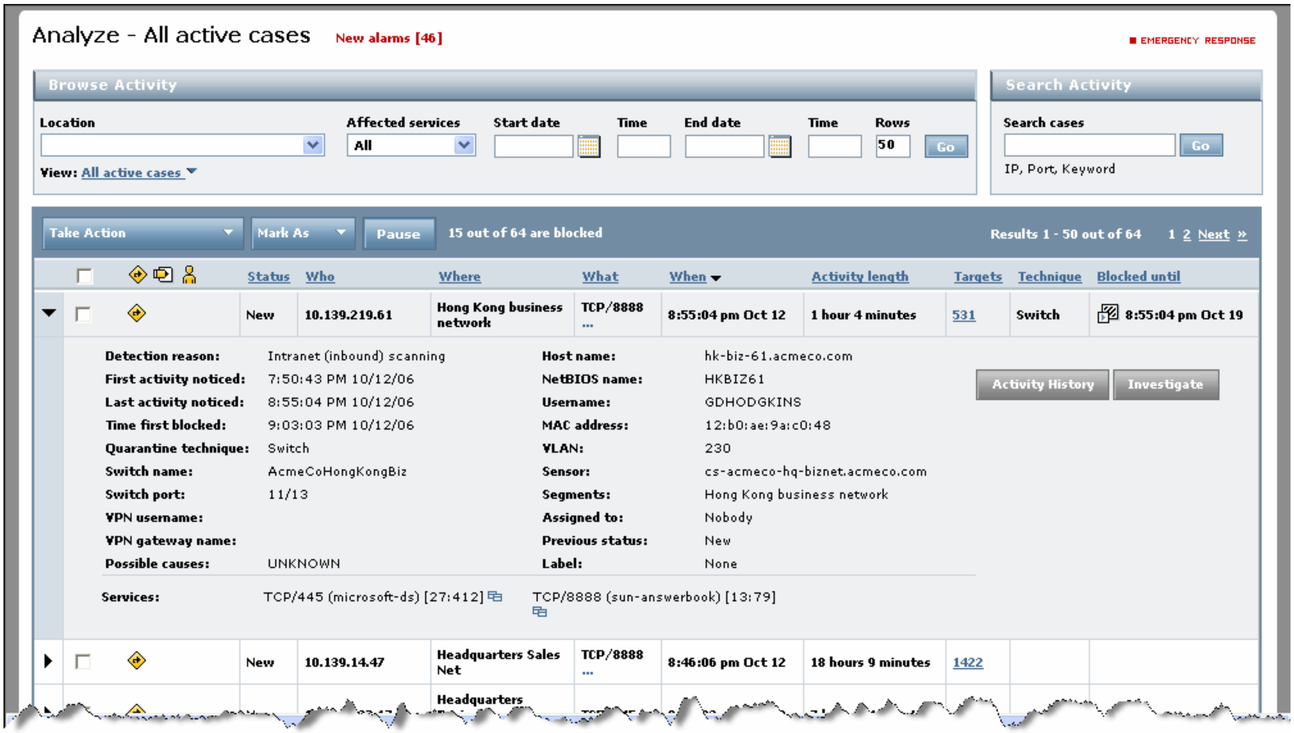
To drill-down on a machine:

1. Select **Analyze** from the Main Toolbar.

   The Analyze screen is displayed.

2. Click ▸ next to the desired machine in the Activity table.

   The Analyze screen displays data about the incident and provides more information about the observed activity.



			Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
▾	□		New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19
▸	□		New	10.139.14.47	Headquarters Sales Net	TCP/8888 ...	8:46:06 pm Oct 12	18 hours 9 minutes	1422		
					Headquarters						

Detection reason: Intranet (inbound) scanning
First activity noticed: 7:50:43 PM 10/12/06
Last activity noticed: 8:55:04 PM 10/12/06
Time first blocked: 9:03:03 PM 10/12/06
Quarantine technique: Switch
Switch name: AcmeCoHongKongBiz
Switch port: 11/13
VPN username:
VPN gateway name:
Possible causes: UNKNOWN

Host name: hk-biz-61.acmeco.com
NetBIOS name: HKBIZ61
Username: GDHODGKINS
MAC address: 12:b0:ae:9a:c0:48
VLAN: 230
Sensor: cs-acmeco-hq-biznet.acmeco.com
Segments: Hong Kong business network
Assigned to: Nobody
Previous status: New
Label: None

Services: TCP/445 (microsoft-ds) [27:412] TCP/8888 (sun-answerbook) [13:79]

The row fields in the Detailed View table provide additional information about the machine and the observed incident.

Column Heading	Descriptions
Detection Reason	Why the system suspects a problem. Descriptions of detection reasons area listed in “Detection Reason Explanation” on page C-1.
Activity first noticed	Timestamp when the attack was first observed.
Activity last noticed	Timestamp when the attack was last observed.
Time first blocked	Timestamp when the blocking or quarantining action was implemented.

Column Heading	Descriptions
Quarantine technique	List of the software and/or hardware blocking actions that were implemented.
Switch Name	The name of the affected switch and its port.
Switch Port	
Attack	Attack name, if the name is available.
Host name	Machine that is affected by the attack.
Mac Address	The MAC address.
VLAN	If available, the ID number of the VLAN.
Previous Status	The last assigned workflow status.
Assigned to	Security personnel responsible for monitoring or remediating the machine or service.
Sensor	Name of the sensor which observed the attack.
Label	If available, an identification statement. Labels are created by users via the Take Action pulldown menu.
Services	List of affected ports/services. Clicking on the link next to services invokes a new browser window that provides more information about threats to that service.

Taking Action On Attacks

CounterStorm-1 applies active responses to stop attack propagation, such as quarantining infected hosts and notifying users of attacks. You can configure actions on attacks by policy (as described in “Configuring Policies” on page 10-2) or you can select specific attacks in the Activity table and apply specific actions. This feature is also available from the Investigate screens.

To manually implement active responses to attacks:

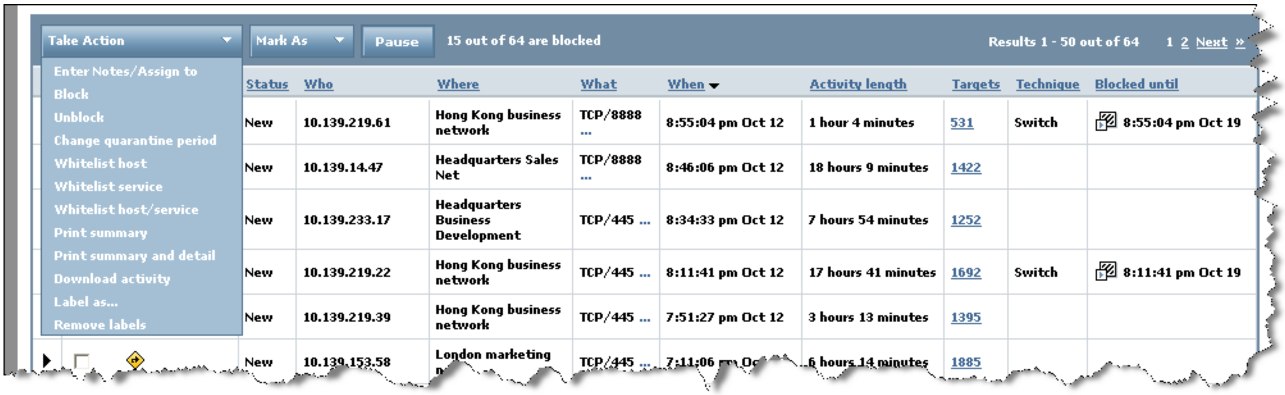
1. Select **Analyze** from the Main Toolbar.

   The Analyze screen is displayed.

2. Select a machine from the Activity table by checking the **Select** checkbox in its row.

Analyzing Attack Activity

3. Click the arrow on the Take Action pulldown and select the desired operation.



15 out of 64 are blocked

Results 1 - 50 out of 64 1 2 Next »

Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19
New	10.139.14.47	Headquarters Sales Net	TCP/8888 ...	8:46:06 pm Oct 12	18 hours 9 minutes	1422		
New	10.139.233.17	Headquarters Business Development	TCP/445 ...	8:34:33 pm Oct 12	7 hours 54 minutes	1252		
New	10.139.219.22	Hong Kong business network	TCP/445 ...	8:11:41 pm Oct 12	17 hours 41 minutes	1692	Switch	8:11:41 pm Oct 19
New	10.139.219.39	Hong Kong business network	TCP/445 ...	7:51:27 pm Oct 12	3 hours 13 minutes	1395		
New	10.139.153.58	London marketing	TCP/445 ...	7:11:06 pm Oc	6 hours 14 minutes	1885		

Action	Enables you to
Enter notes/ Assign to	Record comments about remediation actions and delegate tasks to security personnel. You can mark the activity New, Open, Fixed, Resolved, or Won’t Fix. You can assign the activity to personnel and label it. This workflow is optional. Items marked closed are removed from the activity listing but can be searched and displayed. You can view closed items via the View pulldown. It is helpful to close items in order to unclutter your activity table display.
Block	Quarantine a machine or service according to a previously configured policy.
Unblock	Remove a machine or service from quarantine, thus allowing it to access the rest of the network.
Change quarantine period	Change how long a machine or service will be blocked from the rest of the network.
Whitelist Host	Place the machine on the whitelist, which exempts the specified machine from blocking policies.
Whitelist Host/ Service	Place the machine and/or service on the whitelist, which exempts the specified machine and/or service from blocking policies.
Whitelist Service	Place the service on the whitelist, which exempts the specified service from blocking policies.
Print Summary	Print a summary for selected rows.
Print Summary and Detail	Print expanded detail for selected rows.
Download activity	Download a CSV file for the selected rows.
Label As	Select a label. Labels can be applied to multiple rows in the activity. Click the checkbox for the desired rows and then select the label option from the pulldown. You can enter a letter in the Label window and the list of labels starting with that letter are populated in the label pulldown.
New Label	Create a new label.

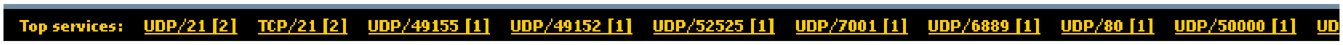
For each action, a popup window appears.

4. Enter the desired information and click on the desired action button to complete the operation.

The action is implemented and you are returned to the activity table. For more information on whitelists, see “Creating the Whitelist” on page 12-4.

Top 10 Services

The top 10 most affected services are listed at the bottom of the activity table. This is a quick way to get current highly affected services.



Top services: UDP/21 [2] TCP/21 [2] UDP/49155 [1] UDP/49152 [1] UDP/52525 [1] UDP/7001 [1] UDP/6889 [1] UDP/80 [1] UDP/50000 [1] UD

These same services may be browsed by selecting the service in the Browse Activity area.

Chapter 7: Investigating Attack Activity

This section explains how to use CounterStorm-1's Investigate capability. The investigate module provides in-depth information about attack activity. You can access this information via the **Activity History** and **Investigate** buttons in each row of the Activity table. The investigate screen displays information about the selected row. You can scroll through machines on that segment using the **Previous machine** and **Next machine** links in the upper-right corner of the screen. The **Take Action** and **Mark as** pulldowns are also available and work as described in "Marking Activity" on page 6-4 and "Taking Action On Attacks" on page 6-7, respectively.

In This Chapter

Infection Details

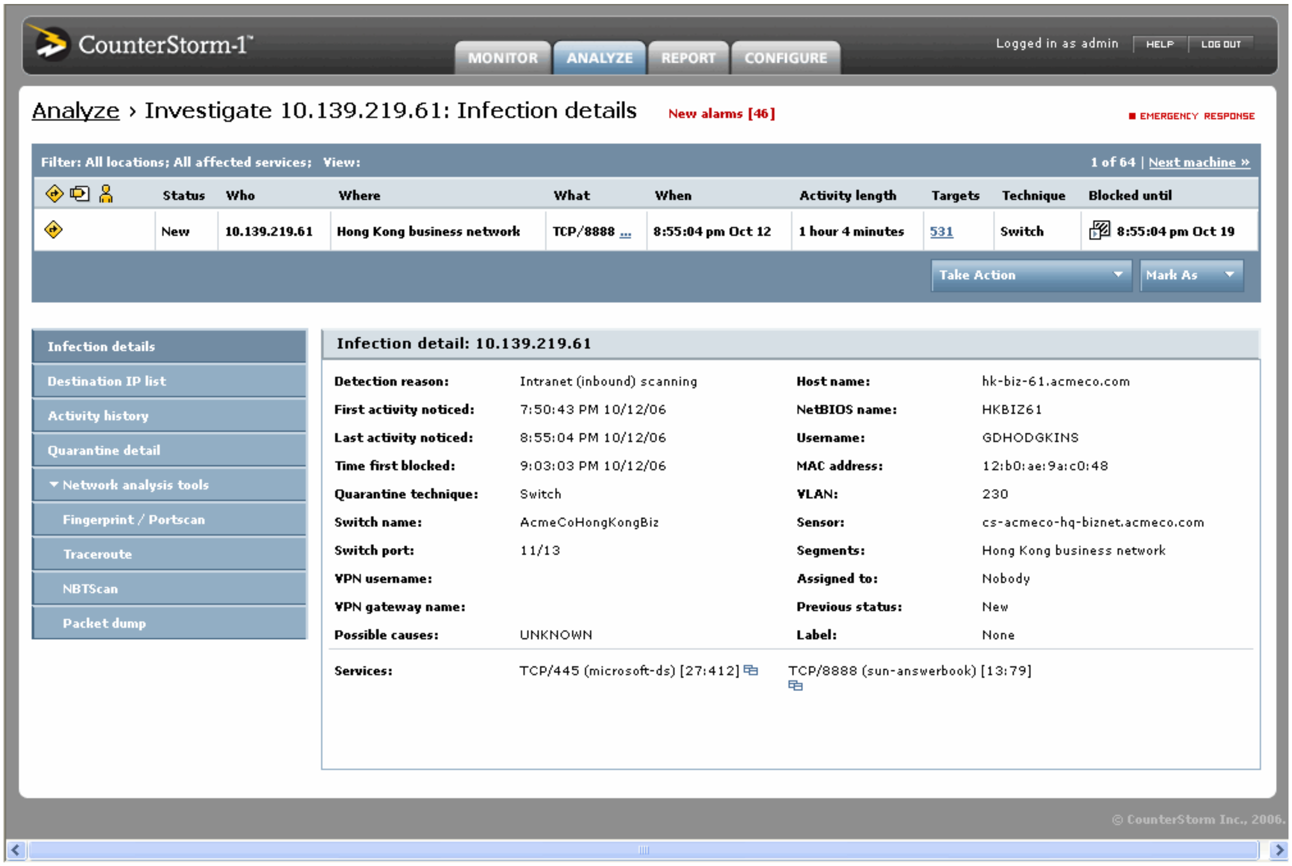
The Infection Details screen provides all known information about the infection.

To access Infection details:

1. Select **Analyze** from the Main Toolbar.

   The Activity screen is displayed.
2. Expand the desired row.
3. Click **Investigate**.

The Investigate screen appears with Infection Details selected.



Analyze › Investigate 10.139.219.61: Infection details

Filter: All locations; All affected services; View:

	Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
	New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19

Infection detail: 10.139.219.61

Detection reason:	Intranet (inbound) scanning	Host name:	hk-biz-61.acmeco.com
First activity noticed:	7:50:43 PM 10/12/06	NetBIOS name:	HKBIZ61
Last activity noticed:	8:55:04 PM 10/12/06	Username:	GDHODGKINS
Time first blocked:	9:03:03 PM 10/12/06	MAC address:	12:b0:ae:9a:c0:48
Quarantine technique:	Switch	VLAN:	230
Switch name:	AcmeCoHongKongBiz	Sensor:	cs-acmeco-hq-biznet.acmeco.com
Switch port:	11/13	Segments:	Hong Kong business network
VPN username:		Assigned to:	Nobody
VPN gateway name:		Previous status:	New
Possible causes:	UNKNOWN	Label:	None
Services:	TCP/445 (microsoft-ds) [27:412]	TCP/8888 (sun-answerbook) [13:79]	

4. View the desired information.

Destination IP List

The Destination IP list provides a list of machines the attack is targeting. It lists the total number of targets, the list of successful connections within and outside of configured segments, and the list of failed connections. You can download the successful or failed connection list to a CSV file. Only those lists that contain data can be downloaded. You can search the connections by IP address.

You can open this file in any spreadsheet program, such as Microsoft Excel, and view the IP addresses of machines the attacker has communicated with. The list includes IP addresses of ports which were not listed in the incident entry, but which have some minor level of attack activity. An **F** indicates that the attack could not communicate with the machine. A **T** indicates that the communication was successful and therefore that infection is possible. This file lists up to 1000 targets.

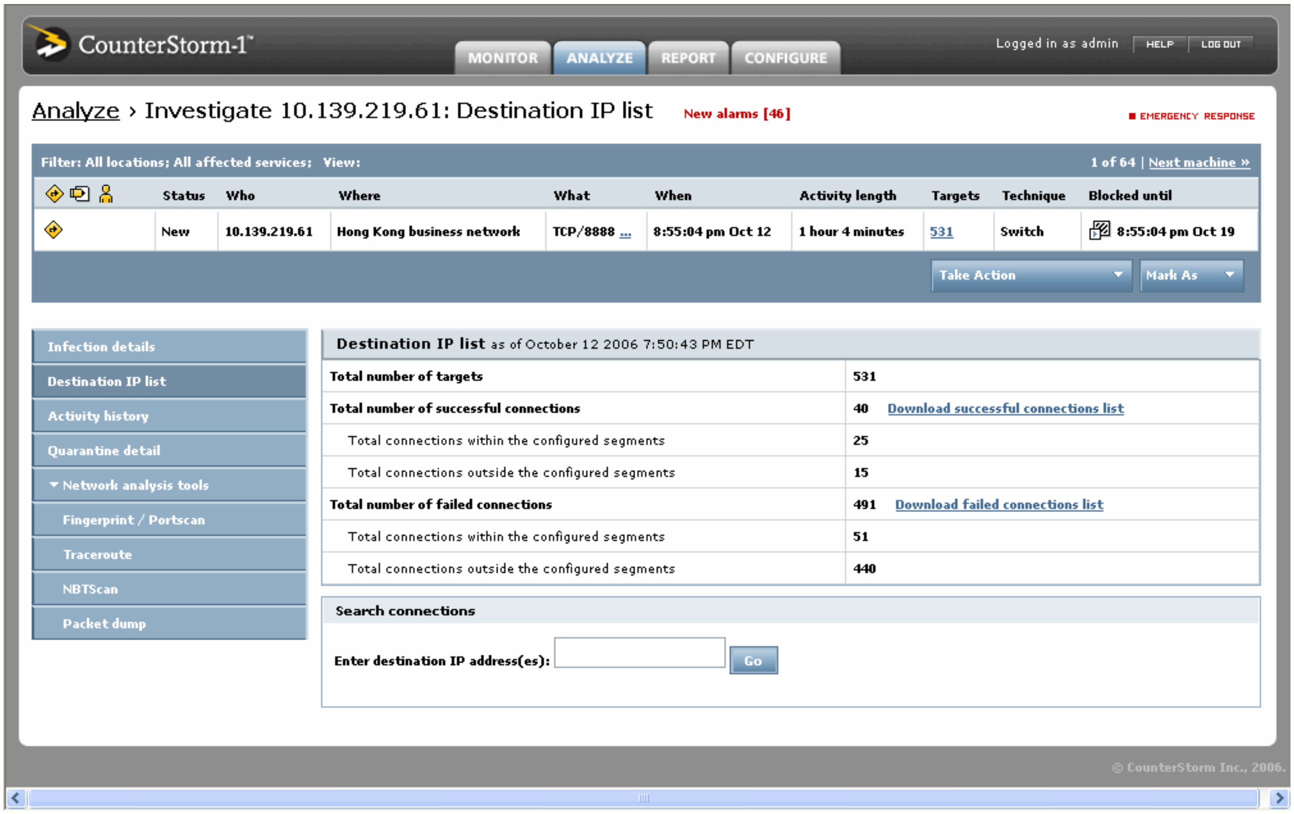
Note: The number of targets is an estimate. The actual number may be larger.

To access the Destination IP list:

1. Select **Analyze** from the Main Toolbar.

   The Activity screen is displayed.
2. Expand the desired row.
3. Click **Investigate**.

   The Investigate screen appears with Infection Details selected.
4. Click **Destination IP list.**



Analyze › Investigate 10.139.219.61: Destination IP list New alarms [46]

Filter: All locations; All affected services; View: 1 of 64 | Next machine »

Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19

Destination IP list as of October 12 2006 7:50:43 PM EDT

Total number of targets	531	
Total number of successful connections	40	Download successful connections list
Total connections within the configured segments	25	
Total connections outside the configured segments	15	
Total number of failed connections	491	Download failed connections list
Total connections within the configured segments	51	
Total connections outside the configured segments	440	

Search connections

Enter destination IP address(es):

5. View the desired information.

   You can enter comma-separated IP addresses in the **Search Connections** box to search the target list for connections.

Activity History

You can view the history of activity for the desired row.

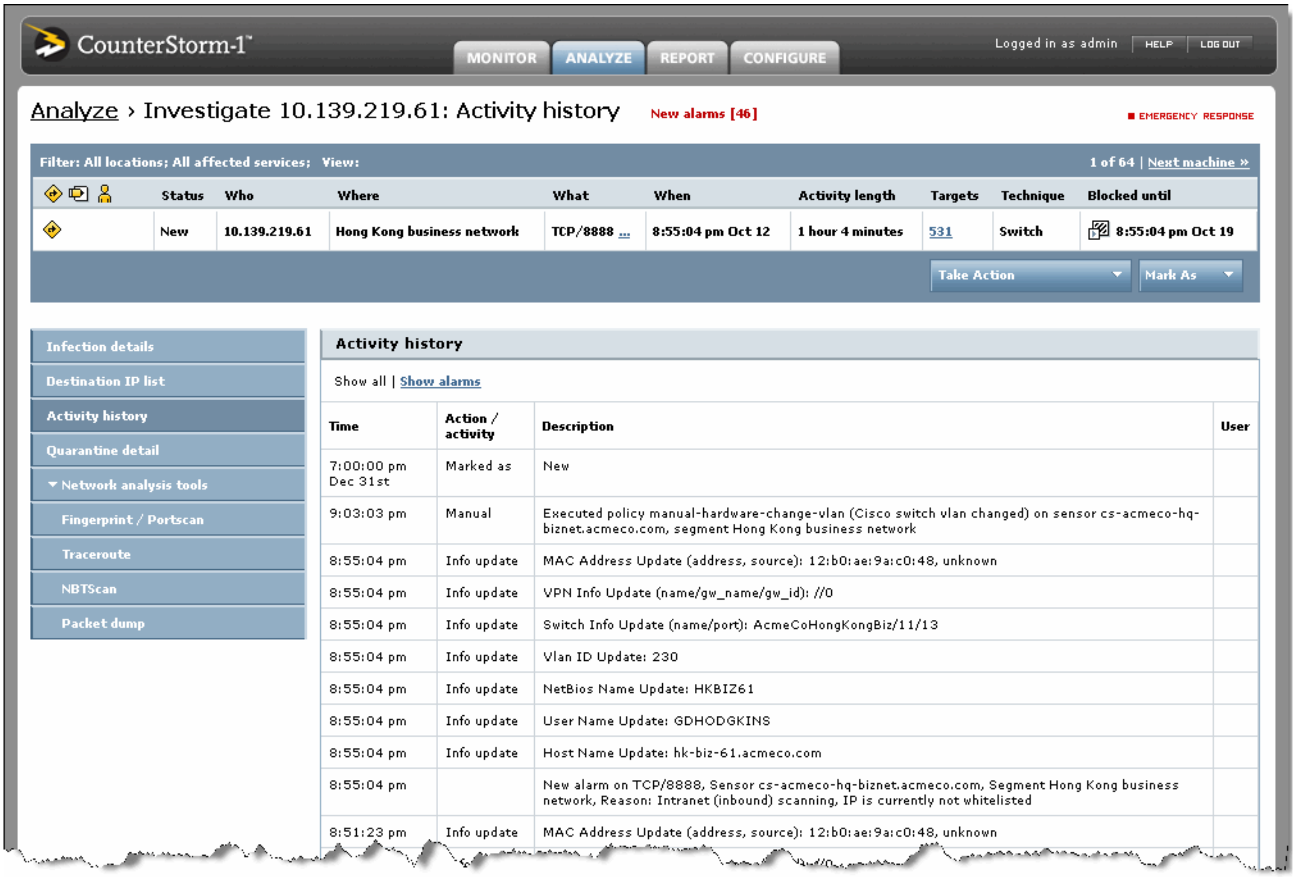
To view activity history:

1. Select **Analyze** from the Main Toolbar.

   The Activity screen is displayed.
2. Expand the desired row.
3. Click **Activity History**.

Investigating Attack Activity

The Investigate screen appears with Activity History selected.



Analyze › Investigate 10.139.219.61: Activity history

Filter: All locations; All affected services; View:

	Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
	New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19

Activity history

Show all | Show alarms

Time	Action / activity	Description	User
7:00:00 pm Dec 31st	Marked as	New	
9:03:03 pm	Manual	Executed policy manual-hardware-change-vlan (Cisco switch vlan changed) on sensor cs-acmeco-hq-biznet.acmeco.com, segment Hong Kong business network	
8:55:04 pm	Info update	MAC Address Update (address, source): 12:b0:ae:9a:c0:48, unknown	
8:55:04 pm	Info update	VPN Info Update (name/gw_name/gw_id): //0	
8:55:04 pm	Info update	Switch Info Update (name/port): AcmeCoHongKongBiz/11/13	
8:55:04 pm	Info update	Vlan ID Update: 230	
8:55:04 pm	Info update	NetBios Name Update: HKBIZ61	
8:55:04 pm	Info update	User Name Update: GDHODGKINS	
8:55:04 pm	Info update	Host Name Update: hk-biz-61.acmeco.com	
8:55:04 pm		New alarm on TCP/8888, Sensor cs-acmeco-hq-biznet.acmeco.com, Segment Hong Kong business network, Reason: Intranet (inbound) scanning, IP is currently not whitelisted	
8:51:23 pm	Info update	MAC Address Update (address, source): 12:b0:ae:9a:c0:48, unknown	

4. View the desired information.

   You can view information about all activity or about alarm activity only by toggling between the **Show All** and **Show Alarms** links.

Quarantine Detail

The Quarantine Detail feature provides details about the actions taken to quarantine the infection.

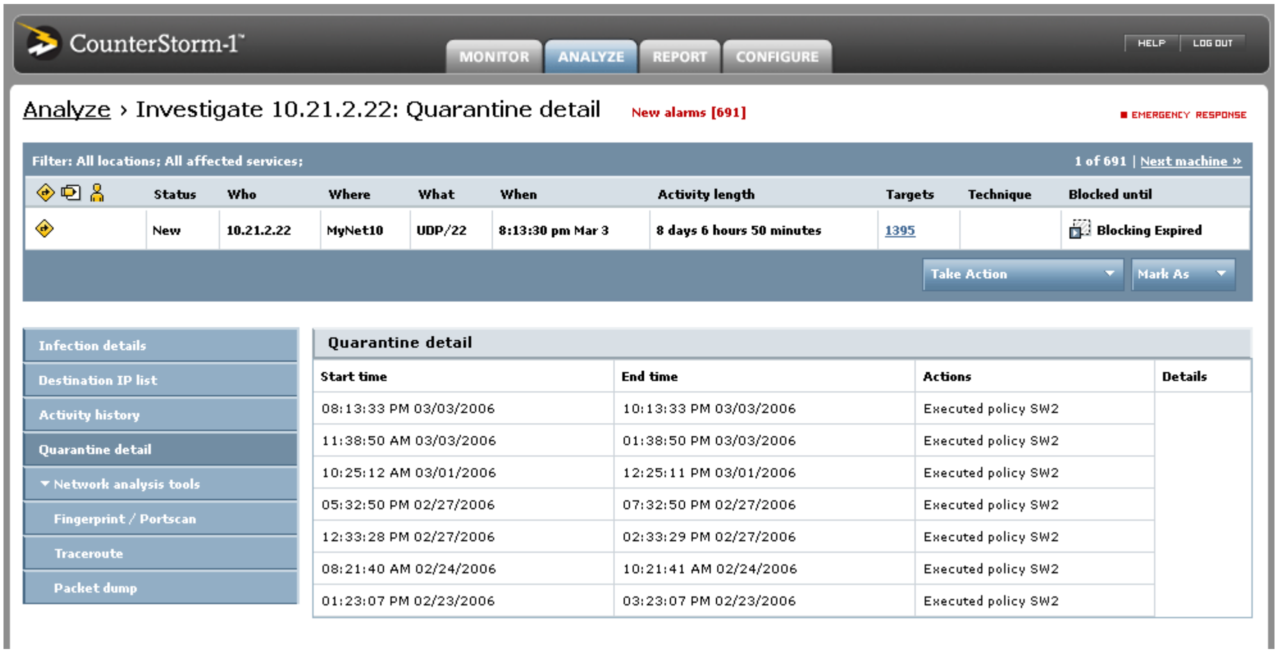
To access the Quarantine detail:

1. Select **Analyze** from the Main Toolbar.

   The Activity screen is displayed.
2. Expand the desired row.
3. Click **Investigate**.

   The Investigate screen appears with Infection Details selected.

4. Click **Quarantine Detail**.



Analyze › Investigate 10.21.2.22: Quarantine detail

Filter: All locations; All affected services;

Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
New	10.21.2.22	MyNet10	UDP/22	8:13:30 pm Mar 3	8 days 6 hours 50 minutes	1395		Blocking Expired

Quarantine detail

Start time	End time	Actions	Details
08:13:33 PM 03/03/2006	10:13:33 PM 03/03/2006	Executed policy SW2	
11:38:50 AM 03/03/2006	01:38:50 PM 03/03/2006	Executed policy SW2	
10:25:12 AM 03/01/2006	12:25:11 PM 03/01/2006	Executed policy SW2	
05:32:50 PM 02/27/2006	07:32:50 PM 02/27/2006	Executed policy SW2	
12:33:28 PM 02/27/2006	02:33:29 PM 02/27/2006	Executed policy SW2	
08:21:40 AM 02/24/2006	10:21:41 AM 02/24/2006	Executed policy SW2	
01:23:07 PM 02/23/2006	03:23:07 PM 02/23/2006	Executed policy SW2	

5. View the desired information.

Network Analysis Tools

A variety of network analysis tools are available. New tools are added as they become available. You can review previous runs and execute new runs for each tool.

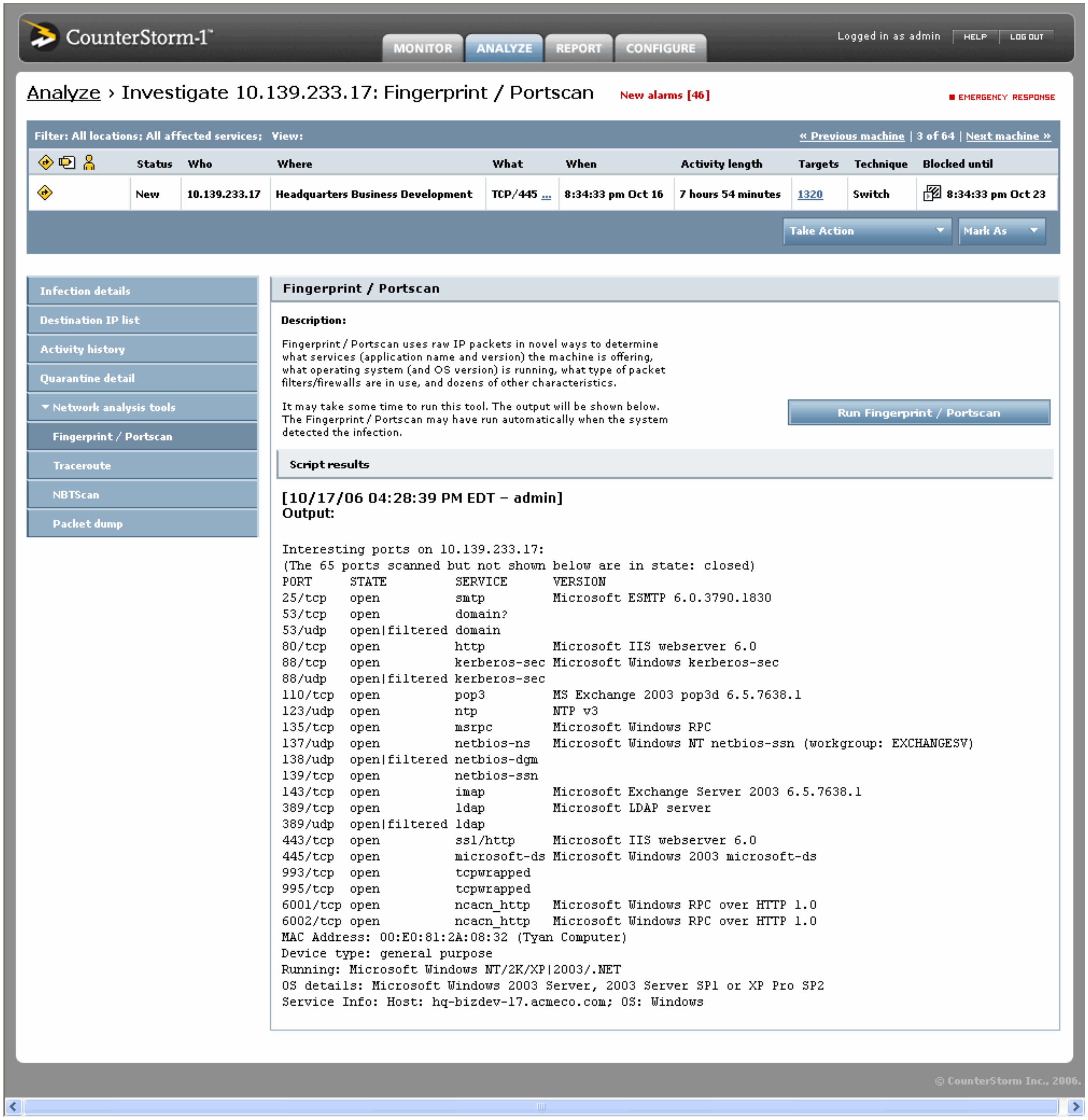
Fingerprint/PortScan

This option displays fingerprint/portscan information based on running nmap. Fingerprint/Portscan uses raw IP packets in novel ways to determine what services (application name and version) the machine is offering, what operating system (and OS version) is running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Fingerprint/Portscan is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Fingerprint/Portscan cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to probes, but Fingerprint/Portscan cannot determine whether they are open or closed. Fingerprint/Portscan reports the state combinations open/filtered and closed/

filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested.

It may take some time to run this tool. The output will be shown below. The Fingerprint/ Portscan may have run automatically when the system detected the infection.



	Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
	New	10.139.233.17	Headquarters Business Development	TCP/445 ...	8:34:33 pm Oct 16	7 hours 54 minutes	1320	Switch	8:34:33 pm Oct 23

Fingerprint / Portscan

Description:

Fingerprint / Portscan uses raw IP packets in novel ways to determine what services (application name and version) the machine is offering, what operating system (and OS version) is running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

It may take some time to run this tool. The output will be shown below. The Fingerprint / Portscan may have run automatically when the system detected the infection.

Script results

[10/17/06 04:28:39 PM EDT – admin]
Output:

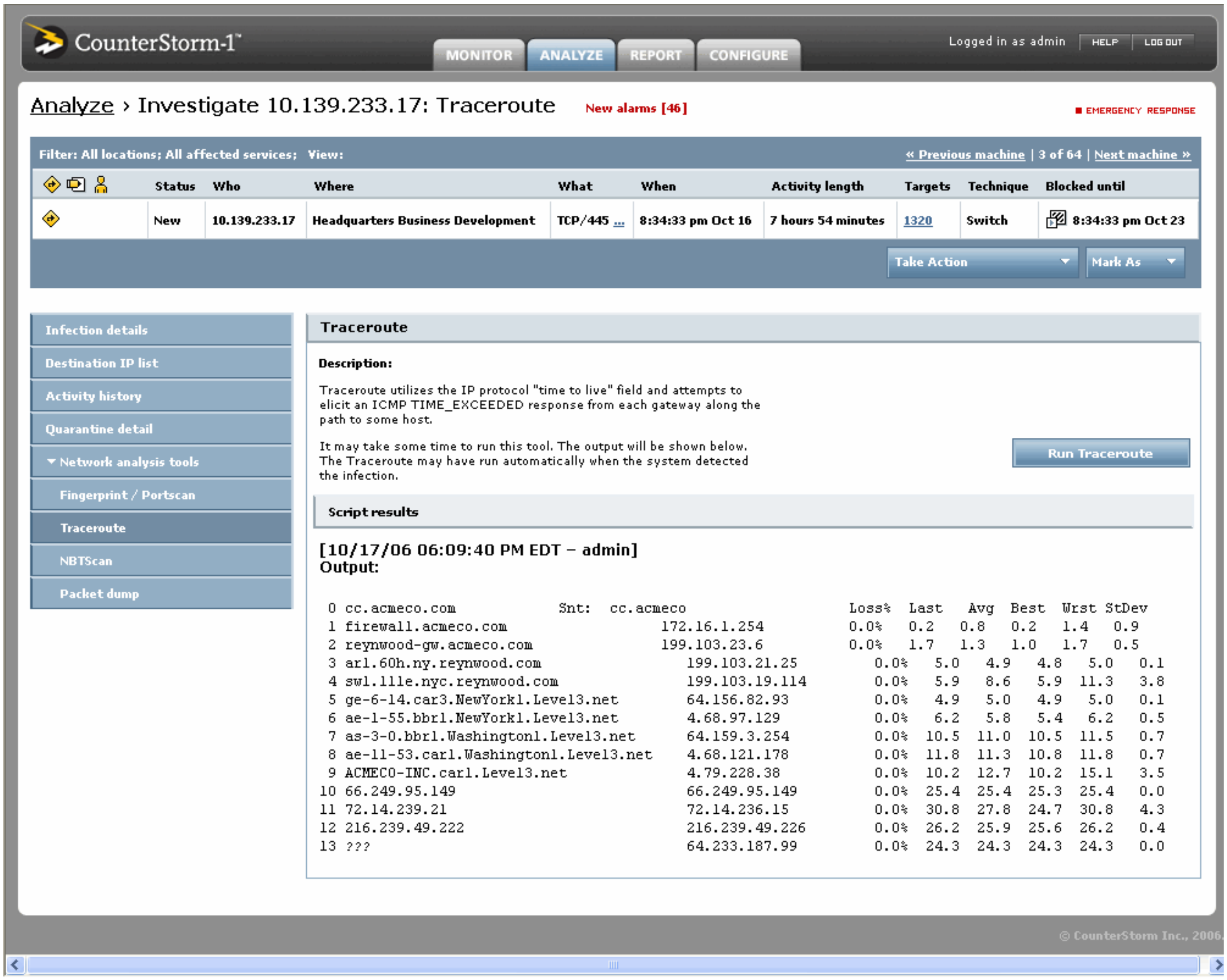
```
Interesting ports on 10.139.233.17:
(The 65 ports scanned but not shown below are in state: closed)
PORT     STATE         SERVICE      VERSION
25/tcp   open          smtp         Microsoft ESMTP 6.0.3790.1830
53/tcp   open          domain?
53/udp   open|filtered domain
80/tcp   open          http         Microsoft IIS webserver 6.0
88/tcp   open          kerberos-sec Microsoft Windows kerberos-sec
88/udp   open|filtered kerberos-sec
110/tcp  open          pop3         MS Exchange 2003 pop3d 6.5.7638.1
123/udp  open          ntp          NTP v3
135/tcp  open          msrpc        Microsoft Windows RPC
137/udp  open          netbios-ns   Microsoft Windows NT netbios-ssn (workgroup: EXCHANGESV)
138/udp  open|filtered netbios-dgm
139/tcp  open          netbios-ssn
143/tcp  open          imap         Microsoft Exchange Server 2003 6.5.7638.1
389/tcp  open          ldap         Microsoft LDAP server
389/udp  open|filtered ldap
443/tcp  open          ssl/http     Microsoft IIS webserver 6.0
445/tcp  open          microsoft-ds Microsoft Windows 2003 microsoft-ds
993/tcp  open          tcpwrapped
995/tcp  open          tcpwrapped
6001/tcp open          ncacn_http   Microsoft Windows RPC over HTTP 1.0
6002/tcp open          ncacn_http   Microsoft Windows RPC over HTTP 1.0
MAC Address: 00:E0:81:2A:08:32 (Tyan Computer)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP|2003/.NET
OS details: Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2
Service Info: Host: hq-bizdev-17.acmeco.com; OS: Windows
```

Note: This tool may return no output if it is unable to reach an IP address due to quarantine blocking.

Traceroute

The Internet is a large and complex aggregation of network hardware that is connected together by gateways. Tracking the route your packets follow (or finding the miscreant gateway that is discarding your packets) can be difficult. Traceroute records the route (the specific gateway computers at each hop) through the destination computer. Traceroute can help you understand where problems are in the network. Traceroute utilizes the IP protocol “time to live” field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

It may take some time to run this tool. The output is shown in script results. The Traceroute may have run automatically when the system detected the infection.



Analyze › Investigate 10.139.233.17: Traceroute

Filter: All locations; All affected services; View:

Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
New	10.139.233.17	Headquarters Business Development	TCP/445 ...	8:34:33 pm Oct 16	7 hours 54 minutes	1320	Switch	8:34:33 pm Oct 23

Traceroute

Description:

Traceroute utilizes the IP protocol "time to live" field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

It may take some time to run this tool. The output will be shown below. The Traceroute may have run automatically when the system detected the infection.

Script results

[10/17/06 06:09:40 PM EDT – admin]
Output:

```
 0 cc.acmeco.com            Snt:  cc.acmeco                    Loss%  Last   Avg  Best  Wrst StDev
 1 firewall.acmeco.com                172.16.1.254             0.0%   0.2   0.8   0.2   1.4   0.9
 2 reynwood-gw.acmeco.com             199.103.23.6             0.0%   1.7   1.3   1.0   1.7   0.5
 3 arl.60h.ny.reynwood.com               199.103.21.25            0.0%   5.0   4.9   4.8   5.0   0.1
 4 swl.llle.nyc.reynwood.com             199.103.19.114           0.0%   5.9   8.6   5.9  11.3   3.8
 5 ge-6-14.car3.NewYorkl.Level3.net      64.156.82.93             0.0%   4.9   5.0   4.9   5.0   0.1
 6 ae-1-55.bbrl.NewYorkl.Level3.net      4.68.97.129              0.0%   6.2   5.8   5.4   6.2   0.5
 7 as-3-0.bbrl.Washingtonl.Level3.net    64.159.3.254             0.0%  10.5  11.0  10.5  11.5   0.7
 8 ae-11-53.carl.Washingtonl.Level3.net  4.68.121.178             0.0%  11.8  11.3  10.8  11.8   0.7
 9 ACMECO-INC.carl.Level3.net            4.79.228.38              0.0%  10.2  12.7  10.2  15.1   3.5
10 66.249.95.149                         66.249.95.149            0.0%  25.4  25.4  25.3  25.4   0.0
11 72.14.239.21                          72.14.236.15             0.0%  30.8  27.8  24.7  30.8   4.3
12 216.239.49.222                        216.239.49.226           0.0%  26.2  25.9  25.6  26.2   0.4
13 ???                                   64.233.187.99            0.0%  24.3  24.3  24.3  24.3   0.0
```

Note: This tool may return no output if it is unable to reach an IP address due to quarantine blocking

Packet Dump

This option allows you to prepare the packet data for download. You can request a quick or a detailed download.

During a quick download, CounterStorm-1 collects all the packets for the most recent alarms on each alarmed port within that time frame. This packet capture is restricted to alarmed services, DNS, ARP, and ICMP traffic.

During a detailed download, CounterStorm-1 collects all packets for the infected IP address in that time frame. Depending on the size of the time frame, detailed downloads can take over an hour to complete.

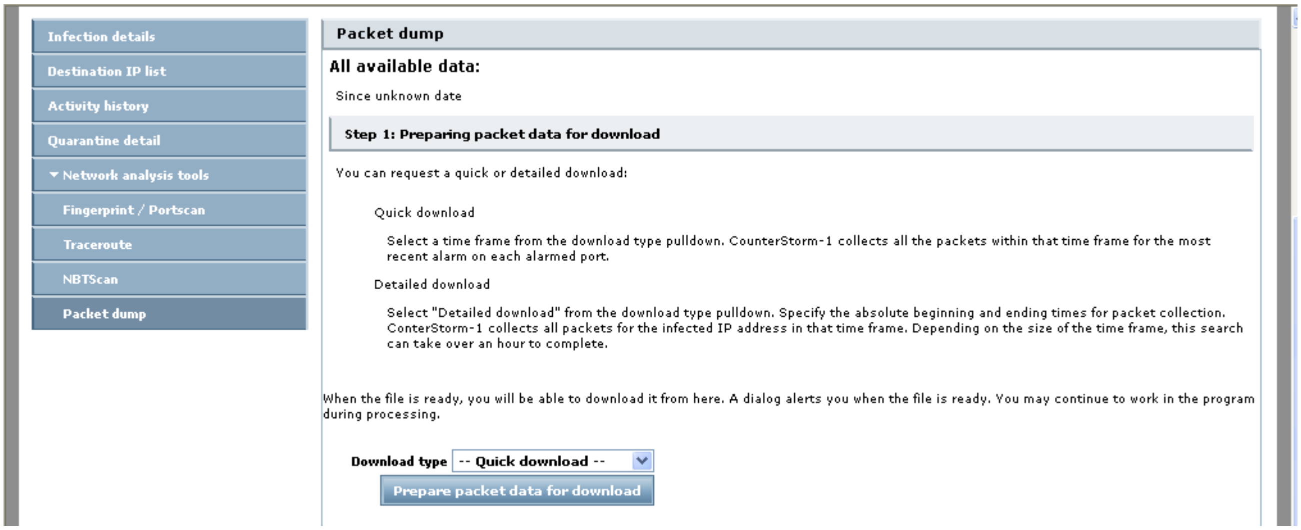
When the file is ready, you can to download it from this screen. A dialog alerts you when the file is ready. You may continue to work in the program during processing.

To download packet data:

1. Select **Analyze** from the Main Toolbar.

   The Activity screen is displayed.
2. Expand the desired row.
3. Click **Investigate**.

   The Investigate screen appears with Infection Details selected.
4. Click **Packet Dump**.
5. Enter the desired information in Step 1.



Packet dump

All available data:

Since unknown date

Step 1: Preparing packet data for download

You can request a quick or detailed download:

Quick download

Select a time frame from the download type pulldown. CounterStorm-1 collects all the packets within that time frame for the most recent alarm on each alarmed port.

Detailed download

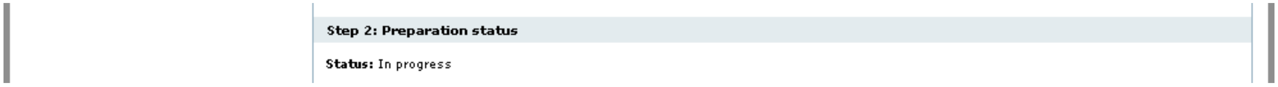
Select "Detailed download" from the download type pulldown. Specify the absolute beginning and ending times for packet collection. ConterStorm-1 collects all packets for the infected IP address in that time frame. Depending on the size of the time frame, this search can take over an hour to complete.

When the file is ready, you will be able to download it from here. A dialog alerts you when the file is ready. You may continue to work in the program during processing.

Download type -- Quick download --

For quick download, select a time frame from the download type pulldown. Select **Detailed download** from the download type pulldown for detailed download. Specify the absolute beginning and ending times for which data is to be collected.

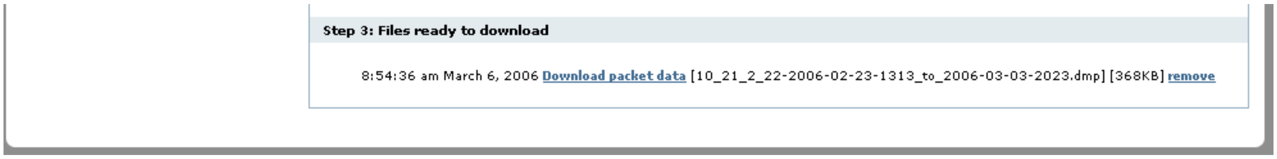
6. Click **Prepare Packet Data for download**.
7. View the desired status in step 2.



Step 2: Preparation status

Status: In progress

When the file is ready, you are notified via a pop-up message and the file is displayed and available for download in step 3. You can continue working in CounterStorm-1 while the file is processing.

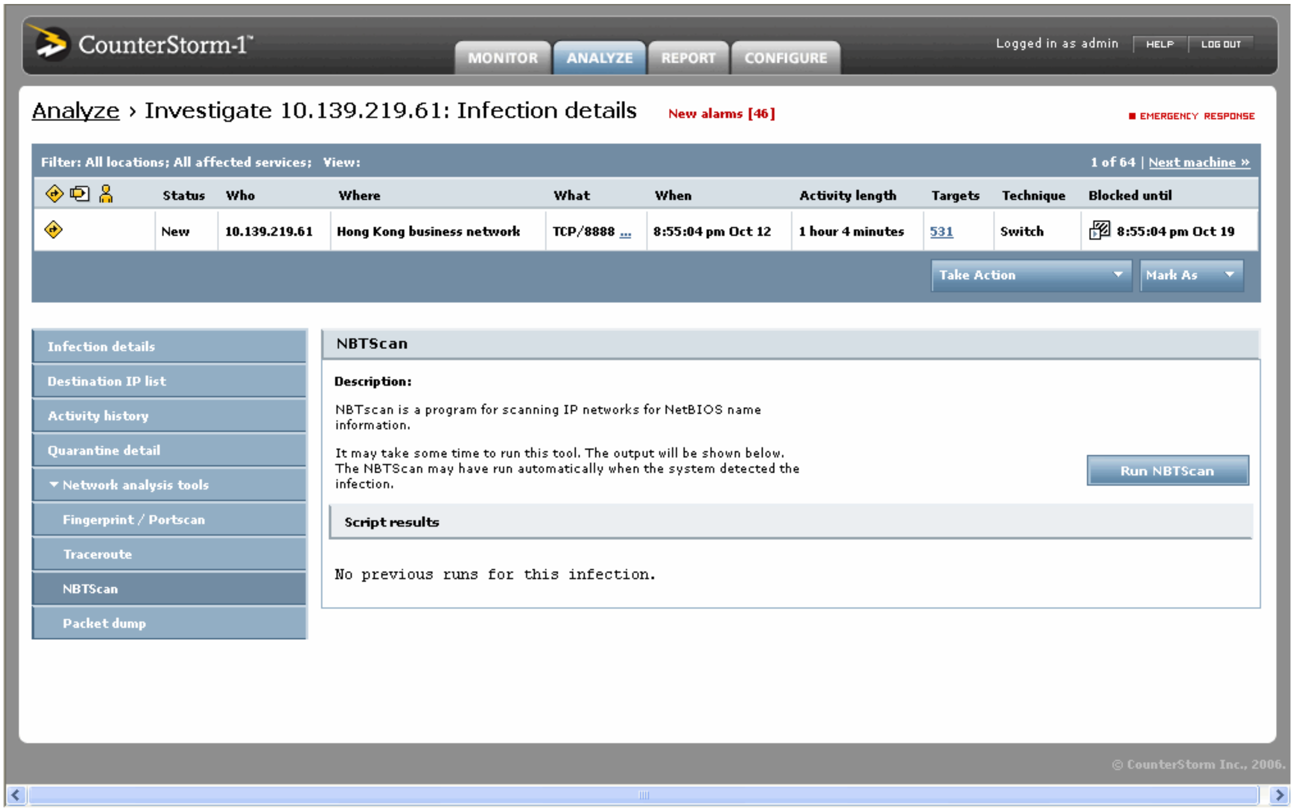


Step 3: Files ready to download

8:54:36 am March 6, 2006 Download packet data [10_21_2_22-2006-02-23-1313_to_2006-03-03-2023.dmp] [368KB] remove

NBTScan

NBTScan is a program for scanning IP networks for NetBIOS name information. It may take some time to run this tool. The output is shown in script results. The NBTScan may have run automatically when the system detected the infection.



Analyze › Investigate 10.139.219.61: Infection details New alarms [46]

Filter: All locations; All affected services; View: 1 of 64 | Next machine »

	Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
◈	New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19

NBTScan

Description:

NBTscan is a program for scanning IP networks for NetBIOS name information.

It may take some time to run this tool. The output will be shown below. The NBTScan may have run automatically when the system detected the infection.

Script results

```
No previous runs for this infection.
```

Note: This tool may return no output if it is unable to reach an IP address due to quarantine blocking.

Chapter 8: Operating Modes

You can work in any of three operational modes: normal, emergency, or non-blocking. In normal mode, infections in segments with appropriately configured policies have quarantine techniques applied to them. CounterStorm-1 should be in normal mode most often. Switch to emergency or non-blocking mode in special scenarios, and then back to normal mode once the threat has been neutralized.

Your current mode is listed in the upper right corner of the Activity table.

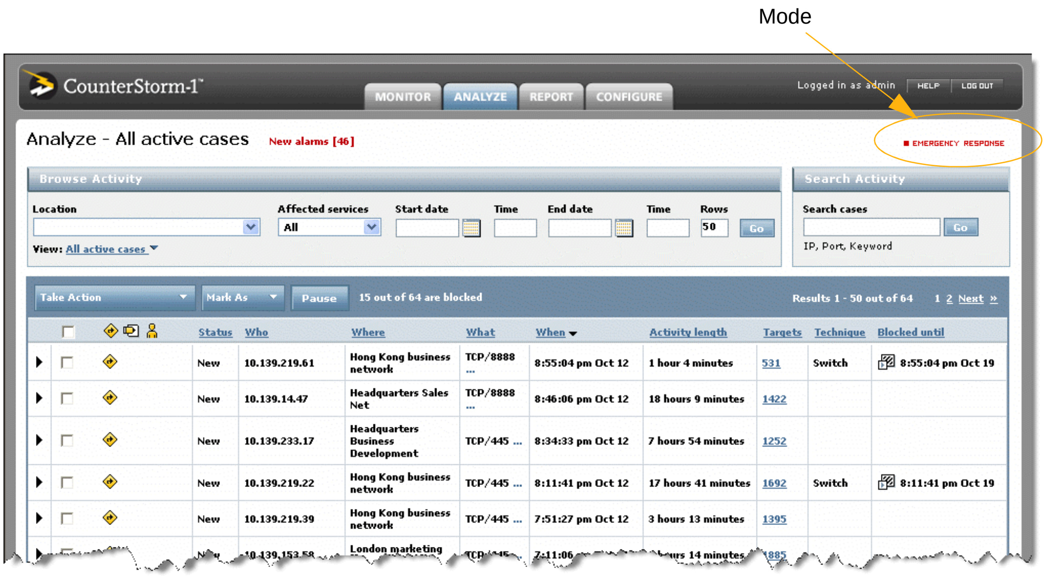
In This Chapter

- Normal Mode
- Non-blocking Mode
- Emergency Mode

To switch modes:

1. Select **Analyze** from the Main Toolbar.

   The Analyze screen is displayed.



Analyze - All active cases   New alarms [46]   ■ EMERGENCY RESPONSE

Location:
Affected services: All
Start date:
Time:
End date:
Time:
Rows: 50
View: All active cases

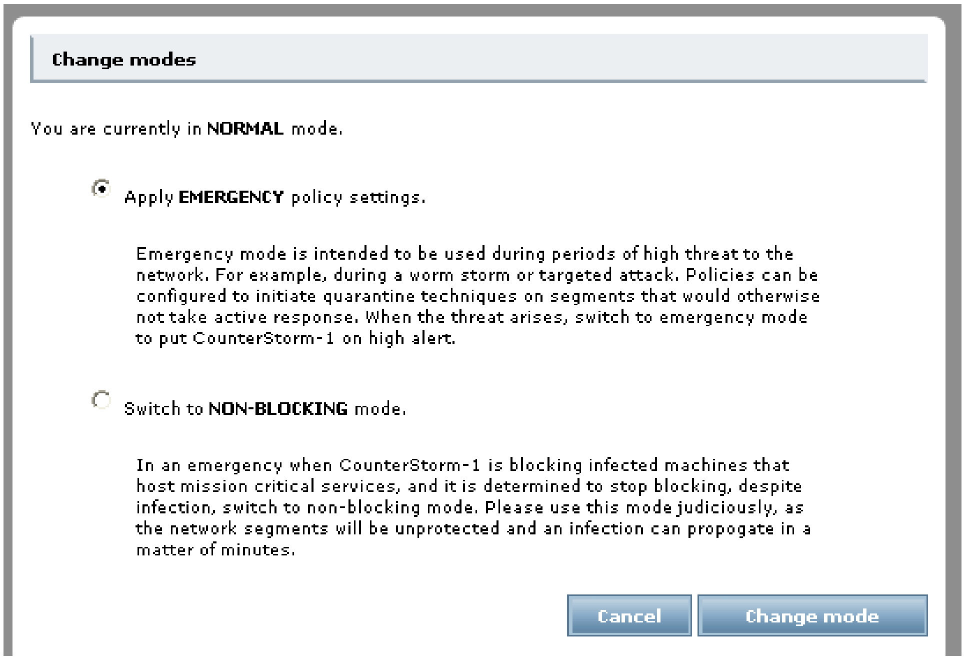
Search cases:
IP, Port, Keyword

15 out of 64 are blocked   Results 1 - 50 out of 64   1 2 Next »

			Status	Who	Where	What	When	Activity length	Targets	Technique	Blocked until
▶	□	◈	New	10.139.219.61	Hong Kong business network	TCP/8888 ...	8:55:04 pm Oct 12	1 hour 4 minutes	531	Switch	8:55:04 pm Oct 19
▶	□	◈	New	10.139.14.47	Headquarters Sales Net	TCP/8888 ...	8:46:06 pm Oct 12	18 hours 9 minutes	1422		
▶	□	◈	New	10.139.233.17	Headquarters Business Development	TCP/445 ...	8:34:33 pm Oct 12	7 hours 54 minutes	1252		
▶	□	◈	New	10.139.219.22	Hong Kong business network	TCP/445 ...	8:11:41 pm Oct 12	17 hours 41 minutes	1692	Switch	8:11:41 pm Oct 19
▶	□	◈	New	10.139.219.39	Hong Kong business network	TCP/445 ...	7:51:27 pm Oct 12	3 hours 13 minutes	1395		
▶			New	10.139.153.58	London marketing	TCP/445 ...	7:11:06	hours 14 minutes	1885		

2. Click on the mode listed in the upper right corner of the Activity table.

A window pops up that allows you to select of the two other modes currently not selected.



Change modes

You are currently in **NORMAL** mode.

● Apply **EMERGENCY** policy settings.

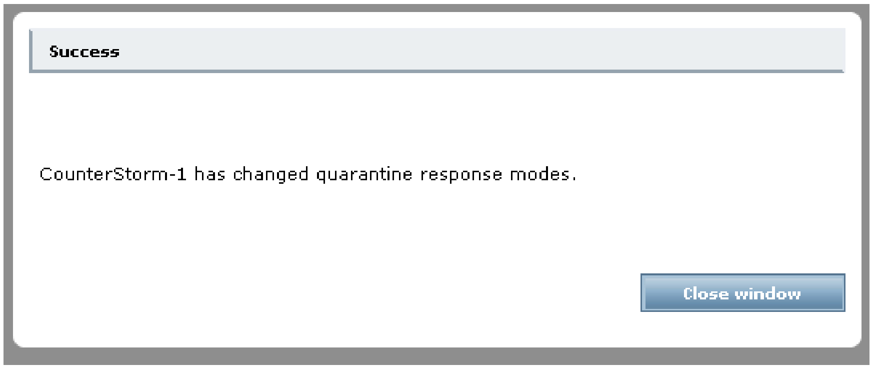
Emergency mode is intended to be used during periods of high threat to the network. For example, during a worm storm or targeted attack. Policies can be configured to initiate quarantine techniques on segments that would otherwise not take active response. When the threat arises, switch to emergency mode to put CounterStorm-1 on high alert.

○ Switch to **NON-BLOCKING** mode.

In an emergency when CounterStorm-1 is blocking infected machines that host mission critical services, and it is determined to stop blocking, despite infection, switch to non-blocking mode. Please use this mode judiciously, as the network segments will be unprotected and an infection can propogate in a matter of minutes.

3. Click the radio button next to the desired mode.
4. Click **Change mode**.

   The mode is changed and a Success message is displayed in the pop up.



Success

CounterStorm-1 has changed quarantine response modes.

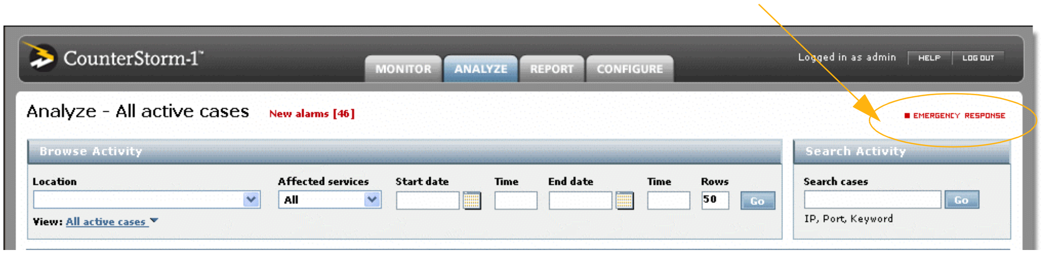
5. Click **Close Window**.

   You are returned to the Analyze screen.

Normal Mode

In normal mode, infections in segments with appropriately configured policies will have standard quarantine techniques applied to them. CounterStorm-1 should be in normal mode most often. Switch to emergency or non-blocking mode during special scenarios, and then back to normal mode once the threat has been neutralized. When you are in normal mode, the Emergency Response button appears in the mode area.

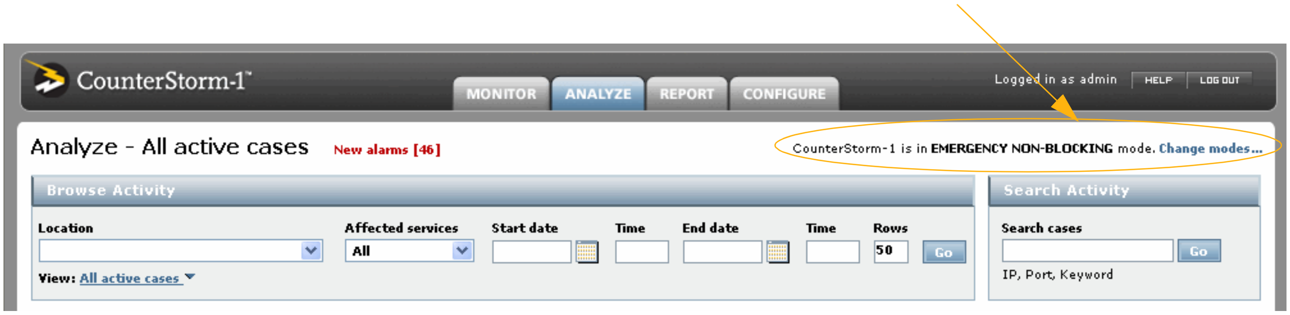
Mode



Non-blocking Mode

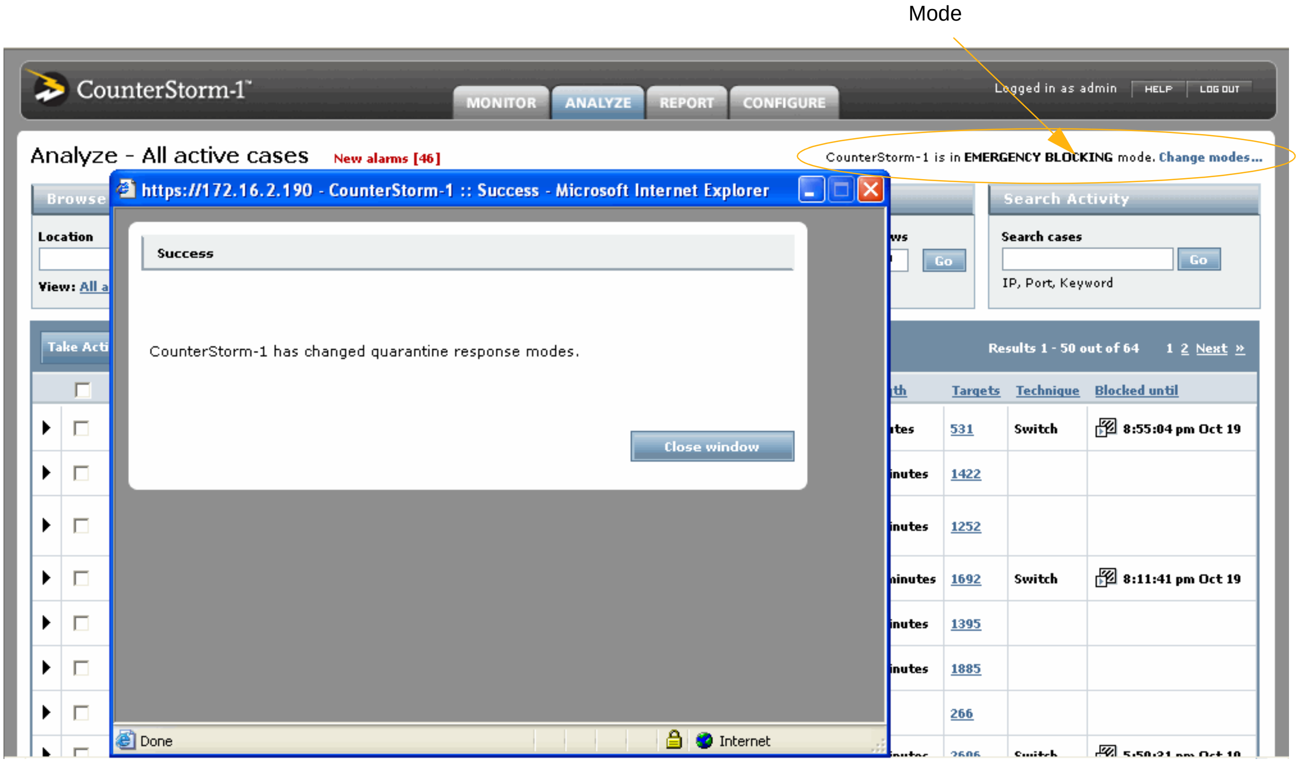
When CounterStorm-1 is blocking infected machines that host mission critical services and you decide to stop blocking, despite infection, switch to non-blocking mode. Please use this mode judiciously, as the network segments are unprotected, and an infection can be propagated in a matter of minutes. From non-blocking mode, you can switch to Normal mode or Emergency mode.

Mode


CounterStorm-1 is in EMERGENCY NON-BLOCKING mode. Change modes...

Emergency Mode

Emergency mode is intended to be used during periods of high threat to the network, such as during a worm storm or a targeted attack. Policies can be configured to initiate quarantine techniques on segments that would otherwise not merit active response. When the threat arises, switch to emergency mode to put CounterStorm-1 on high alert and activate emergency mode policies. From emergency mode, you can switch to normal mode and non-blocking mode.


Mode

Analyze - All active cases New alarms [46]

CounterStorm-1 is in **EMERGENCY BLOCKING** mode. Change modes...

https://172.16.2.190 - CounterStorm-1 :: Success - Microsoft Internet Explorer

Success

CounterStorm-1 has changed quarantine response modes.

Results 1 - 50 out of 64 1 2 Next »

th	Targets	Technique	Blocked until
tes	531	Switch	8:55:04 pm Oct 19
inutes	1422		
inutes	1252		
ninutes	1692	Switch	8:11:41 pm Oct 19
inutes	1395		
inutes	1885		
	266		
inutes	2606	Switch	5:50:31 pm Oct 19

Note: Emergency mode applies from the point at which the mode is activated. It will not block or unblock machines that were blocked or unblocked prior to the mode change.

Chapter 9: Configuring Segments

This section explains how to configure segments. A segment is a group of systems defined by their contiguous IP address range. A segment defines a contiguous range of IP addresses which are expected to have common behavior and that have a common response policy whenever an attack is detected on any of the hosts in that segment.

Note: Whenever you reconfigure your network, you must update your segment configuration. Changes in the network such as e-mail relays (which affect e-mail addresses), SPAN ports, IP addresses, VPN gateways, and switches will affect the operation of segments.

In This Chapter

Understanding Asymmetric Traffic

Routing must be symmetrical (where CounterStorm-1 always sees the reply packet to any query packet, and vice versa) to and from CounterStorm-1 segments. Asymmetric routing (where CounterStorm-1 only sees the reply or query packet, but not the other half of the network conversation) may cause false positives.

A sensor can best protect a segment when all of the traffic to or from any host in that segment is visible to the sensor via the span port (or tap). This is generally the case at access-layer switches. A sensor provides very good protection to a segment if the sensor sees all traffic going into or coming out of a segment. This is the case when the sensor is on a tap on the upstream link from an access-layer switch. A sensor can provide reasonable protection to a segment if it sees all of the traffic going into or coming out a set of IP addresses that contains the protected segment. This is the case when routing takes place downstream from the tap/span point in the network. This is also the case when not all of the IP ranges associated with an access-layer (or upstream) switch are protected by the sensor and the sensor is on an upstream tap from the access layer. In this case, the segment's hosts can communicate with some hosts, and the sensor cannot see that traffic via the span port (or tap).

Viewing Segments

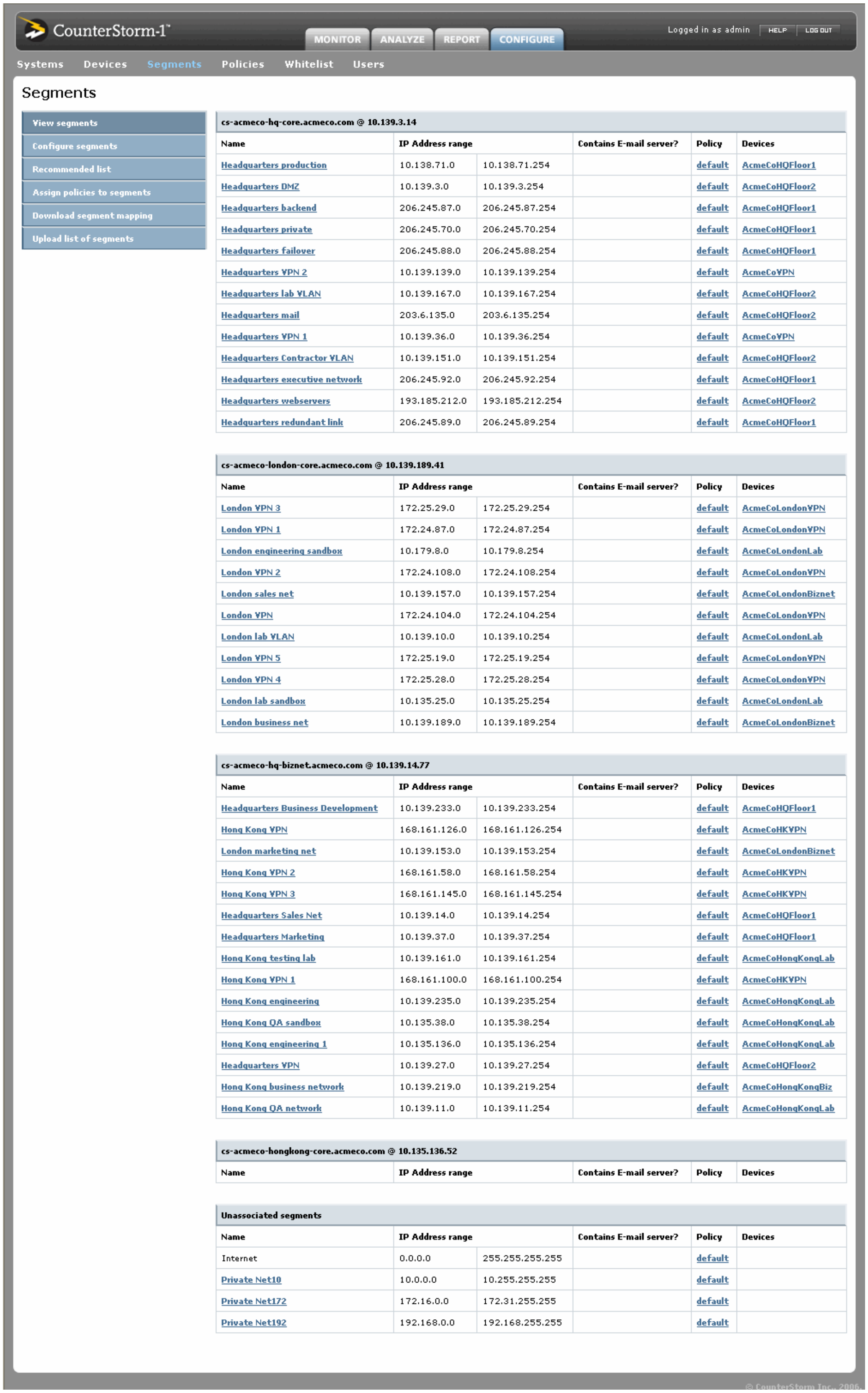
When you access the segments page, all segments are shown in the list. You can return to the segment list at anytime.

To view network segments:

1. Select **Configure** from the Main Toolbar and **Segments** from the Interactive Toolbar.

   The Segments screen is displayed.
2. Click **View segments**.

A list of segments is displayed.



cs-acmeco-hq-core.acmeco.com @ 10.139.3.14

Name	IP Address range		Contains E-mail server?	Policy	Devices
Headquarters production	10.138.71.0	10.138.71.254		default	AcmeCoHQFloor1
Headquarters DMZ	10.139.3.0	10.139.3.254		default	AcmeCoHQFloor2
Headquarters backend	206.245.87.0	206.245.87.254		default	AcmeCoHQFloor1
Headquarters private	206.245.70.0	206.245.70.254		default	AcmeCoHQFloor1
Headquarters failover	206.245.88.0	206.245.88.254		default	AcmeCoHQFloor1
Headquarters VPN 2	10.139.139.0	10.139.139.254		default	AcmeCoVPN
Headquarters lab VLAN	10.139.167.0	10.139.167.254		default	AcmeCoHQFloor2
Headquarters mail	203.6.135.0	203.6.135.254		default	AcmeCoHQFloor2
Headquarters VPN 1	10.139.36.0	10.139.36.254		default	AcmeCoVPN
Headquarters Contractor VLAN	10.139.151.0	10.139.151.254		default	AcmeCoHQFloor2
Headquarters executive network	206.245.92.0	206.245.92.254		default	AcmeCoHQFloor1
Headquarters webservers	193.185.212.0	193.185.212.254		default	AcmeCoHQFloor2
Headquarters redundant link	206.245.89.0	206.245.89.254		default	AcmeCoHQFloor1

cs-acmeco-london-core.acmeco.com @ 10.139.189.41

Name	IP Address range		Contains E-mail server?	Policy	Devices
London VPN 3	172.25.29.0	172.25.29.254		default	AcmeCoLondonVPN
London VPN 1	172.24.87.0	172.24.87.254		default	AcmeCoLondonVPN
London engineering sandbox	10.179.8.0	10.179.8.254		default	AcmeCoLondonLab
London VPN 2	172.24.108.0	172.24.108.254		default	AcmeCoLondonVPN
London sales net	10.139.157.0	10.139.157.254		default	AcmeCoLondonBiznet
London VPN	172.24.104.0	172.24.104.254		default	AcmeCoLondonVPN
London lab VLAN	10.139.10.0	10.139.10.254		default	AcmeCoLondonLab
London VPN 5	172.25.19.0	172.25.19.254		default	AcmeCoLondonVPN
London VPN 4	172.25.28.0	172.25.28.254		default	AcmeCoLondonVPN
London lab sandbox	10.135.25.0	10.135.25.254		default	AcmeCoLondonLab
London business net	10.139.189.0	10.139.189.254		default	AcmeCoLondonBiznet

cs-acmeco-hq-biznet.acmeco.com @ 10.139.14.77

Name	IP Address range		Contains E-mail server?	Policy	Devices
Headquarters Business Development	10.139.233.0	10.139.233.254		default	AcmeCoHQFloor1
Hong Kong VPN	168.161.126.0	168.161.126.254		default	AcmeCoHKVPN
London marketing net	10.139.153.0	10.139.153.254		default	AcmeCoLondonBiznet
Hong Kong VPN 2	168.161.58.0	168.161.58.254		default	AcmeCoHKVPN
Hong Kong VPN 3	168.161.145.0	168.161.145.254		default	AcmeCoHKVPN
Headquarters Sales Net	10.139.14.0	10.139.14.254		default	AcmeCoHQFloor1
Headquarters Marketing	10.139.37.0	10.139.37.254		default	AcmeCoHQFloor1
Hong Kong testing lab	10.139.161.0	10.139.161.254		default	AcmeCoHongKongLab
Hong Kong VPN 1	168.161.100.0	168.161.100.254		default	AcmeCoHKVPN
Hong Kong engineering	10.139.235.0	10.139.235.254		default	AcmeCoHongKongLab
Hong Kong QA sandbox	10.135.38.0	10.135.38.254		default	AcmeCoHongKongLab
Hong Kong engineering 1	10.135.136.0	10.135.136.254		default	AcmeCoHongKongLab
Headquarters VPN	10.139.27.0	10.139.27.254		default	AcmeCoHQFloor2
Hong Kong business network	10.139.219.0	10.139.219.254		default	AcmeCoHongKongBiz
Hong Kong QA network	10.139.11.0	10.139.11.254		default	AcmeCoHongKongLab

cs-acmeco-hongkong-core.acmeco.com @ 10.135.136.52

Name	IP Address range	Contains E-mail server?	Policy	Devices

Unassociated segments

Name	IP Address range		Contains E-mail server?	Policy	Devices
Internet	0.0.0.0	255.255.255.255		default	
Private Net10	10.0.0.0	10.255.255.255		default	
Private Net172	172.16.0.0	172.31.255.255		default	
Private Net192	192.168.0.0	192.168.255.255		default	

The table lists the segment name, IP address range, assigned policy, devices on the segment, and whether the segment contains e-mail servers.

Recommended Segment List

CounterStorm-1 analyzes the activity on the network to determine a list of recommended segments. This list is generated during initial configuration and whenever the **Recommended segment** button is clicked. Please check the suggestions carefully before adding them so as not to risk leaving critical resources unprotected.

Note: It may take some time to produce the list.

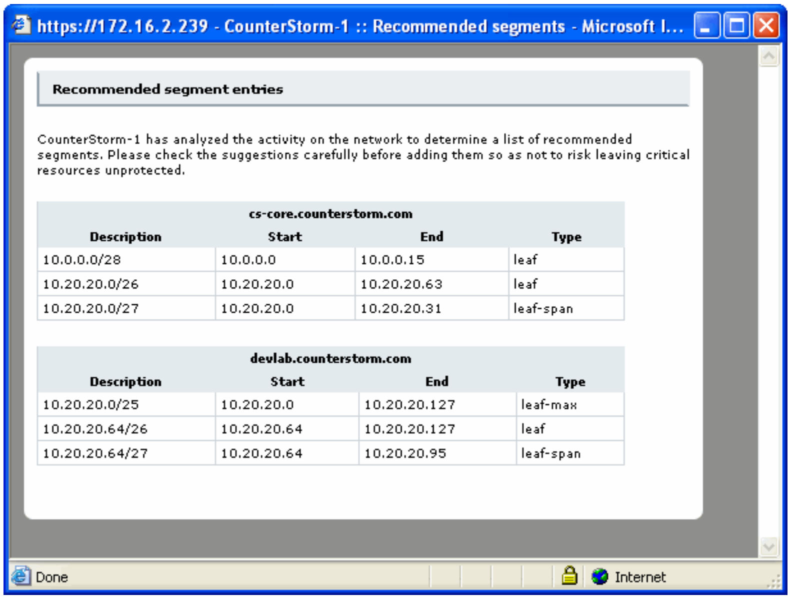
To view recommended segments:

1. Select **Configure** from the Main Toolbar and **Segments** from the Interactive Toolbar.

   The Segments screen is displayed.

2. Click **Recommended segments**.

   A list of segments is displayed in a new window.


https://172.16.2.239 - CounterStorm-1 :: Recommended segments - Microsoft I...
Done
Internet

Recommended segment entries

CounterStorm-1 has analyzed the activity on the network to determine a list of recommended segments. Please check the suggestions carefully before adding them so as not to risk leaving critical resources unprotected.

cs-core.counterstorm.com			
Description	**Start**	**End**	**Type**
10.0.0.0/28	10.0.0.0	10.0.0.15	leaf
10.20.20.0/26	10.20.20.0	10.20.20.63	leaf
10.20.20.0/27	10.20.20.0	10.20.20.31	leaf-span

devlab.counterstorm.com			
Description	**Start**	**End**	**Type**
10.20.20.0/25	10.20.20.0	10.20.20.127	leaf-max
10.20.20.64/26	10.20.20.64	10.20.20.127	leaf
10.20.20.64/27	10.20.20.64	10.20.20.95	leaf-span

The segment description, IP address range, and type of segment are listed.

The description is the CIDR netblock of the identified range, or a single IP, or an IP address range (if it doesn't collapse nicely into a CIDR block). The IP address range includes the start and end of the identified segment.

Types include:

Type	Description
e-mail	CounterStorm-1 detects SMTP traffic to hosts on this network segment, indicating that it's an e-mail server. In general, these segments will be single hosts. If there are multiple nearby hosts (within same /28 of network range) and the addresses are not allocated via DHCP, it may make sense to aggregate them into a single range.
leaf-span	CounterStorm-1 detects unicast ARP traffic over this range, indicating that it's local switch traffic seen via a SPAN port. These are almost surely segments that should be defined; it's possible that it may make sense to aggregate them into larger, enclosing “leaf” segments.
leaf	CounterStorm-1 detects broadcast ARP traffic over this range, and the segment is either broadcast ARP or broadcast IP; the segment is the smallest range (with a minimum granularity of /28, i.e. 16 addresses) that covers all observed traffic during the sampling interval. Since CounterStorm-1 hasn’t detected non-broadcast ARPs in this range, it is possible that this is non-spanned traffic that is leaking onto the spanned segment, or if there is an enclosed leaf-span segment, it may reflect an incomplete span for the segment in question. This can cause problems with asymmetric traffic if there are other transit or asymmetric segments. Nearly-adjacent leaf segments should probably be aggregated together into a single segment (possibly a leaf-max segment) including all of them, or if the network ranges are not of interest, simply deleted or ignored.
leaf-max	CounterStorm-1 detects broadcast IP traffic over this range, and it isthe largest range possible based on observed traffic during the sampling interval. Most frequently, these should be deleted or ignored, but they provide a useful guideline for a largest meaningful segment definition. It rarely makes sense to define segments larger than these.
transit	CounterStorm-1 detects small numbers of source IPs on the network, and there is a possibility of asymmetric traffic (there cannot be problems with asymmetric traffic if only leaf segments are observed). The source IP ranges are within five router hops. There is a possibility of problems with the span setup and you should look closely at the router/span configuration.
asymmetric	CounterStorm-1 detects sources, but no replies to those sources, meaning the span or routing is probably broken. The source IP ranges are within five router hops. There is a possibility of problems with the span setup and you should look closely at the router/span configuration.

In all cases, you should validate the ranges, and expand/consolidate them as necessary. For example, if the is 10.0.0.0/8, but CounterStorm-1 detects10.0.0.0/9 and 10.128.0.0/10, manually set the 10.0.0.0/8 range.

Note: Ensure that **segment includes mail servers** is checked in segment configuration for all e-mail segments.

3. Review the list segments and add the desired segments using the segment configuration button.

   See “Configuring Segments” on page 9-6.

Configuring Segments

Segment to sensor mapping allows you to create segments and to configure which sensors monitor which segments. Each segment in the network can be mapped, or assigned, to a specified CounterStorm-1 sensor. Segments may also be created, while remaining unmapped. See “Mapping the sensor” on page 9-8 for information on mapped and unmapped segments.

Note: Routing must be symmetrical (where CounterStorm-1 always sees the reply packet to any query packet, and vice versa) to and from CounterStorm-1 segments. Asymmetric routing (where CounterStorm-1 only sees the reply or query packet, but not the other half of the network conversation) will cause false positives.

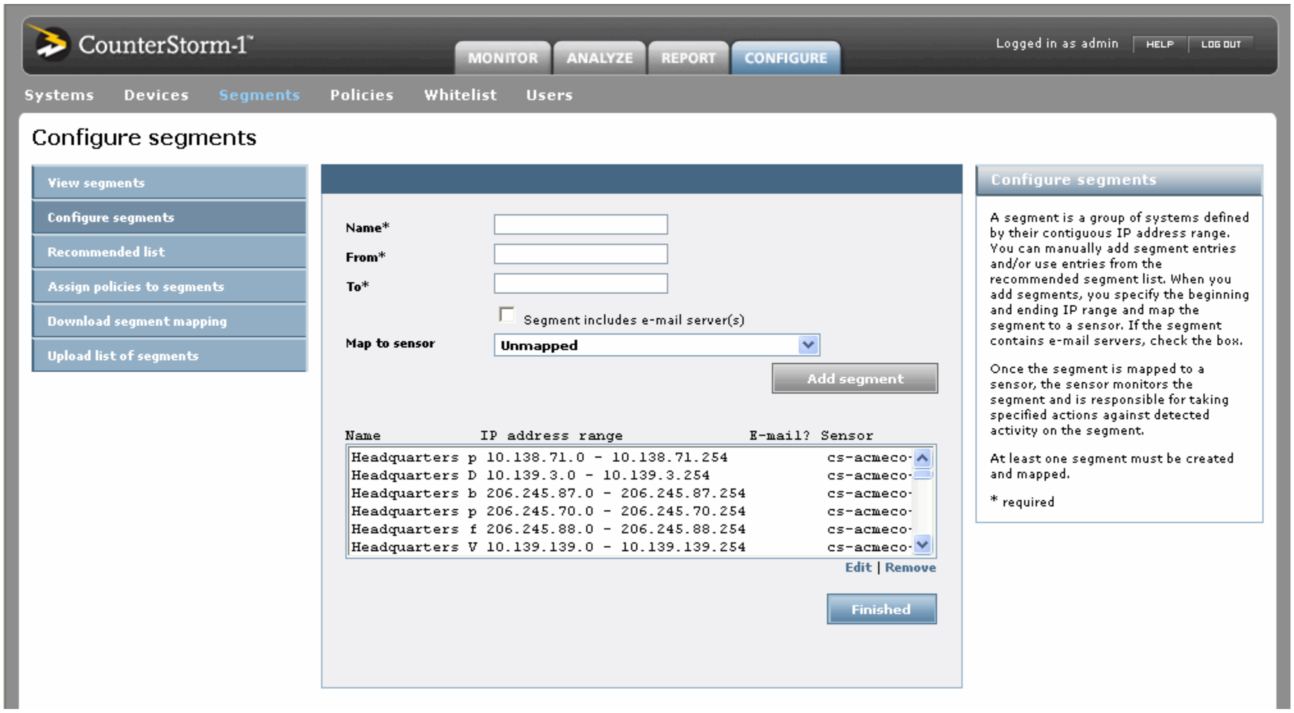
To configure specific network segments for monitoring:

1. Select **Configure** from the Main Toolbar and **Segments** from the Interactive Toolbar.

   The Segments screen is displayed.

2. Click **Configure Segments**.

   The Configure segments screen is displayed.



Configure segments

Name*

From*

To*

□ Segment includes e-mail server(s)

Map to sensor: Unmapped

```
Name              IP address range                   E-mail? Sensor
Headquarters p 10.138.71.0 - 10.138.71.254              cs-acmeco-
Headquarters D 10.139.3.0 - 10.139.3.254                cs-acmeco-
Headquarters b 206.245.87.0 - 206.245.87.254            cs-acmeco-
Headquarters p 206.245.70.0 - 206.245.70.254            cs-acmeco-
Headquarters f 206.245.88.0 - 206.245.88.254            cs-acmeco-
Headquarters V 10.139.139.0 - 10.139.139.254            cs-acmeco-
```

Configure segments

A segment is a group of systems defined by their contiguous IP address range. You can manually add segment entries and/or use entries from the recommended segment list. When you add segments, you specify the beginning and ending IP range and map the segment to a sensor. If the segment contains e-mail servers, check the box.

Once the segment is mapped to a sensor, the sensor monitors the segment and is responsible for taking specified actions against detected activity on the segment.

At least one segment must be created and mapped.

* required

3. Enter the desired information to configure each segment.

Define the segment and map the segment to a sensor.

Naming the segment

The segment ***Name*** indicates the physical location of the segment, for example, “Accounting” or “5th Floor.” The segment name is displayed with alarm details, so you may wish to create segments even though they do not have a distinct response policy in order to remind the alarm viewer of certain information, such as the department or the physical location the IP addresses represent.

Defining Segment Ranges

The segment range (***To*** and ***From***) indicates the included machines as identified by the highest and lowest IP addresses of the selected machines. You can upload a CSV file that contains a list of segments or configure them one at a time.

Segments can be of any size. Segments may be proper subsets of another. For example, segment A may be 10.10.10.0-10.10.10.255, while segment B may be 10.10.10.1-10.10.10.10

The larger the superset of IP address with which the segment hosts can communicate without being seen by the sensor, the less effective the sensor is at detecting (and hence stopping) attacks. For example: if 10.0.1.0/24 is the protected segment, and it can communicate with 10.0.2.0/24 without the sensor seeing that traffic, then this is acceptable. However, if traffic from 10.0.1.0/24 to/from 10.0.0.0/8 is not seen by the sensor, the sensor might miss seeing a class-B or class-A based attack until it had already infected many systems in 10.0.0.0/8.

Segment range definitions must be unique. The same range or name cannot be repeated. You may have multiple segments with the same IP range, but with different name, and different mapping. For example, you may have a segment mapped on sensor A, a segment mapped on sensor B, and a segment unmapped (effectively on sensors C-Z), all with the same range 10.10.10.1-10.10.10.10. This is necessary because of distribution level sensors, which may look at traffic also covered by leaf-level sensors.

CounterStorm recommends that one sensor attempt to protect no more than 65,000 IP addresses in one VLAN if the sensor does not see the majority of all traffic in the VLAN. Attempting to protect more can cause a degradation in performance. However, you may have essentially unlimited addresses if each VLAN (where the sensor sees all traffic going in or out of the VLAN) has less than 65,000 addresses or the sensor can see all traffic sent to or from each host in the VLAN.

Note: If you change segment definitions (after initial creation), e-mail traffic anomaly alarms are delayed for one week while the system retrains on the new segment definitions.

Checking the e-mail box

The ***Segment includes e-mail servers(s)*** box refers to e-mail servers, relays, list servers, SMTP mail traffic usage, and any type of machine that passes e-mail related traffic. It tells CounterStorm-1 how to assess the machine's activity.

If a segment contains only a few mail servers with static IP addresses, create a smaller segment with only those IP addresses in it, also with the e-mail server box checked. If your hosts have dynamic IP addresses, or do not have distinct and persistent SMTP usage, you should not check the e-mail server button.

Each known mail server in the protected segment should be defined in its own smaller segment. Multiple servers (in small ranges) can be in the same defined segment, but that segment should contain no non-mail-server systems.

Mapping the sensor

The ***Map to Sensor*** field indicates which sensor monitors the selected segments.

You cannot have multiple machines with the same IP address map to the same or different sensor. For example, you cannot have two segments both configured with net 10, with the different machines responding to 10.1.1.1.

You may create unmapped segments. Unmapped segments may be used to monitor segments outside of your immediate responsibility. For example, you might maintain your corporate network, but receive data from a corporate partner. You would be aware of their IP range. You can create a segment, and map it to “unmapped.” The segment would be created and placed in the same table as your Internet segment in the Policies window. See “Assigning Policies to Specific Segments” on page 10-5 for more information on assigning policies to segments. It is better to define a segment that is unmapped than to leave a segment undefined.

Note: Load balancing policies can work with proper network configuration. In load-balancing class situations where traffic may go to A or B (where A and B are so separated so that traffic cannot be re-aggregated), both A and B may need to have the same ranges defined as a segment. However, you cannot have switch response on the same IP address on both sensors.

4. Click **Add Segment**.

   Segments are added and listed in the table below.

5. When all segments have been added, click **Finished**.

   You may also Edit and Remove segments.

Assigning Policies to Segments

See “Assigning Policies to Specific Segments” on page 10-5.

Uploading List of Segments

You can upload a CSV file containing segment mapping.

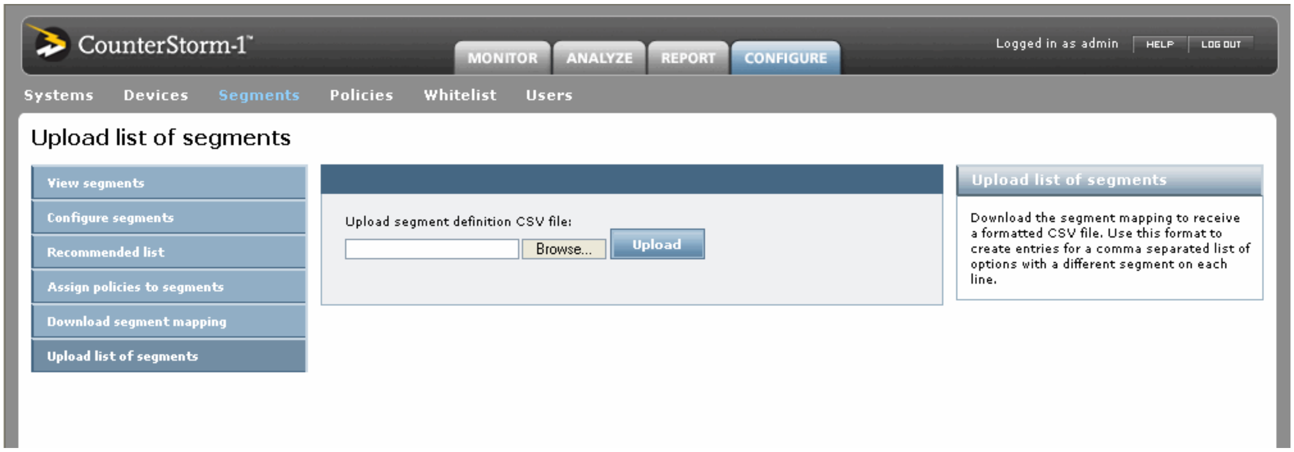
To upload segment mapping:

1. Select **Configure** from the Main Toolbar and **Segments** from the Interactive Toolbar.

   The Segments screen is displayed.

2. Click **Upload list of segments**.

   The screen appears with a box that allows you to browse for the CSV file.



Upload list of segments

Upload segment definition CSV file:

Upload list of segments

Download the segment mapping to receive a formatted CSV file. Use this format to create entries for a comma separated list of options with a different segment on each line.

3. Browse to locate the file.
4. Click **Upload**.

Downloading Segment Mapping

You can download a CSV file that contains the segments mapped in “Assigning Policies to Segments” on page 9-8.

To download segment mapping:

1. Select **Configure** from the Main Toolbar and **Segments** from the Interactive Toolbar.

   The Segments screen is displayed.
2. Click **Download segment mapping**.

   You are prompted to open or save a CSV file containing the configured segment mapping. You can open this file in any spreadsheet program, such as Microsoft Excel.

Chapter 10: Configuring Policies

In This Chapter

This section explains how to configure CounterStorm-1 policies. Policies implement the quarantine techniques that prevent attack propagation. Policies are notification and quarantine settings that may be configured in various combinations and applied to specified segments.

Note: Whenever you reconfigure your network, you must update your policy configuration. Changes in the network such as e-mail relays (that effect e-mail addresses), SPAN ports, and switches will effect the operation of policies.

Viewing Policies

When you access the Policies page, all policies are shown. You can return to the policy list at anytime.

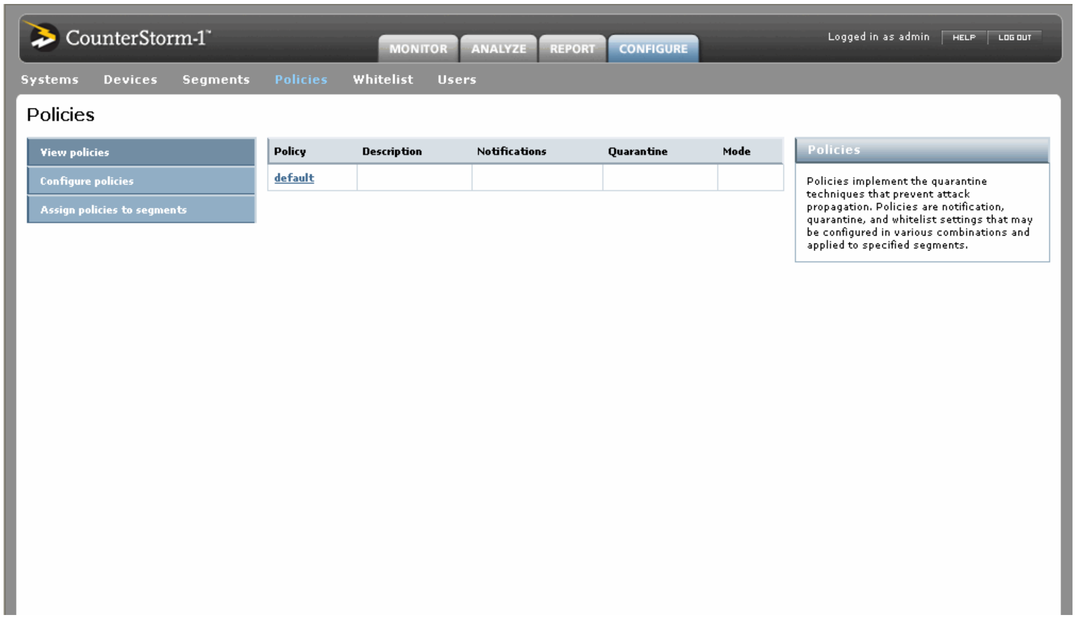
To view policies:

1. Select **Configure** from the Main Toolbar and **Policies** from the Interactive Toolbar.

   The Policies screen is displayed.

2. Click **View Policies**.

   A list of policies is displayed.



Policy	Description	Notifications	Quarantine	Mode
default				

Policies

Policies implement the quarantine techniques that prevent attack propagation. Policies are notification, quarantine, and whitelist settings that may be configured in various combinations and applied to specified segments.

Configuring Policies

Policies are the active responses taken by CounterStorm-1 to quarantine attacks and notify users about attacks. Policies include the notification and quarantine settings that may be configured in various combinations and applied to specified segments. You may configure multiple policies, one for each type of response policy you wish to allow.

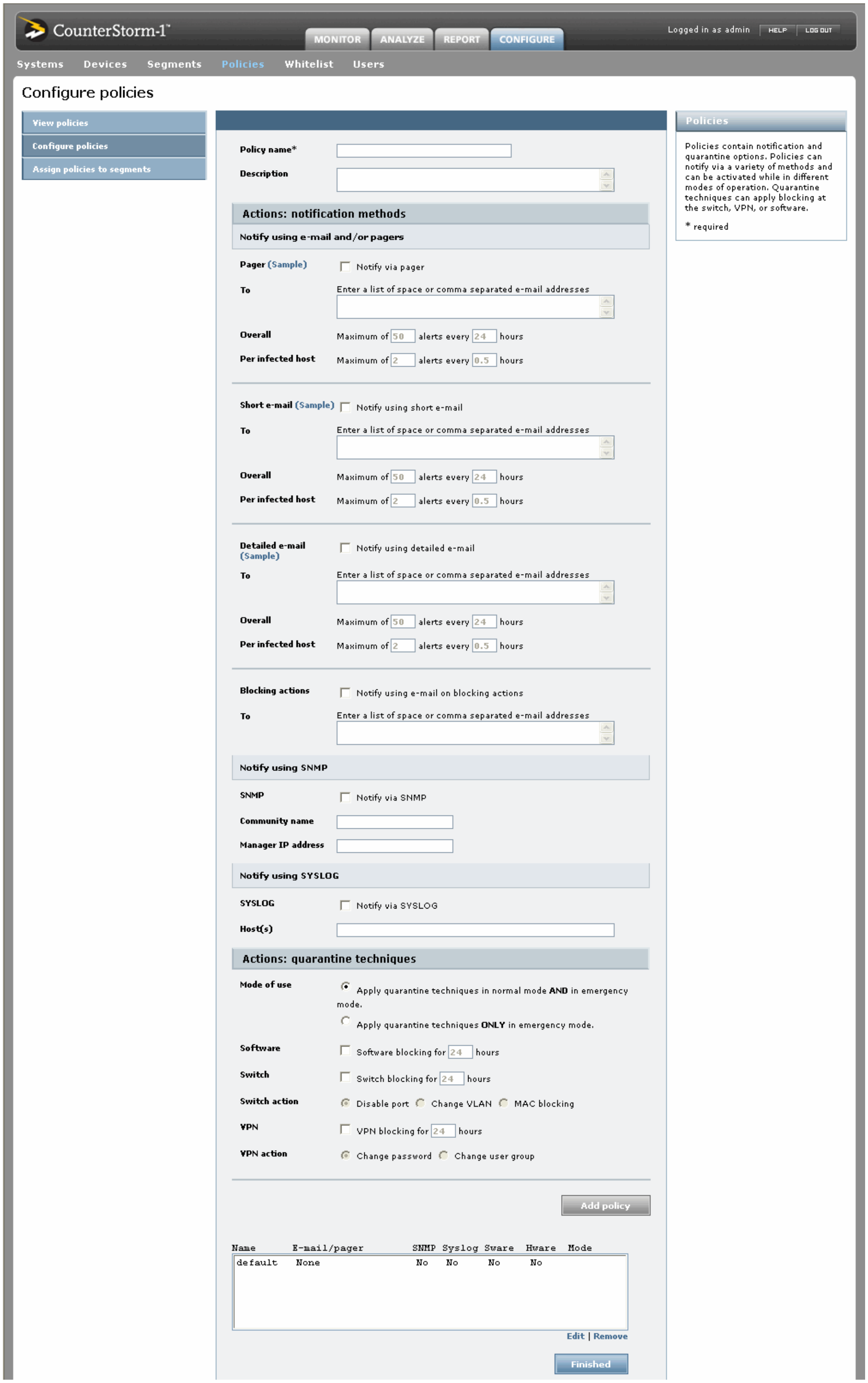
Policies contain notification and quarantine options. Policies can notify you via a variety of methods and can be activated while in different modes of operation. Quarantine techniques can apply blocking at the switch, VPN, or software level.

To configure new policies:

1. Select **Configure** from the Main Toolbar and **Policies** from the Interactive Toolbar.

   The policies screen is displayed.
2. Click **Configure policies**.

The Policies screen displays.



Configure policies

Policy name*

Description

Actions: notification methods

Notify using e-mail and/or pagers

Pager (Sample) □ Notify via pager

To Enter a list of space or comma separated e-mail addresses

Overall Maximum of 50 alerts every 24 hours

Per infected host Maximum of 2 alerts every 0.5 hours

Short e-mail (Sample) □ Notify using short e-mail

To Enter a list of space or comma separated e-mail addresses

Overall Maximum of 50 alerts every 24 hours

Per infected host Maximum of 2 alerts every 0.5 hours

Detailed e-mail (Sample) □ Notify using detailed e-mail

To Enter a list of space or comma separated e-mail addresses

Overall Maximum of 50 alerts every 24 hours

Per infected host Maximum of 2 alerts every 0.5 hours

Blocking actions □ Notify using e-mail on blocking actions

To Enter a list of space or comma separated e-mail addresses

Notify using SNMP

SNMP □ Notify via SNMP

Community name

Manager IP address

Notify using SYSLOG

SYSLOG □ Notify via SYSLOG

Host(s)

Actions: quarantine techniques

Mode of use ● Apply quarantine techniques in normal mode **AND** in emergency mode.
○ Apply quarantine techniques **ONLY** in emergency mode.

Software □ Software blocking for 24 hours

Switch □ Switch blocking for 24 hours

Switch action ● Disable port ○ Change VLAN ○ MAC blocking

VPN □ VPN blocking for 24 hours

VPN action ● Change password ○ Change user group

```
Name      E-mail/pager          SNMP  Syslog  Sware  Hware  Mode
default   None                   No    No      No     No
```

Policies

Policies contain notification and quarantine options. Policies can notify via a variety of methods and can be activated while in different modes of operation. Quarantine techniques can apply blocking at the switch, VPN, or software.

* required

Configuring Policies

3. Enter the ***Policy name*** and a ***Description*** of the new policy.
4. Enter the desired notification methods.

   CounterStorm-1 alarms notify you about attacks. Notifications can be provided via e-mails, pager messages, SNMP, and syslog. You may also have multiple types of notification in a single policy.

   You can select the length of the e-mail that is sent.You can customize how many notification alarms you receive per hour and from each host by specifying ***Overall*** and ***Per infected host***. Enter the maximum number of alarms you wish to receive and the time period.

Note: Do not reconfigure your e-mail relays without updating your policies. CounterStorm-1 cannot notify to non-existent e-mail accounts.

   You can also be notified when automatic blocking occurs.

5. Enter the desired Mode of Use.

   Select your ***mode of use***. These modes are applied when the emergency response mode button is activated. See “Operating Modes” on page 8-1 for more information on modes of operation.

6. Enter the desired Quarantine technique.

   CounterStorm-1 quarantines infected machines, using hardware (switch/VPN) and/or software blocking to stop traffic to and from specified machines. Quarantines prevent infections from spreading throughout the network.

   Software blocking uses a combination of TCP RST packets and ARP poisoning techniques to block traffic to and from malicious devices. These techniques are not recommended, nor are they guaranteed to successfully terminate connections. To be effective, TCP resets must win a race and reach the network endpoints before they receive actual replies from the other side. Depending on the network latency, load on the sensor, and the speed of the two other systems, software response may lose this race, in which case it has no effect. Also, an attacker can ignore or filter RST packets, preventing them from blocking backdoors or control channels. ARP poisoning cannot cross layer 3 (network segment) boundaries, and therefore can only be used to quarantine a local system; it is also possible for an attacker to ignore or filter ARP traffic in a way that makes the poisoning ineffective.

   Software response is provided for evaluation or use in smaller networks, and should only be deployed in addition to Switch and/or VPN responses. It should never be relied upon to protect systems by itself. Proper configuration and deployment of software response is difficult in enterprise networks. Switch and/or VPN responses are more effective and easier to use for containing malicious devices or users. Please contact CounterStorm Technical Support if you are interested in using software response in your network.

   Switch blocking automatically locates the physical port of an infected machine and halts attack propagation either by disabling the port or placing it on a remediation VLAN where clean-up can occur without the risk of further damage.

   VPN gateways are used to quarantine infected machines from the rest of the network.

   Conversely, if there is a machine that you never want to block, no matter what its infection status is, you can configure a whitelist. The whitelist is a list of machines that are never blocked, as per your specifications. To configure a whitelist, see “Creating the Whitelist” on page 12-4.

Note: CounterStorm recommends that you not enable quarantine techniques during the first week of operation. You can use the Take Action feature in the Monitoring Activity Table to block attacks as you see them. See “Taking Action On Attacks” on page 6-7. After you are comfortable with the product, modify your policies to enable quarantine techniques. Switch info should be entered, even if you do not initially intend to use switch blocking, so that blocking strategies can be quickly implemented.

7. Click **Add Policy.**

Note: You may add many policies before clicking Finished.

8. Click **Finished**.

   You may delete a policy by highlighting the desired policy in the policy table and clicking the **Remove** link. You may modify a policy by highlighting the desired policy in the policy table and clicking the **Edit** link.

Assigning Policies to Specific Segments

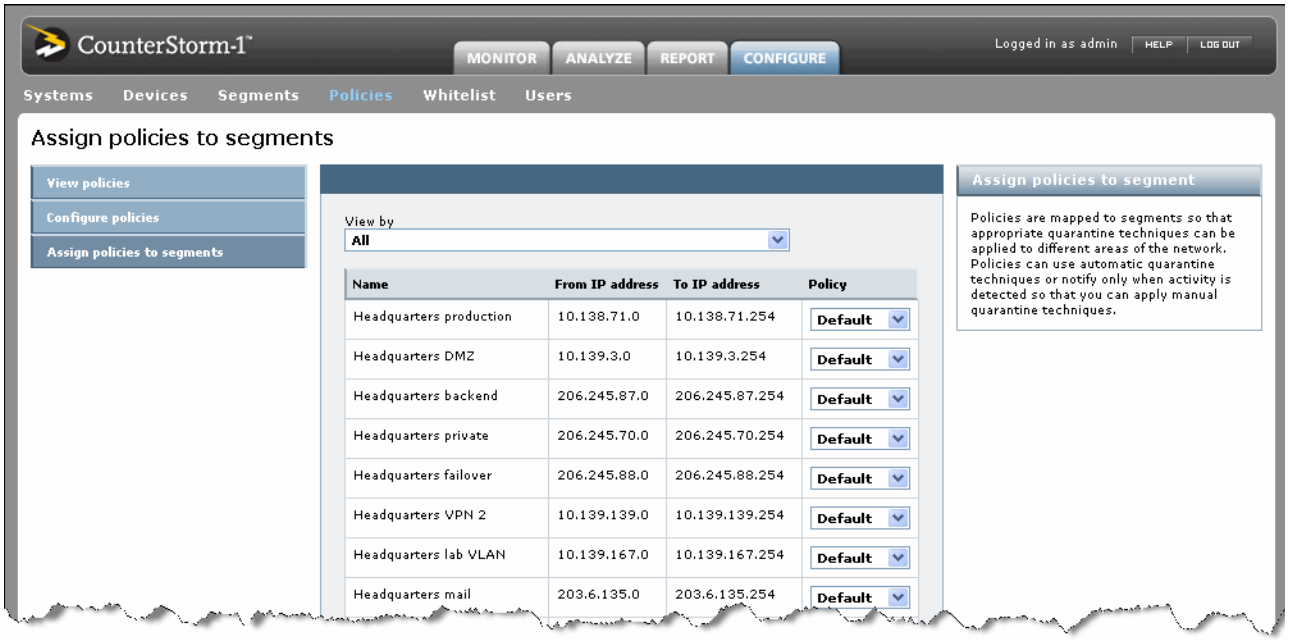
Active response policies may be applied to all segments, or they may be customized to a specific segment. Policies are mapped to segments so that an appropriate defense strategy can be applied to different areas of the network. If there is an area of the network for which active responses are not optimal, it is advisable to create and map a notification-only policy. Alternatively, in a segment with critical assets, an aggressive blocking strategy is the best way to mitigate attack propagation.

To configure policies to specific segments:

1. Select **Configure** from the Main Toolbar and **Policies** from the Interactive Toolbar.

   The policies screen is displayed.
2. Click **Assign policies to segments**.

The map segment info screen displays.



Assign policies to segments

View by: All

Name	From IP address	To IP address	Policy
Headquarters production	10.138.71.0	10.138.71.254	Default
Headquarters DMZ	10.139.3.0	10.139.3.254	Default
Headquarters backend	206.245.87.0	206.245.87.254	Default
Headquarters private	206.245.70.0	206.245.70.254	Default
Headquarters failover	206.245.88.0	206.245.88.254	Default
Headquarters VPN 2	10.139.139.0	10.139.139.254	Default
Headquarters lab VLAN	10.139.167.0	10.139.167.254	Default
Headquarters mail	203.6.135.0	203.6.135.254	Default

Assign policies to segment

Policies are mapped to segments so that appropriate quarantine techniques can be applied to different areas of the network. Policies can use automatic quarantine techniques or notify only when activity is detected so that you can apply manual quarantine techniques.

You can choose to show all segments or only those that apply to a particular sensor by changing the ***View By*** setting.

The Internet segment, a default segment, is the segment whose policy is used if no other segment matches the source of the attack. However, you may wish to have different policies for other groups of IP addresses which are not protected. For example, you may wish to have a segment for each division in the company so that you can define a response policy that involves notifying the responsible administrator of each division, but not disturbing administrators of uninvolved divisions.

Unmapped segments are listed in the same table with the Internet segment. All other segments are listed by their mapped sensor.

3. Find the segment to which you wish to apply a particular policy.
4. From the pulldown menu, select the policy you wish to apply.
5. Click **Save** to assign the policy.

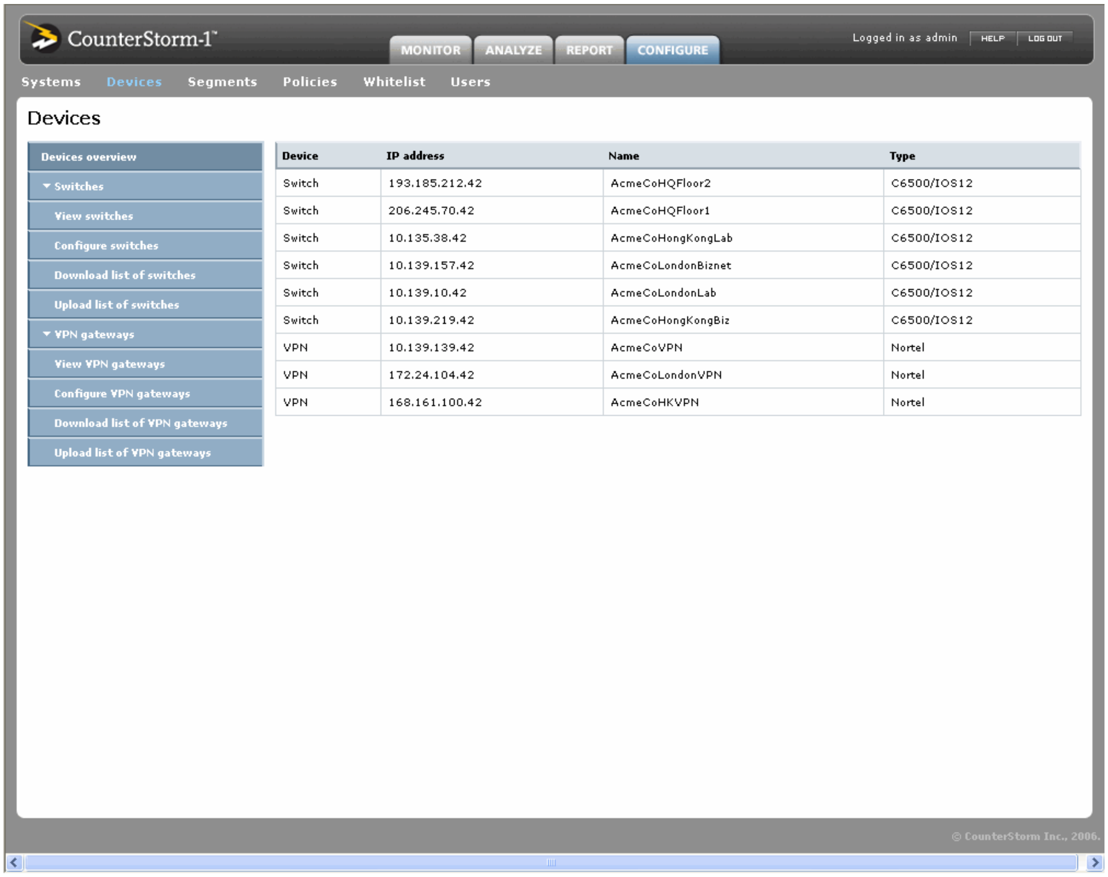
Chapter 11: Configuring Devices

You can configure a variety of devices. It is important to configure all devices for proper CounterStorm operation.

In This Chapter

Viewing Devices

You can view a list of all configured devices by clicking the View Device button.



Device	IP address	Name	Type
Switch	193.185.212.42	AcmeCoHQFloor2	C6500/IOS12
Switch	206.245.70.42	AcmeCoHQFloor1	C6500/IOS12
Switch	10.135.38.42	AcmeCoHongKongLab	C6500/IOS12
Switch	10.139.157.42	AcmeCoLondonBiznet	C6500/IOS12
Switch	10.139.10.42	AcmeCoLondonLab	C6500/IOS12
Switch	10.139.219.42	AcmeCoHongKongBiz	C6500/IOS12
VPN	10.139.139.42	AcmeCoVPN	Nortel
VPN	172.24.104.42	AcmeCoLondonVPN	Nortel
VPN	168.161.100.42	AcmeCoHKVPN	Nortel

Switches

Switches are used to quarantine infected machines from the rest of the network. Switch blocking can be performed automatically as a quarantine technique in Policies or manually via the Take Action pulldown. Switch information is also used for discovery of MAC address and switch port/blade information.

Even if you don’t intend to use your switches for blocking, it is recommended that they be added to the list.

Note: It is recommended that you configure the switch used for blocking even if you do not intend to activate the automatic active responses in case you ever need to manually activate blocking.

Viewing Switch Information

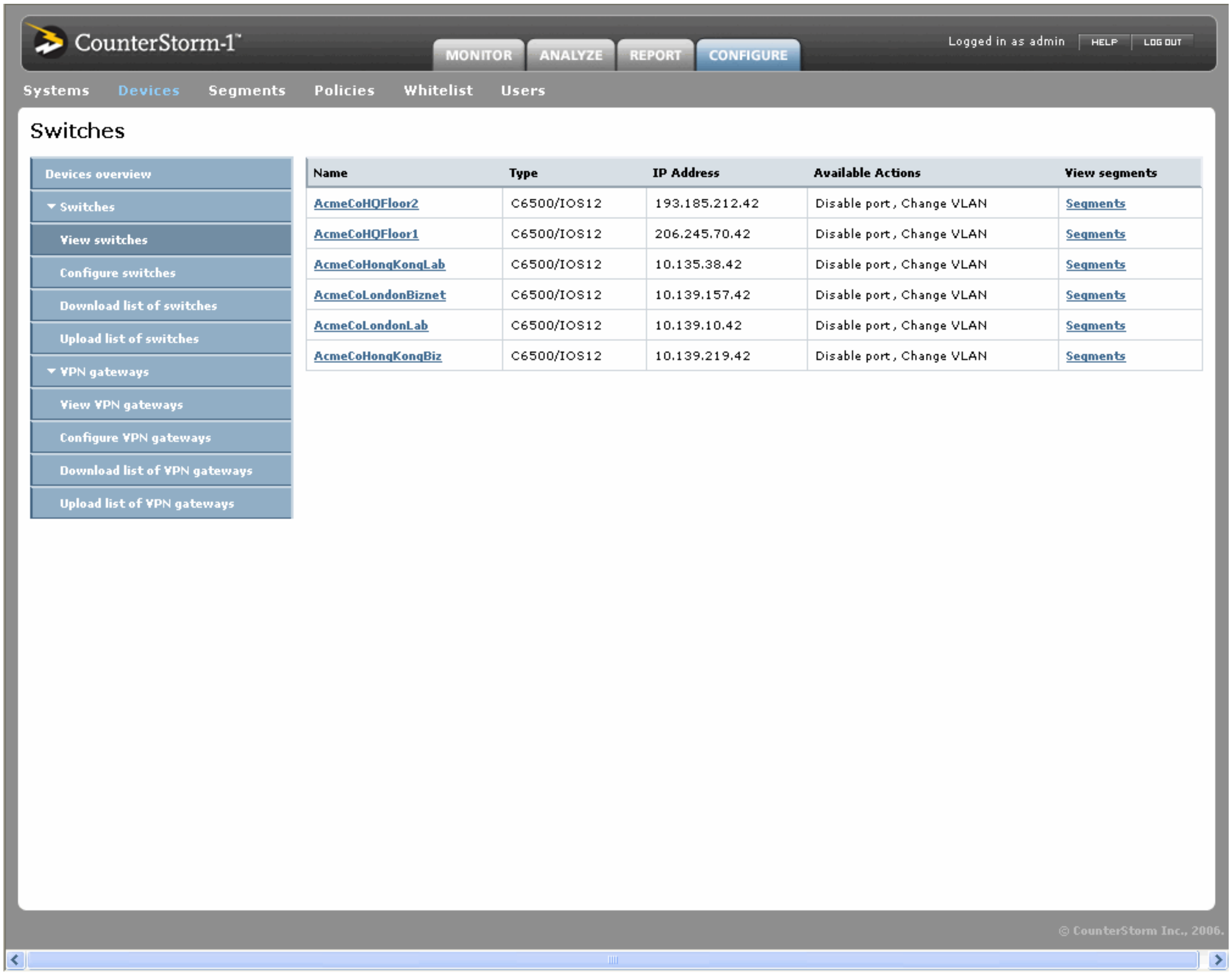
You can view a list of configured switches at any time.

To view switches:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed.
2. Click **View Switches**.

A list of switches is displayed.



Name	Type	IP Address	Available Actions	View segments
AcmeCoHQFloor2	C6500/IOS12	193.185.212.42	Disable port , Change VLAN	Segments
AcmeCoHQFloor1	C6500/IOS12	206.245.70.42	Disable port , Change VLAN	Segments
AcmeCoHongKongLab	C6500/IOS12	10.135.38.42	Disable port , Change VLAN	Segments
AcmeCoLondonBiznet	C6500/IOS12	10.139.157.42	Disable port , Change VLAN	Segments
AcmeCoLondonLab	C6500/IOS12	10.139.10.42	Disable port , Change VLAN	Segments
AcmeCoHongKongBiz	C6500/IOS12	10.139.219.42	Disable port , Change VLAN	Segments

Configuring Switch Information

Switch information is provided in alarms and is useful in tracking infections. Switches can also be used to block the spread of an infection. Even if you don't intend to use your switches for blocking, it is recommended that they be added to the list.

It is recommended that you configure the switch used for blocking even if you do not intend to activate the automatic active responses in case you ever need to manually activate blocking.

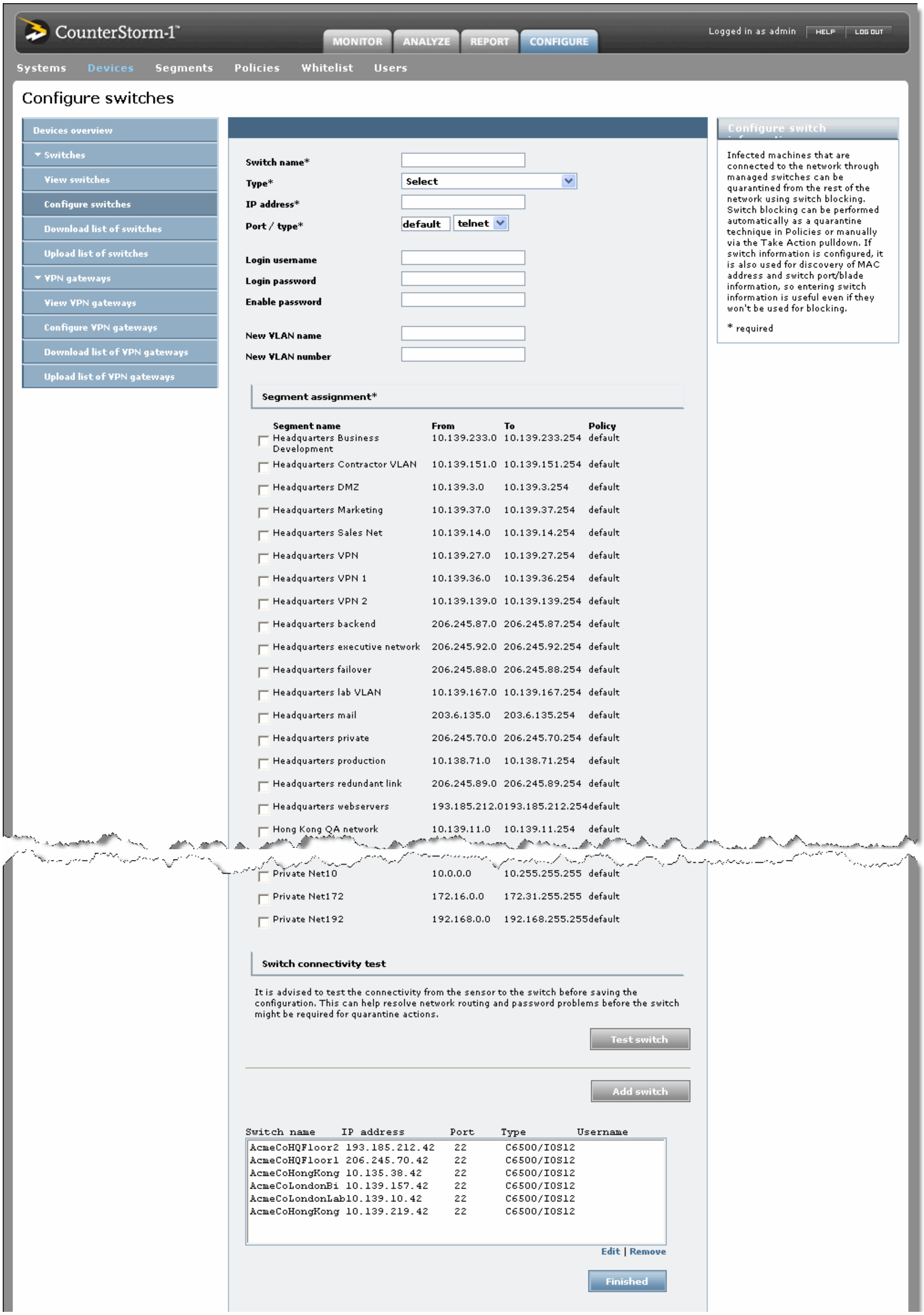
To configure switch data:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed. Existing switch blocking information is displayed in the Switch Information section.
2. Click the **Configure switch blocking** link.

Configuring Devices

The Configure switch information screen displays.



Configure switches

Switch name*	
Type*	Select
IP address*	
Port / type*	default telnet
Login username	
Login password	
Enable password	
New VLAN name	
New VLAN number	

Configure switch information

Infected machines that are connected to the network through managed switches can be quarantined from the rest of the network using switch blocking. Switch blocking can be performed automatically as a quarantine technique in Policies or manually via the Take Action pulldown. If switch information is configured, it is also used for discovery of MAC address and switch port/blade information, so entering switch information is useful even if they won't be used for blocking.

* required

Segment assignment*

	Segment name	From	To	Policy
□	Headquarters Business Development	10.139.233.0	10.139.233.254	default
□	Headquarters Contractor VLAN	10.139.151.0	10.139.151.254	default
□	Headquarters DMZ	10.139.3.0	10.139.3.254	default
□	Headquarters Marketing	10.139.37.0	10.139.37.254	default
□	Headquarters Sales Net	10.139.14.0	10.139.14.254	default
□	Headquarters VPN	10.139.27.0	10.139.27.254	default
□	Headquarters VPN 1	10.139.36.0	10.139.36.254	default
□	Headquarters VPN 2	10.139.139.0	10.139.139.254	default
□	Headquarters backend	206.245.87.0	206.245.87.254	default
□	Headquarters executive network	206.245.92.0	206.245.92.254	default
□	Headquarters failover	206.245.88.0	206.245.88.254	default
□	Headquarters lab VLAN	10.139.167.0	10.139.167.254	default
□	Headquarters mail	203.6.135.0	203.6.135.254	default
□	Headquarters private	206.245.70.0	206.245.70.254	default
□	Headquarters production	10.138.71.0	10.138.71.254	default
□	Headquarters redundant link	206.245.89.0	206.245.89.254	default
□	Headquarters webservers	193.185.212.0	193.185.212.254	default
□	Hong Kong QA network	10.139.11.0	10.139.11.254	default
□	Private Net10	10.0.0.0	10.255.255.255	default
□	Private Net172	172.16.0.0	172.31.255.255	default
□	Private Net192	192.168.0.0	192.168.255.255	default

Switch connectivity test

It is advised to test the connectivity from the sensor to the switch before saving the configuration. This can help resolve network routing and password problems before the switch might be required for quarantine actions.

```
Switch name    IP address        Port     Type          Username
AcmeCoHQFloor2 193.185.212.42     22      C6500/IOS12
AcmeCoHQFloor1 206.245.70.42      22      C6500/IOS12
AcmeCoHongKong 10.135.38.42       22      C6500/IOS12
AcmeCoLondonBi 10.139.157.42      22      C6500/IOS12
AcmeCoLondonLab10.139.10.42       22      C6500/IOS12
AcmeCoHongKong 10.139.219.42      22      C6500/IOS12
```

3. Enter the desired information to configure alternate switches to be used when applying switch blocking.

   The switch name is a unique identifier. If no name is specified, the default name of the switch is its IP address.

   The switch type identifies the switch model. Currently, CounterStorm-1 supports the following types of switches:

   - Cisco 2950 Series (IOS 12, CatOS 7)
   - Cisco 3550 Series (IOS 12, CatOS 7)
   - Cisco 4500 Series (IOS 12, CatOS 7)
   - Cisco 6500 Series (IOS 12, CatOS 7)

   CounterStorm-1 also supports TACACS. When the sensor blocks a Cisco Hardware port it logs into the Cisco Switch. With TACACS you can use one login credential to access all the switches.

   The switch IP address and switch TCP port identifies the switch on the network.

   You can choose to connect with the switch via a SSH or Telnet connection type. Telnet is the default.

   You can enter the remediation VLAN name and number.

   One or more segments can be moved to a switch when switch blocking is implemented. Selecting segments for this switch configures which segments are moved to this switch.

   It is advised to test the connectivity from the sensor to the switch before saving the configuration. This can help resolve network routing and password problems before the switch is required for quarantine actions. Click **Test switch** to test connectivity.

4. Click **Add Switch**.

   Segments are listed in the table below the add segments button. You can add many switches prior to clicking finished.

5. When all segments have been added, click **Finished**.

   You may also edit and remove switches.

Uploading Switch Information

You can upload a CSV file containing switches.

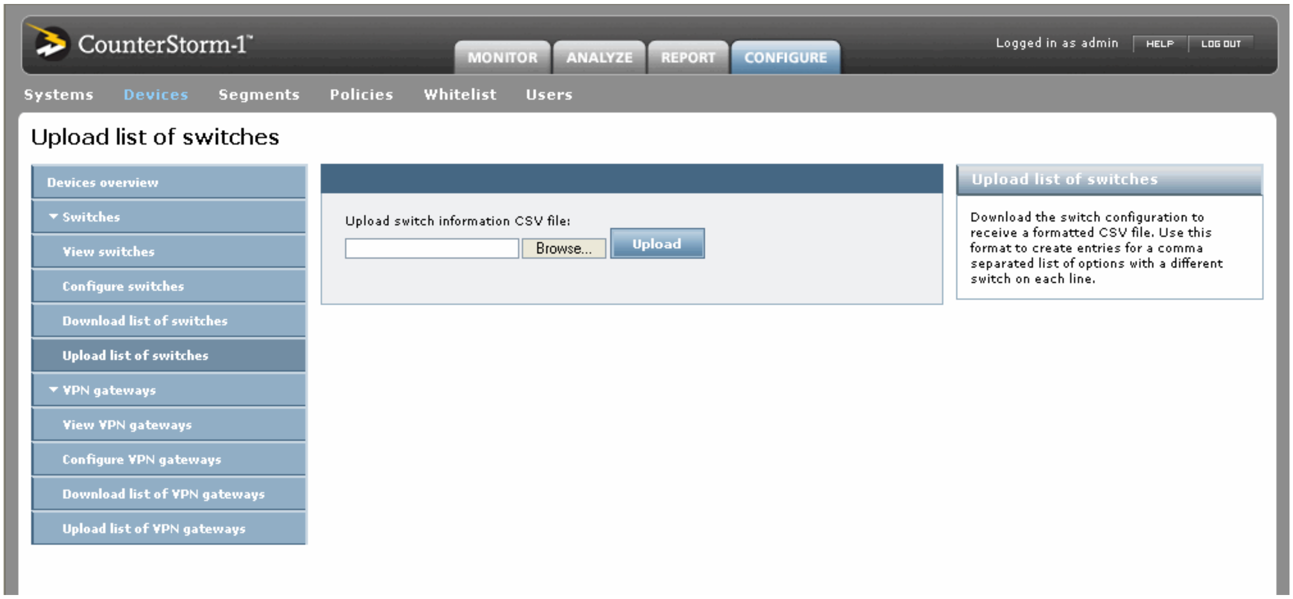
To upload switches:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed.

2. Click **Upload list of switches**.

The screen appears with a box allowing you to browse for the CSV file.



Download the switch configuration to receive a formatted CSV file. Use this format to create entries for a comma separated list of options with a different switch on each line.

3. Browse to locate the file.
4. Click **Upload**.

Downloading Switch Information

You can download a CSV file that contains the switches specified in “Configuring Switch Information” on page 11-3.

To download switch information:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed.
2. Click **Download switch information**.

   You are prompted to open or save a CSV file containing the configured switch. You can open this file in any spreadsheet program, such as Microsoft Excel.

VPN Gateways

VPN gateways are used to quarantine infected machines from the rest of the network. VPN blocking can be performed automatically as a quarantine technique in Policies or manually via the Take Action pulldown. CounterStorm-1 currently supports Nortel™ brand VPN gateways.

Note: VPNs need to be deployed at the same segment as the VPN termination device.

Viewing VPN Information

You can view a list of configured VPNs Gateways at any time.

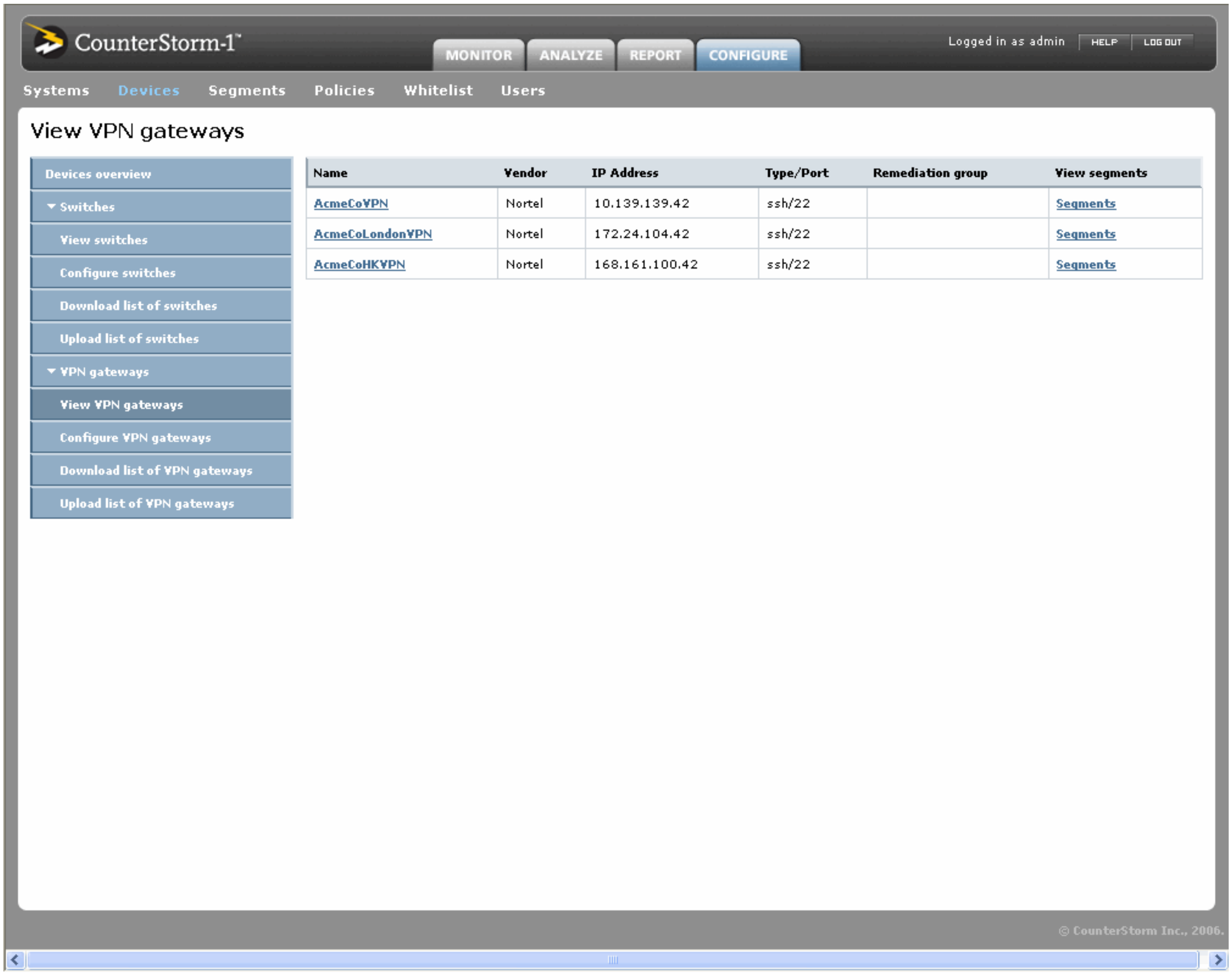
To view VPN gateways:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed.

2. Click **View VPN gateways**.

   A list of VPN gateways is displayed.



View VPN gateways

Name	Vendor	IP Address	Type/Port	Remediation group	View segments
AcmeCoVPN	Nortel	10.139.139.42	ssh/22		Segments
AcmeCoLondonVPN	Nortel	172.24.104.42	ssh/22		Segments
AcmeCoHKVPN	Nortel	168.161.100.42	ssh/22		Segments

Configuring VPN Gateway Information

VPN gateway information is provided in alarms and is useful in tracking infections. VPN gateways can also be used to block the spread of an infection. Even if you don’t intend to use your VPN gateways for blocking, it is recommended that they be added to the list. It is recommended that you configure the VPN gateway used for blocking even if you do not intend to activate the automatic active responses in case you ever need to manually activate blocking.

Configuring Devices

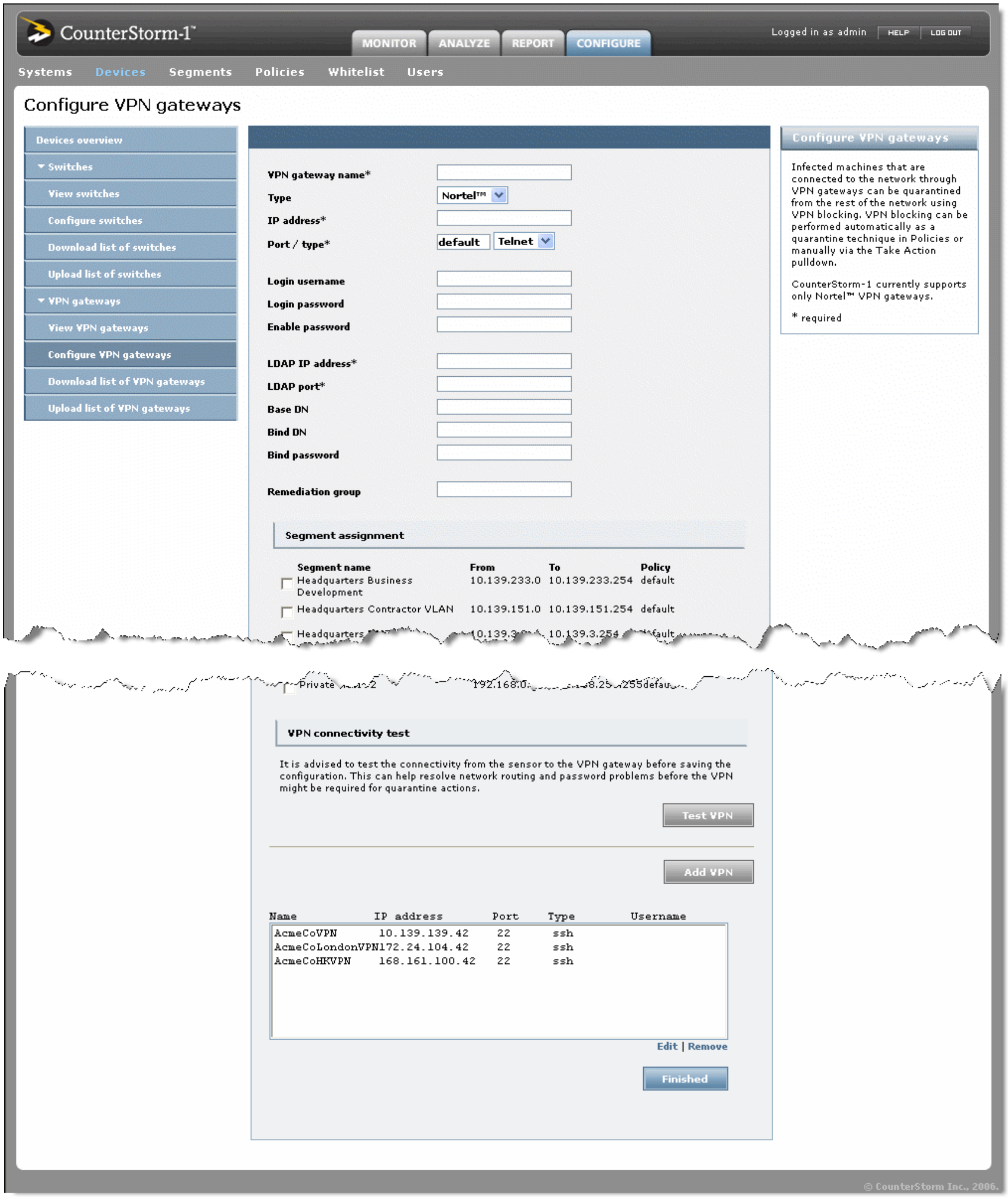
To configure VPN gateway data:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed. Existing VPN gateway blocking information is displayed in the VPN gateway information section.

2. Click the **Configure VPN gateways** link.

   The configure VPN gateways screen displays.



Configure VPN gateways

VPN gateway name*	
Type	Nortel™
IP address*	
Port / type*	default Telnet
Login username	
Login password	
Enable password	
LDAP IP address*	
LDAP port*	
Base DN	
Bind DN	
Bind password	
Remediation group	

Segment assignment

	Segment name	From	To	Policy
□	Headquarters Business Development	10.139.233.0	10.139.233.254	default
□	Headquarters Contractor VLAN	10.139.151.0	10.139.151.254	default
□	Headquarters	10.139.3.	10.139.3.254	fault
□	Private 2	192.168.0.	8.25 255	defau

VPN connectivity test

It is advised to test the connectivity from the sensor to the VPN gateway before saving the configuration. This can help resolve network routing and password problems before the VPN might be required for quarantine actions.

```
Name            IP address        Port    Type        Username
AcmeCoVPN        10.139.139.42     22      ssh
AcmeCoLondonVPN172.24.104.42      22      ssh
AcmeCoHKVPN      168.161.100.42    22      ssh
```

Configure VPN gateways

Infected machines that are connected to the network through VPN gateways can be quarantined from the rest of the network using VPN blocking. VPN blocking can be performed automatically as a quarantine technique in Policies or manually via the Take Action pulldown.

CounterStorm-1 currently supports only Nortel™ VPN gateways.

* required

3. Enter the desired information to configure VPN gateways to be used when applying blocking.

   Enter the name, IP address, and port/type of the VPN device.

   Enter information about LDAP configuration.

   Enter the remediation group name as well as login information.

   Check the segments to which this gateways applies.

   You can test VPN connectivity by clicking the **Test VPN** button.

4. Click **Add VPN**.

   You can add many VPN gateways prior to clicking finished.

5. When all VPN gateways have been added, click **Finished**.

   You may also edit and remove VPNs.

Uploading VPN Gateway Information

You can upload a CSV file containing VPN gateways.

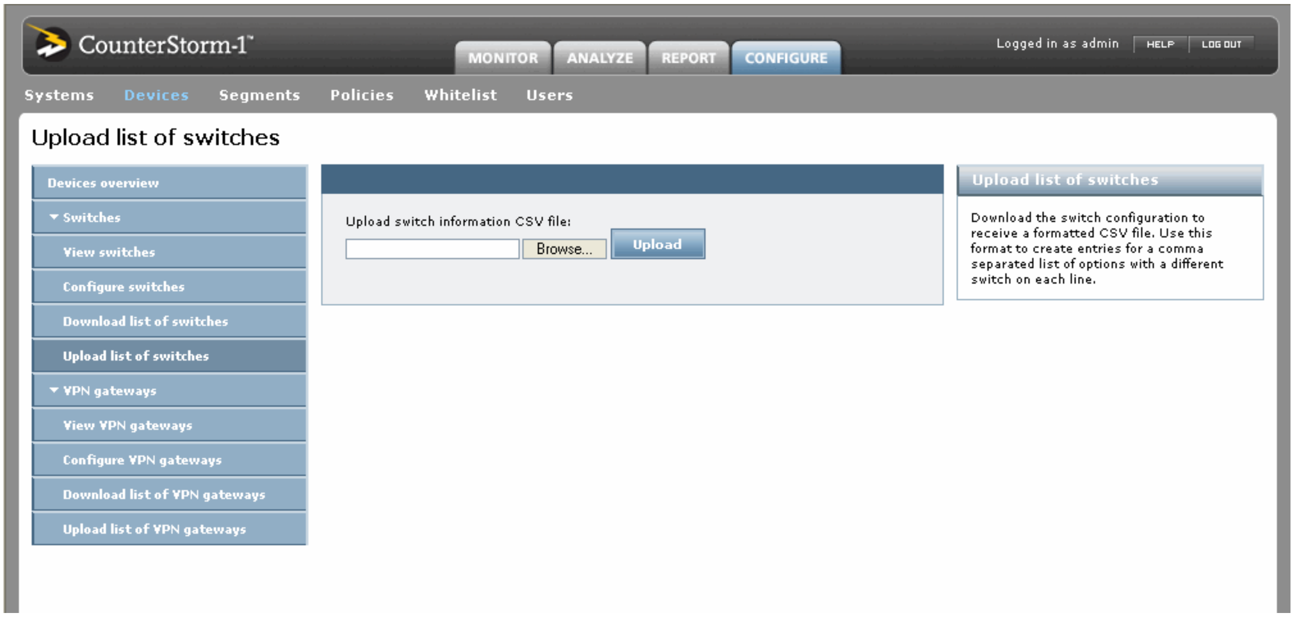
To upload VPN gateways:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed.

2. Click **Upload list of VPN gateways**.

   The screen appears with a box allowing you to browse for the CSV file.



Upload list of switches

Upload switch information CSV file:

Download the switch configuration to receive a formatted CSV file. Use this format to create entries for a comma separated list of options with a different switch on each line.

3. Browse to locate the file.
4. Click **Upload**.

Downloading VPN Gateways Information

You can download a CSV file that contains the VPNs specified in “Configuring VPN Gateway Information” on page 11-7.

To download VPN gateway information:

1. Select **Configure** from the Main Toolbar and **Devices** from the Interactive Toolbar.

   The Devices screen is displayed.

2. Click **Download VPN gateway information**.

   You are prompted to open or save a CSV file containing the configured switch. You can open this file in any spreadsheet program, such as Microsoft Excel.

Chapter 12: Configuring Whitelists

This section explains how to configure CounterStorm-1's whitelist.

A whitelist is a list of critical systems that are exempt from the quarantine techniques. You can whitelist machines, services, or machines and services. The following types of machines and services should be considered as whitelist candidates:

- Any system, especially mission-critical machines or services, that should not be disconnected or acted against even if it is infected.
- Any system that regularly does vulnerability assessment and port mapping of any service (whitelist both the port and protocol used).
- Any system that regularly probes many IP addresses, even if there are no systems associated with those IP addresses.
- Machines and/or services whose legitimate traffic mimics attacks.

Some example machines to whitelist are e-commerce systems, vulnerability assessments systems, and Citrix servers.

Note: Items can also be added to the whitelist via the Take Action Pulldown.

In This Chapter

First Week Whitelist

The following process is a suggested methodology for creating a whitelist in the first week of CounterStorm-1 operation.

To determine which hosts or services should be whitelisted:

1. Select **Configure** from the Main Toolbar and **Whitelist** from the Interactive Toolbar and review the items listed.

   The Whitelist screen is displayed with a summary of whitelist configurations. The categories include the system's IP address, services or ports, a description of why the system is whitelisted, and the active response selections.
2. Identify hosts and services that are in your network and may be candidates for whitelisting by matching them with the criteria in the table in "Creating the Whitelist" on page 12-4.

3. View the recommended whitelist as described in “Recommended Whitelist” on page 12-8.
4. Install and run CounterStorm-1 without a whitelist for one week.
5. When CounterStorm-1 alarms on the machines, confirm that the alarms concern expected and legitimate traffic and add the machines/services to the whitelist.

Note: Sometimes alarms are triggered by misconfigured systems, legacy servers, peer-to-peer activity, and unauthorized use of vulnerability or inventory tools such as nmap and nessis. It is recommended that these systems be remediated rather than whitelisted. However, you may wish to add these systems to the whitelist while they are being remediated. Do this only if you have a rigid process in place for removing the systems from the whitelist when they are remediated. This process is useful for improving the network’s security practices as unauthorized and inappropriate activities are identified.

Note: It is recommended that you whitelist the fewest number of machines and services. Whitelist entries should be reviewed quarterly to remove outdated entries.

Viewing the Whitelist

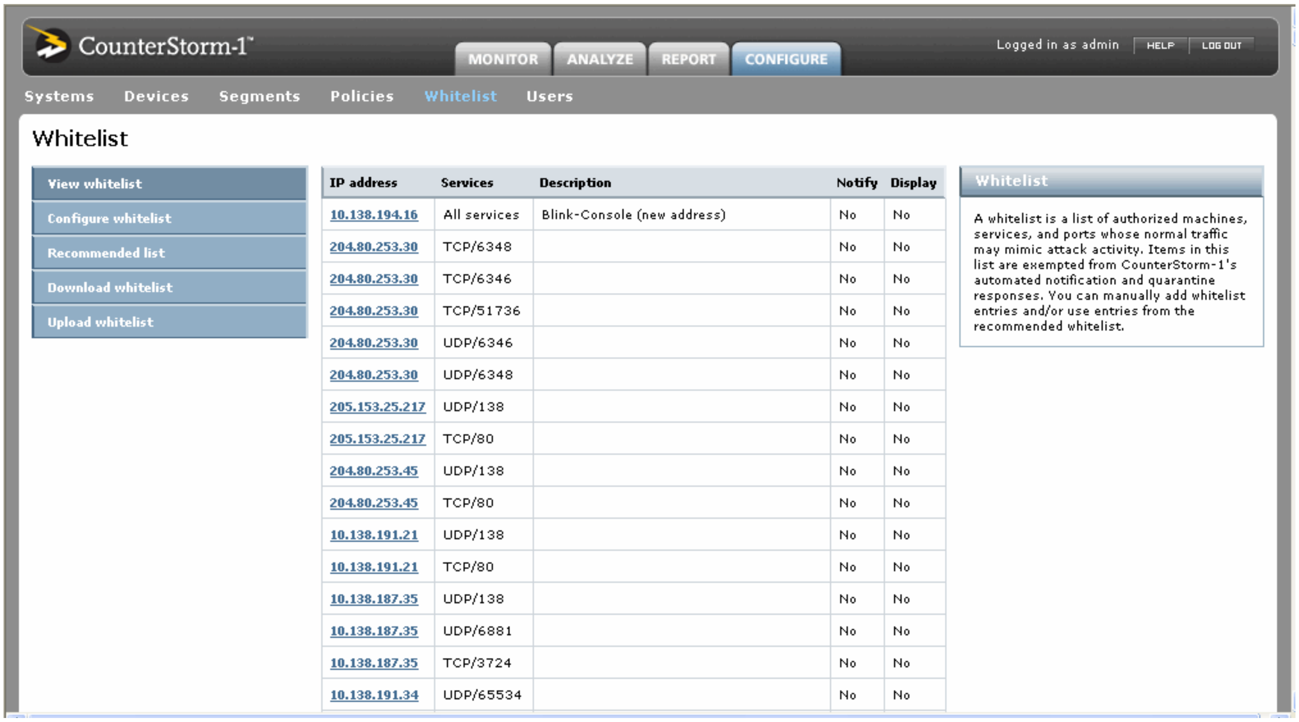
When you access the whitelist page, all whitelist entries are shown. You can return to the list at anytime.

To view the whitelist:

1. Select **Configure** from the Main Toolbar and **Whitelist** from the Interactive Toolbar.

   The Whitelist screen is displayed.
2. Click **View Whitelist**.

   The whitelist is displayed.



IP address	Services	Description	Notify	Display
10.138.194.16	All services	Blink-Console (new address)	No	No
204.80.253.30	TCP/6348		No	No
204.80.253.30	TCP/6346		No	No
204.80.253.30	TCP/51736		No	No
204.80.253.30	UDP/6346		No	No
204.80.253.30	UDP/6348		No	No
205.153.25.217	UDP/138		No	No
205.153.25.217	TCP/80		No	No
204.80.253.45	UDP/138		No	No
204.80.253.45	TCP/80		No	No
10.138.191.21	UDP/138		No	No
10.138.191.21	TCP/80		No	No
10.138.187.35	UDP/138		No	No
10.138.187.35	UDP/6881		No	No
10.138.187.35	TCP/3724		No	No
10.138.191.34	UDP/65534		No	No

Whitelist

A whitelist is a list of authorized machines, services, and ports whose normal traffic may mimic attack activity. Items in this list are exempted from CounterStorm-1's automated notification and quarantine responses. You can manually add whitelist entries and/or use entries from the recommended whitelist.

Understanding the Default Whitelist

Whenever a new sensor is registered, the default whitelist entries for CounterStorm-1 are refreshed. The entries are always marked with "[auto-whitelisted]." Defaiult entries are added upon every sensor registration to ensure that the new networks associated with these sensors are not degraded by CounterStorm-1's automatic blocking of newly visible network nodes, before the sensor has time to train and the whitelists can be refined by suggestions.

ARCserve backup discovery

Although in most cases, the scanning that is performed by an ARCserve backup client is normal, there is a known vulnerability (http://www.kb.cert.org/vuls/id/864801) for this application. It is therefore globally whitelisted for blocking, but not whitelisted for notifications or display. If your ARCserve software is a new version that is not vulnerable, you should whitelist for notification and perhaps even display as well. If you do not use ARCserve, you can delete this whitelist entry, but it will be re-added on any new sensor registration.

Symantec/Norton AntiVirus client polling

This section applies to Symantec/Norton AntiVirus legacy client discovery and Symantec/Norton AntiVirus server discovery. There are three cases when the behavior of a Symantec AntiVirus (AV) server or client may appear like that of a worm scanning for victims. The first one occurs when an AV server is attempting to push out an update, but a large number of clients are turned off or unavailable. The second occurs when an AV server is scanning for newly installed, old versions of clients on the network, and the third one is caused by newer clients scanning for a server to update from. Generally, a whitelist of TCP/2967 (the first of these three) for all machines is not necessary; only the AV server machines need to be whitelisted.

ISAKMP security key management (RFC 2408)

Some systems with IPSEC support attempt to make an ISAKMP connection to every machine that any application on the system is connecting to, which results in an apparent scan of TCP/500.

SNMP trap notifications

SNMP traps sent to management stations by the SNMP agents on devices are never acknowledged, and if an agent is configured with many trap destinations, this may appear to be scanning activity. Since the sources of SNMP traps are typically network devices that are unlikely to be vulnerable to worms, this service is automatically whitelisted for all machines.

NTP server

NTP servers may be configured to contact many different servers to compare time offsets; this may appear as scanning if there are enough configured peer servers due to dropped responses or other reachability problems. For this reason, any NTP servers that are configured by IP address (not by name) for a sensor or Command Center (excluding the Command Center itself) are automatically whitelisted. If you have other NTP servers, you should whitelist them for UDP/123 as well.

DHCP/BootP relay forwarding and DHCP/BootP responses to clients

DHCP is especially prone to false alarms because the clients often use an address of all-zeros to make the initial request; additionally, the relay forwarding makes the activity on these ports look like scans of incomplete connections. The relay forwarding entry is not whitelisted for notification since there are presumably a small number of DHCP relays on the network, each of which should be whitelisted individually for UDP/67. The whitelisting of UDP/68 for notification and display for all machines is done because the level of false alarms would be significant due to the unusual traffic flows for this protocol. As DHCP servers frequently check for expired/inactive leases using ICMP, you may want to whitelist DHCP servers (individually) for ICMP as well.

NetBIOS Datagrams

NetBIOS datagram/UDP service (UDP/138) is whitelisted for notification and display on all machines because of the wide variety of services that run over this transport, and because their frequently asymmetric communication patterns are often mistaken for worm scanning. While there are exploits that attack UDP/138, all of them involve other Microsoft networking ports that are not whitelisted, so ignoring apparent scanning activity on this port does not affect the detection capabilities of the CounterStorm-1 product.

DNS server

DNS servers that have recursion enabled contact many different DNS servers on the Internet, and if any of them are down for any reason, it may appear like worm scanning activity. For this reason, any DNS servers that are configured for a sensor or Command Center, or which are authoritative servers for the domain in which the sensor resides, are automatically whitelisted. If you have other DNS servers that perform recursive queries, you should whitelist them for UDP/53 as well.

Creating the Whitelist

You should add entries to the whitelist as you find activity that is deemed acceptable. For optimal operation of your CounterStorm-1 system, it is important that you whitelist certain types of normal activity so that they do not generate spurious notifications or cause uninfected systems to be quarantined. During the initial installation, a number of default (auto-whitelisted) whitelist entries are generated, and these cover cases that cause problems at nearly all sites. However, every network is different, and you need to add whitelist entries that are particular to your network. When you add a whitelist entry, there are a number of levels of whitelisting that you can apply. All whitelist entries prevent any automatic blocking (quarantine) technique that is part of the policy assigned to the segment from being applied to the machine that has caused an alarm, but whitelist entries can also prevent other actions. If you click the box labeled **Do not notify** when adding the whitelist entry, both blocking and notification actions will be suppressed. If you click the box labeled **Do not display**, not only are blocking and notification actions suppressed, but the display of matching alarms is disabled on the Analyze screen (even if you select the Whitelisted Activity View option in the Browse Activity area).

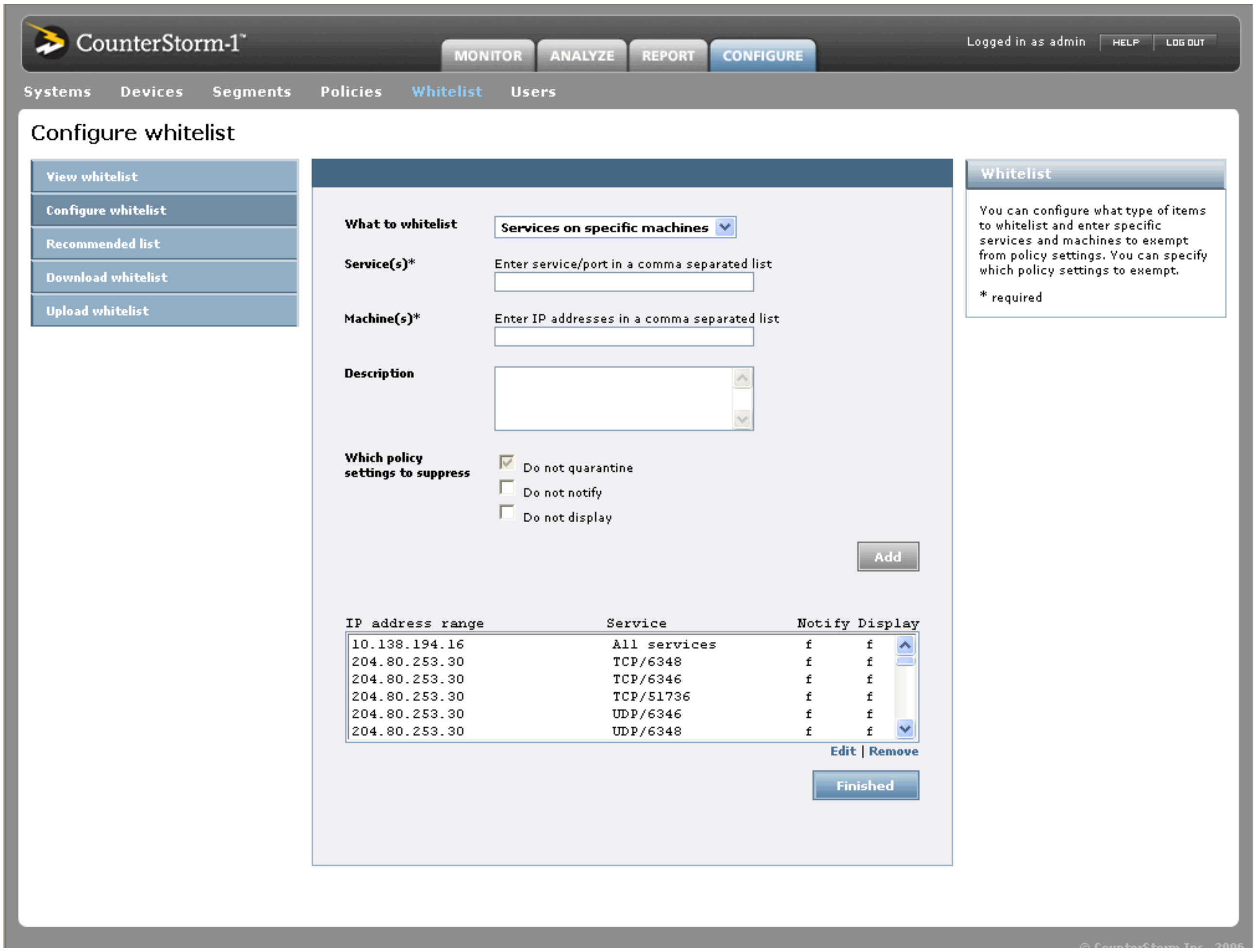
To add a host or service to the whitelist:

1. Select **Configure** from the Main Toolbar and **Whitelist** from the Interactive Toolbar.

   The whitelist screen is displayed with a summary of whitelist configurations.

   Clicking a whitelist entry or the configure whitelist button takes you to the whitelist configuration screen.
2. Click **Configure whitelist**.

   The Configure whitelist screen displays.



Configure whitelist

What to whitelist: Services on specific machines

Service(s)*: Enter service/port in a comma separated list

Machine(s)*: Enter IP addresses in a comma separated list

Description

Which policy settings to suppress:
☑ Do not quarantine
□ Do not notify
□ Do not display

```
IP address range              Service         Notify Display
10.138.194.16                 All services      f       f
204.80.253.30                 TCP/6348          f       f
204.80.253.30                 TCP/6346          f       f
204.80.253.30                 TCP/51736         f       f
204.80.253.30                 UDP/6346          f       f
204.80.253.30                 UDP/6348          f       f
```

Whitelist

You can configure what type of items to whitelist and enter specific services and machines to exempt from policy settings. You can specify which policy settings to exempt.

* required

3. Select the type of whitelist you want.

   The choices are: Services on specific machines (the most common case), Services across all machines, Entire machines, and E-mail worms. If you select Entire machines, you can choose to whitelist e-mail worms on those machines or not.

4. Select the specific machine(s) and/or service(s) that you want to whitelist.

   Note that if you specify more than one service or machine, multiple whitelist entries are automatically created.

   Some whitelist entries (such as DNS servers) are automatically added. Add the service/ ports that you want to whitelist. Ranges are separated by a “-”. For example: UDP53-67. You should view the recommended whitelist as described in “Recommended Whitelist” on page 12-8. This will help you decide on some entries. In addition, you should consider the whitelist suggestions on page 3-13 as well as the specific recommendations in the table below.

Types of Machines	What to Whitelist	Do Not Notify	Do Not Display
E-mail Gateways	Services on specific machines: TCP/25	•	•
E-mail List Servers	E-mail worms		
DNS Name Servers	Services on specific machines: UDP/53	•	•
DHCP Servers/Relays	Services on specific machines: UDP/67, UDP/68, ICMP	•	•
HTTP Proxies	Services on specific machines: TCP/80	•	•
NTP Time Servers	Services on specific machines: UDP/123	•	•
Network Management	Services on specific machines: ICMP, UDP/161	•	•
RADIUS Proxies	Services on specific machines: UDP/1645, UDP 1812	•	•
Microsoft Domain Controllers	Services on specific machines: ICMP, UDP/137	•	
Microsoft Active Directory Domain Controllers	Entire Machines	•	
Vulnerability/Asset Management	Entire Machines	•	
Mission Critical Systems	Entire Machines		
Trend Micro OfficeScan	Services on specific machines: TCP/12345	•	•

Select the machines on which to whitelist the service(s). You can whitelist a service on one machine, on all machines, or on a range of machines. The machines are identified by IP address.

This description field is useful when evaluating the whitelist, because it explains why you added this host or service to the whitelist.

Turn off the selected active responses for that system. These include:

- Blocking machine or service from the rest of the network. This is the default selection.
- Notification of alarms.
- Display of alarms in the user interface.

It is recommended that whitelist entries for critical servers (which you do not wish to ever shut down) should still notify administrators and display so that problems are still detected and remediation can take place. While no blocking action is implemented automatically against a whitelisted machine, it is useful to receive alarms about the machine in case of infection. You can Take action on a whitelist machine manually as you review it in the Monitoring Activity Table.

For systems that generate known false alarms, it is recommended that you disable display and notification responses. You may find it useful to track certain systems that generate known false alarms, such as vulnerability assessment tools. You can view the resulting false alarms in the analyze screen for verification of each tool's functionalitity.

5. Click the **Add** button.

   Each item is added to the table.
6. When all list entries are added, click **Finished**.

To edit or remove a host or service from a whitelist:

1. Select **Configure** from the Main Toolbar and **Whitelist** from the Interactive Toolbar.

   The whitelist screen is displayed with a summary of whitelist configurations.
2. Click **Configure whitelist**.

   The Whitelist configuration screen displays.
3. Click the desired entry in the table at the bottom of the screen.

   The whitelist configuration screen displays populated with the selected entry's information.
4. Click **Edit** or **Remove.**
5. Make the desired changes.
6. Click **Update Changes**.

   You can click the **Remove** link to remove the entry. To modify or remove additional entries, select them from the table on the configure page or return to the main View page.

Uploading the Whitelist

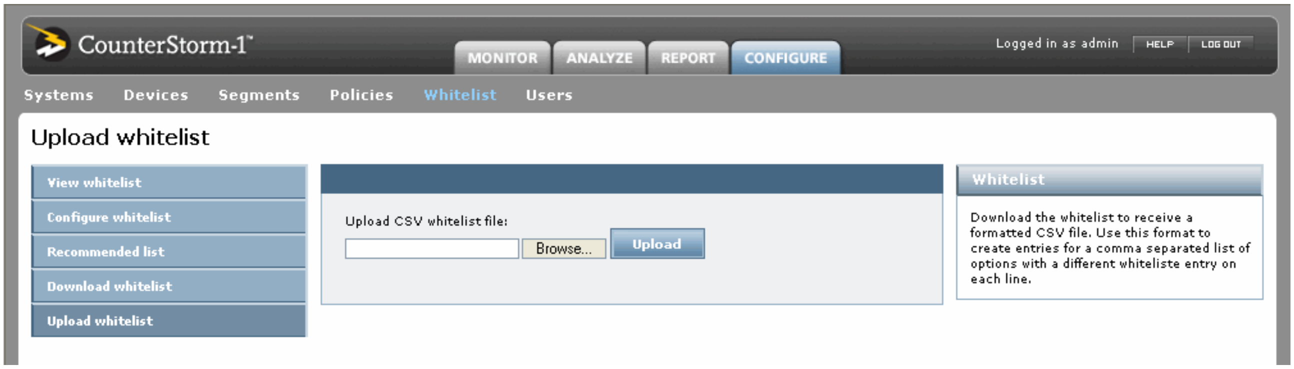
You can upload a CSV file containing whitelist entries.

To upload whitelist entries:

1. Select **Configure** from the Main Toolbar and **Whitelist** from the Interactive Toolbar.

   The Whitelist screen is displayed
2. Click **Upload whitelist entries**.

The screen appears with a box allowing you to browse for the CSV file.



Download the whitelist to receive a formatted CSV file. Use this format to create entries for a comma separated list of options with a different whiteliste entry on each line.

3. Browse to locate the file.
4. Click **Upload**.

Downloading the Whitelist to a CSV file

You can download a CSV file that contains the whitelist.

To download whitelist information:

1. Select **Configure** from the Main Toolbar and **Whitelist** from the Interactive Toolbar.

   The Whitelist screen is displayed.
2. Click **Download whitelist information**.

   You are prompted to open or save a CSV file containing the configured whitelist information. You can open this file in any spreadsheet program, such as Microsoft Excel.

Recommended Whitelist

CounterStorm-1 analyzes the activity on the network to determine a list of recommended whitelist entries. Please check the suggestions carefully before adding them so as not to risk leaving critical resources unprotected. It is advisable to let the system run for at least two weeks in order to accumulate a good recommended list.

After your CounterStorm-1 systems have been running for a while, you can use the Whitelist Recommendations to provide suggestions for new whitelist entries that can help to eliminate false alarms for normal behavior at your site. The recommendations are merely suggestions; some activity that is normal but has generated alarms may not be included, and the list may include some activity that is caused by real infections. Use caution when adding whitelist entries, and if you are not sure that particular activity is normal for your site, do not add a whitelist entry for it. Also, you should use the most specific whitelist entry possible in order to prevent false alarms. If you can prevent false alarms for a service with four or five machine-specific whitelist entries instead of whitelisting the service for all machines, it is usually better to add the machine-specific entries. Adding whitelist entries for services on all machines when this is not actually necessary can significantly reduce the effectiveness of your CounterStorm-1 installation.

The whitelist recommendations are made on the basis of repeated alarms in the past two weeks for the same services and/or machines, but any alarms for a machine which has had an identified alarm are not considered as candidates. (Identified alarms are those which have identification information other than UNKNOWN or PENDING in the Analyze Activity table Possible Cause field.) This restriction helps to prevent recommending whitelists for any machine that is actually infected, but also prevents whitelist recommendations for machines running SNMP (UDP/161) management software or common peer-to-peer (P2P) file-sharing or gaming applications, as well as machines which have had e-mail worm alarms.

If you wish to whitelist those types of activity, either for all machines, or for a specific machine, you will find it easiest to use the Take Action pulldown menu on the Analyze screen, selecting Whitelist service or Whitelist host/service respectively. Alarms that would have been whitelisted by the current entries (regardless of whether they were whitelisted at the time) are not considered as candidates when generating suggestions; as a result, after adding or removing whitelist entries, new lists of suggestions will have different entries.

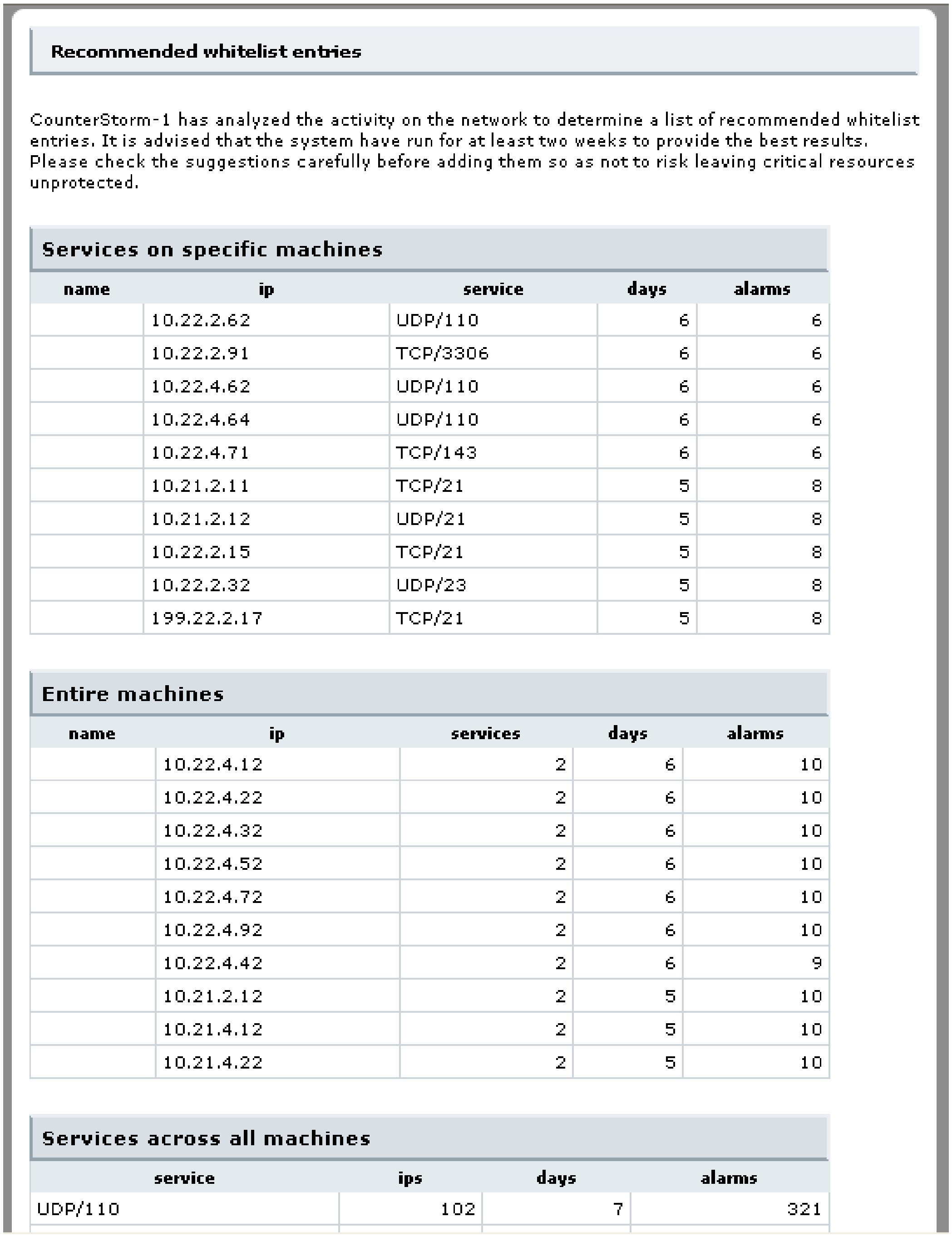
Note: Items with Snort signatures will not appear in the recommended whitelist.

To view recommended whitelist information:

1. Select **Configure** from the Main Toolbar and **Whitelist** from the Interactive Toolbar.

   The Whitelist screen is displayed.

2. Click **Recommended whitelist**.



Recommended whitelist entries

CounterStorm-1 has analyzed the activity on the network to determine a list of recommended whitelist entries. It is advised that the system have run for at least two weeks to provide the best results. Please check the suggestions carefully before adding them so as not to risk leaving critical resources unprotected.

Services on specific machines

name	ip	service	days	alarms
	10.22.2.62	UDP/110	6	6
	10.22.2.91	TCP/3306	6	6
	10.22.4.62	UDP/110	6	6
	10.22.4.64	UDP/110	6	6
	10.22.4.71	TCP/143	6	6
	10.21.2.11	TCP/21	5	8
	10.21.2.12	UDP/21	5	8
	10.22.2.15	TCP/21	5	8
	10.22.2.32	UDP/23	5	8
	199.22.2.17	TCP/21	5	8

Entire machines

name	ip	services	days	alarms
	10.22.4.12	2	6	10
	10.22.4.22	2	6	10
	10.22.4.32	2	6	10
	10.22.4.52	2	6	10
	10.22.4.72	2	6	10
	10.22.4.92	2	6	10
	10.22.4.42	2	6	9
	10.21.2.12	2	5	10
	10.21.4.12	2	5	10
	10.21.4.22	2	5	10

Services across all machines

service	ips	days	alarms
UDP/110	102	7	321

Host-wide, service-wide, and specific whitelist entries are listed. You must manually add these entries into your whitelist.

Whitelist recommendations are presented in three groups, which correspond to the three types of whitelist entries that can be created: for services on specific machines, for entire machines, and for services across all machines. In the first group are the top ten specific whitelist entries (service and machine) that had multiple candidate alarms across multiple days. If fewer than ten entries meet these criteria, only those entries are displayed. If your CounterStorm-1 installation hasn't been running for long, or if there are very few unidentified alarms that are not covered by the current whitelist, there may be no whitelist recommendations at all. Before adding a specific whitelist entry based on a recommendation, try to confirm that the service in question is one that is normally used by the machine, and that any scanning activity observed is not the result of any infection.

In the second group are recommendations for entire machine whitelist entries. The top ten machines that have had multiple candidate alarms across multiple days and multiple services will appear in this list. If there are entire machine whitelist recommendations, you should evaluate them to see if it makes sense to apply the whitelist to the entire machine, rather than as specific whitelist entries for certain services on the machine. In most cases, it is better to use specific whitelist entries. One notable exception where whitelisting an entire machine is perhaps the best solution is in cases where a particular machine has asymmetric traffic routing (possibly due to a multi-homed configuration). In these cases, the CounterStorm-1 sensors see traffic from the machine when they cannot observe the corresponding traffic to the machine, and this may result in false alarms on many different services (especially UDP/1027 through UDP/1057 and above). As it is impractical to whitelist all the services for the machine (and any other services that were not whitelisted may still generate false alarms), it is best to whitelist the entire machine in these cases.

In the third group are recommendations for service whitelist entries across all machines. The top ten services that have had multiple candidate alarms across multiple machines and multiple days will appear in this list. Just as with entire-machine whitelist suggestions, it is often better to add whitelist entries that are specific to particular machines (especially if the machines generating false alarms are servers that can be enumerated fully in a short list). However, if false alarms for a particular service are widespread, and particularly if non-server machines are involved, it may be simpler to whitelist the service across all machines. A particular example where this might be the best solution would be if many clients are using network printer drivers that scan for available printers using SNMP (UDP/161), ICMP, or other services.

Chapter 13: Generating Reports

Reports provide detailed and summary information about activity within the network and can be used for recording activity and reporting to management about such activity. Reports can be customized to display only specified data about specified segments. These settings can be saved in a template or selected each time a new report is needed. After its creation, the report is generated for a specific time period and distributed in a variety of methods and formats. This section describes how to generate and view reports.

In This Chapter

- Viewing Reports
- Creating Templates
- Managing Scheduled Reports
- Managing Report Templates
- Generating Reports

Viewing Reports

When you access the reports page, all reports are shown. You can return to the reports list at anytime.

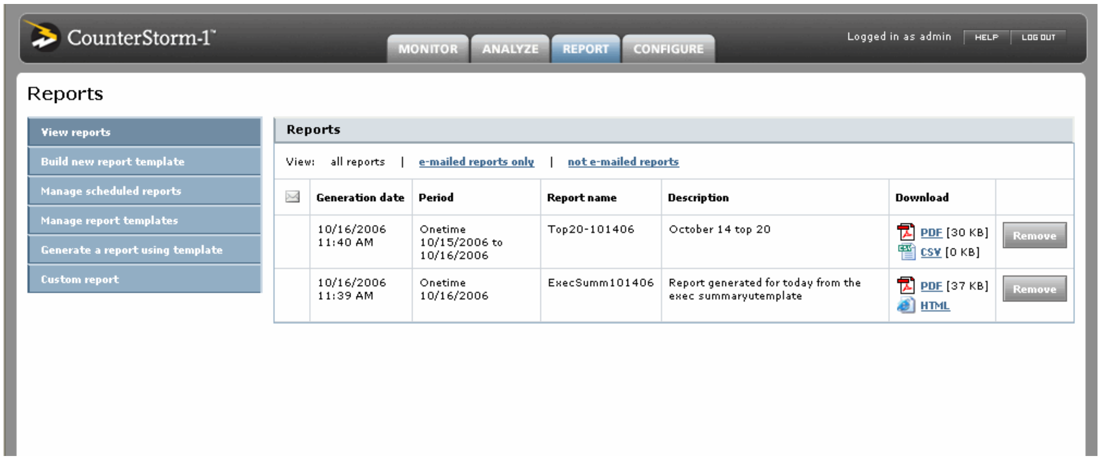
To view reports:

1. Select **Reports** from the Main Toolbar.

   The Reports screen is displayed.

2. Click **View Reports**.

   A list of generated reports is displayed. You can select the type of reports to view by clicking all reports, e-mailed reports, or not e-mailed reports. By defaults, all reports are displayed. You can view a report by clicking the PDF, HTML or CSV link for the report. You can delete a report by clicking the remove button.



Reports

Reports

View: all reports | e-mailed reports only | not e-mailed reports

✉	Generation date	Period	Report name	Description	Download
	10/16/2006 11:40 AM	Onetime 10/15/2006 to 10/16/2006	Top20-101406	October 14 top 20	PDF [30 KB] CSV [0 KB]
	10/16/2006 11:39 AM	Onetime 10/16/2006	ExecSumm101406	Report generated for today from the exec summaryutemplate	PDF [37 KB] HTML

Creating Templates

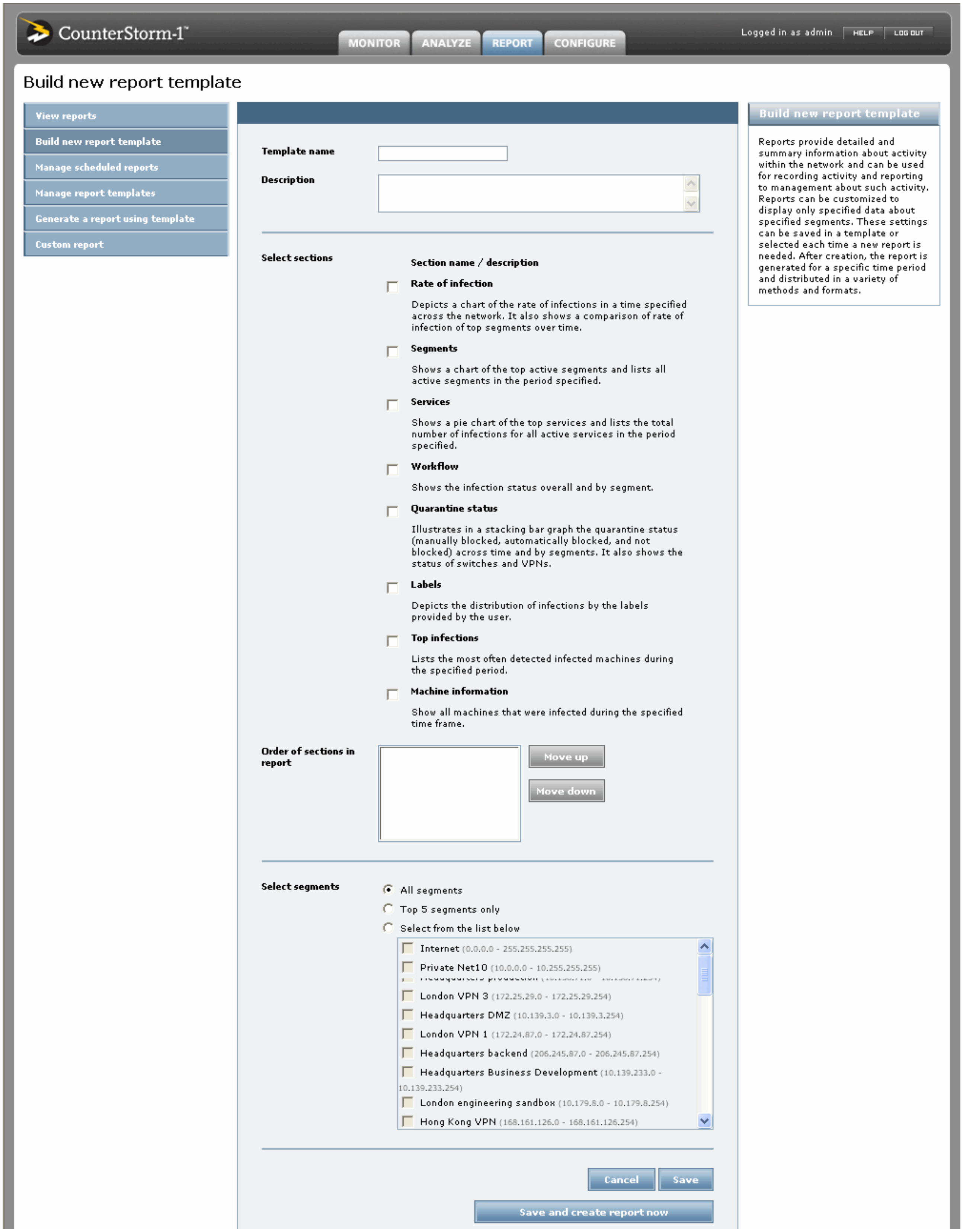
Report templates can be created and then used to generate reports. The template describes how you wish the report to look and what sections you wish to appear in the report.

To create report templates:

1. Select **Reports** from the Main Toolbar.

   The Reports screen is displayed.
2. Click **Build new report template**.

The report selection window appears.



Build new report template

Template name

Description

Select sections

Section name / description

□ **Rate of infection**

Depicts a chart of the rate of infections in a time specified across the network. It also shows a comparison of rate of infection of top segments over time.

□ **Segments**

Shows a chart of the top active segments and lists all active segments in the period specified.

□ **Services**

Shows a pie chart of the top services and lists the total number of infections for all active services in the period specified.

□ **Workflow**

Shows the infection status overall and by segment.

□ **Quarantine status**

Illustrates in a stacking bar graph the quarantine status (manually blocked, automatically blocked, and not blocked) across time and by segments. It also shows the status of switches and VPNs.

□ **Labels**

Depicts the distribution of infections by the labels provided by the user.

□ **Top infections**

Lists the most often detected infected machines during the specified period.

□ **Machine information**

Show all machines that were infected during the specified time frame.

Order of sections in report

Select segments

● All segments
○ Top 5 segments only
○ Select from the list below

□ Internet (0.0.0.0 - 255.255.255.255)
□ Private Net10 (10.0.0.0 - 10.255.255.255)
□ Headquarters production
□ London VPN 3 (172.25.29.0 - 172.25.29.254)
□ Headquarters DMZ (10.139.3.0 - 10.139.3.254)
□ London VPN 1 (172.24.87.0 - 172.24.87.254)
□ Headquarters backend (206.245.87.0 - 206.245.87.254)
□ Headquarters Business Development (10.139.233.0 - 10.139.233.254)
□ London engineering sandbox (10.179.8.0 - 10.179.8.254)
□ Hong Kong VPN (168.161.126.0 - 168.161.126.254)

Build new report template

Reports provide detailed and summary information about activity within the network and can be used for recording activity and reporting to management about such activity. Reports can be customized to display only specified data about specified segments. These settings can be saved in a template or selected each time a new report is needed. After creation, the report is generated for a specific time period and distributed in a variety of methods and formats.

3. Enter the template name and description.
4. Check the desired report components.

   As high-level items are checked, lower-level items are revealed for selection. Selection descriptions are provided on-screen. The selected sections are placed in the order of selections table. You can reorder the sections using the Move up and Move down arrows.
5. Select the segments on which the report should chronicle.
6. Click **Save**.

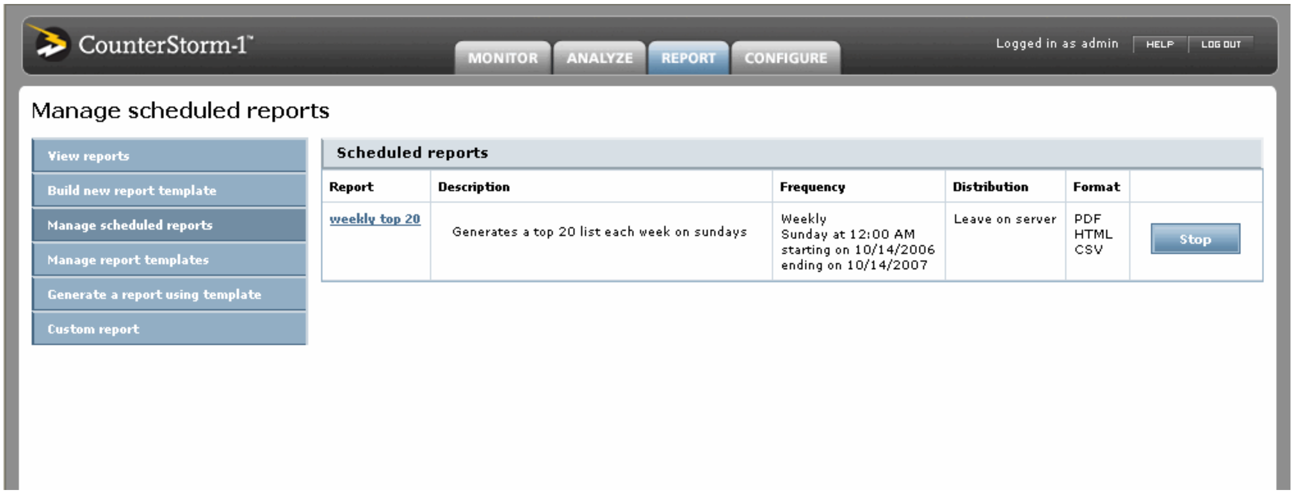
Managing Scheduled Reports

This button shows only those reports that are specified to run at periodic intervals as opposed to running them one time. You can review the report settings and stop the reports from running.

To manage scheduled reports:

1. Select **Reports** from the Main Toolbar.

   The Reports screen is displayed.
2. Click **Manage schedule reports**.

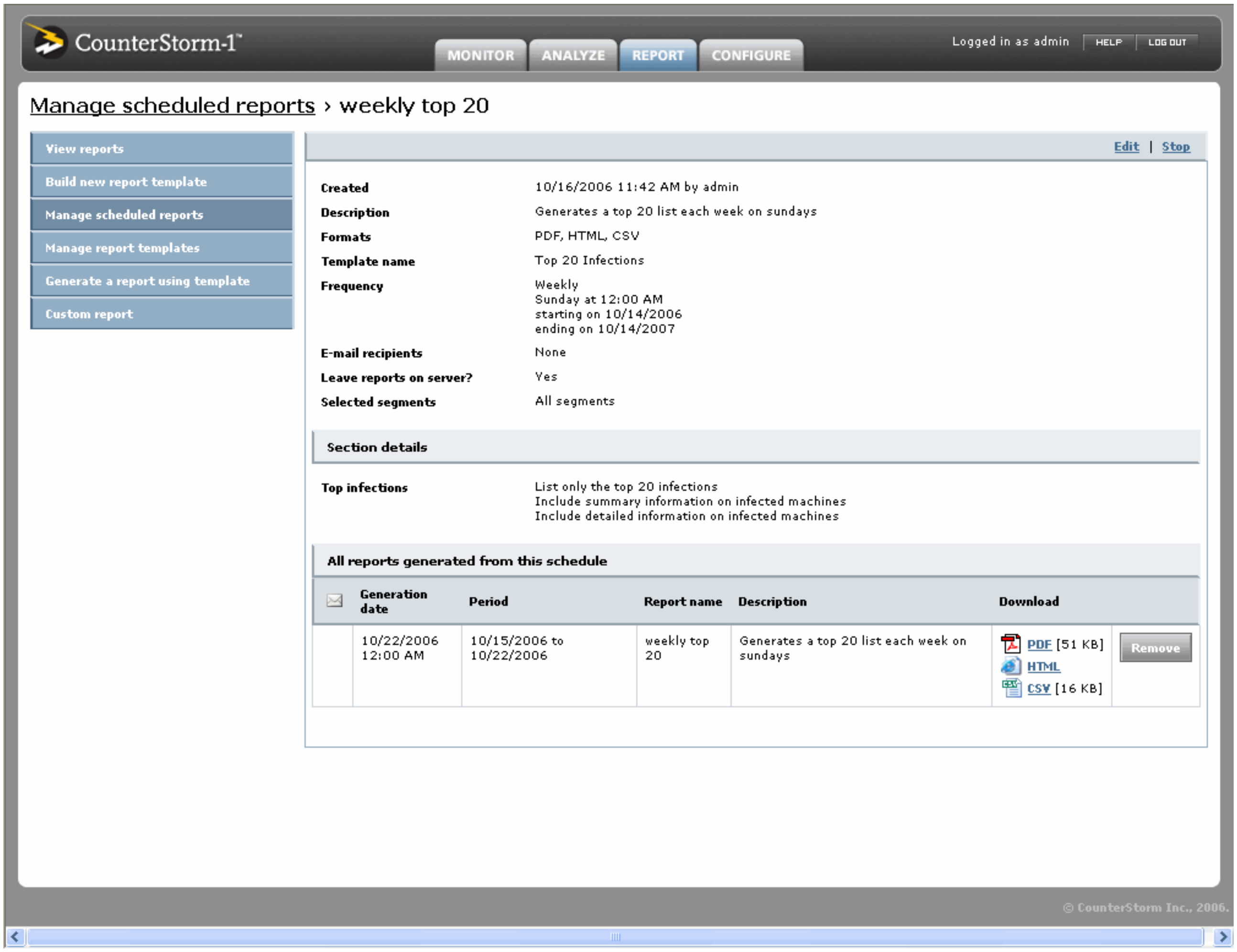


Manage scheduled reports

Scheduled reports

Report	Description	Frequency	Distribution	Format	
weekly top 20	Generates a top 20 list each week on sundays	Weekly Sunday at 12:00 AM starting on 10/14/2006 ending on 10/14/2007	Leave on server	PDF HTML CSV	Stop

Reports that run at periodic intervals are displayed. Click the report name to review its settings. You can click **Edit**, to change the report generation settings or **Stop** to stop the reports from running at the specified interval.



Manage scheduled reports › weekly top 20

Created	10/16/2006 11:42 AM by admin
Description	Generates a top 20 list each week on sundays
Formats	PDF, HTML, CSV
Template name	Top 20 Infections
Frequency	Weekly Sunday at 12:00 AM starting on 10/14/2006 ending on 10/14/2007
E-mail recipients	None
Leave reports on server?	Yes
Selected segments	All segments

Section details

Top infections	List only the top 20 infections Include summary information on infected machines Include detailed information on infected machines

All reports generated from this schedule

✉	Generation date	Period	Report name	Description	Download	
	10/22/2006 12:00 AM	10/15/2006 to 10/22/2006	weekly top 20	Generates a top 20 list each week on sundays	PDF [51 KB] HTML CSV [16 KB]	Remove

You may also click Stop from the Scheduled reports table.

Managing Report Templates

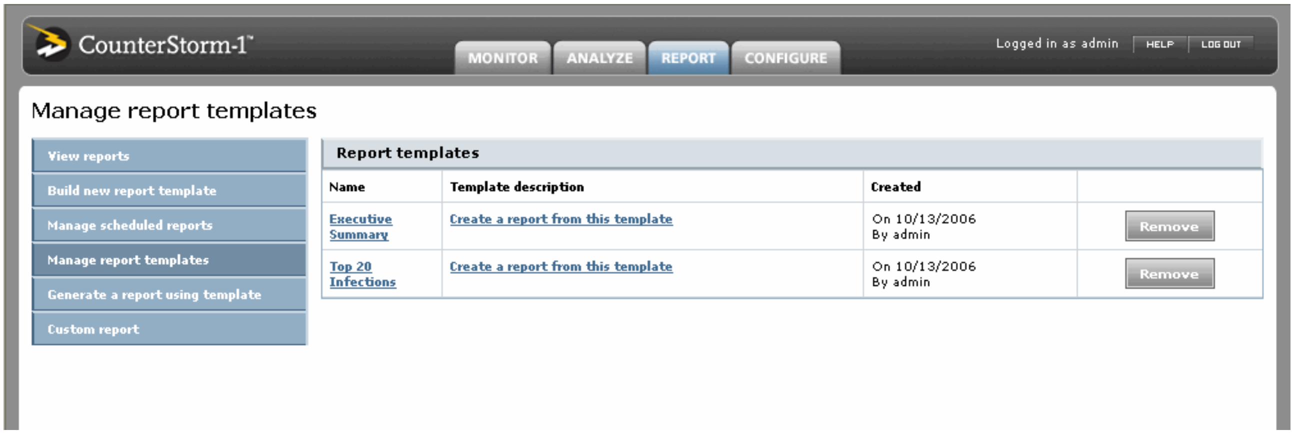
This button lists all existing report templates created via the **Build new report templates** button.

To manage report templates:

1. Select **Reports** from the Main Toolbar.

   The Reports screen is displayed.

2. Click **Manage report templates**.



Manage report templates

Report templates

Name	Template description	Created	
Executive Summary	Create a report from this template	On 10/13/2006 By admin	Remove
Top 20 Infections	Create a report from this template	On 10/13/2006 By admin	Remove

All existing templates are shown. You can view their settings and generate reports from these templates. Click the report name to review its settings. You can click **Edit**, to change the report generation settings or **Remove** to delete the reports . You may also click Remove from the Report templates table

Generating Reports

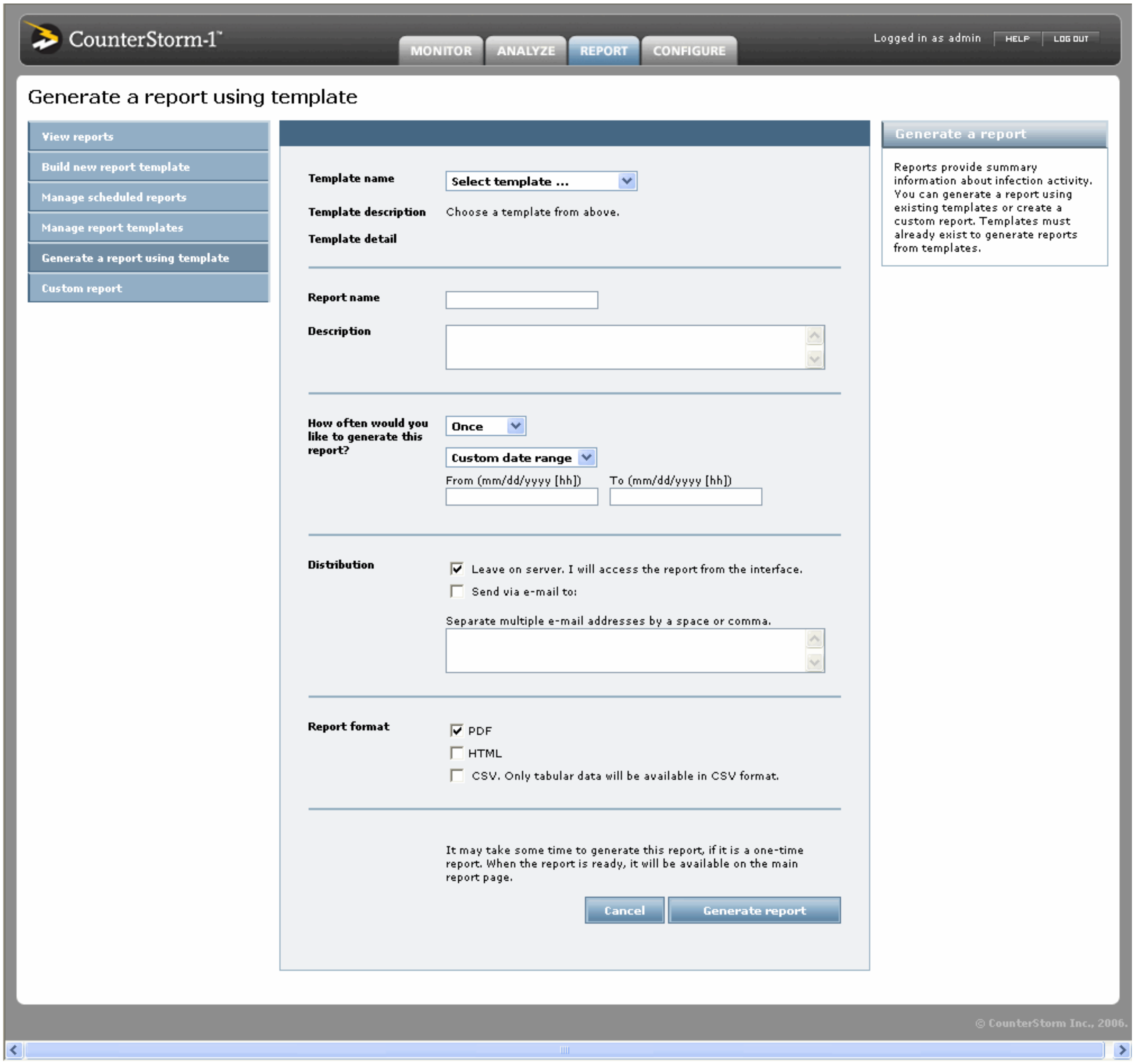
You can generate reports from templates or create custom reports.

To generate reports from templates:

1. Select **Reports** from the Main Toolbar.

   The Reports screen is displayed.

2. Click **Generate a report using template**.



Generate a report using template

Template name: Select template ...

Template description: Choose a template from above.

Template detail

Report name

Description

How often would you like to generate this report? Once

Custom date range

From (mm/dd/yyyy [hh]) To (mm/dd/yyyy [hh])

Distribution

☑ Leave on server. I will access the report from the interface.

□ Send via e-mail to:

Separate multiple e-mail addresses by a space or comma.

Report format

☑ PDF

□ HTML

□ CSV. Only tabular data will be available in CSV format.

It may take some time to generate this report, if it is a one-time report. When the report is ready, it will be available on the main report page.

Generate a report

Reports provide summary information about infection activity. You can generate a report using existing templates or create a custom report. Templates must already exist to generate reports from templates.

This option assumes you have already created templates from which to choose. You can also generate custom reports. The custom report functionality invokes options similar to creating a new template for the first page. See “Creating Templates” on page 13-2 for details. Once you have selected the desired sections for a custom report and selected **Next**, go to step 5. If you are generating a report using a template, go to step 3.

3. Select the template name.
4. Enter the name of the report and a description.
5. Enter generation date parameters.

   Enter how often you would like to run the report. You can select from preset date ranges or custom dates.
6. Select if you wish to retrieve the report via the interface and/or have it e-mailed.

Generating Reports

You can do both. For e-mail, enter addresses in a comma-separated list.

7. Choose the types of report formats to generate.

   Available options are PDF, HTML, and CSV.

8. Click **Generate Report**.

   The report is generated in the desired format. Reports that are available in the interface are accessible via the View Reports options as described in .

Chapter 14: Managing Your Sensors and Command Center

In This Chapter

- Viewing Systems
- Changing System Settings

This section explains how to modify existing CounterStorm-1 appliance administrative settings. Configuration information entered during Console Configuration is shown in these configuration screens. You can modify those items and add new configuration.

Viewing Systems

The System Overview screen displays the current status of the Command Center and sensor operation. The Command Center manages a distributed deployment of CounterStorm-1 sensors and is the central point for configuration, administration, real-time monitoring, and reporting. It receives alarms from each of the deployed sensors.

The sensors observe all traffic on their assigned segments and monitor them for attacks. Sensors apply notification and response policies to take action on malicious activity.

The System Overview screen shows the current status of the Command Center and sensors with which it communicates. Each device has its own row in the screen.

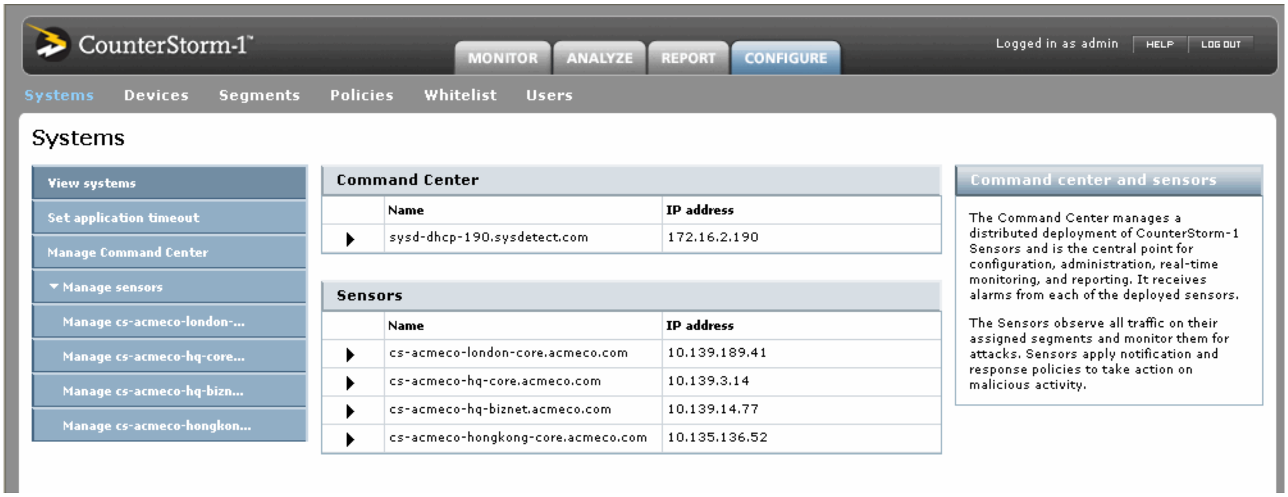
When you access the Systems page, the Command Center and all sensors are shown. You can return to the list at anytime.

To view systems:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.

   The Systems screen is displayed.
2. Click **View systems**.

The Command Center and sensors are displayed. You can view or modify configuration for items in the list by clicking on the desired system.



Systems

Command Center

	Name	IP address
▶	sysd-dhcp-190.sysdetect.com	172.16.2.190

Sensors

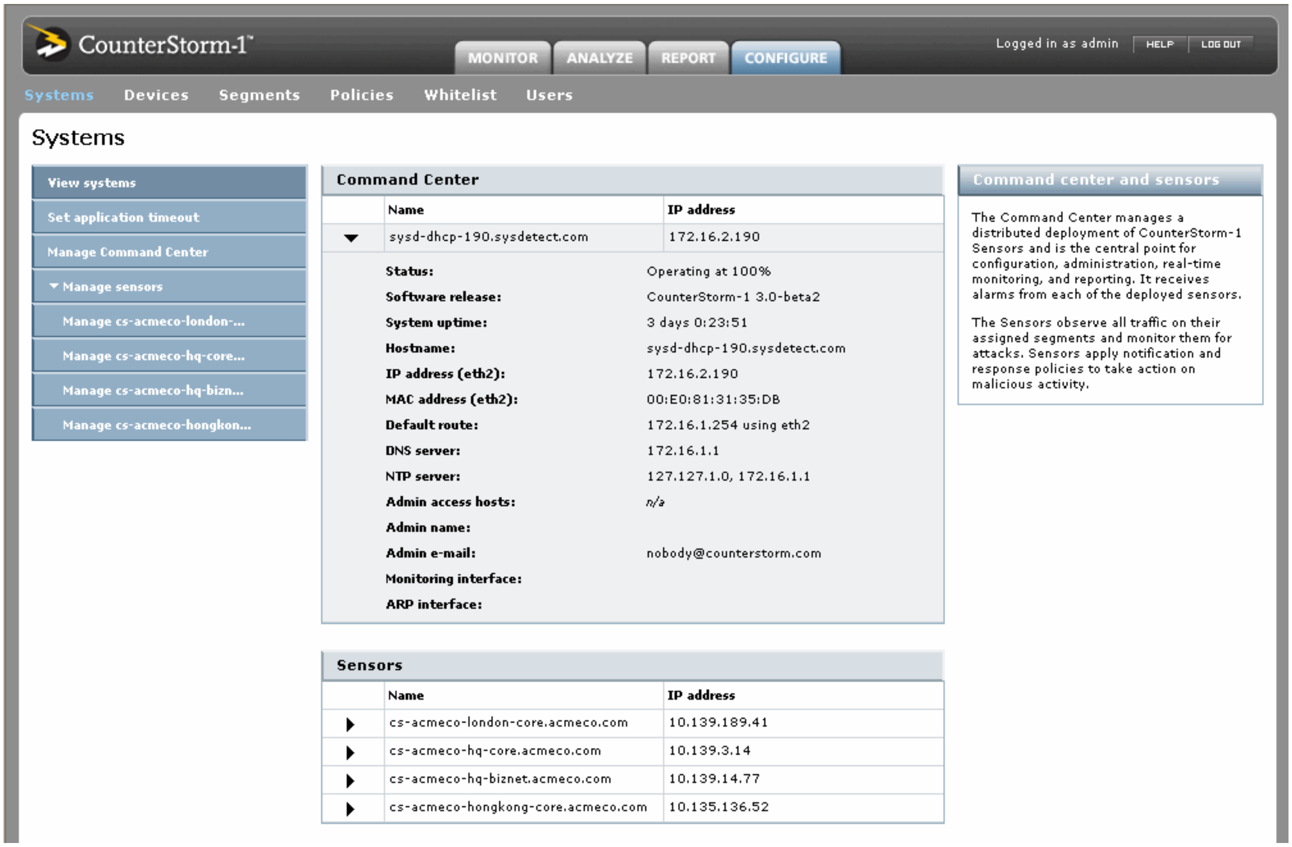
	Name	IP address
▶	cs-acmeco-london-core.acmeco.com	10.139.189.41
▶	cs-acmeco-hq-core.acmeco.com	10.139.3.14
▶	cs-acmeco-hq-biznet.acmeco.com	10.139.14.77
▶	cs-acmeco-hongkong-core.acmeco.com	10.135.136.52

Command center and sensors

The Command Center manages a distributed deployment of CounterStorm-1 Sensors and is the central point for configuration, administration, real-time monitoring, and reporting. It receives alarms from each of the deployed sensors.

The Sensors observe all traffic on their assigned segments and monitor them for attacks. Sensors apply notification and response policies to take action on malicious activity.

3. Click ▸ to expand the row.



Systems

Command Center

	Name	IP address
▼	sysd-dhcp-190.sysdetect.com	172.16.2.190

Status:	Operating at 100%
Software release:	CounterStorm-1 3.0-beta2
System uptime:	3 days 0:23:51
Hostname:	sysd-dhcp-190.sysdetect.com
IP address (eth2):	172.16.2.190
MAC address (eth2):	00:E0:81:31:35:DB
Default route:	172.16.1.254 using eth2
DNS server:	172.16.1.1
NTP server:	127.127.1.0, 172.16.1.1
Admin access hosts:	*n/a*
Admin name:	
Admin e-mail:	nobody@counterstorm.com
Monitoring interface:	
ARP interface:	

Sensors

	Name	IP address
▶	cs-acmeco-london-core.acmeco.com	10.139.189.41
▶	cs-acmeco-hq-core.acmeco.com	10.139.3.14
▶	cs-acmeco-hq-biznet.acmeco.com	10.139.14.77
▶	cs-acmeco-hongkong-core.acmeco.com	10.135.136.52

Command center and sensors

The Command Center manages a distributed deployment of CounterStorm-1 Sensors and is the central point for configuration, administration, real-time monitoring, and reporting. It receives alarms from each of the deployed sensors.

The Sensors observe all traffic on their assigned segments and monitor them for attacks. Sensors apply notification and response policies to take action on malicious activity.

4. Review the current status of the machine.

The name of the Command Center or sensor is listed as well as its IP address. Listed are: the system operating status (also mailed to designated e-mail addresses daily), current software version, and the amount of time the system has been up. Much of the remaining information listed is the information that was supplied during Console Configuration. This information can be modified, if necessary.

Changing System Settings

You can change the system settings for the Command Center or sensors. The administrative menus expand, allowing you to modify appliance settings. Information entered during Console Configuration is shown in these screens. You can modify this information as well as configure a variety of additional administrative items.

Clicking the arrow icon next to high-level items expands the menu tree on the left. Clicking blue underlined items repopulates the display area with the selected functionality.

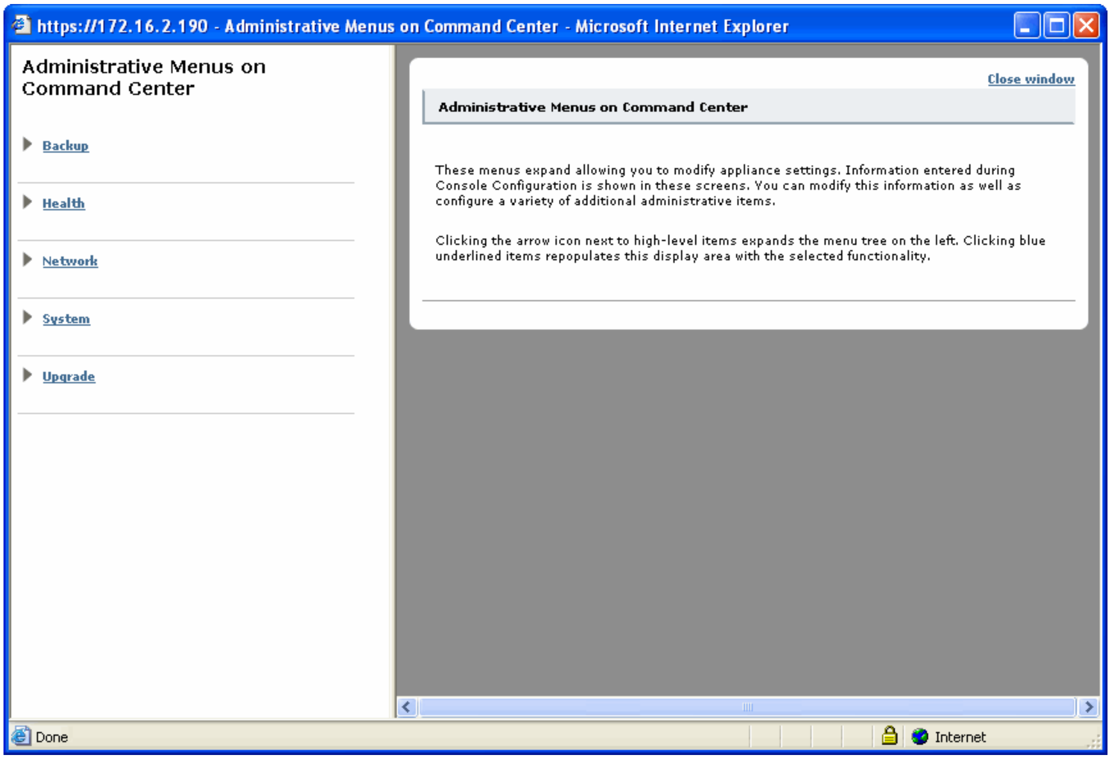
To change appliance settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.

   The System Overview screen is displayed.
2. Click ▸ to expand the row.
3. Review the Current status of the machine.
4. Click **Manage Command Center** or **Manage** *sensor_name.*

   Each sensor has it own button.

   A window pops up with configuration choices. Some of these choices allow you to modify the configuration that you set up during the console configuration process. Others provide additional administrative features.


https://172.16.2.190 - Administrative Menus on Command Center - Microsoft Internet Explorer
Administrative Menus on Command Center
Backup
Health
Network
System
Upgrade
Close window
Administrative Menus on Command Center
Done
Internet

These menus expand allowing you to modify appliance settings. Information entered during Console Configuration is shown in these screens. You can modify this information as well as configure a variety of additional administrative items.

Clicking the arrow icon next to high-level items expands the menu tree on the left. Clicking blue underlined items repopulates this display area with the selected functionality.

Option	Description
Backups	This menu allows you to perform a variety of backup options.
Networking	This menu provides configuration options for network administration and diagnostics.
Health	This menu provides health status options and reboot/restart options.
System	This menu provides configuration options for system administration, detection and response, and notification.
Upgrades	This menu allows you to check and manage the general health of the Command Center.

5. Click the desired menu item.

   The pop-up window is repopulated.
6. Enter the desired criteria and take the appropriate action (commit, apply, return to previous).

Backups

This menu allows you to modify or view health diagnostic information.

To modify or view health diagnostic information:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Backups**.

   The window is repopulated with the following selections:

Option	Description
Backup Device	Backs up the device.
Backup Network (Command Center Only)	Backs up network.
Review Backup	Provides information about backups.
Download Backup File	Allows you to download the backup file.
Download Network Backup File (Command Center Only)	Allows you to download the network backup file from the Command Center.
Upload Restore File	Allows you to upload a restore file.

4. Select the desired item to back up.

   You should backup the network and download the network backup file every time you change configuration. This ensures that changes are not lost in the event of a machine failure.
5. Perform actions as required for each menu item.
6. Click **Previous Menu**.

Backup Device

This item creates a backup of the system configuration. The backup file can be retrieved with Download Backup File. This command can take up to 10 minutes to complete.

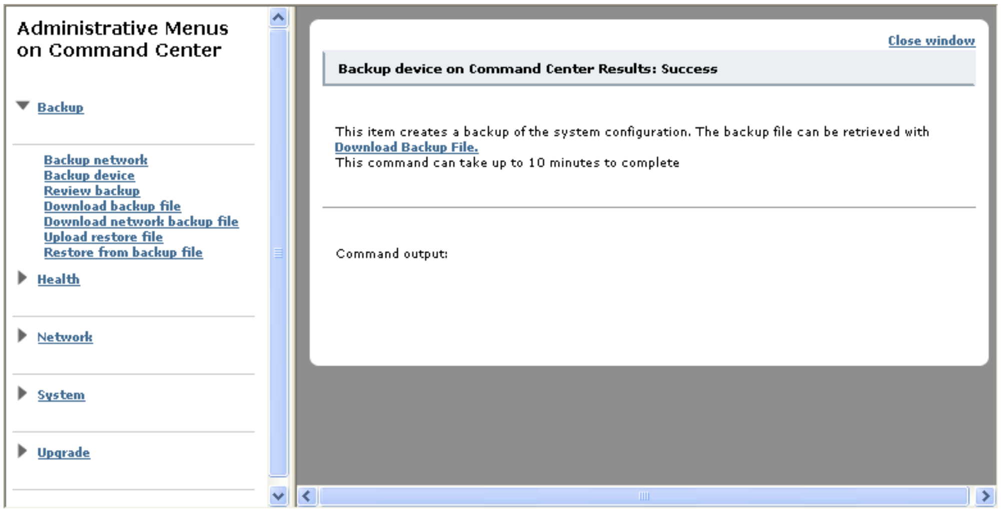
To back up a device:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Backup.**

   The window is repopulated.
4. Click **Backup Device**.

   The window is repopulated.



Backup device on Command Center Results: Success

This item creates a backup of the system configuration. The backup file can be retrieved with Download Backup File.
This command can take up to 10 minutes to complete

Command output:

Backup Network (Command Center Only)

This item creates a backup of the system configuration of the command center and all sensors. This command can take up to 10 minutes per machine backed up.

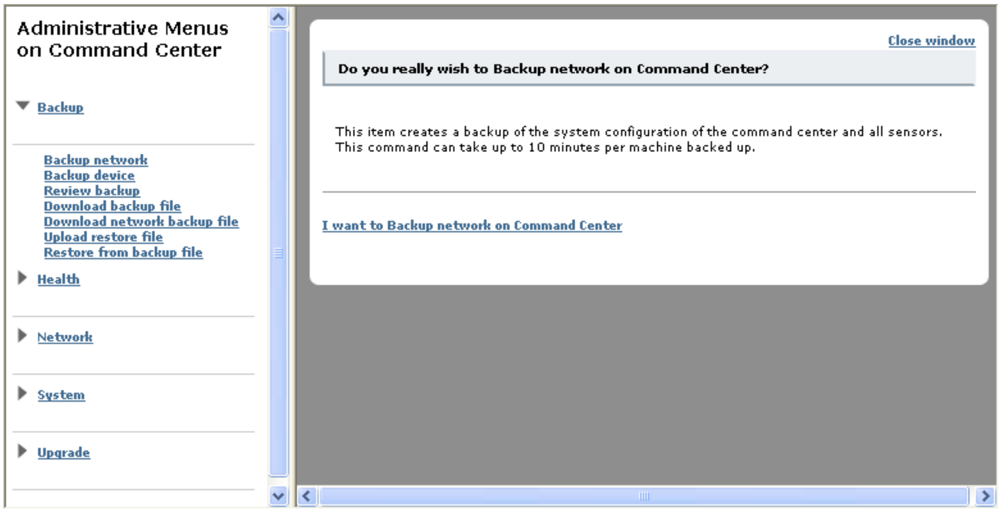
To back up the network:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center**.

   A window pops up with configuration choices.
3. Click **Backup**.

   The window is repopulated.
4. Click **Backup Device**.

The window is repopulated.



Do you really wish to Backup network on Command Center?

This item creates a backup of the system configuration of the command center and all sensors. This command can take up to 10 minutes per machine backed up.

I want to Backup network on Command Center

5. Click **I want to Backup Network**.

Review Backup

This item lists the contents of the backup/restore file uploaded with Upload Restore File.

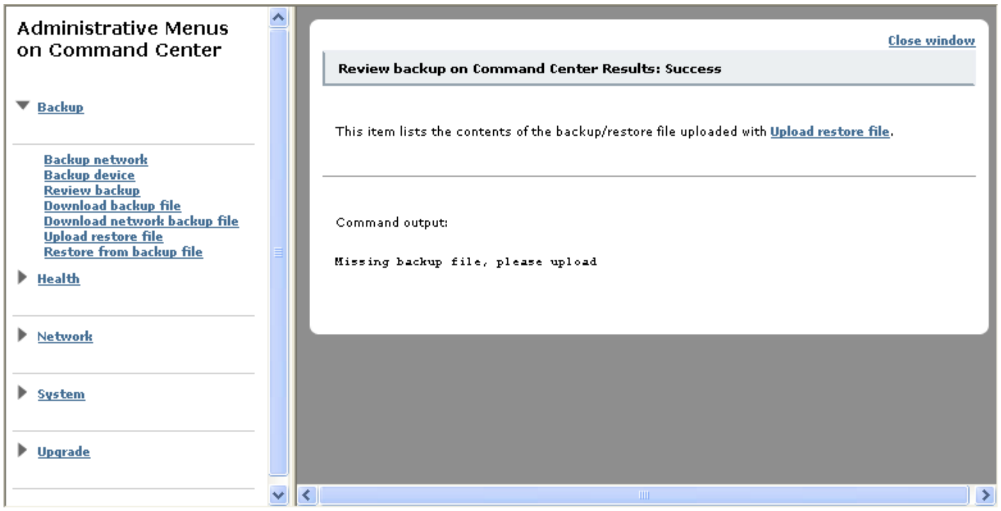
To review backup information:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Backup**.

   The window is repopulated.
4. Click **Backup Review**.

   The window is repopulated.



Review backup on Command Center Results: Success

This item lists the contents of the backup/restore file uploaded with Upload restore file.

Command output:

```
Missing backup file, please upload
```

5. Review the information displayed.

Download Backup File

This item allows you to download the file produced with Backup Device.

To download the backup file:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Backup**.

   The window is repopulated.
4. Click **Download Backup File**.

   A window pops up, allowing you to save the file.
5. Save the file.

Download Network Backup File (Command Center Only)

This item allows you to download the file produced with Backup Network.

To download the network backup file:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center**.

   A window pops up with configuration choices.
3. Click **Backup**.

   The window is repopulated.
4. Click **Download Network Backup File**.

   A window pops up, allowing you to save the file.
5. Save the file.

Upload Restore File

This item uploads a file created by either the Backup Device or Backup Network command. The uploaded file is used by the Backup Extract and Backup Review commands.

To upload restore files:

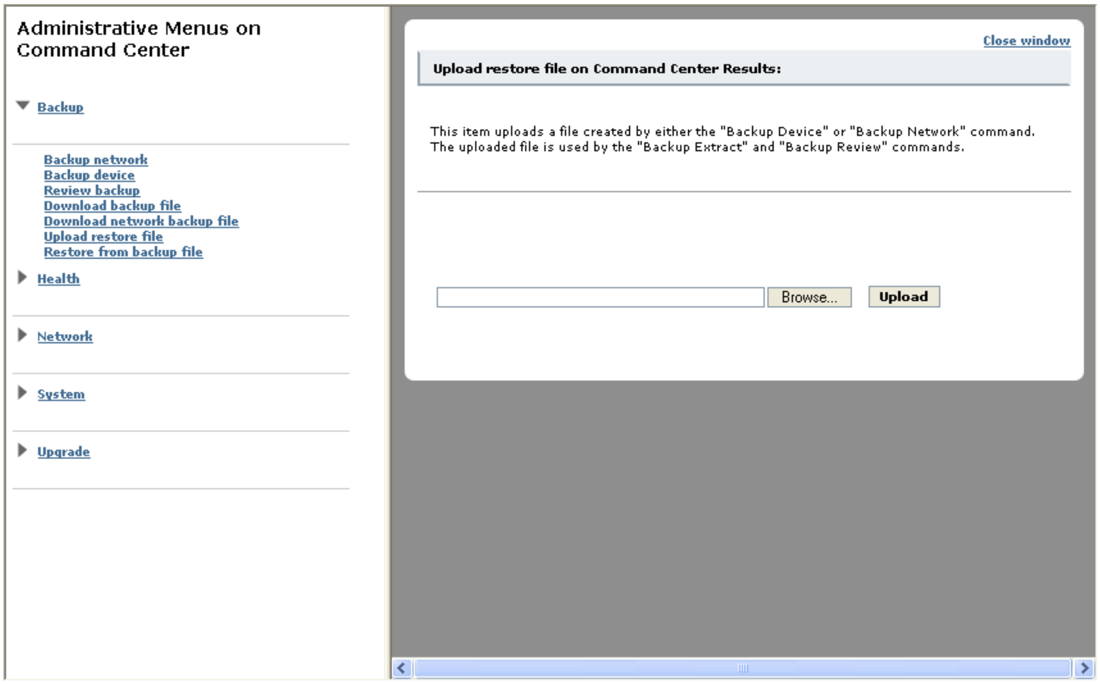
1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Backup**.

   The window is repopulated.

4. Click **Upload Restore File**.

   The window is repopulated, allowing you to save the file.



Upload restore file on Command Center Results:

This item uploads a file created by either the "Backup Device" or "Backup Network" command. The uploaded file is used by the "Backup Extract" and "Backup Review" commands.

5. Upload the file.

Restore From Backup File

This item restores the system from the backup/restore file uploaded with Upload Restore File.

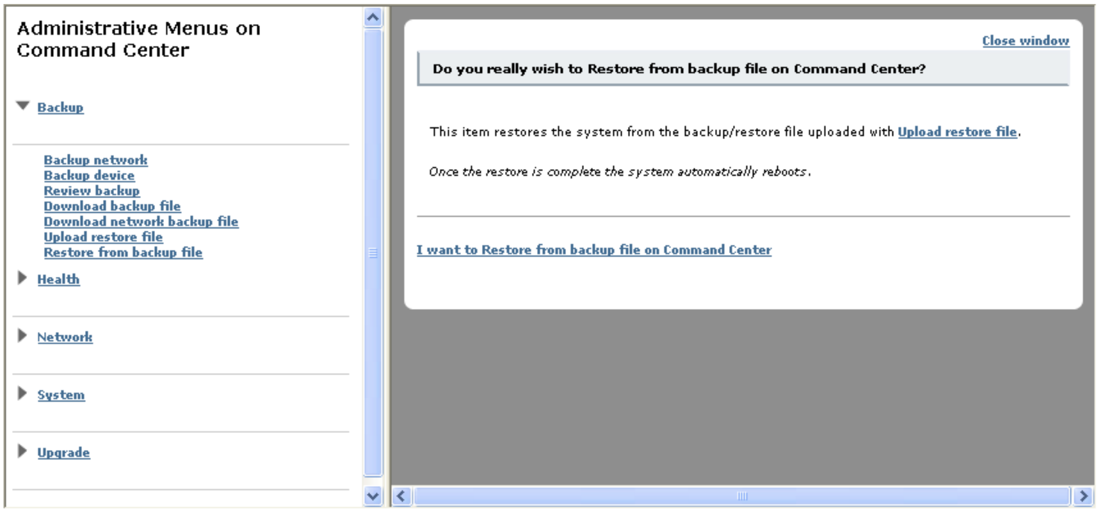
To upload restore files:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Backup**.

   The window is repopulated.
4. Click **Restore From Backup File**.

The window is repopulated, allowing you to restore the backup.



Do you really wish to Restore from backup file on Command Center?

This item restores the system from the backup/restore file uploaded with Upload restore file.

Once the restore is complete the system automatically reboots.

I want to Restore from backup file on Command Center

5. Click **I want to Restore from Backup file**.

Network Administration

This menu provides configuration options for network administration.

To review or change network administration configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Administration**.

   The window is repopulated with the following selections:

Option	Description
Modify ACL Setup	Allows you to modify ACL configuration.
Modify DNS Configuration	Adjusts the DNS resolver configuration.
Modify Default Route	Changes the default gateway used for non-local Internet access.
Modify Interface Configuration	This item modifies the IP configuration.
Modify NTP Setup	This item presents a review of the NTP configuration of this machine and the ability to modify the displayed configuration.
Modify e-mail gateway	This item allows you modify the e-mail gateway.
Modify Static Routing Configuration	This item allows you to manipulate simple static non-default routes.

4. Click the desired option.
5. Follow the specific instructions for each option as described in the following sections.

Modify ACL Setup

Administrative access via SSH/HTTPS is restricted to the IP addresses and ranges listed on this screen; at a minimum, the address of the Command Center must have access to all sensors and vice versa in order to perform initial registration of sensors. IP addresses can be listed one per field, and you can specify ranges in CIDR notation (e.g. 10.1.1.0/24 for the addresses 10.1.1.0 to 10.1.1.255 inclusive). If you are modifying access remotely, make sure not to lock yourself out.

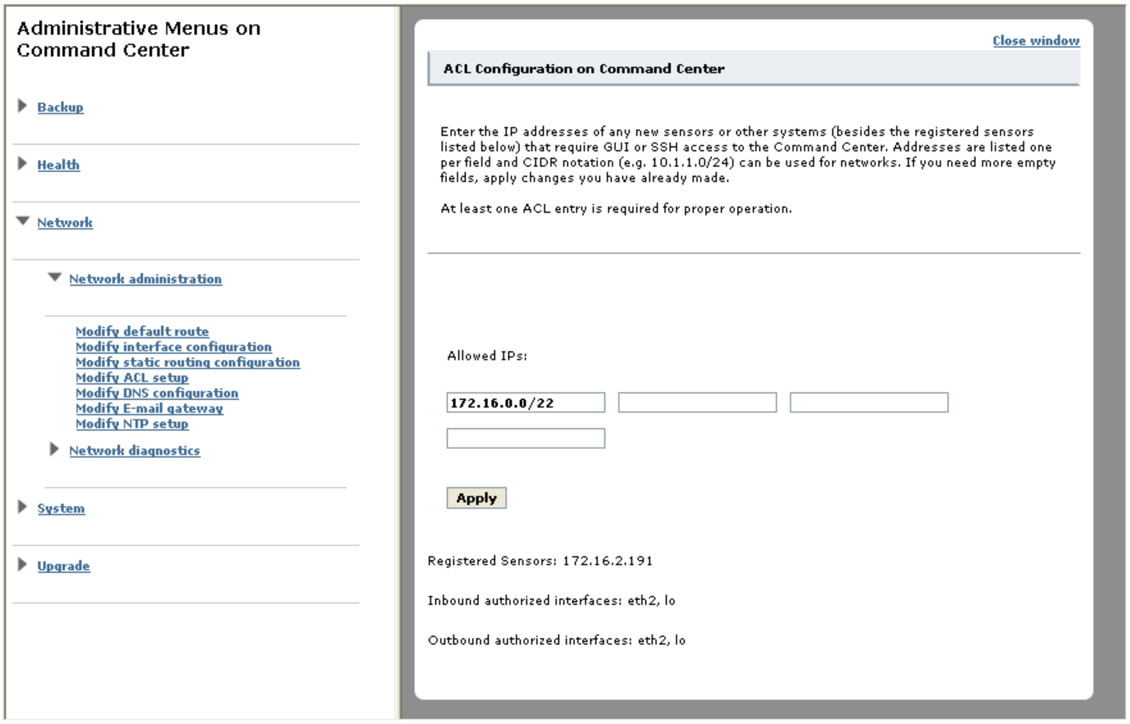
To modify ACL configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Administration**.

   The window is repopulated.
4. Click **Modify ACL Setup**.

   The window is repopulated.



ACL Configuration on Command Center

Enter the IP addresses of any new sensors or other systems (besides the registered sensors listed below) that require GUI or SSH access to the Command Center. Addresses are listed one per field and CIDR notation (e.g. 10.1.1.0/24) can be used for networks. If you need more empty fields, apply changes you have already made.

At least one ACL entry is required for proper operation.

Allowed IPs: 172.16.0.0/22

Registered Sensors: 172.16.2.191

Inbound authorized interfaces: eth2, lo

Outbound authorized interfaces: eth2, lo

5. Enter the desired criteria.
6. Click **Commit** or **Commit and Activate Now**.

Modify DNS Configuration

This item adjusts the DNS resolver configuration. This may be automatically configured by DHCP, in which case changes are lost when the system restarts. Programs that are already running use the old DNS information until the system is restarted. The order of entries matters for both the domain search list and the server list. Earlier entries are used before later entries.

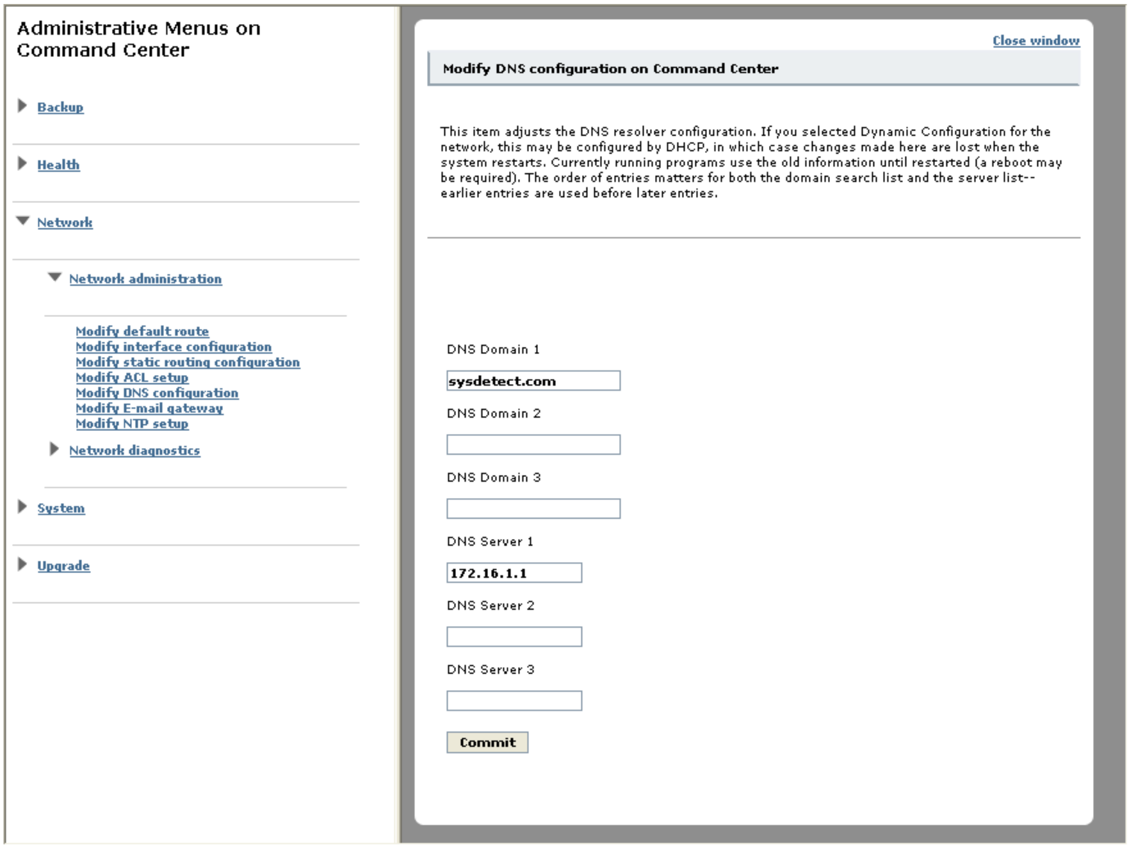
To modify DNS configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Administration**.

   The window is repopulated.
4. Click **Modify DNS Configuration**.

   The window is repopulated.



Modify DNS configuration on Command Center

This item adjusts the DNS resolver configuration. If you selected Dynamic Configuration for the network, this may be configured by DHCP, in which case changes made here are lost when the system restarts. Currently running programs use the old information until restarted (a reboot may be required). The order of entries matters for both the domain search list and the server list--earlier entries are used before later entries.

DNS Domain 1: sysdetect.com
DNS Domain 2:
DNS Domain 3:
DNS Server 1: 172.16.1.1
DNS Server 2:
DNS Server 3:

5. Enter the desired criteria.
6. Click **Commit**.

Modify Default Route

This item changes the default gateway used for non-local Internet access. It may be automatically configured by DHCP, in which case changes are lost when the system restarts. The change is activated immediately.

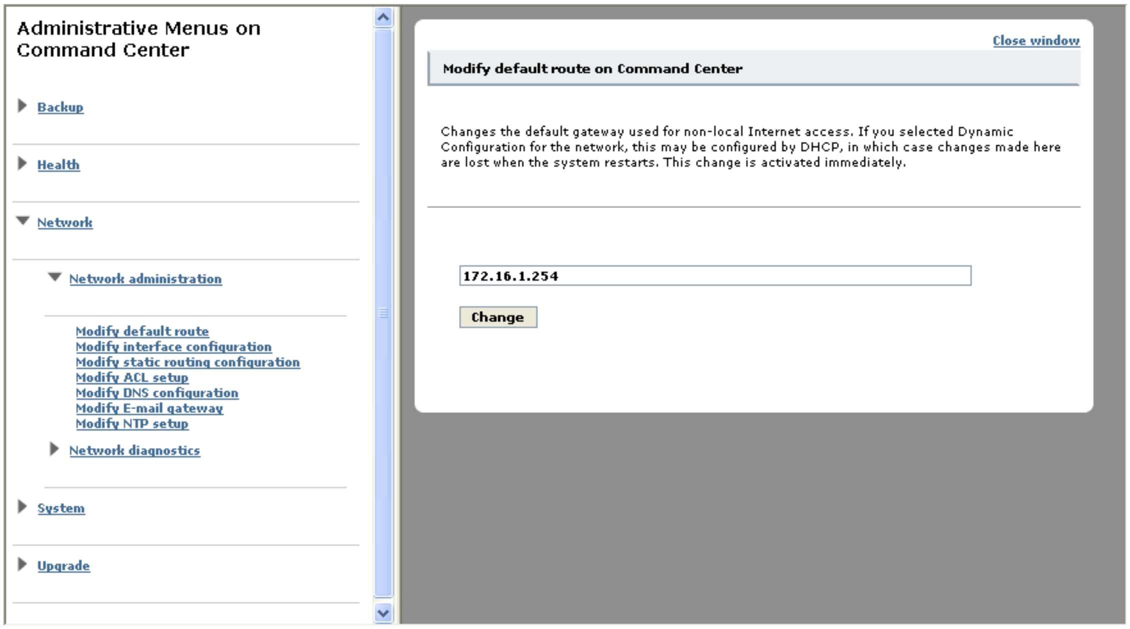
To modify the default route configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Administration**.

   The window is repopulated.
4. Click **Modify Default Route**.

   The window is repopulated.



Modify default route on Command Center

Changes the default gateway used for non-local Internet access. If you selected Dynamic Configuration for the network, this may be configured by DHCP, in which case changes made here are lost when the system restarts. This change is activated immediately.

172.16.1.254

5. Enter the desired criteria.
6. Click **Change**.

Modify Interface Configuration

You can use this form to modify the IP configuration. Do not change the IP configuration of the management interface after Sensor/Command Center registration. Do not disable DHCP on the management interface if it was initially configured to use DHCP. In general, modifying the management interface is dangerous, especially if you are connected to the system via the network rather than the console.

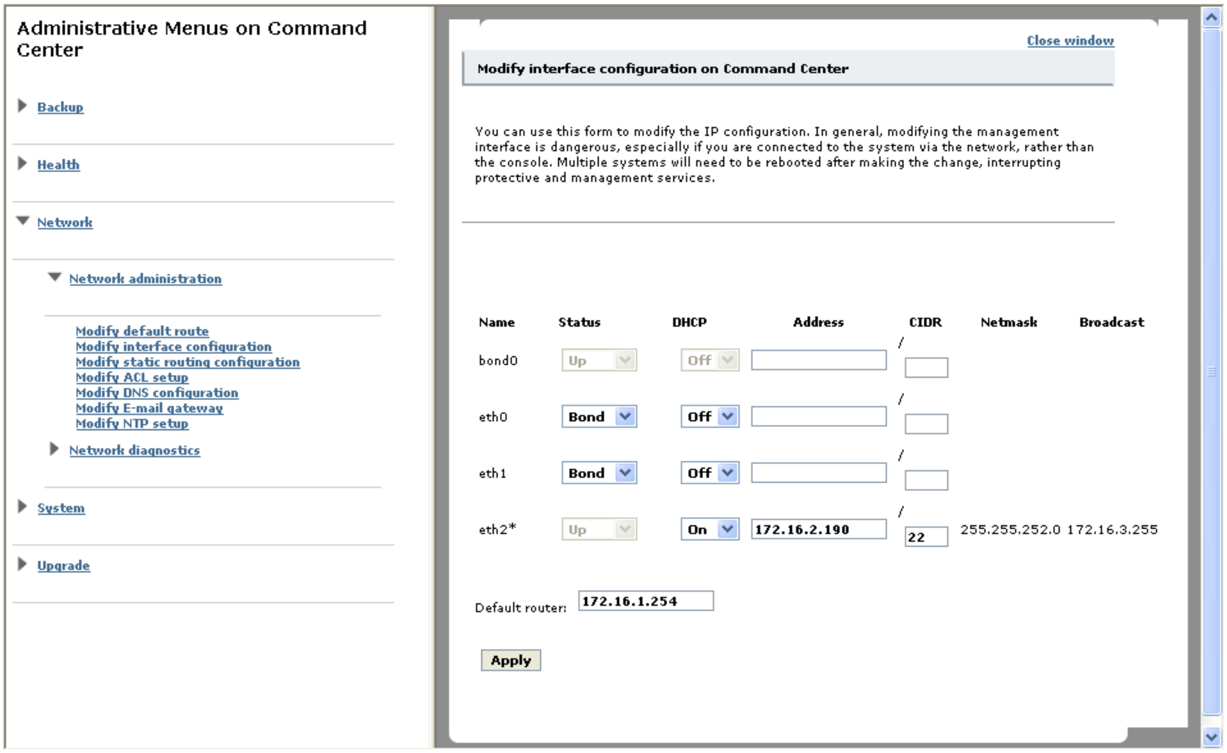
To modify interface configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Administration**.

   The window is repopulated.
4. Click **Modify Interface Configuration**.

The window is repopulated.



Administrative Menus on Command Center

- Backup
- Health
- Network
  - Network administration
    - Modify default route
    - Modify interface configuration
    - Modify static routing configuration
    - Modify ACL setup
    - Modify DNS configuration
    - Modify E-mail gateway
    - Modify NTP setup
  - Network diagnostics
- System
- Upgrade

Close window

Modify interface configuration on Command Center

You can use this form to modify the IP configuration. In general, modifying the management interface is dangerous, especially if you are connected to the system via the network, rather than the console. Multiple systems will need to be rebooted after making the change, interrupting protective and management services.

Name	Status	DHCP	Address	CIDR	Netmask	Broadcast
bond0	Up	Off		/		
eth0	Bond	Off		/		
eth1	Bond	Off		/		
eth2*	Up	On	172.16.2.190	/ 22	255.255.252.0	172.16.3.255

Default router: 172.16.1.254

5. Enter the desired criteria.
6. Click **Commit** or **Commit and Activate Now**.

Modify NTP Setup

This option presents a review of the NTP configuration of the machine and the ability to modify the displayed configuration. Typically, the sensors all synchronize with the Command Center to ensure network-wide timestamp consistency, and the Command Center synchronizes with an external source. The form modifies the NTP network time synchronization configuration for this system. The table specifies the hostnames or addresses of the NTP servers that are used for time synchronization. If you do not have an NTP server, and the internet pool servers are blocked by a firewall, you can use any other CounterStorm-1 Command Center or sensor as an NTP server.

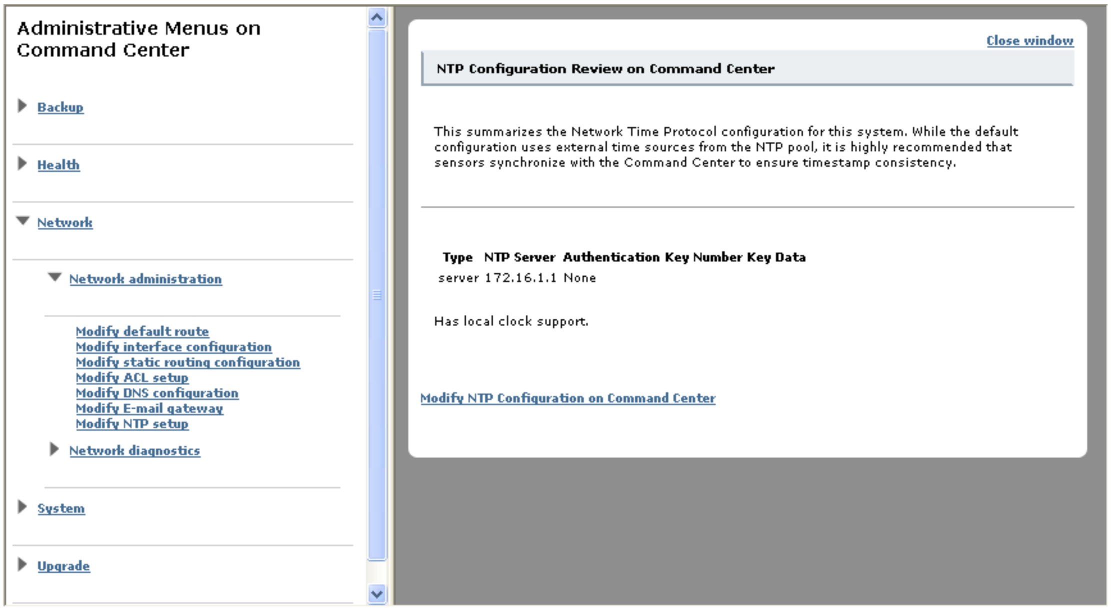
To modify NTP configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Administration**.

   The window is repopulated.
4. Click **Modify NTP Setup**

The window is repopulated.



NTP Configuration Review on Command Center

This summarizes the Network Time Protocol configuration for this system. While the default configuration uses external time sources from the NTP pool, it is highly recommended that sensors synchronize with the Command Center to ensure timestamp consistency.

Type	NTP Server	Authentication Key Number	Key Data
server	172.16.1.1	None	

Has local clock support.

5. Enter the desired criteria.
6. Click **Commit**.

Modify E-mail Gateway

The system may not be able to deliver e-mail directly to the recipients configured for notification or health e-mail due to firewalls or other reasons. You must specify an e-mail gateway that can always deliver mail. If an e-mail gateway is configured, it is used for all e-mail generated by this system.

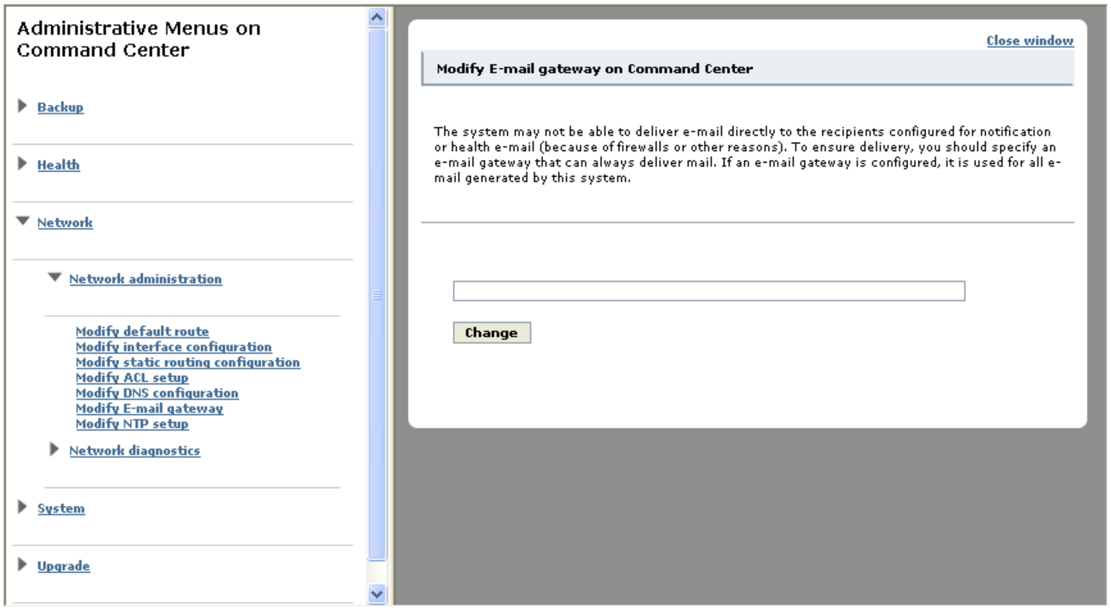
To modify the e-mail gateway:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Administration**.

   The window is repopulated.
4. Click **Modify e-mail gateway**.

The window is repopulated.



Modify E-mail gateway on Command Center

The system may not be able to deliver e-mail directly to the recipients configured for notification or health e-mail (because of firewalls or other reasons). To ensure delivery, you should specify an e-mail gateway that can always deliver mail. If an e-mail gateway is configured, it is used for all e-mail generated by this system.

5. Enter the desired criteria.
6. Click **Change**.

Modify Static Routing Configuration

This item allows you to manipulate simple static non-default routes. You must manage the default route through the IP configuration page. Dynamic routes are managed by the routing program(s). More advanced routes such as reject routes and interface routes cannot be managed.

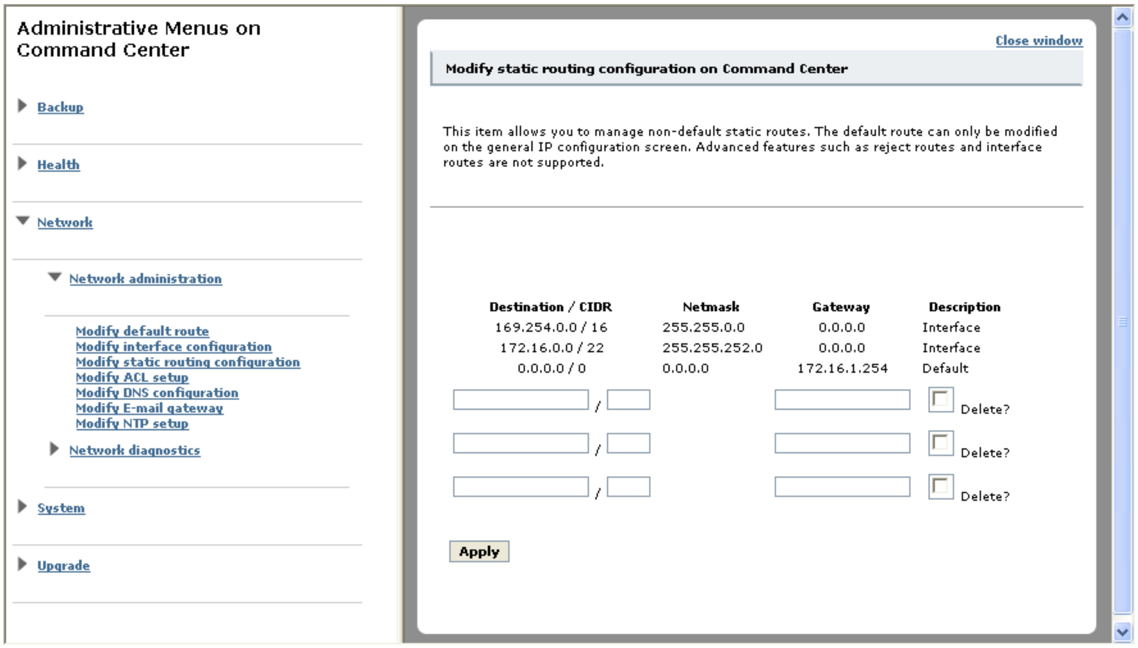
To modify static routing configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Administration**.

   The window is repopulated.
4. Click **Modify Static Routing Configuration**.

The window is repopulated.



Modify static routing configuration on Command Center

This item allows you to manage non-default static routes. The default route can only be modified on the general IP configuration screen. Advanced features such as reject routes and interface routes are not supported.

Destination / CIDR	Netmask	Gateway	Description
169.254.0.0 / 16	255.255.0.0	0.0.0.0	Interface
172.16.0.0 / 22	255.255.252.0	0.0.0.0	Interface
0.0.0.0 / 0	0.0.0.0	172.16.1.254	Default

5. Enter the desired criteria.
6. Click **Commit** or **Commit and Activate Now**.

Network Diagnostics

This menu provides configuration options for network administration.

To review or change network diagnostics configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.

3. Click **Network** and then **Network Diagnostics**.

   The window is repopulated with the following selections to the right:

Option	Description
Blink Interface Lights	This item allows you to blink the interface lights for a period of time so that you can visually identify the interface.
Show IP Routes	This item shows the IP address routes for all interfaces on the system.
Show Interface Address Configuration	This item shows the interface address configuration for all interfaces on the system.
Show Interface Media Configuration	This item shows the interface media configuration for all interfaces on the system.
Show NTP Status	This item prints the NTP configuration and status of the system.
Send Test E-mail	This items allows you test the current e-mail configuration by sending a test message. The default values are the configured health check recipient and sender, but you may specify other values.

4. Follow the specific instructions for each option as described in the following sections.

Blink Interface Lights

This item allows you to blink the interface lights for a period of time so that you can visually identify the interface. The functionality is fully supported on the management interface, eth2.

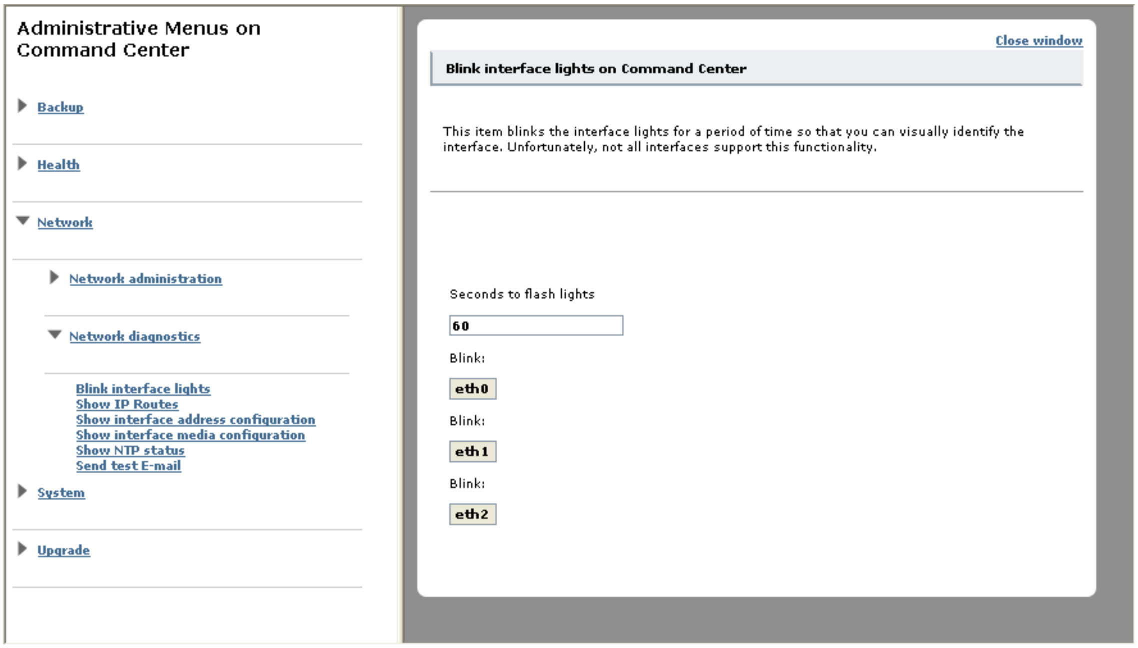
To blink the interface lights:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Diagnostics**.

   The window is repopulated.
4. Click **Blink Interface Lights**.

The window is repopulated.



Blink interface lights on Command Center

This item blinks the interface lights for a period of time so that you can visually identify the interface. Unfortunately, not all interfaces support this functionality.

Seconds to flash lights: 60

Blink:

Blink:

Blink:

5. Enter the desired criteria.
6. Click **Previous Menu**.

Show IP Routes

This item prints the IP routes for all addresses on the system.

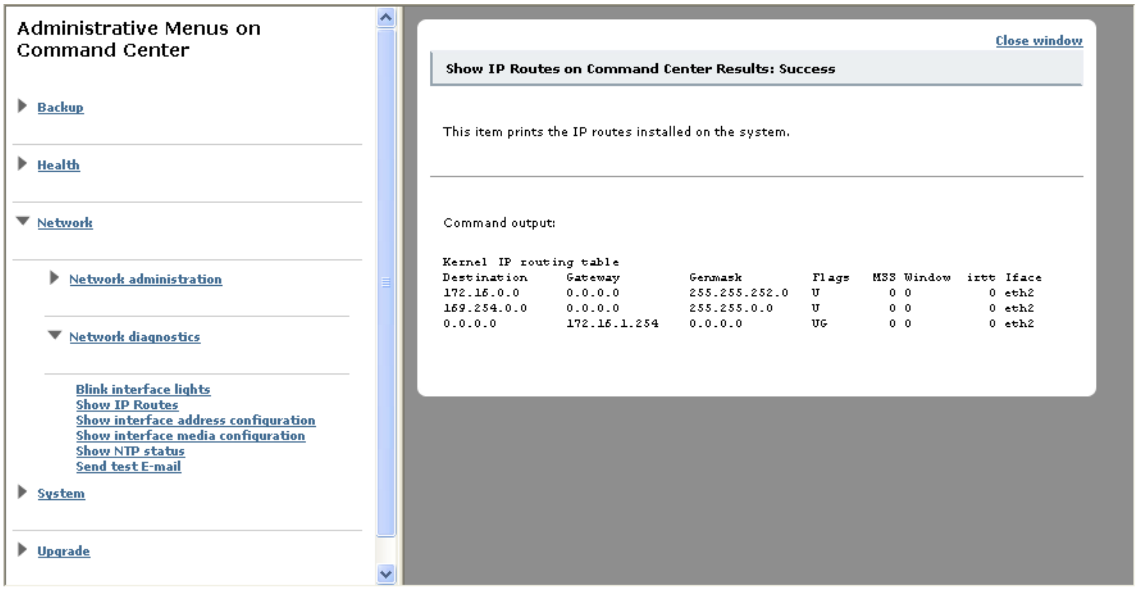
To show IP routes:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Diagnostics**.

   The window is repopulated.
4. Click **IP Routes**.

The window is repopulated.



Show IP Routes on Command Center Results: Success

This item prints the IP routes installed on the system.

Command output:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.0.0      0.0.0.0         255.255.252.0   U         0 0          0 eth2
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth2
0.0.0.0         172.16.1.254    0.0.0.0         UG        0 0          0 eth2
```

5. Click **Previous Menu**.

Show Interface Address Configuration

This item prints the interface address configuration for all interfaces on the system.

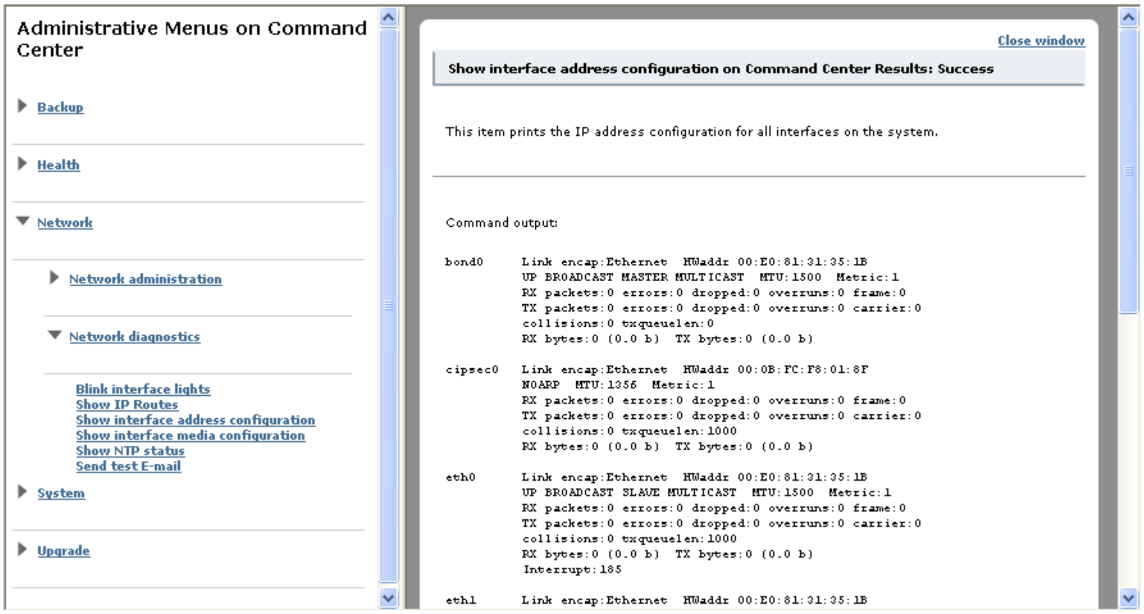
To show interface address configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Diagnostics**.

   The window is repopulated.
4. Click **Show Interface Address Configuration**.

The window is repopulated.



Show interface address configuration on Command Center Results: Success

This item prints the IP address configuration for all interfaces on the system.

Command output:

```
bond0     Link encap:Ethernet  HWaddr 00:E0:81:31:35:1B
          UP BROADCAST MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

cipsec0   Link encap:Ethernet  HWaddr 00:0B:FC:F8:01:8F
          NOARP  MTU:1356  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

eth0      Link encap:Ethernet  HWaddr 00:E0:81:31:35:1B
          UP BROADCAST SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:185

eth1      Link encap:Ethernet  HWaddr 00:E0:81:31:35:1B
```

5. Click **Previous Menu**.

Show Interface Media Configuration

This item prints the media configuration for all interfaces on the system.

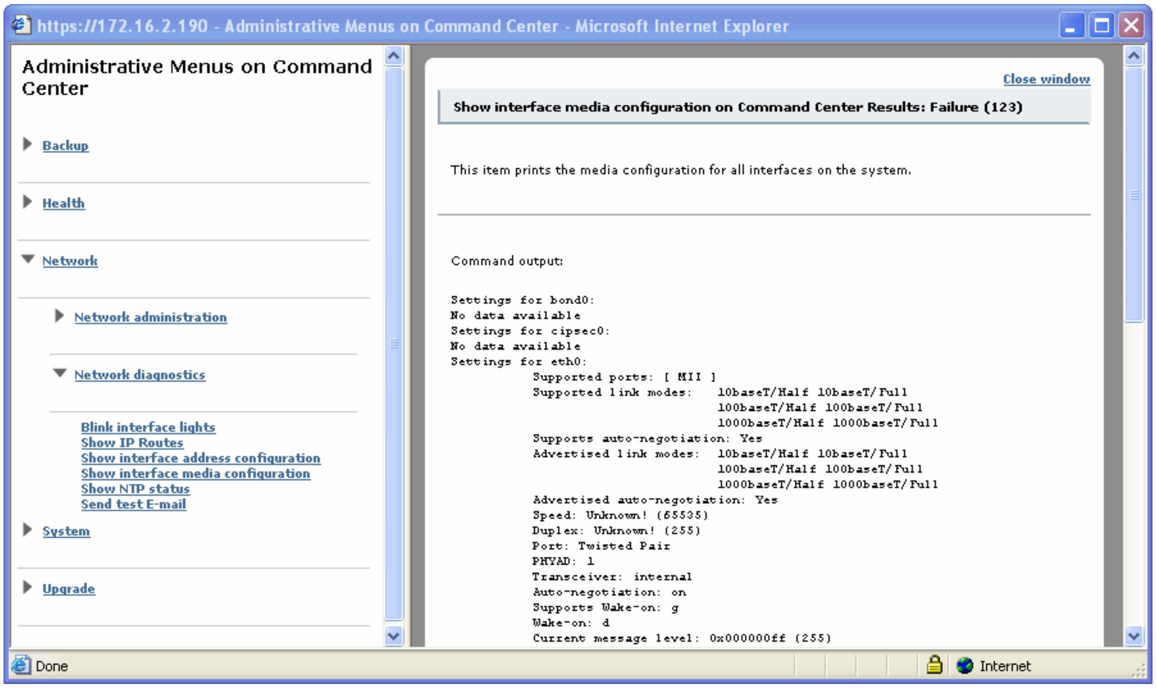
To show interface media configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Diagnostics**.

   The window is repopulated.
4. Click **Show Interface Media Configuration**.

The window is repopulated.


https://172.16.2.190 - Administrative Menus on Command Center - Microsoft Internet Explorer
Administrative Menus on Command Center
Backup
Health
Network
Network administration
Network diagnostics
Blink interface lights
Show IP Routes
Show interface address configuration
Show interface media configuration
Show NTP status
Send test E-mail
System
Upgrade
Close window
Done
Internet

Show interface media configuration on Command Center Results: Failure (123)

This item prints the media configuration for all interfaces on the system.

Command output:

```
Settings for bond0:
No data available
Settings for cipsec0:
No data available
Settings for eth0:
        Supported ports: [ MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: Unknown! (65535)
        Duplex: Unknown! (255)
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: g
        Wake-on: d
        Current message level: 0x000000ff (255)
```

5. Click **Previous Menu**.

Show NTP Status

This item prints the NTP configuration and the status of the system.

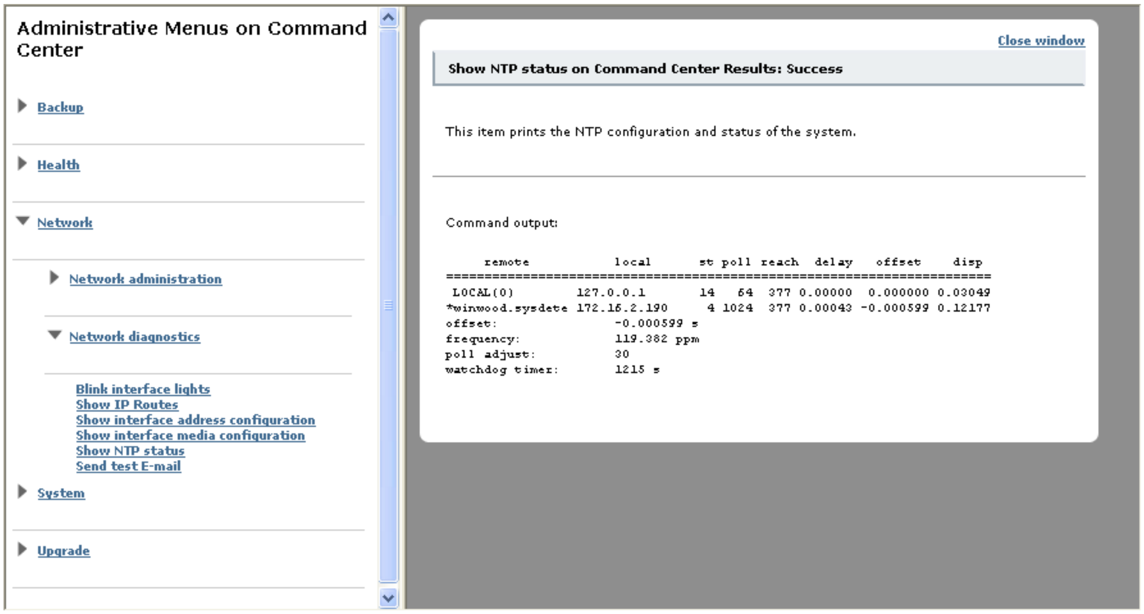
To show NTP status:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Diagnostics**.

   The window is repopulated.
4. Click **Show NTP Status**.

The window is repopulated.



Show NTP status on Command Center Results: Success

This item prints the NTP configuration and status of the system.

Command output:

```
     remote           local      st poll reach  delay   offset    disp
=======================================================================
 LOCAL(0)        127.0.0.1       14   64  377 0.00000  0.000000 0.03049
*winwood.sysdete 172.16.2.190     4 1024  377 0.00043 -0.000599 0.12177
offset:               -0.000599 s
frequency:            119.382 ppm
poll adjust:          30
watchdog timer:       1215 s
```

5. Click **Previous Menu**.

Send Test E-mail

This allows you to test the current e-mail configuration by sending a test message. The default values are the configured health check recipient and sender, but you may specify other values.

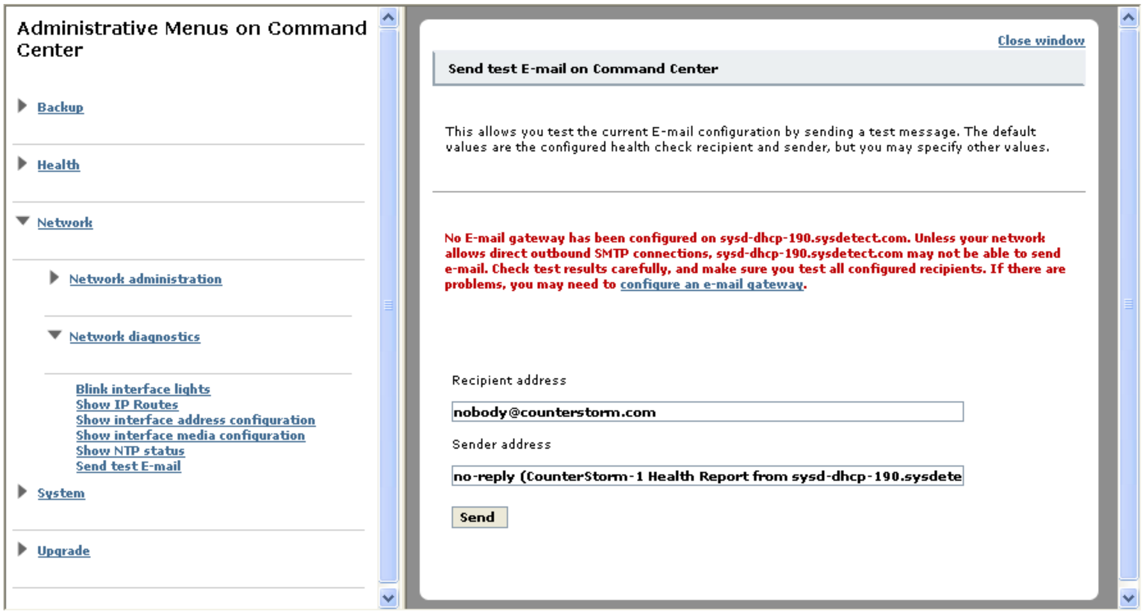
To send a test e-mail:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network** and then **Network Diagnostics**.

   The window is repopulated.
4. Click **Send test e-mail**.

The window is repopulated.



Send test E-mail on Command Center

This allows you test the current E-mail configuration by sending a test message. The default values are the configured health check recipient and sender, but you may specify other values.

No E-mail gateway has been configured on sysd-dhcp-190.sysdetect.com. Unless your network allows direct outbound SMTP connections, sysd-dhcp-190.sysdetect.com may not be able to send e-mail. Check test results carefully, and make sure you test all configured recipients. If there are problems, you may need to configure an e-mail gateway.

Recipient address

nobody@counterstorm.com

Sender address

no-reply (CounterStorm-1 Health Report from sysd-dhcp-190.sysdete

5. Enter the desired addresses.
6. Click **Send**.

Health Diagnostics

This menu allows you modify or view health diagnostic information.

To modify or view health diagnostic information:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Health** and then **Diagnostics**.

   The window is repopulated with the following selections

Option	Description
Show Core Program Status	Displays core program status.
Check Current System Health	Displays the complete system health status.
Get Last Failed Health Report	Displays the last failed periodic system health status.
Get Current System Health Check	Displays the last periodic system health status.

4. Follow the specific instructions for each option as described in the following sections.

Show Core Program Status

Core program status displays Successful if all programs appear to be running, and Failure if one or more programs appear not to be operating correctly. It will also display an opaque summary of its findings on program status.

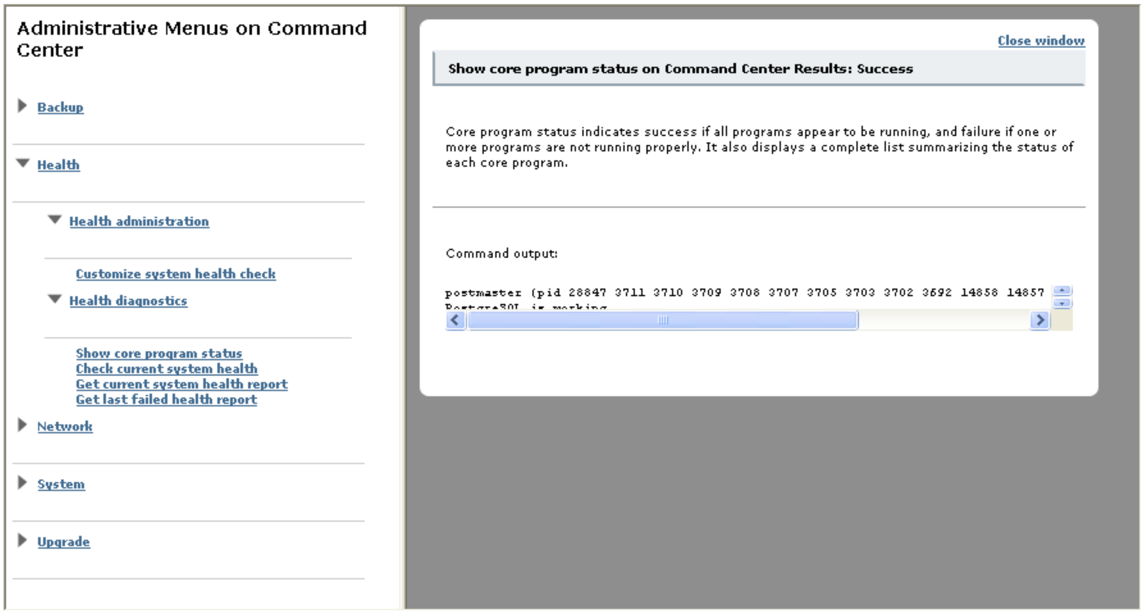
To show core program status:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Health** and then **Health Diagnostics**.

   The window is repopulated.
4. Click **Show Core Program Status**.

   The window is repopulated and status is shown.


Administrative Menus on Command Center
Backup
Health
Health administration
Customize system health check
Health diagnostics
Show core program status
Check current system health
Get current system health report
Get last failed health report
Network
System
Upgrade
Close window

Show core program status on Command Center Results: Success

Core program status indicates success if all programs appear to be running, and failure if one or more programs are not running properly. It also displays a complete list summarizing the status of each core program.

Command output:

```
postmaster (pid 28847 3711 3710 3709 3708 3707 3705 3703 3702 3692 14858 14857
PostgreSQL is working
```

5. Click **Previous Window**.

Check Current System Health

This item displays the complete current system health status. Check at the top to see the operating percentage. If problems exist, the percentage listed at the top of the report is less than 100% and the problem is listed at the top of the report. Generating this report may take some time.

To check system health:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

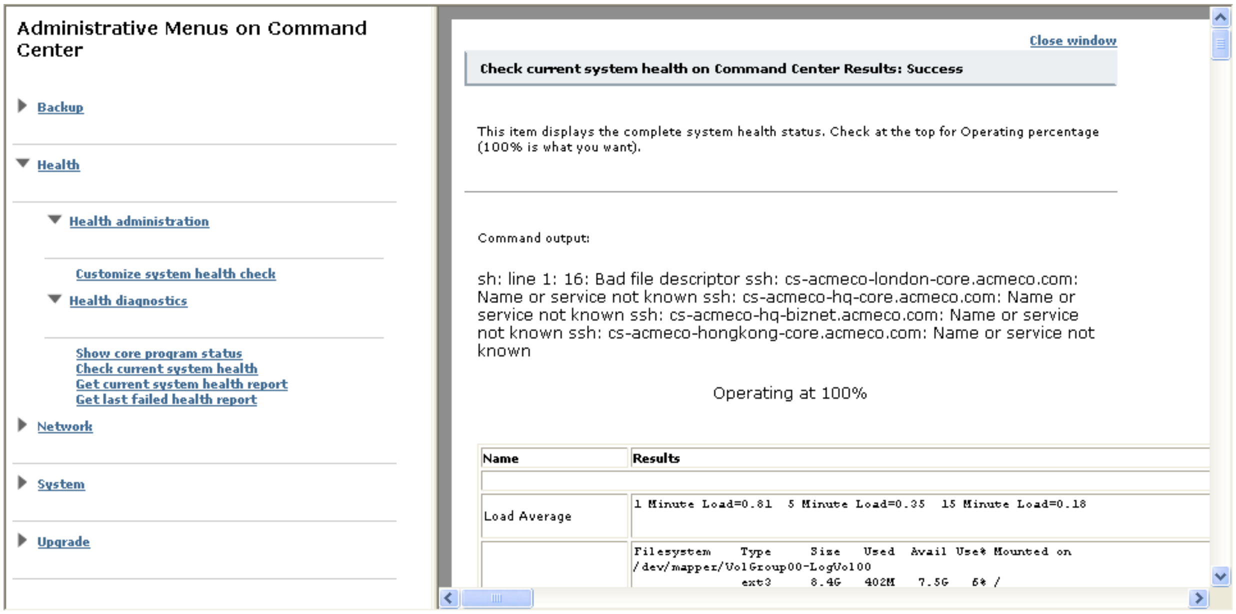
A window pops up with configuration choices.

3. Click **Health** and then **Health Diagnostics**.

   The window is repopulated.

4. Click **Check Current System Health**.

   The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Health administration
Customize system health check
Health diagnostics
Show core program status
Check current system health
Get current system health report
Get last failed health report
Network
System
Upgrade
Close window

Check current system health on Command Center Results: Success

This item displays the complete system health status. Check at the top for Operating percentage (100% is what you want).

Command output:

```
sh: line 1: 16: Bad file descriptor ssh: cs-acmeco-london-core.acmeco.com: Name or service not known ssh: cs-acmeco-hq-core.acmeco.com: Name or service not known ssh: cs-acmeco-hq-biznet.acmeco.com: Name or service not known ssh: cs-acmeco-hongkong-core.acmeco.com: Name or service not known
```

Operating at 100%

Name	Results
Load Average	1 Minute Load=0.81 5 Minute Load=0.35 15 Minute Load=0.18
	Filesystem Type Size Used Avail Use% Mounted on /dev/mapper/VolGroup00-LogVol00 ext3 8.4G 402M 7.5G 6% /

5. Click **Previous Menu**.

Get Last Failed Health Report

This item displays the most recent failed periodic system health status. This report may take some time.

To check the last failed system health:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

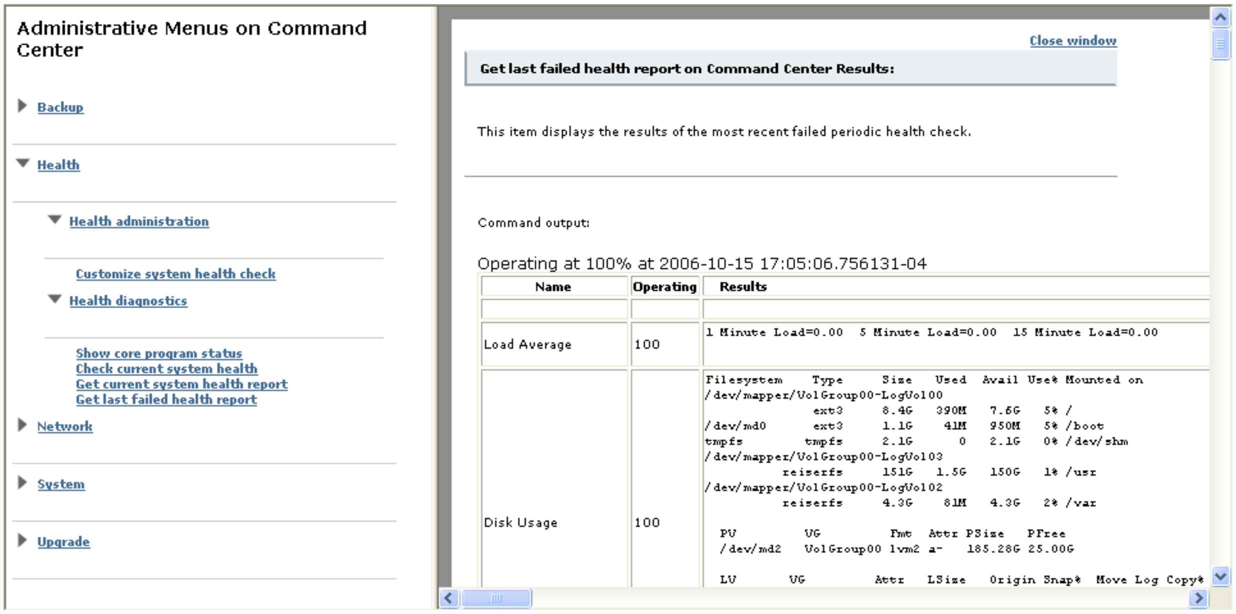
   A window pops up with configuration choices.

3. Click **Health** and then **Health Diagnostics**.

   The window is repopulated.

4. Click **Get Last Failed Health Report**.

The window is repopulated.



Administrative Menus on Command Center
Backup
Health
Health administration
Customize system health check
Health diagnostics
Show core program status
Check current system health
Get current system health report
Get last failed health report
Network
System
Upgrade
Close window

Get last failed health report on Command Center Results:

This item displays the results of the most recent failed periodic health check.

Command output:

Operating at 100% at 2006-10-15 17:05:06.756131-04

Name	Operating	Results
Load Average	100	1 Minute Load=0.00 5 Minute Load=0.00 15 Minute Load=0.00
Disk Usage	100	Filesystem Type Size Used Avail Use% Mounted on /dev/mapper/VolGroup00-LogVol00 ext3 8.4G 390M 7.6G 5% / /dev/md0 ext3 1.1G 41M 950M 5% /boot tmpfs tmpfs 2.1G 0 2.1G 0% /dev/shm /dev/mapper/VolGroup00-LogVol03 reiserfs 151G 1.5G 150G 1% /usr /dev/mapper/VolGroup00-LogVol02 reiserfs 4.3G 81M 4.3G 2% /var PV VG Fmt Attr PSize PFree /dev/md2 VolGroup00 lvm2 a- 185.28G 25.00G LV VG Attr LSize Origin Snap% Move Log Copy%

5. Click **Previous Menu**.

Get Current System Health Check

This item displays the last periodic system health status. Check at the top for operating percentage. If problems exist, the percentage listed at the top of the report is less than 100% and the problem is listed at the top of the report. This may take some time.

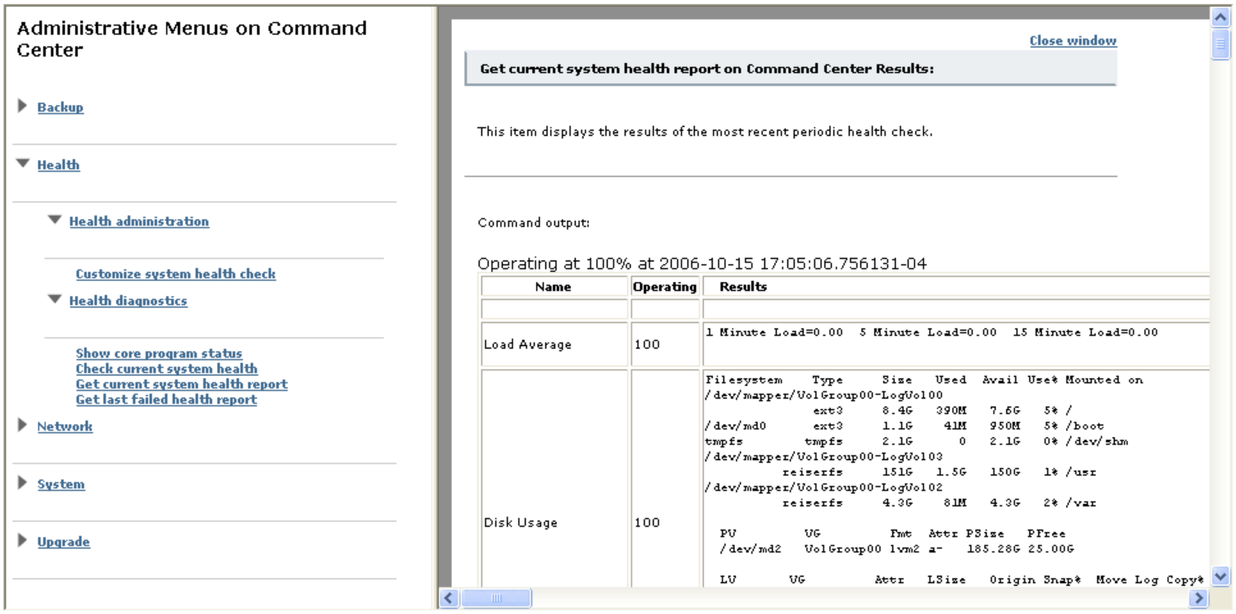
To check system health:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Health** and then **Health Diagnostics**.

   The window is repopulated.
4. Click **Get Current System Health Check**.

The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Health administration
Customize system health check
Health diagnostics
Show core program status
Check current system health
Get current system health report
Get last failed health report
Network
System
Upgrade
Close window

Get current system health report on Command Center Results:

This item displays the results of the most recent periodic health check.

Command output:

Operating at 100% at 2006-10-15 17:05:06.756131-04

```
Name            Operating   Results

Load Average    100         1 Minute Load=0.00   5 Minute Load=0.00   15 Minute Load=0.00

Disk Usage      100         Filesystem    Type      Size   Used  Avail Use% Mounted on
                            /dev/mapper/VolGroup00-LogVol00
                                          ext3      8.4G   390M   7.6G   5% /
                            /dev/md0      ext3      1.1G    41M   950M   5% /boot
                            tmpfs        tmpfs      2.1G      0   2.1G   0% /dev/shm
                            /dev/mapper/VolGroup00-LogVol03
                                      reiserfs      151G   1.5G   150G   1% /usr
                            /dev/mapper/VolGroup00-LogVol02
                                      reiserfs      4.3G    81M   4.3G   2% /var

                              PV         VG         Fmt  Attr PSize   PFree
                              /dev/md2   VolGroup00 lvm2 a-   185.28G 25.00G

                              LV       VG           Attr   LSize   Origin Snap%  Move Log Copy%
```

5. Click **Previous Menu**.

Health Administration

This menu allows you to perform administrative health tasks.

To modify or view health diagnostic information:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Health** and then **Health Administration**.

   The window is repopulated with the following selections

Option	Description
Customize System Health Check	This item allows you to customize the health reports which are sent from a machine.
Silence RAID Alarm	Turns off the audible alarm.
Configure Third Party Devive Testing	This items specifies how often sensors test third party devices.

4. Follow the specific instructions for each option as described in the following sections.

Customize System Health Check

This item allows you to customize the health reports which are sent from a machine.

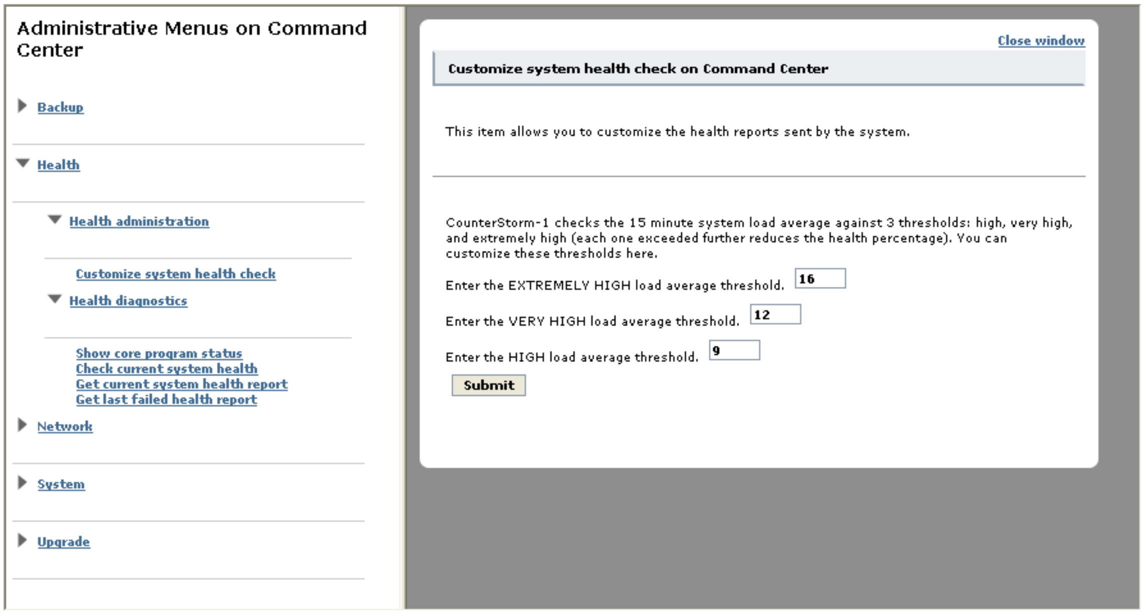
To customize the system health check:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Health** and then **Health Administration**.

   The window is repopulated.
4. Click **Customize System Health Check**.

   The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Health administration
Customize system health check
Health diagnostics
Show core program status
Check current system health
Get current system health report
Get last failed health report
Network
System
Upgrade
Close window
Customize system health check on Command Center
Submit

This item allows you to customize the health reports sent by the system.

CounterStorm-1 checks the 15 minute system load average against 3 thresholds: high, very high, and extremely high (each one exceeded further reduces the health percentage). You can customize these thresholds here.

Enter the EXTREMELY HIGH load average threshold. 16

Enter the VERY HIGH load average threshold. 12

Enter the HIGH load average threshold. 9

5. Enter the desired criteria.
6. Click **Submit**.

Silence RAID Alarm (Command Center Only)

This item silences the Command Center RAID alarm. It does not fix the RAID problem.

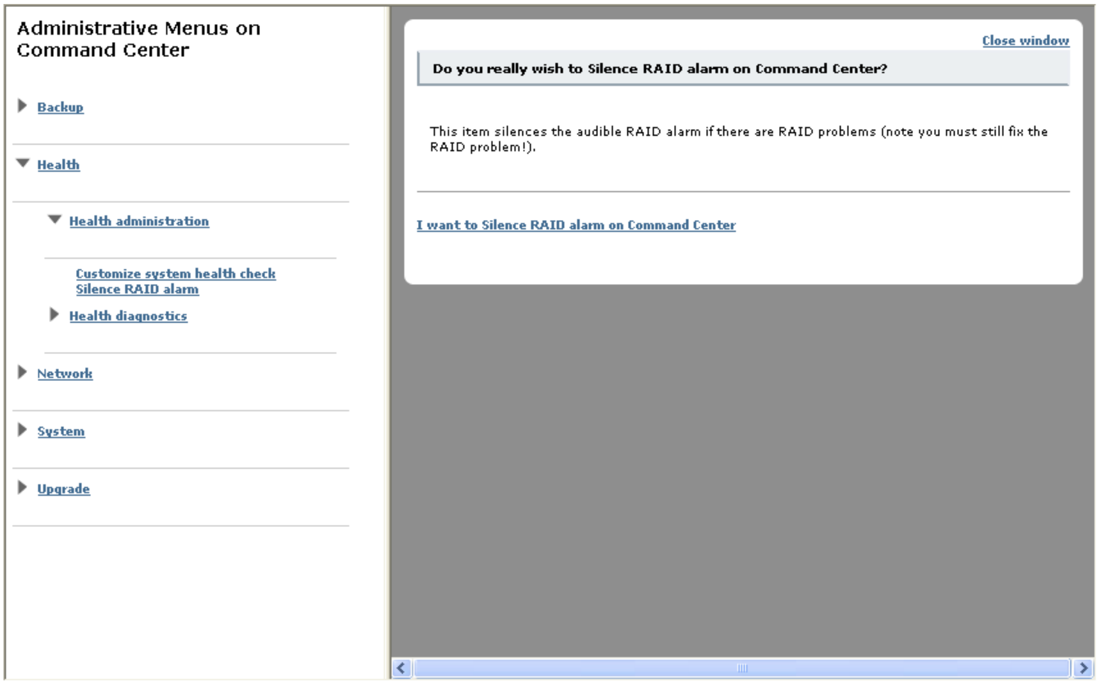
To silence the RAID alarm:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center**.

   A window pops up with configuration choices.
3. Click **Health** and then **Health Administration**.

   The window is repopulated.
4. Click **Silence RAID Alarm**.

The window is repopulated.



Administrative Menus on Command Center

Do you really wish to Silence RAID alarm on Command Center?

This item silences the audible RAID alarm if there are RAID problems (note you must still fix the RAID problem!).

I want to Silence RAID alarm on Command Center

5. Click **Previous Menu**.

Configure Third Party Device Testing (Sensor Only)

This item specifies how often you wish the CounterStorm sensors to test third party devices, such as switches and VPN concentrators. These devices are tested to help validate that the system will be able to successfully manage these devices in the event of an appropriate manual or automatic response.

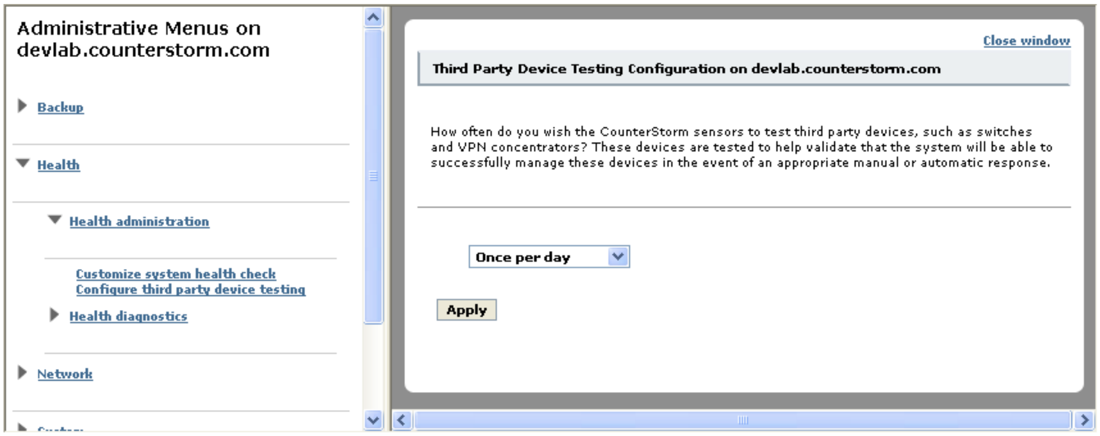
To configure third party device testing:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Health** and then **Health Administration**.

   The window is repopulated.
4. Click **Configure Third Party Device Testing**.

The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Health administration
Customize system health check
Configure third party device testing
Health diagnostics
Network
Close window
Apply

Third Party Device Testing Configuration on devlab.counterstorm.com

How often do you wish the CounterStorm sensors to test third party devices, such as switches and VPN concentrators? These devices are tested to help validate that the system will be able to successfully manage these devices in the event of an appropriate manual or automatic response.

Once per day

5. Enter the desired criteria.
6. Click **Apply**.

System Administration

This menu provides configuration options for system administration.

To review or change system administration configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **System Administration**.

   The window is repopulated with the following selections:

Option	Description
Change Root Password	This item allows you to change the password for local root accounts.
Modify Hostname	This item allows you to change the hostname of this device.
Review Configuration	This item allows you to review IP configuration.
Restart Core Programs	Allows you to restart core programs.
Halt System	Allows you to stop all system activity.
Reboot System	Reboots the system.
Administer Time Zone Configuration	This item allows you to review and modify the time zone configuration.
Stop Core Programs	Allows you to stop core programs.

4. Click the desired option.
5. Follow the specific instructions for each option as described in the following sections.

Change Root Password

This item allows you to change the password for local root accounts. Note that the new password must be 6 or more characters in length, and must have both alphabetic and non-alphabetic characters internally (i.e., not the first and last character). For example: 'foobar1' is not valid, but 'foo1bar' is.

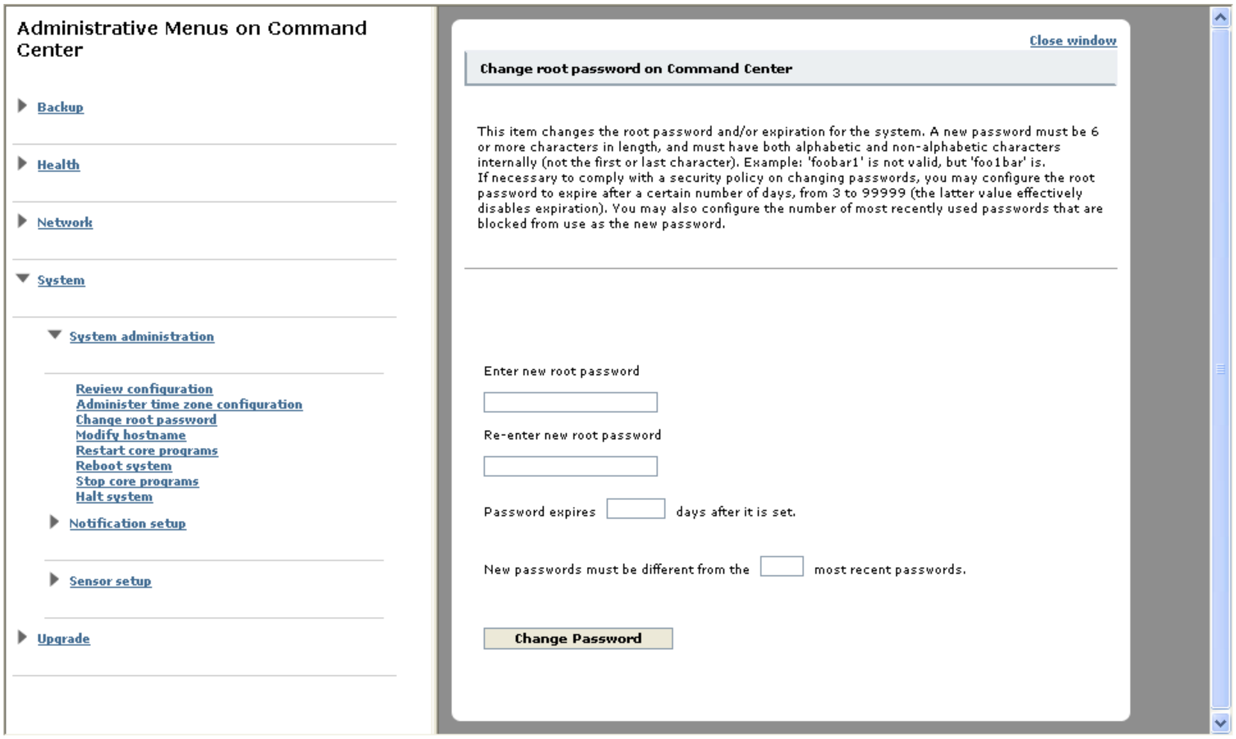
To change the root password:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **System Administration**.

   The window is repopulated.
4. Click **Change Root Password**.

   The window is repopulated.



Change root password on Command Center

This item changes the root password and/or expiration for the system. A new password must be 6 or more characters in length, and must have both alphabetic and non-alphabetic characters internally (not the first or last character). Example: 'foobar1' is not valid, but 'foo1bar' is.
If necessary to comply with a security policy on changing passwords, you may configure the root password to expire after a certain number of days, from 3 to 99999 (the latter value effectively disables expiration). You may also configure the number of most recently used passwords that are blocked from use as the new password.

Enter new root password

Re-enter new root password

Password expires days after it is set.

New passwords must be different from the most recent passwords.

5. Enter the desired criteria.
6. Click **Change Password**.

Modify Hostname

This item allows you to change the hostname of this device. All systems must be up and operational for this to succeed. The hostname you are changing from should be fully qualified and/or unique (an old hostname of 'key' is going to cause problems, but 'key.example.com' is fine). No other administrative activities should be performed while the hostname is being changed. All protective services will be suspended for the potentially ten or more minutes it can take to update all systems, the system whose name is being changed will be rebooted, and all GUI users will be disconnected and forced to reauthenticate after the change is complete.

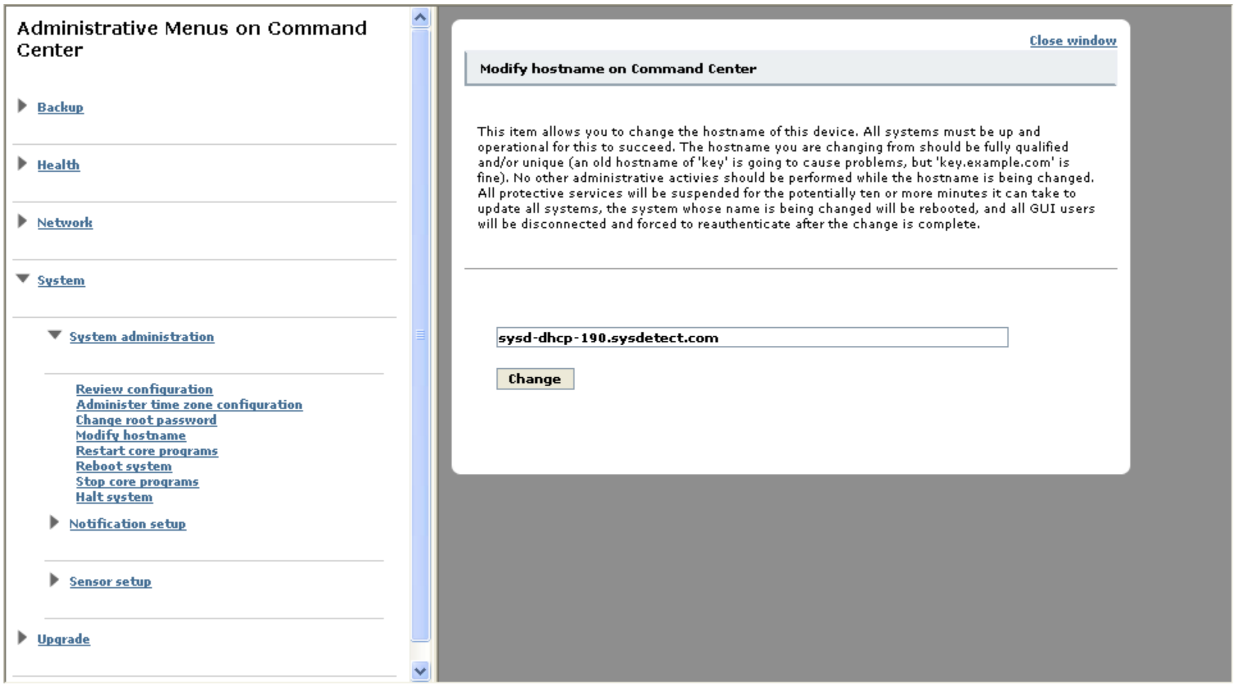
To change the hostname:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **System Administration**.

   The window is repopulated.
4. Click **Modify Hostname**.

   The window is repopulated.



Modify hostname on Command Center

This item allows you to change the hostname of this device. All systems must be up and operational for this to succeed. The hostname you are changing from should be fully qualified and/or unique (an old hostname of 'key' is going to cause problems, but 'key.example.com' is fine). No other administrative activies should be performed while the hostname is being changed. All protective services will be suspended for the potentially ten or more minutes it can take to update all systems, the system whose name is being changed will be rebooted, and all GUI users will be disconnected and forced to reauthenticate after the change is complete.

sysd-dhcp-190.sysdetect.com

5. Enter the new name.
6. Click **Change**.

Review Configuration

This is a review of the IP configuration for dva.sysdetect.com.

To review current configuration:

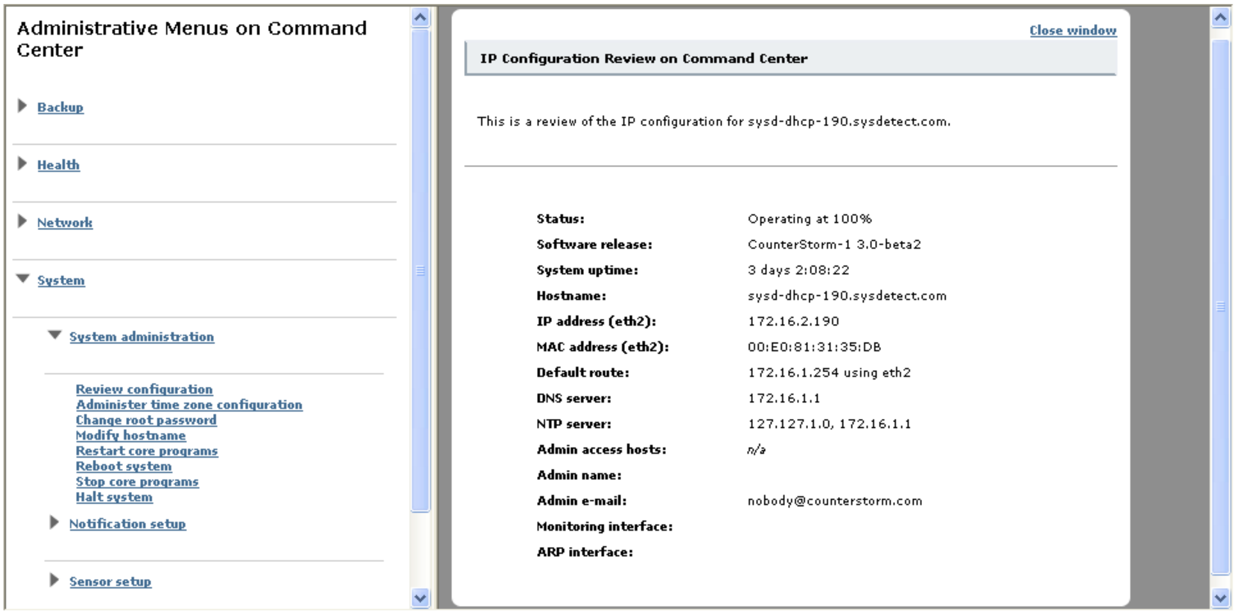
1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.

3. Click **System** and then **System Administration**.

   The window is repopulated.

4. Click **Review configuration**.



IP Configuration Review on Command Center

This is a review of the IP configuration for sysd-dhcp-190.sysdetect.com.

Status:	Operating at 100%
Software release:	CounterStorm-1 3.0-beta2
System uptime:	3 days 2:08:22
Hostname:	sysd-dhcp-190.sysdetect.com
IP address (eth2):	172.16.2.190
MAC address (eth2):	00:E0:81:31:35:DB
Default route:	172.16.1.254 using eth2
DNS server:	172.16.1.1
NTP server:	127.127.1.0, 172.16.1.1
Admin access hosts:	n/a
Admin name:	
Admin e-mail:	nobody@counterstorm.com
Monitoring interface:	
ARP interface:	

Restart Core Programs

Restarting core programs temporarily stops all system activity, thereby losing all protective states. The detection of new infections is disabled for five minutes. This is rarely necessary, except to activate certain configuration changes.

To restart core programs:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

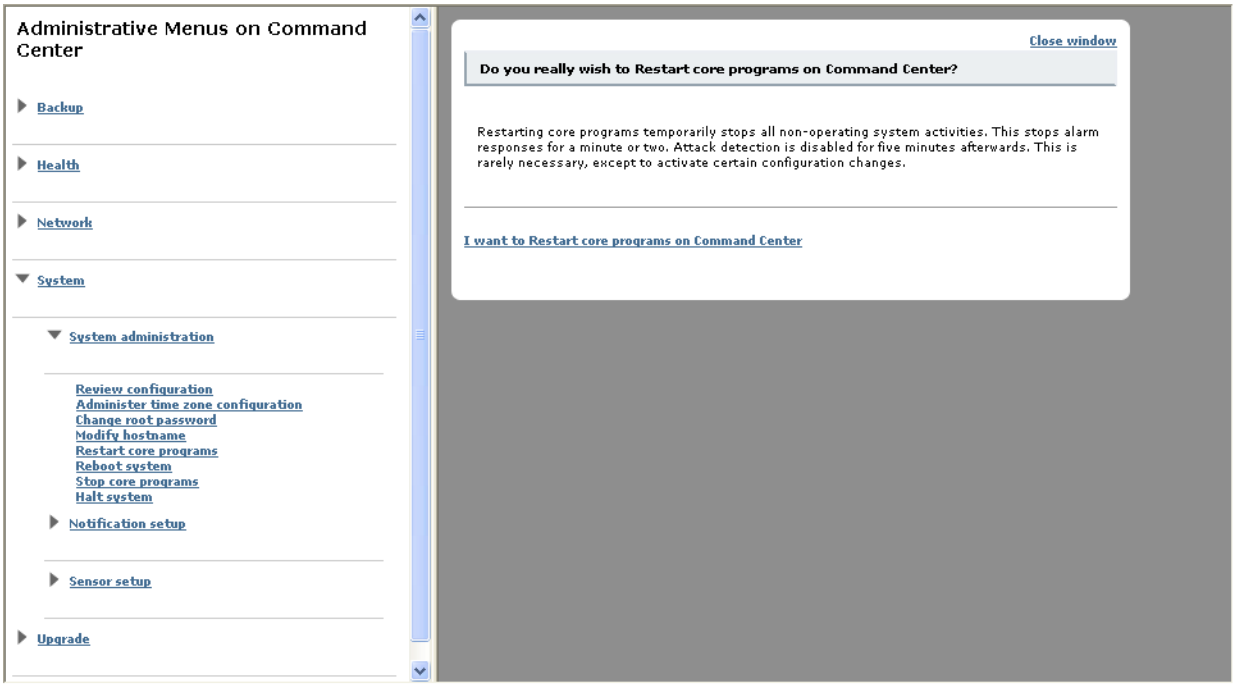
   A window pops up with configuration choices.

3. Click **System** and then **System Administration**.

   The window is repopulated.

4. Click **Restart Core Programs**.

The window is repopulated.



Do you really wish to Restart core programs on Command Center?

Restarting core programs temporarily stops all non-operating system activities. This stops alarm responses for a minute or two. Attack detection is disabled for five minutes afterwards. This is rarely necessary, except to activate certain configuration changes.

I want to Restart core programs on Command Center

5. Confirm your decision by selecting **I want to Restart Core Programs**.

Halt System

Halting stops all system activity and, when possible, turns off the hardware. All system functions, including attack detection and alarm responses, are disabled until they are manually restarted. Attack detection is disabled for five minutes after core programs are restarted.

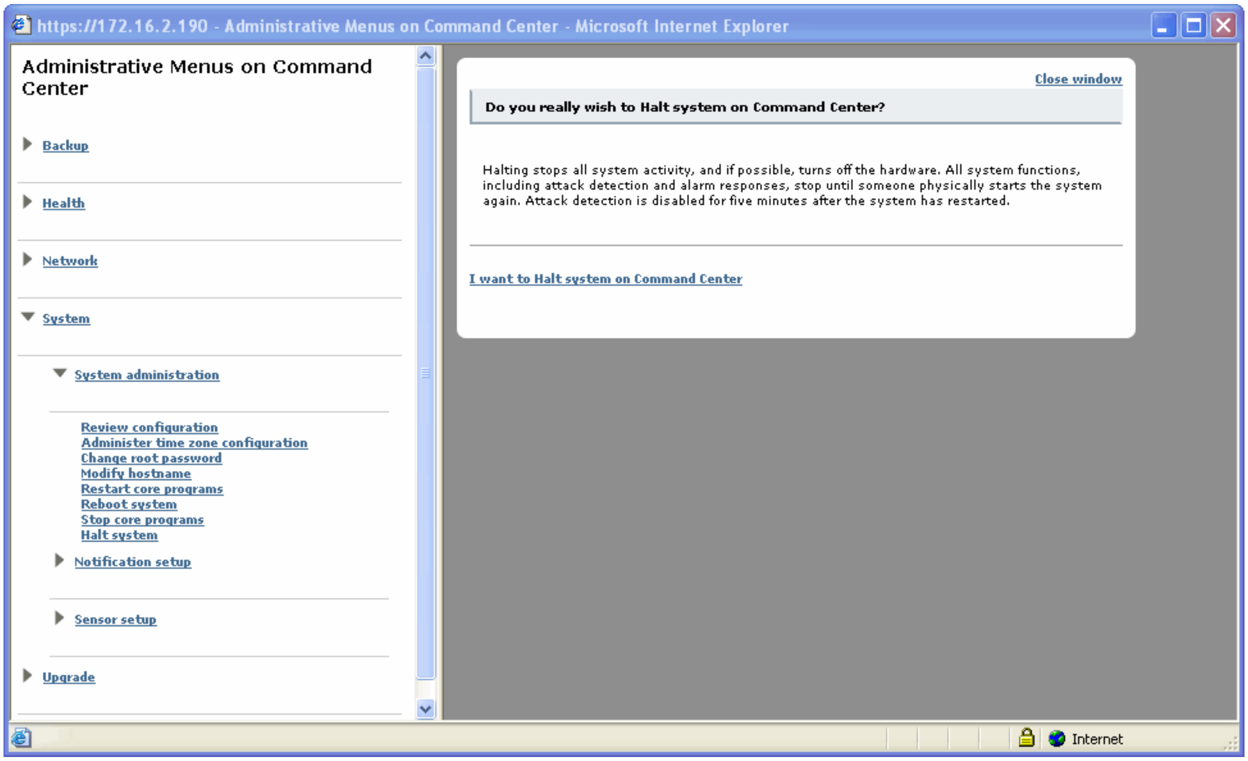
To halt the system program status:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **System Administration**.

   The window is repopulated.
4. Click **Halt System**.

The window is repopulated.



Do you really wish to Halt system on Command Center?

Halting stops all system activity, and if possible, turns off the hardware. All system functions, including attack detection and alarm responses, stop until someone physically starts the system again. Attack detection is disabled for five minutes after the system has restarted.

I want to Halt system on Command Center

5. Confirm your decision by selecting **I want to Halt System**.

Reboot System

Rebooting the system briefly stops all activity and performs a hardware restart. All system functions, including alarm responses, stop for a few minutes. Attack detection is disabled for five minutes after core programs are restarted.

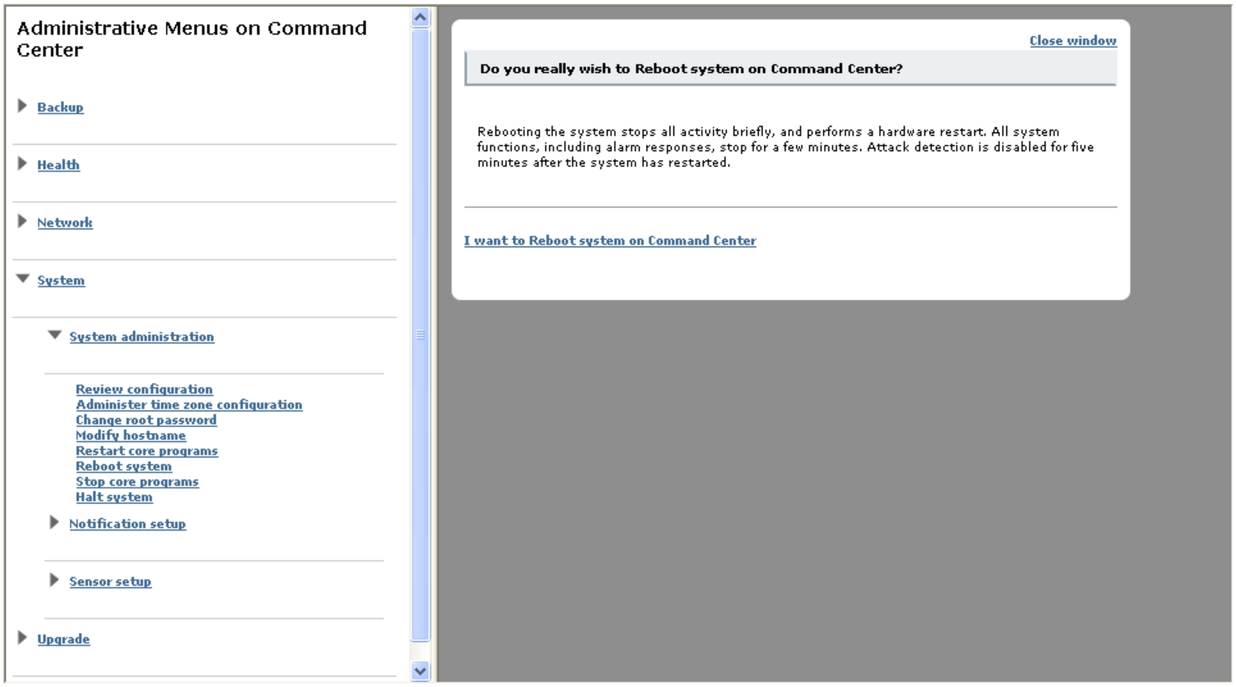
To reboot the system:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **System Administration**.

   The window is repopulated.
4. Click **Reboot System.**

The window is repopulated.



Do you really wish to Reboot system on Command Center?

Rebooting the system stops all activity briefly, and performs a hardware restart. All system functions, including alarm responses, stop for a few minutes. Attack detection is disabled for five minutes after the system has restarted.

5. Confirm your decision by selecting **I want to System Reboot**.

Administer Time Zone Configuration

This item allows you to review and modify the time zone configuration.

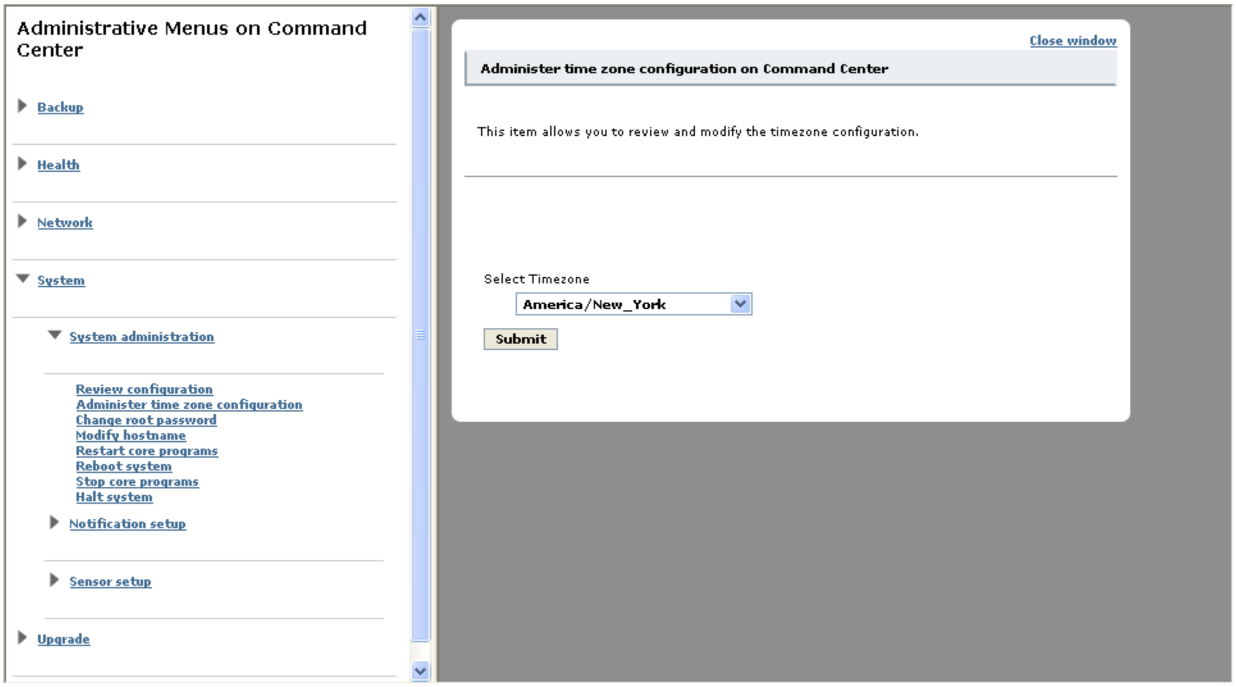
To reboot the system:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **System Administration**.

   The window is repopulated.
4. Click **Administer Time Zone Configuration**

The window is repopulated.



Administer time zone configuration on Command Center

This item allows you to review and modify the timezone configuration.

Select Timezone: America/New_York

5. Select the desired time zone.
6. Click **Submit**.

Stop Core Programs

Stopping core programs stops all system activities, including attack detection and alarm responses, until they are manually restarted. Attack detection is disabled for five minutes after core programs are restarted. This is almost never necessary or desirable.

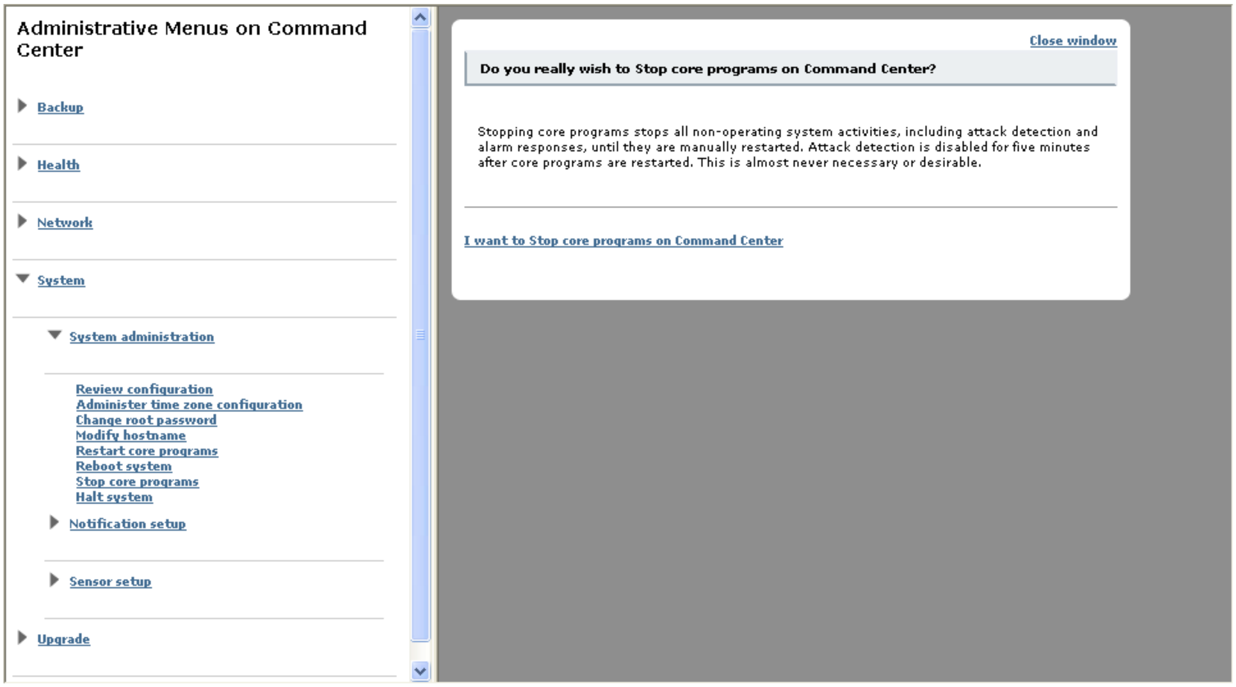
To stop core program status:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Health** and then **Diagnostics**.

   The window is repopulated.
4. Click **Stop Core Programs**.

The window is repopulated.



Do you really wish to Stop core programs on Command Center?

Stopping core programs stops all non-operating system activities, including attack detection and alarm responses, until they are manually restarted. Attack detection is disabled for five minutes after core programs are restarted. This is almost never necessary or desirable.

I want to Stop core programs on Command Center

5. Confirm your decision by selecting **I want to Stop Core Programs**.

System Detection and Response (Sensor Only)

This menu provides configuration options for system detection and response.

To review or change system detection and response configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated with the following selections to the right:

Option	Description
Modify Manual Filters	These entries allow for manual traffic filters that specify which traffic different parts of the system can view.
Modify ARP Daemon operation	This item changes whether or not arpd runs. If possible, it is strongly suggested that arpd operate.
Set ARP Response Interface	This item allows you to select the interface that is used for ARP responses.
Modify VLAN tRunking Mode	This item allows you to change the VLAN trunking mode.
Set Netbios/TCP Name Querying	This item allows you to change Netbios/TCP name-querying settings.

Option	Description
Set Router SNMP community string	This item allows you to change the SNMP community string.
Set Monitoring Interface	This item allows you to select the interface used for monitoring network traffic for attacks.
Set Monitoring Interface	Allows you to modify the IP configuration.

4. Click the desired option.
5. Follow the specific instructions for each option as described in the following sections.

Modify Manual Filters

These entries allow for manual traffic filters that specify which traffic different parts of the system can view. These filter entries supplement the traffic filters which are automatically created by your segment definitions. These filters are in the BPF pcap language, which programs such as tcpdump use. Typically, these filters are used to manually eliminate certain traffic sources or destinations which are problematic in one way or another. Please discuss any changes here with technical support.

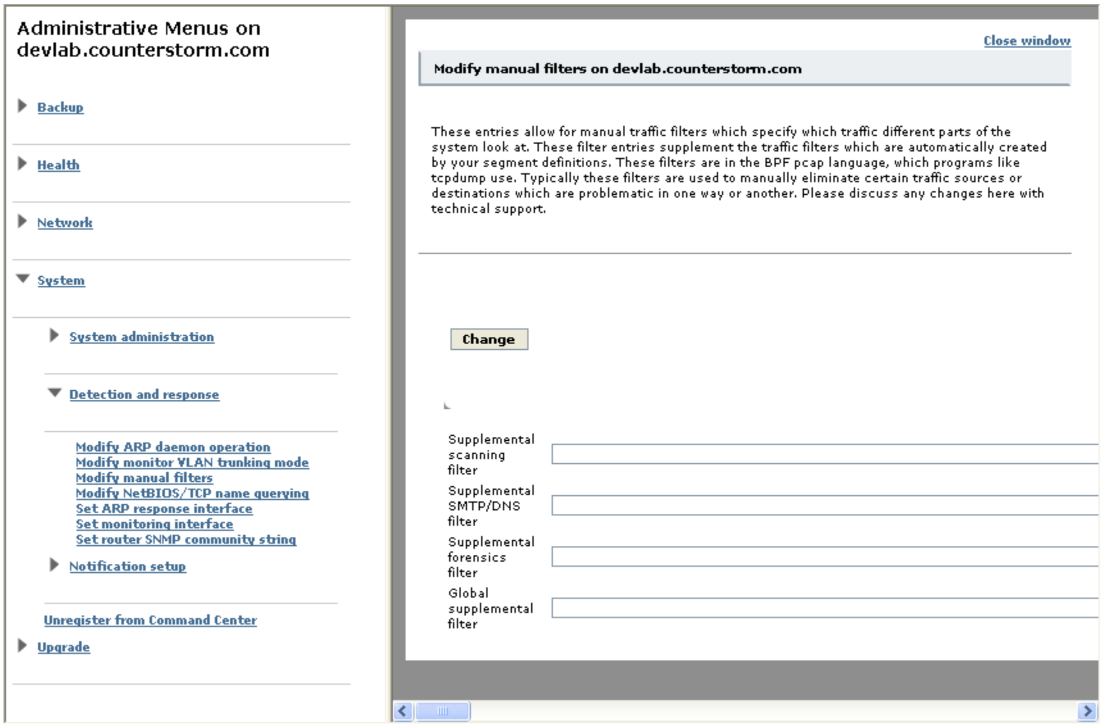
To modify manual filters:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated.
4. Click **Modify Manual Filters**.

The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Change
Supplemental scanning filter
Supplemental SMTP/DNS filter
Supplemental forensics filter
Global supplemental filter

Modify manual filters on devlab.counterstorm.com

These entries allow for manual traffic filters which specify which traffic different parts of the system look at. These filter entries supplement the traffic filters which are automatically created by your segment definitions. These filters are in the BPF pcap language, which programs like tcpdump use. Typically these filters are used to manually eliminate certain traffic sources or destinations which are problematic in one way or another. Please discuss any changes here with technical support.

5. Enter the desired criteria.
6. Click **Change**.

Modify ARP Daemon operation (Sensor Only)

This item controls whether or not arpd runs. The ARP daemon (arpd) is a “honeypot” that directs packets sent to unused IP addresses to the sensor. It is highly recommended that you run arpd, but you may disable it if health reports indicate that it will not run in your configuration.

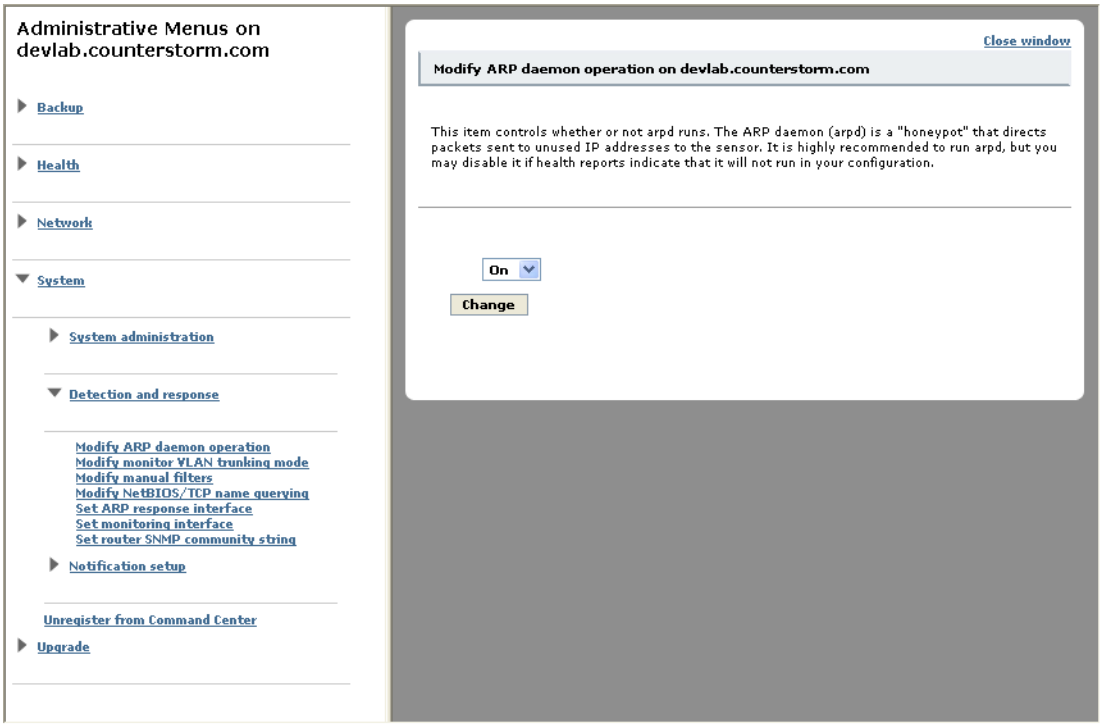
To modify ARP Daemon operation settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated.
4. Click **Modify Daemon ARP operation**.

The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Change

Modify ARP daemon operation on devlab.counterstorm.com

This item controls whether or not arpd runs. The ARP daemon (arpd) is a "honeypot" that directs packets sent to unused IP addresses to the sensor. It is highly recommended to run arpd, but you may disable it if health reports indicate that it will not run in your configuration.

On

5. Select **On** or **OFF** from the pulldown menu.
6. Click **Change**.

Set ARP Response Interface (Sensor Only)

This item allows you to select the interface that is used for ARP responses. You must restart core programs in order to activate any changes.

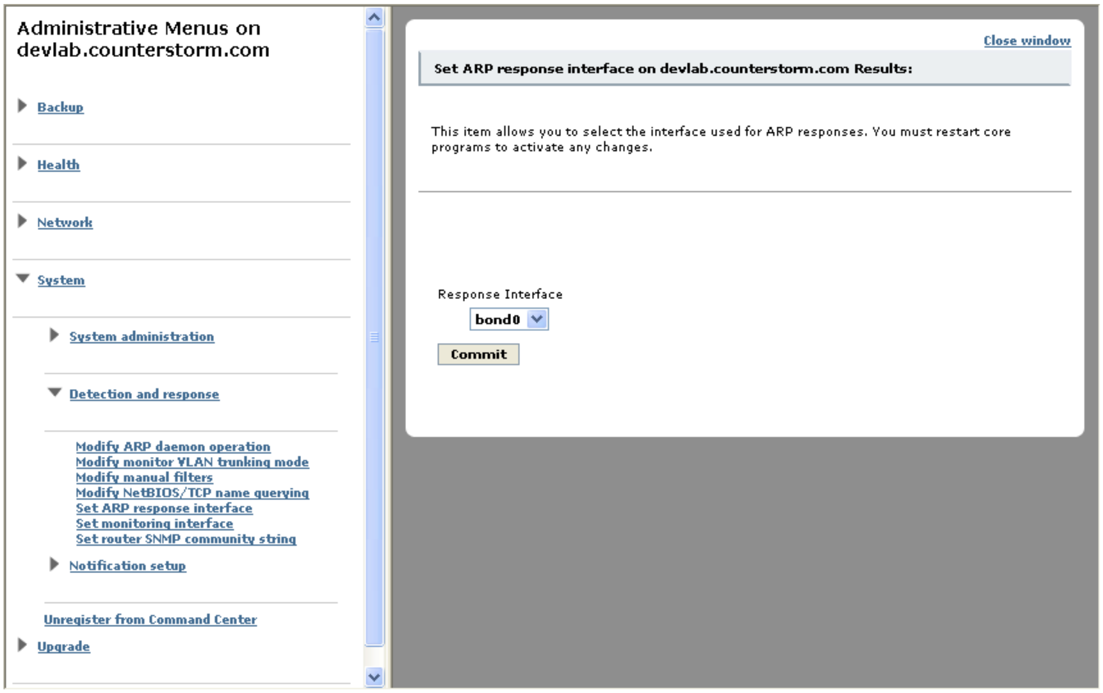
To modify the ARP Response interface settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated.
4. Click **Set ARP response interface**.

The window is repopulated.



Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Commit

Set ARP response interface on devlab.counterstorm.com Results:

This item allows you to select the interface used for ARP responses. You must restart core programs to activate any changes.

Response Interface: bond0

5. Select the desired interface from the pulldown menu.
6. Click **Commit**.

Modify VLAN Trunking Mode (Sensor Only)

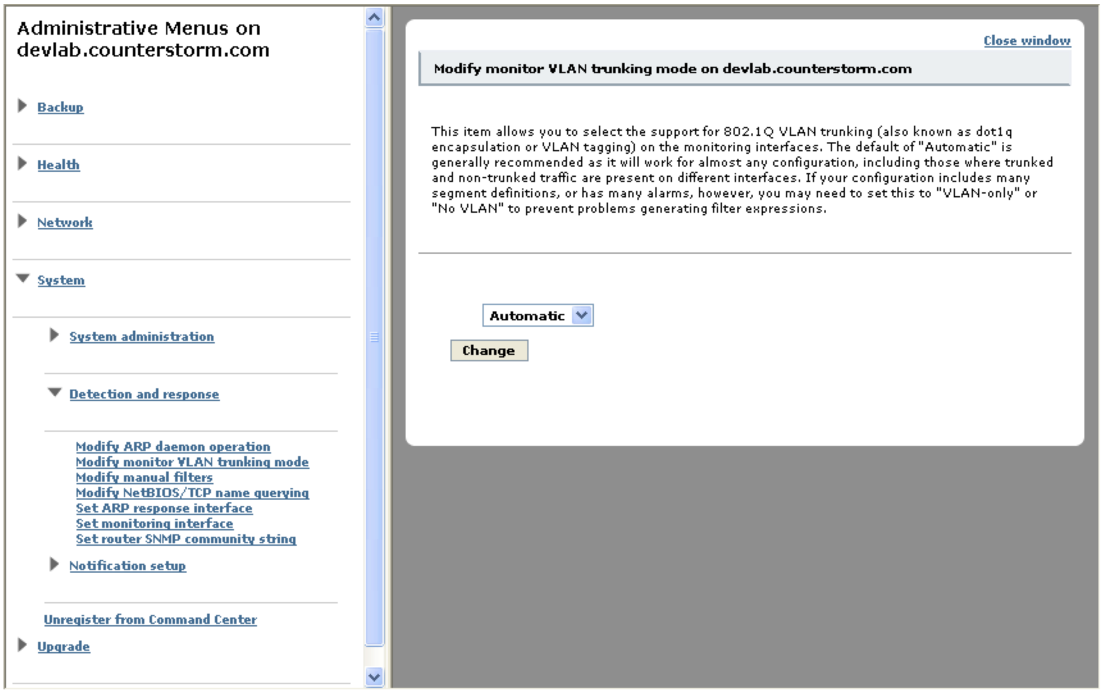
This item allows you to select the support for 802.1Q VLAN trunking (also known as dot1q encapsulation or VLAN tagging) on the monitoring interfaces. The default of Automatic is generally recommended as it will work for almost any configuration, including those where trunked and non-trunked traffic are present on different interfaces. If your configuration includes many segment definitions, or has many alarms, however, you may need to set this to VLAN-only or No VLAN to prevent problems generating filter expressions and on any sensor which has twenty or more non-overlapping segments mapped to it.

To monitor the VLAN trunking mode:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Change

Modify monitor VLAN trunking mode on devlab.counterstorm.com

This item allows you to select the support for 802.1Q VLAN trunking (also known as dot1q encapsulation or VLAN tagging) on the monitoring interfaces. The default of "Automatic" is generally recommended as it will work for almost any configuration, including those where trunked and non-trunked traffic are present on different interfaces. If your configuration includes many segment definitions, or has many alarms, however, you may need to set this to "VLAN-only" or "No VLAN" to prevent problems generating filter expressions.

Automatic

4. Click **Modify VLAN trunking Mode**.
5. Select the mode.
6. Click **Change**.

Set Router SNMP Community String (Sensor Only)

This item configures the SNMP Community String for querying the NetToMedia table on routers when attempting to determine the MAC address of an infected machine. If this is blank, no attempt will be made to use SNMP to obtain MAC addresses from routers. It is only necessary to configure this if neither the sensor nor the switches can use ARP to get the MAC addresses; i.e. neither the sensor monitoring interfaces nor the management IP of any switch mapped to the segment are on the VLAN for the segment. This functionality is only needed if you have configured switch response. If switch response is enabled, but all or most observed traffic is on “transit” segments, and the management IP of the switches is not on the actual segments being switched (but instead, presumably, some management subnet on one of the switch ports) the only way CounterStorm-1 can map IP addresses to MAC addresses is by getting it via SNMP from the router(s) for the segment, and to do that, CounterStorm-1 needs an SNMP community string. CounterStorm-1 needs to be able to access SNMP MIB variables using this community string; specifically, the ipNetToMediaPhysAddress subtree, also known as.1.3.6.1.2.1.4.22.1.2 or more verbosely as .iso.org.dod.internet.mgmt.mib-2.ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaPhysAddress.

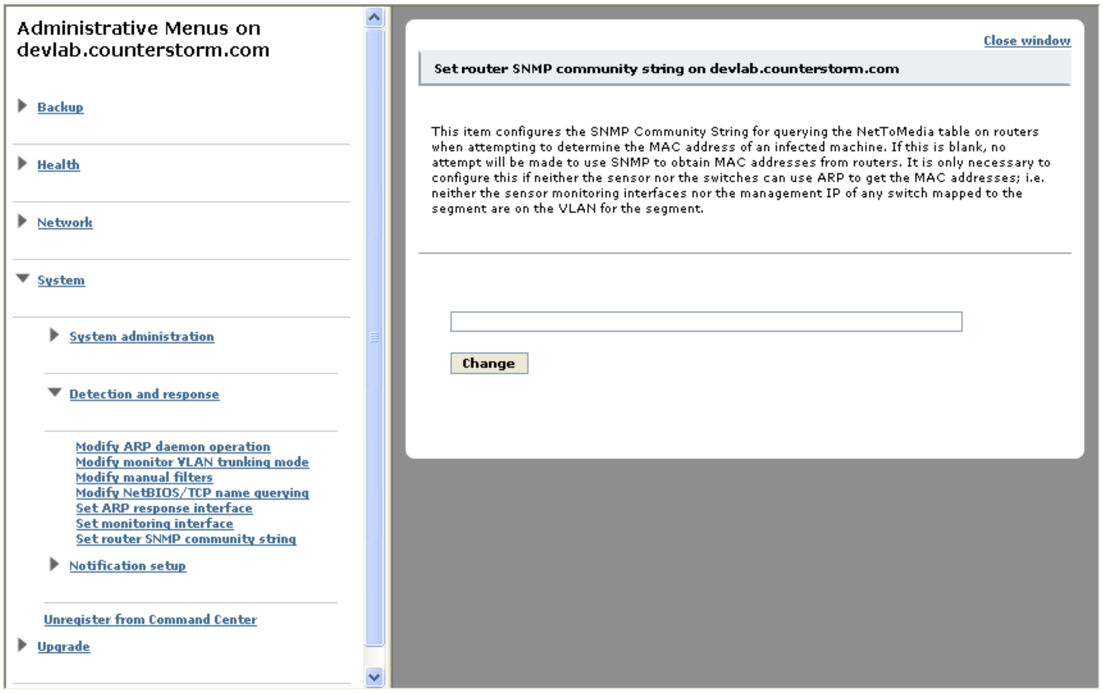
To modify the community string:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated.
4. Click **Set router SNMP community string**.

   The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Change

Set router SNMP community string on devlab.counterstorm.com

This item configures the SNMP Community String for querying the NetToMedia table on routers when attempting to determine the MAC address of an infected machine. If this is blank, no attempt will be made to use SNMP to obtain MAC addresses from routers. It is only necessary to configure this if neither the sensor nor the switches can use ARP to get the MAC addresses; i.e. neither the sensor monitoring interfaces nor the management IP of any switch mapped to the segment are on the VLAN for the segment.

5. Enter the desired string and click **Change**.

Set NetBIOS/TCP Name-Querying (Sensor Only)

This item controls whether or not NetBIOS name queries are sent to infected systems. These UDP/137 queries are used to get additional host and user name information from Windows machines and their servers. It is recommended to perform these queries, but you may disable them if they are not useful or desirable for any reason.

To modify NetBIOS/TCP name-querying:

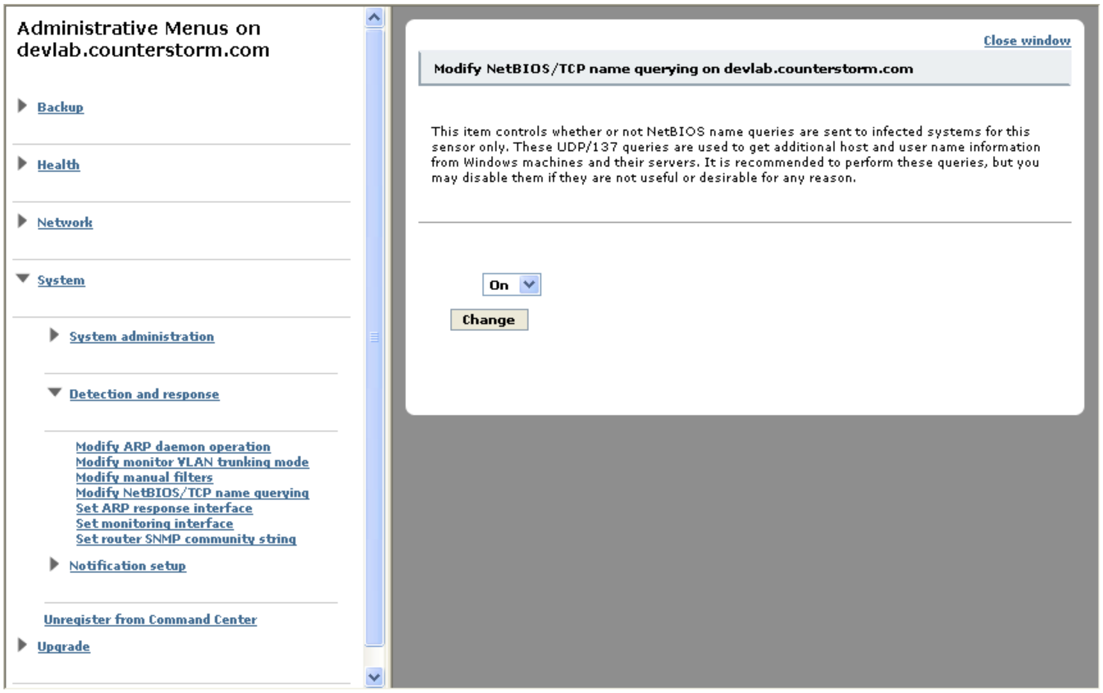
1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

The window is repopulated.

4. Click **Set NetBIOS Name-Querying**.

   The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Change

Modify NetBIOS/TCP name querying on devlab.counterstorm.com

This item controls whether or not NetBIOS name queries are sent to infected systems for this sensor only. These UDP/137 queries are used to get additional host and user name information from Windows machines and their servers. It is recommended to perform these queries, but you may disable them if they are not useful or desirable for any reason.

On

5. Enter the desired criteria and click **Change**.

Set Monitoring Interface (Sensor Only)

This item allows you to select the interface that is used for monitoring network traffic for attacks. You must restart core programs in order to activate any changes.

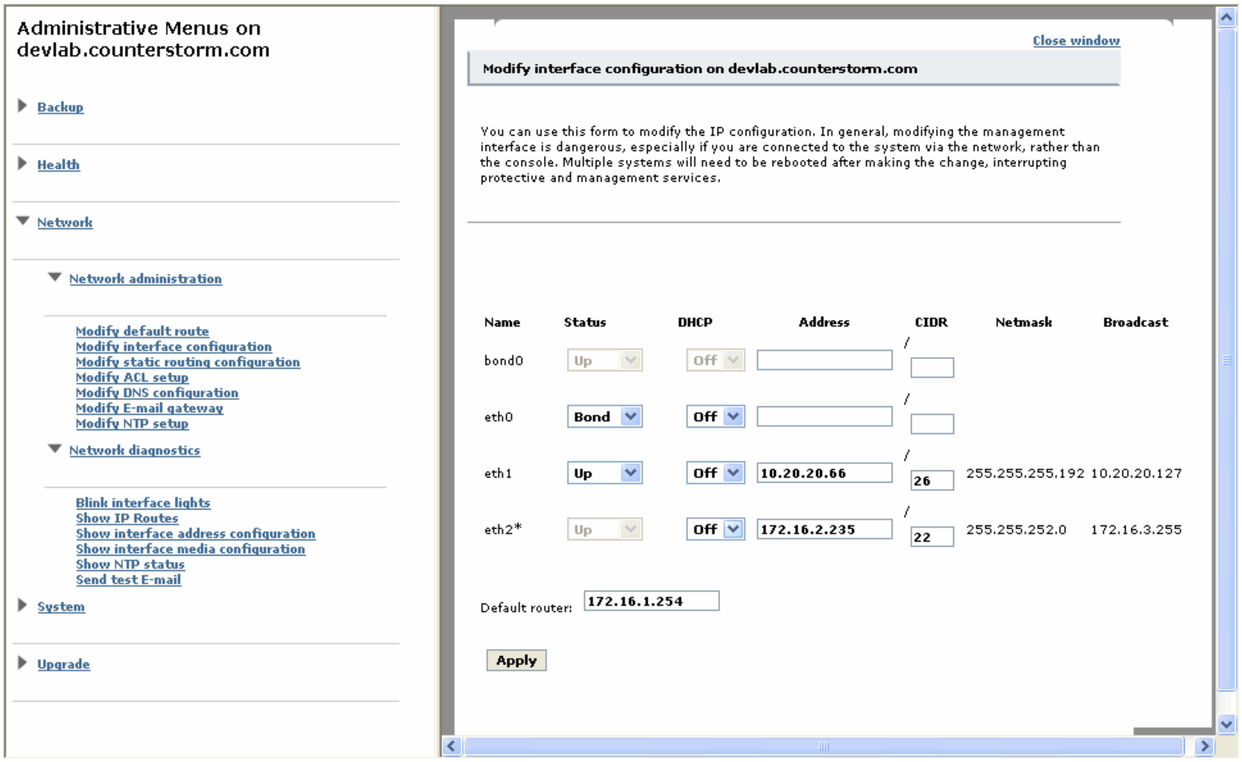
To monitoring the interface settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Network and Network Administration**.

   The window is repopulated.
4. Click **Set monitoring interface**.

The window is repopulated.



Modify interface configuration on devlab.counterstorm.com

You can use this form to modify the IP configuration. In general, modifying the management interface is dangerous, especially if you are connected to the system via the network, rather than the console. Multiple systems will need to be rebooted after making the change, interrupting protective and management services.

Name	Status	DHCP	Address	CIDR	Netmask	Broadcast
bond0	Up	Off		/		
eth0	Bond	Off		/		
eth1	Up	Off	10.20.20.66	/ 26	255.255.255.192	10.20.20.127
eth2*	Up	Off	172.16.2.235	/ 22	255.255.252.0	172.16.3.255

Default router: 172.16.1.254

5. Select the desired interface from the pulldown menu.

   eth2 is reserved for the management interface.

6. Click **Commit**.

Sensor Setup

This menu provides options for registering sensors with the Command Center. You can unregister sensors from the Command Center at the Command Center by selecting the Unregister Sensor option or the Custom Unregister Sensor option from the Sensor Registration/Synchronization menu.

To review or change system detection and response configuration:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.

3. Click **System** and then **Sensor Setup**.

The window is repopulated with the following selections to the right:

Option	Description
Register Sensor	This item is used on the Command Center to register a remote sensor.
Unregister	The unregister option unregisters the sensor from its Command Center and removes only configuration data.
Force Sensor Synchronization	This item, which must be run on the Command Center, resynchronizes the configuration files and database tables on the sensors to the Command Center.
Register Sensor with CC	This item allows you to register the sensor with the Command Center

4. Click the desired option.
5. Follow the specific instructions for each option as described in the following sections.

Register Sensor

This item is used on the Command Center to register a remote sensor. Make sure that you have configured the sensor to allow administrative access from the local IP address of the Command Center.

The registration process takes about 15-20 seconds.

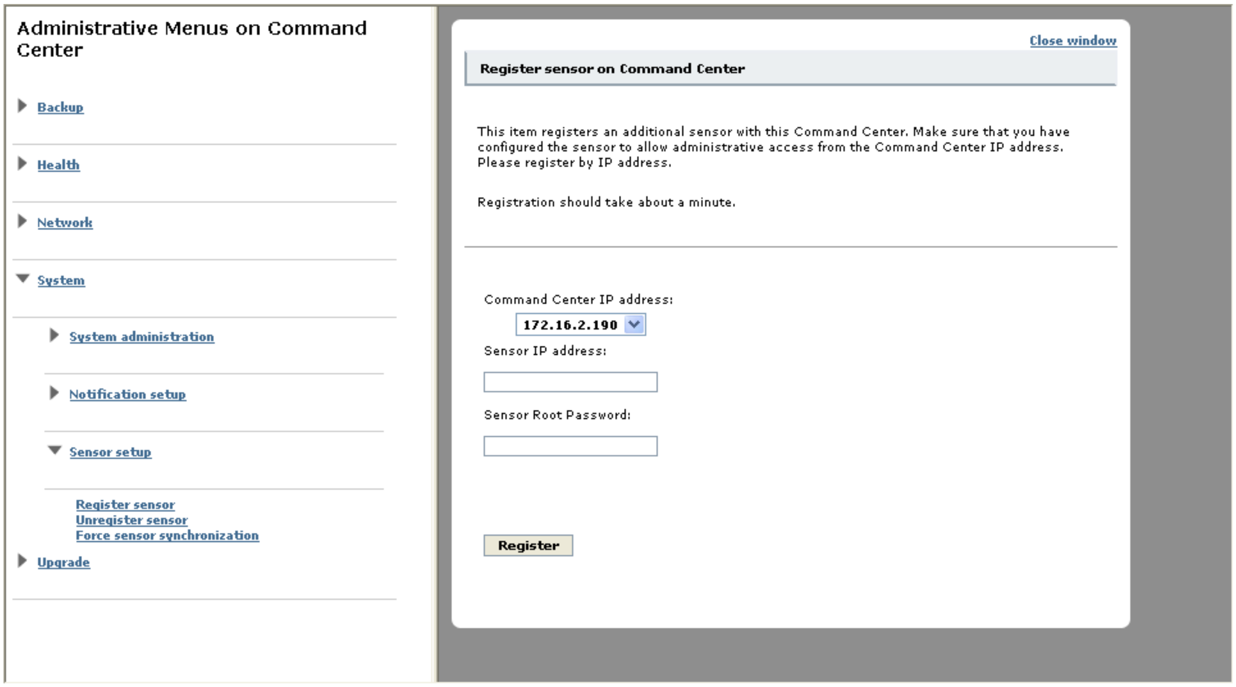
To register the sensor:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated.
4. Click **Register**.

The window is repopulated.



This item registers an additional sensor with this Command Center. Make sure that you have configured the sensor to allow administrative access from the Command Center IP address. Please register by IP address.

Registration should take about a minute.

Command Center IP address: 172.16.2.190

Sensor IP address:

Sensor Root Password:

5. Enter the desired criteria.
6. Click **Register**.

   You are returned to the Sensor Registration/Synchronization Menu.

Force Sensor Synchronization

This item, which must be run on the Command Center, resynchronizes the configuration files and database tables on the sensors to the Command Center. Detection of new infections are disabled for five minutes. You should not normally need to do this.

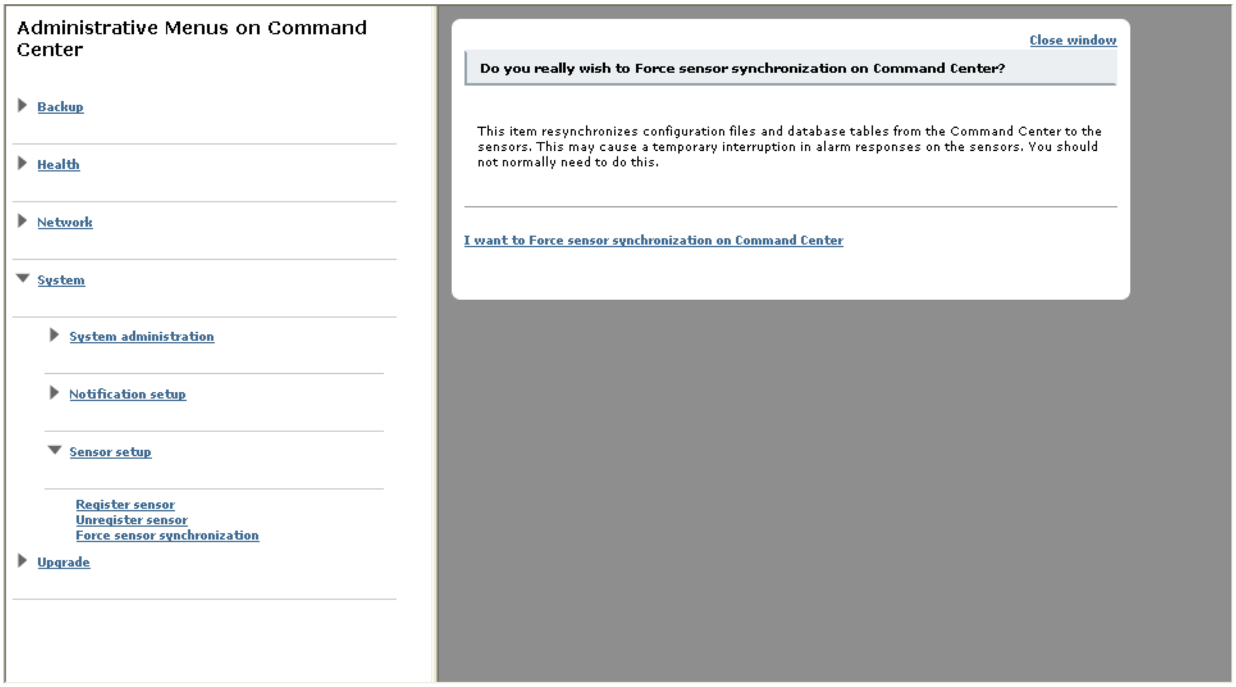
To force sensor synchronization:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated.
4. Click **Force sensor synchronization**.

   The window is repopulated.



Do you really wish to Force sensor synchronization on Command Center?

This item resynchronizes configuration files and database tables from the Command Center to the sensors. This may cause a temporary interruption in alarm responses on the sensors. You should not normally need to do this.

I want to Force sensor synchronization on Command Center

5. Click **I want to force Sensor Synchronization**.

   You are returned to the Sensor Registration/Synchronization Menu.

Unregister Sensor

The unregister option unregisters the sensor from its Command Center and removes configuration data only.

This option allows you to control exactly where machine unregistration takes place and how much data is removed from those machines. The basic unregister option is reproduced here by selecting the Command Center & Sensor and the Configuration data items. Select Command Center Only if you do not have full network connectivity between the two machines.

Additionally, you can choose to eliminate all configuration, alarm, and blocking data. This item is not often used. The following steps show custom unregistration at the sensor.

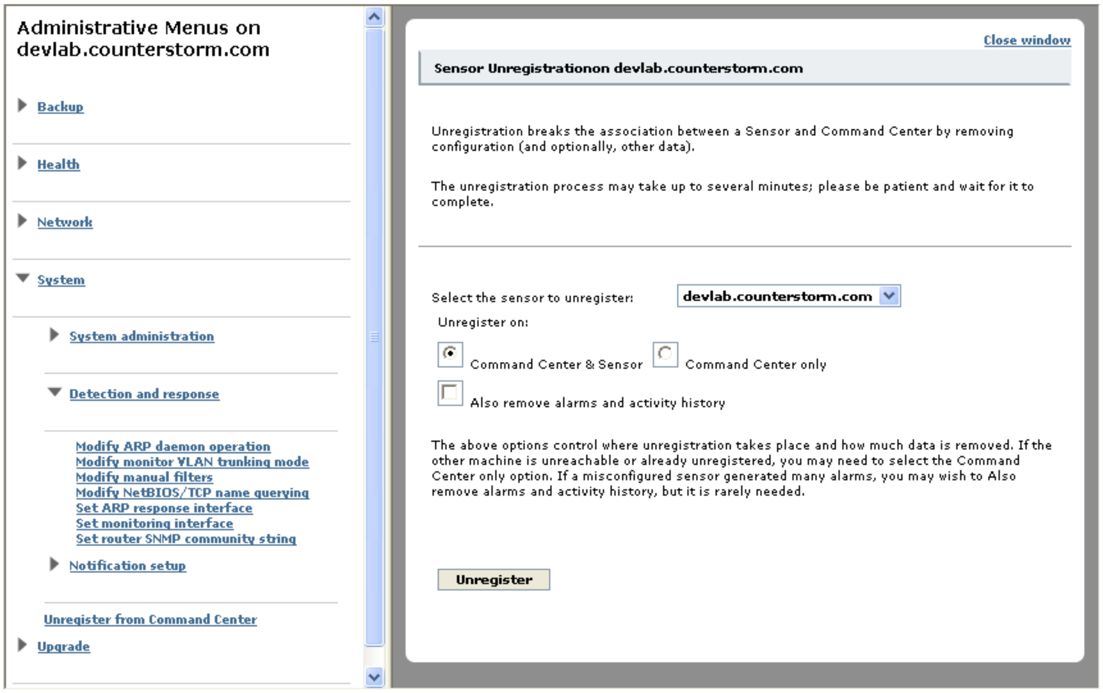
To unregister the sensor at the sensor:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Detection and Response**.

   The window is repopulated.
4. Click **Unregister**.

   The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Unregister

Sensor Unregistrationon devlab.counterstorm.com

Unregistration breaks the association between a Sensor and Command Center by removing configuration (and optionally, other data).

The unregistration process may take up to several minutes; please be patient and wait for it to complete.

Select the sensor to unregister: devlab.counterstorm.com

Unregister on:

● Command Center & Sensor ○ Command Center only

□ Also remove alarms and activity history

The above options control where unregistration takes place and how much data is removed. If the other machine is unreachable or already unregistered, you may need to select the Command Center only option. If a misconfigured sensor generated many alarms, you may wish to Also remove alarms and activity history, but it is rarely needed.

5. Select the sensor to unregister and click **Unregister**.

Register sensor with CC (Sensor Only)

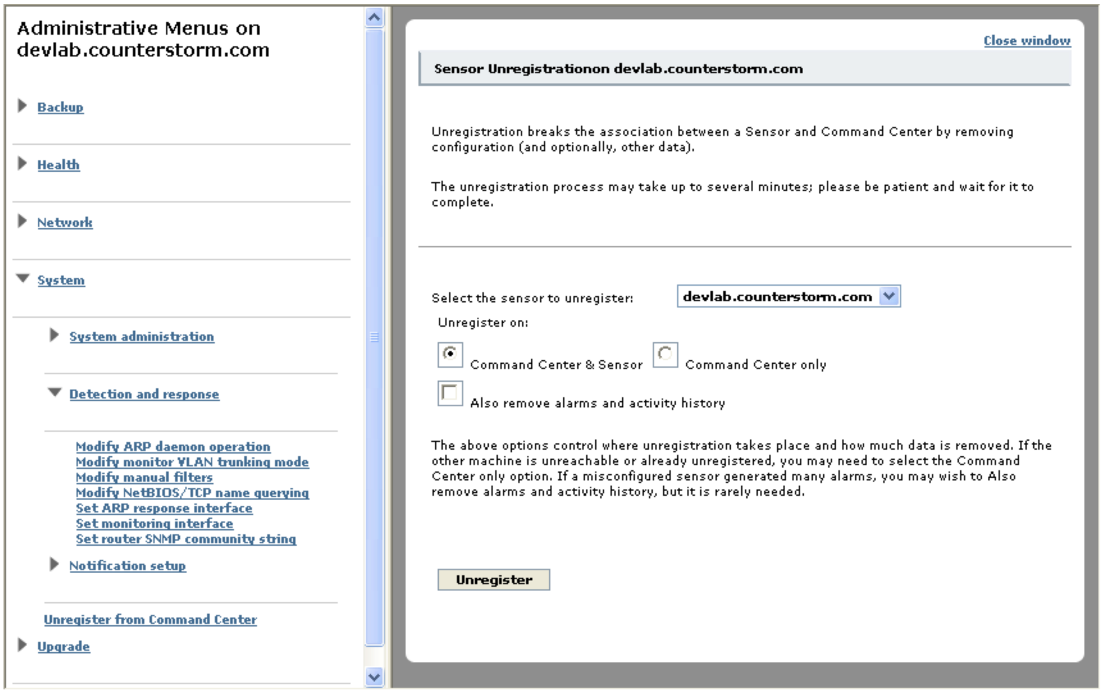
This is a toggle item that only appears on the sensor. It allows you to register/unregister the sensor with the Command Center.

To register/unregister:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Unregister**/**Register Sensor**.

   The window is repopulated.


Administrative Menus on devlab.counterstorm.com
Backup
Health
Network
System
System administration
Detection and response
Modify ARP daemon operation
Modify monitor VLAN trunking mode
Modify manual filters
Modify NetBIOS/TCP name querying
Set ARP response interface
Set monitoring interface
Set router SNMP community string
Notification setup
Unregister from Command Center
Upgrade
Close window
Unregister

Sensor Unregistrationon devlab.counterstorm.com

Unregistration breaks the association between a Sensor and Command Center by removing configuration (and optionally, other data).

The unregistration process may take up to several minutes; please be patient and wait for it to complete.

Select the sensor to unregister: devlab.counterstorm.com

Unregister on:

● Command Center & Sensor ○ Command Center only

□ Also remove alarms and activity history

The above options control where unregistration takes place and how much data is removed. If the other machine is unreachable or already unregistered, you may need to select the Command Center only option. If a misconfigured sensor generated many alarms, you may wish to Also remove alarms and activity history, but it is rarely needed.

4. Select the desired criteria.
5. Click **Unregister/register**.

System Notification Setup

This menu provides configuration options for system notifications.

To review or change system notification:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Notification**.

The window is repopulated with the following selections to the right:

Option	Description
Set administrator e-mail	The administrator e-mail address lists the e-mail addresses of everyone who receives e-mail notifications of system problems.
Set administrator name	The administrator name is the name of the person responsible for the system.
Modify health report from address	The address from which the health check e-mails are sent.
Modify activity report from address	This item allows you to change the activity report From address.
Modify notification from address and subject	The e-mail address from which notifications are sent and the subject line of the message.
Modify response notification from address and subject	The e-mail sender address and subject line that e-mail response notifications should use.

4. Click the desired option.
5. Follow the specific instructions for each option as described in the following sections.

Set administrator e-mail

The administrator e-mail address lists the e-mail addresses of everyone who receives e-mail notifications of system problems. The addresses may be space- or comma-separated.

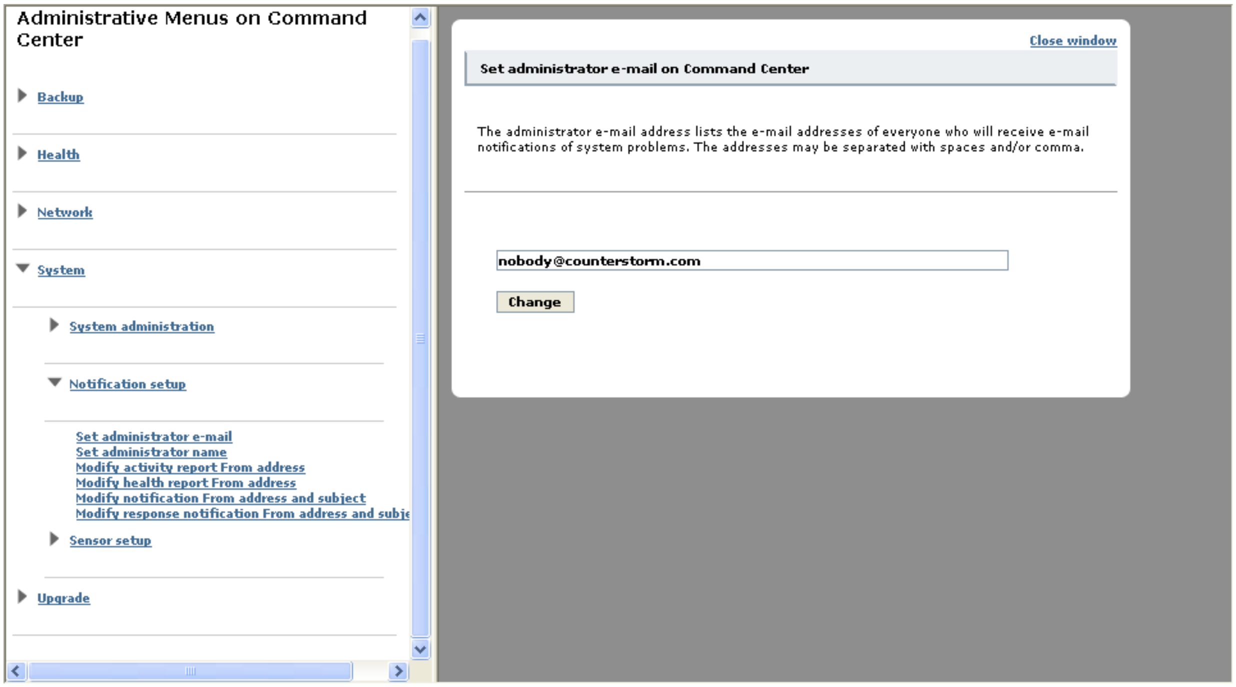
To modify the administrator e-mail settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Notification**.

   The window is repopulated.
4. Click **Set administrator e-mail**.

The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
System administration
Notification setup
Set administrator e-mail
Set administrator name
Modify activity report From address
Modify health report From address
Modify notification From address and subject
Modify response notification From address and subje
Sensor setup
Upgrade
Close window
Change

Set administrator e-mail on Command Center

The administrator e-mail address lists the e-mail addresses of everyone who will receive e-mail notifications of system problems. The addresses may be separated with spaces and/or comma.

nobody@counterstorm.com

5. Enter the desired e-mail.
6. Click **Change**.

Set administrator name

The administrator name is the name of the person responsible for the system.

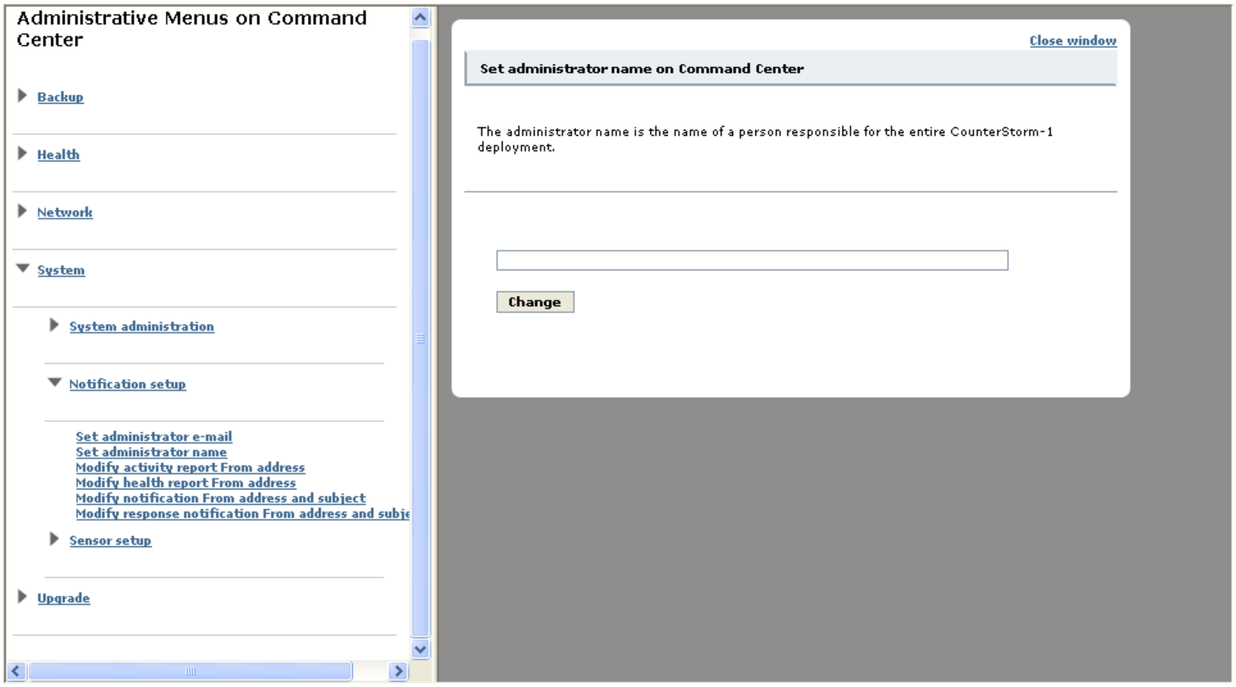
To modify the administrator name settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Notification**.

   The window is repopulated.
4. Click **Set administrator name**.

The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
System administration
Notification setup
Set administrator e-mail
Set administrator name
Modify activity report From address
Modify health report From address
Modify notification From address and subject
Modify response notification From address and subje
Sensor setup
Upgrade
Close window
Change

Set administrator name on Command Center

The administrator name is the name of a person responsible for the entire CounterStorm-1 deployment.

5. Enter the desired name.
6. Click **Change**.

Modify Health Report From Address

This is the address from which the health check e-mails are sent.

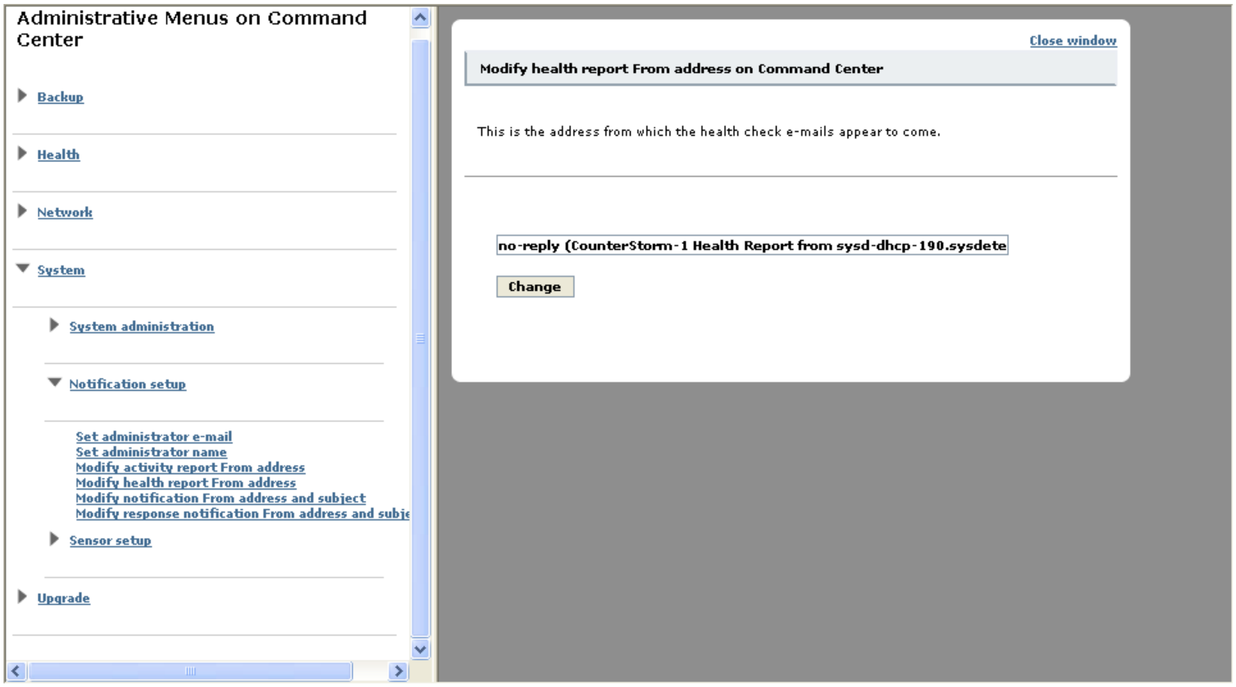
To modify health report from address settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Notification**.

   The window is repopulated.
4. Click **Modify health report from address**.

The window is repopulated.



Administrative Menus on Command Center
Backup
Health
Network
System
System administration
Notification setup
Set administrator e-mail
Set administrator name
Modify activity report From address
Modify health report From address
Modify notification From address and subject
Modify response notification From address and subje
Sensor setup
Upgrade
Close window
Change

Modify health report From address on Command Center

This is the address from which the health check e-mails appear to come.

no-reply (CounterStorm-1 Health Report from sysd-dhcp-190.sysdete

5. Enter the desired address (username).
6. Click **Change**.

Modify Activity Report From Address

This is the address from which the activity check e-mails are sent.

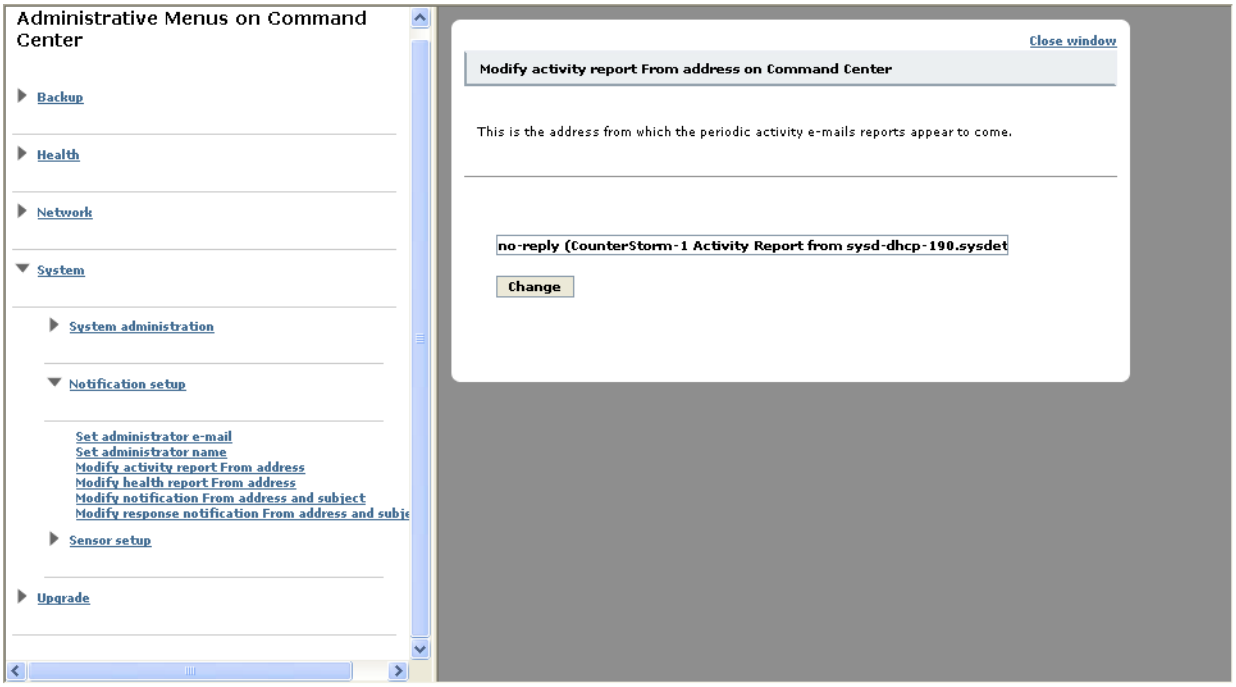
To modify health report from address settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **System** and then **Notification**.

   The window is repopulated.
4. Click **Modify Activity report from address**.

The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
System administration
Notification setup
Set administrator e-mail
Set administrator name
Modify activity report From address
Modify health report From address
Modify notification From address and subject
Modify response notification From address and subje
Sensor setup
Upgrade
Close window
Modify activity report From address on Command Center
Change

This is the address from which the periodic activity e-mails reports appear to come.

no-reply (CounterStorm-1 Activity Report from sysd-dhcp-190.sysdet

5. Enter the desired address (username).
6. Click **Change**.

Modify Notification From Address and Subject (Command Center Only)

This item allows you to modify the e-mail address from which notifications are sent, as well as subject line of the message.

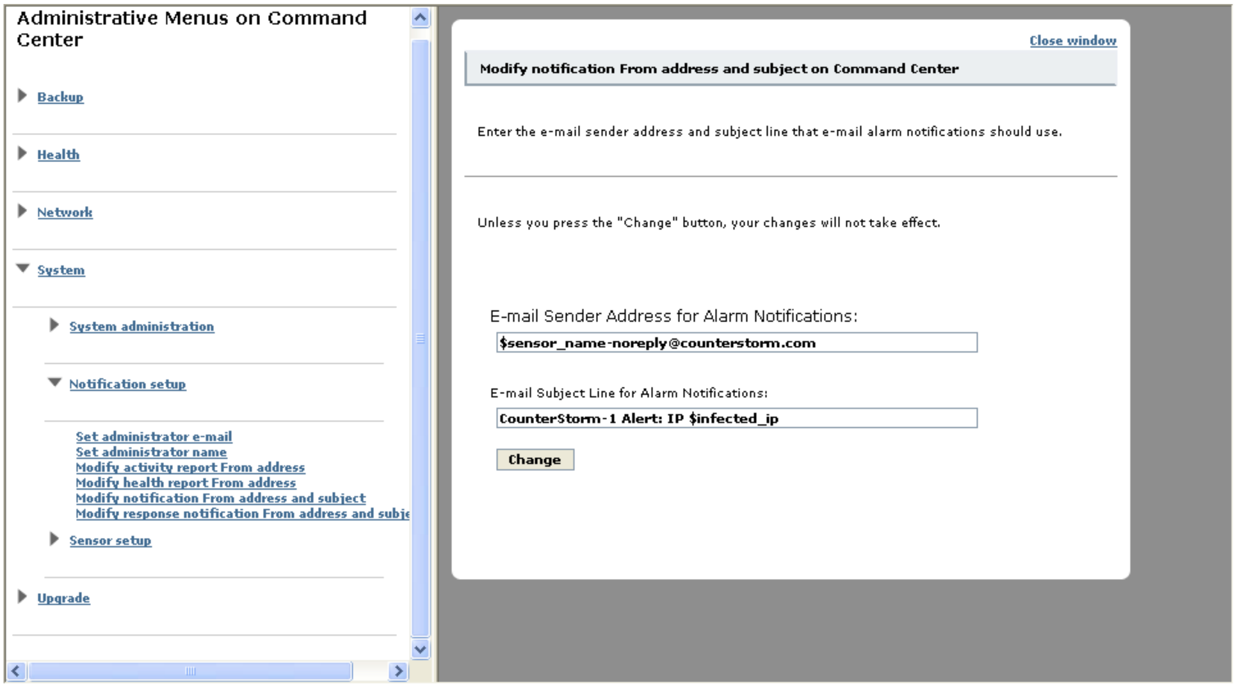
To modify notification from address and subject settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center**.

   A window pops up with configuration choices.
3. Click **System** and then **Notification**.

   The window is repopulated.
4. Click **Modify notification from address and subject**.

The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
System administration
Notification setup
Set administrator e-mail
Set administrator name
Modify activity report From address
Modify health report From address
Modify notification From address and subject
Modify response notification From address and subje
Sensor setup
Upgrade
Close window
Change

Modify notification From address and subject on Command Center

Enter the e-mail sender address and subject line that e-mail alarm notifications should use.

Unless you press the "Change" button, your changes will not take effect.

E-mail Sender Address for Alarm Notifications:
$sensor_name-noreply@counterstorm.com

E-mail Subject Line for Alarm Notifications:
CounterStorm-1 Alert: IP $infected_ip

5. Enter the address from which notifications are sent and the subject line of the message.
6. Click **Change**.

Modify Response Notification From Address and Subject (Command Center Only)

This item allows you to modify the e-mail sender address and subject line that e-mail response notifications should use.

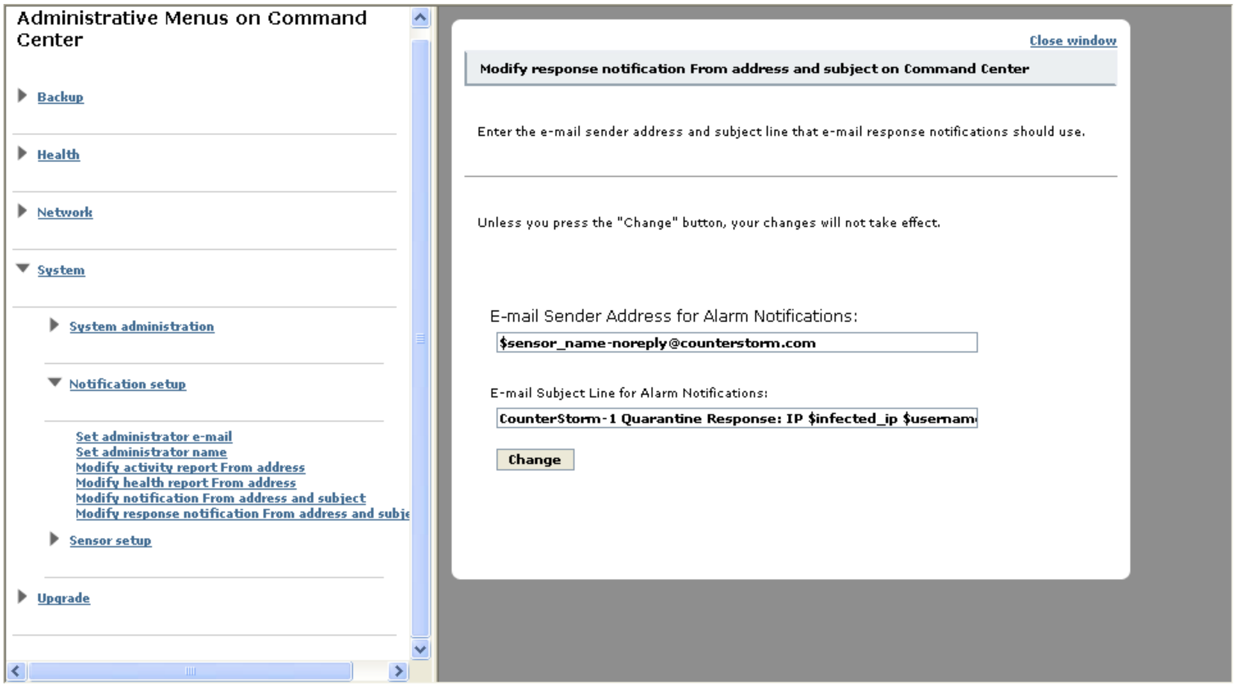
To modify notification from address and subject settings:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center**.

   A window pops up with configuration choices.
3. Click **System** and then **Notification**.

   The window is repopulated.
4. Click **Modify response notification from address and subject**.

The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
System administration
Notification setup
Set administrator e-mail
Set administrator name
Modify activity report From address
Modify health report From address
Modify notification From address and subject
Modify response notification From address and subje
Sensor setup
Upgrade
Close window
Change

Modify response notification From address and subject on Command Center

Enter the e-mail sender address and subject line that e-mail response notifications should use.

Unless you press the "Change" button, your changes will not take effect.

E-mail Sender Address for Alarm Notifications: $sensor_name-noreply@counterstorm.com

E-mail Subject Line for Alarm Notifications: CounterStorm-1 Quarantine Response: IP $infected_ip $usernam

5. Enter the address from which notifications are sent and the subject line of the message.
6. Click **Change**.

Upgrades

This menu allows you to modify or view health diagnostic information.

To modify or view health diagnostic information:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Upgrades**.

   The window is repopulated with the following selections

Option	Description
Install Upgrade	Install patches.
Upload Upgrade File	Install patches from disk.
Uninstall Upgrade	Uninstall existing patches.
View Upgrade History	Allows you to review patch history.

Install Upgrade

This item allows you to install patches.

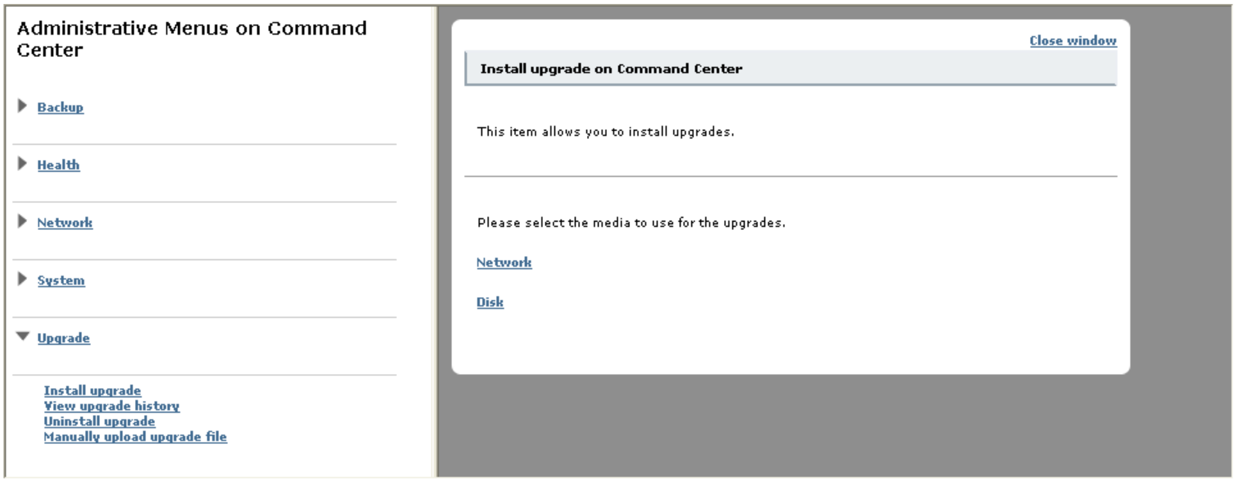
To install upgrades:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Upgrades**.

   The window is repopulated.
4. Click **Install Upgrade**.

   The window is repopulated.



This item allows you to install upgrades.

Please select the media to use for the upgrades.

5. Select **Network** or **Disk** to select which media you wish to use to retrieve the patches.

   The window is repopulated.
6. Enter the name of the patch.
7. Click **Previous Menu**.

Upload Upgrade File

This item allows you to upload the file of CounterStorm-1 patches in preparation for installing from disk. First, download the file of patches from this the link indicated to your machine and then upload it from there to the destination via the upload dialog.

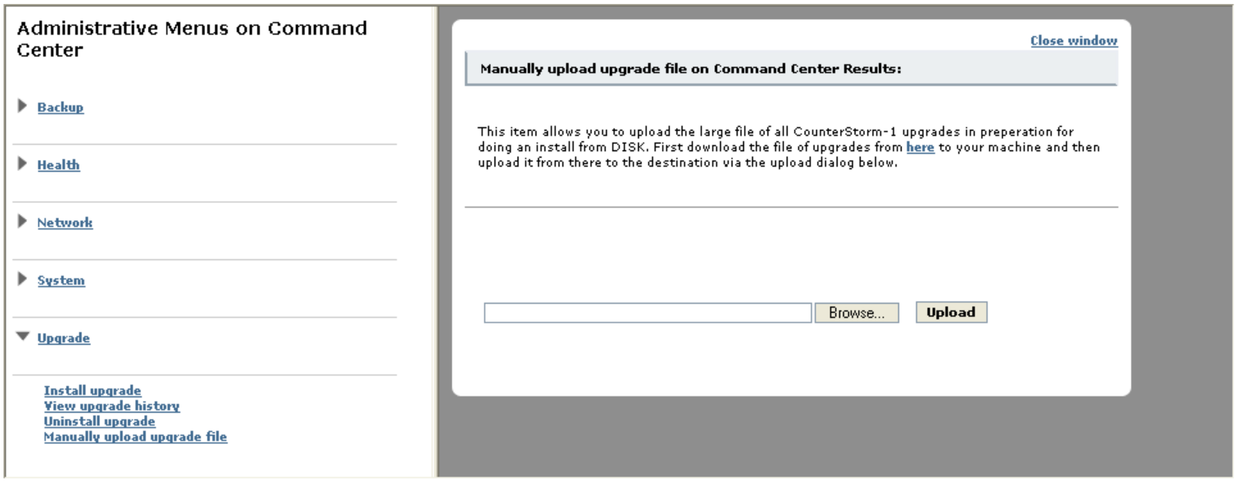
To upgrade from disk:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Upgrades**.

   The window is repopulated.
4. Click **Upload Upgrade File**.

The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
Upgrade
Install upgrade
View upgrade history
Uninstall upgrade
Manually upload upgrade file
Close window
Manually upload upgrade file on Command Center Results:
Browse...
Upload

This item allows you to upload the large file of all CounterStorm-1 upgrades in preperation for doing an install from DISK. First download the file of upgrades from here to your machine and then upload it from there to the destination via the upload dialog below.

5. Click the link and then select the file to upload.

Uninstall Upgrade

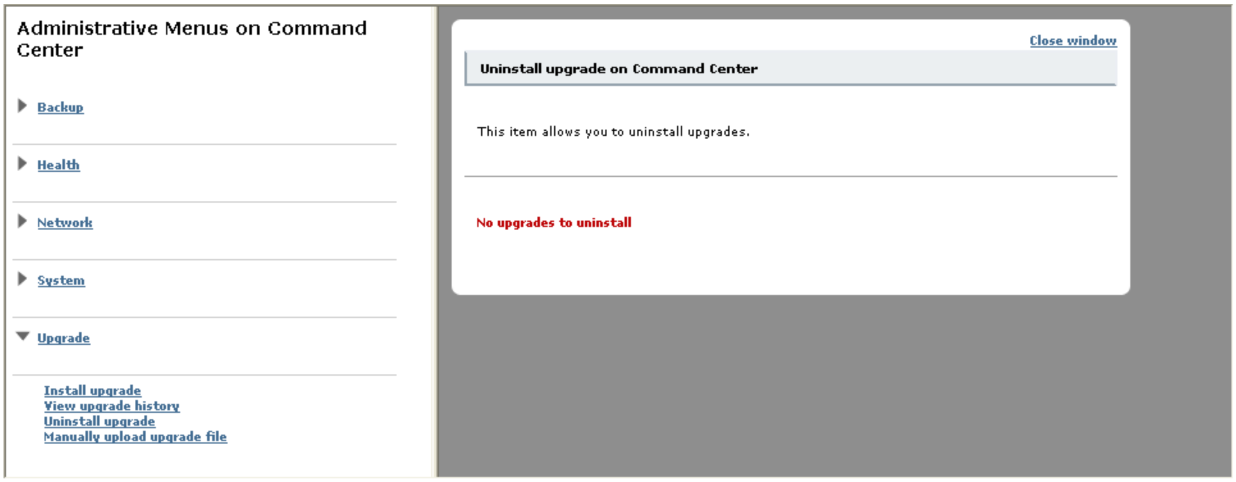
This item uninstalls existing patches.

To uninstall a patch:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Upgrades**.

   The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
Upgrade
Install upgrade
View upgrade history
Uninstall upgrade
Manually upload upgrade file
Close window
Uninstall upgrade on Command Center

This item allows you to uninstall upgrades.

No upgrades to uninstall

4. Click **Uninstall Upgrade.**

   The window is repopulated.
5. Select the name of the patch to uninstall.
6. Click **Change**.

View Upgrade History

This item allows you to view the history of saved patches that are installed on the machine.

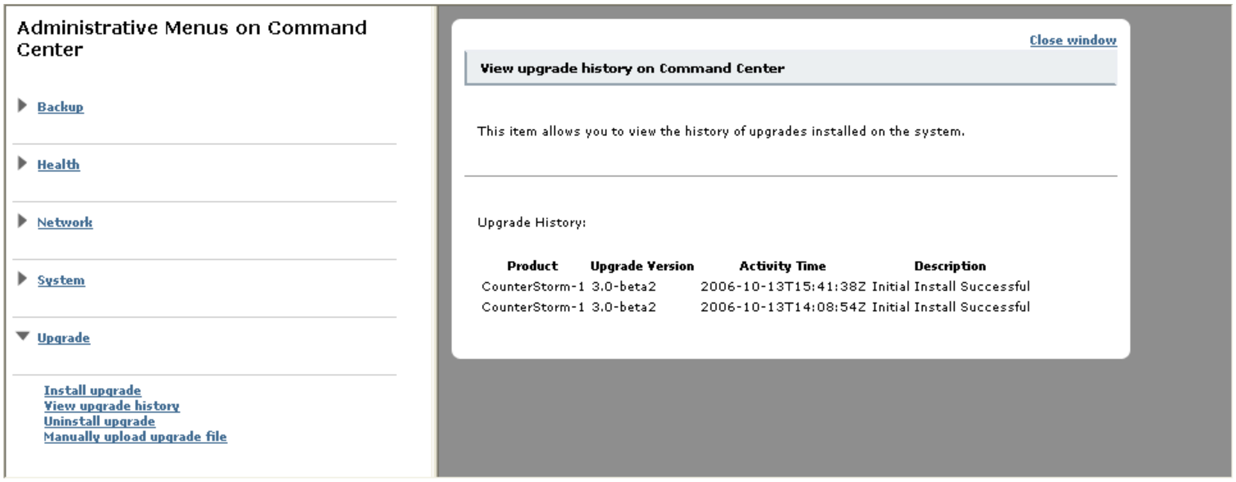
To view upgrade history:

1. Select **Configure** from the Main Toolbar and **Systems** from the Interactive Toolbar.
2. Click **Manage Command Center** or **Manage** *sensor_name*.

   A window pops up with configuration choices.
3. Click **Upgrades**.

   The window is repopulated.
4. Click **View Upgrade History**.

   The window is repopulated.


Administrative Menus on Command Center
Backup
Health
Network
System
Upgrade
Install upgrade
View upgrade history
Uninstall upgrade
Manually upload upgrade file
Close window
View upgrade history on Command Center

This item allows you to view the history of upgrades installed on the system.

Upgrade History:

Product	Upgrade Version	Activity Time	Description
CounterStorm-1	3.0-beta2	2006-10-13T15:41:38Z	Initial Install Successful
CounterStorm-1	3.0-beta2	2006-10-13T14:08:54Z	Initial Install Successful

5. Click **Previous Menu**.

Appendix A: Sample Status E-mail

Sample E-mail Alarms

Alarms can be sent in many ways. The examples listed are via e-mail.

Alarm on a Specific Segment via Short E-mail

This alarm tells you that there is a UDP/21 related problem on machine 10.21.32.12 in the segment 21. It indicates that there is Intranet UDP scanning.

```
Subject: CounterStorm-1 Alert: IP 10.21.2.21
Sent: Friday, March 03, 2006 7:40 PM
From: root@cs1-sensor1.counterstorm.com
To: test@counterstorm.com

When: 2006-03-03 19:40:14 EST
Who: 10.21.32.12 | ?
Where: seg21 | 10.21.0.0-10.21.255.255
What: UDP/21
Sensor: sysd-dhcp-4.counterstorm.com
Reason: Intranet UDP scanning
Response: TCP Host Blocking (started).
Response: ARP Host Blocking (started).

Previous Alarm: N/A
Previous Alarm Reason: N/A
First Alarm: N/A
First Alarm Reason: N/A
Whitelisted: No
More Details: https://sysd-dhcp-123.counterstorm.com/investigate.php?ip=10.21.32.12
```

Alarm on a Specific Segment via Detailed E-mail

This alarm tells you that there is a UDP/21 related problem on machine 10.21.32.12 in the segment 21. It indicates that there is Intranet UDP scanning and includes more information than the short e-mail format.

```
Subject: CounterStorm-1 Alert: IP 10.21.2.21
Sent: Friday, March 03, 2006 7:40 PM
From: root@cs1-sensor1.counterstorm.com
To: test@counterstorm.com

When: 2006-03-03 19:40:14 EST
Who: 10.21.32.12 | ?
Where: seg21 | 10.21.0.0-10.21.255.255
What: UDP/21
Sensor: sysd-dhcp-4.counterstorm.com
Reason: Intranet UDP scanning
Response: TCP Host Blocking (started).
Response: ARP Host Blocking (started).
```

```
Previous Alarm: N/A
Previous Alarm Reason: N/A
First Alarm: N/A
First Alarm Reason: N/A
First Activity Noticed: 2006-03-03 19:39:59 EST
Last Activity Noticed: 2006-03-03 19:40:14 EST
MAC Address: 00:e0:81:27:40:44
VLAN: Unknown
Whitelisted: No
More Details: https://sysd-dhcp-123.counterstorm.com/investigate.php?ip=10.21.32.12
```

Alarm on Default Internet Segment via Short E-mail

This alarm indicates that there is UDP scanning on the default internet segment.

```
Subject: CounterStorm-1 alert | IP 199.5.8.64
Sent: Friday, July 29, 2005 10:19AM
From: root@cs1-sensor1.counterstorm.com
To: test@counterstorm.com

When:2005-07-27 12:13:50.065409 EDT
Who:199.5.8.64 | ?
Where:Internet | 0.0.0.0-255.255.255.255
What:UDP/110
Sensor: cs1-sensor1.counterstorm.com
Reason: External (inbound) UDP scanning
Response: TCP Host Blocking (started).

Previous Alarm: N/A
Previous Alarm Reason: N/A
First Alarm: N/A
First Alarm Reason: N/A
More Details: https://sysd-dhcp-133.sysdetect.com/monitor-investigate.php?&q=10.8.3.15
```

Alarm Due to Excessive E-mail Connections

This alarm indicates that there are excessive e-mail connections on the MSJ 2 segment.

```
Subject: CounterStorm-1 alert | IP 10.30.30.120
Sent: Friday, July 29, 2005 10:19AM
From: root@cs1-sensor1.counterstorm.com
To: test@counterstorm.com

When:2005-07-19 14:12:02.289723 EDT
Who:10.30.30.120 | ?
Where:msj 0 | 10.0.0.1-10.255.255.255
What:TCP/25
Sensor: cs1-sensor1.counterstorm.com
Reason: Excessive e-mail connections
Response: TCP Host Blocking (started).

Previous Alarm: TCP/25 2005-07-19 18:12:02.256064
Previous Alarm Reason: Excessive e-mail volume
First Alarm: TCP/25 2005-07-18 14:37:52.232613
First Alarm Reason: Outbound TCP scanning (public internet)
More Details: https://sysd-dhcp-133.sysdetect.com/monitor-investigate.php?&q=10.8.3.15
```

Sample E-mail Status Reports

Unhealthy Status Report

In this status report, there is a problem. The operational status percentage is low and a NO TRAFFIC OBSERVED problem is listed at the top of the report. The rest of the report is similar in content to a healthy status report as shown in “Healthy Status Report” on page A-4. This report continues to be e-mailed (approximately every 15 minutes) until the problem is fixed.

```
Subject: CounterStorm-1 cs1-sensor1.couterstorm.com Health Report at 25%
Sent: Friday, July 29, 2005 10:19AM
From: root@cs1-sensor1.counterstorm.com
To: test@counterstorm.com


                                               Operating at 50%
                     +-------------------------------------------------------------------+
                                            * * * PROBLEM * * *
                                    * Wire bits progress of sysd-dhcp-4_1:
                                  NO TRAFFIC OBSERVED (remains 18822192 bits)
                    +--------------------------------------------------------------------+
```

Sample Status E-mail

Healthy Status Report

In this status report, the system is healthy. There are no problems.

```
Subject: CounterStorm cs1-sensor1.counterstorm.com Health Report at 100%
Sent: Friday, July 29, 2005 10:19AM
From: root@cs1-sensor1.counterstorm.com
To: test@counterstorm.com


Operating at 100%

Operating at 100%


    +--------------------------------------------------------------------+
    Load Average:
    1 Minute Load=0.54 5 Minute Load=0.31 15 Minute Load=0.48
    +--------------------------------------------------------------------+
    Disk Usage:
    Filesystem Type Size Used Avail Use% Mounted on
    /dev/mapper/VolGroup00-LogVol00
    ext3 8.5G 400M 7.7G 5% /
    /dev/md0 ext3 1.1G 45M 963M 5% /boot
    none tmpfs 2.1G 0 2.1G 0% /dev/shm
    /dev/mapper/VolGroup00-LogVol03
    reiserfs 350G 1.3G 349G 1% /usr
    /dev/mapper/VolGroup00-LogVol02
    reiserfs 4.3G 1.4G 3.0G 31% /var
    +--------------------------------------------------------------------+
    Top Status:
    top - 17:05:02 up 4:42, 2 users, load average: 0.54, 0.31, 0.48
    Tasks: 108 total, 2 running, 106 sleeping, 0 stopped, 0 zombie
    Cpu(s): 3.2% us, 1.4% sy, 0.1% ni, 94.6% id, 0.5% wa, 0.0% hi, 0.1% si
    Mem: 4058776k total, 1095376k used, 2963400k free, 168236k buffers
    Swap: 8388600k total, 0k used, 8388600k free, 517124k cached
    PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
    29180 antura 17 0 240m 58m 48m D 7.9 1.5 0:23.12 postgres: sysd sysd 127.0.0.1 INSERT
    23016 root 18 0 15996 3580 1588 R 7.9 0.1 0:00.04 /usr/bin/perl -w /usr/counterstorm/bin/jump.pl --raw -
    -worker-status sysd-dhcp-4_2
    8896 root 16 0 55056 19m 3612 S 4.0 0.5 0:06.75 antura-batcher
    28885 root 15 0 215m 34m 4176 S 4.0 0.9 2:36.35 /usr/counterstorm/bin/worker --no-seatbelts --server-on-
    stdin --one-shot --threads --log-stderr=/us
    22959 root 16 0 29408 10m 1800 S 2.0 0.3 0:00.14 /usr/bin/perl -w /usr/counterstorm/bin/BkReportGen --
    locking -P 300 -C onfailure -o postgres:////an
    1 root 16 0 4816 524 436 S 0.0 0.0 0:00.89 init [3]
    2 root RT 0 0 0 0 S 0.0 0.0 0:00.07 [migration/0]
    3 root 34 19 0 0 0 S 0.0 0.0 0:00.00 [ksoftirqd/0]
    4 root RT 0 0 0 0 S 0.0 0.0 0:00.07 [migration/1]
    5 root 34 19 0 0 0 S 0.0 0.0 0:00.00 [ksoftirqd/1]
    12573 root 15 0 27096 1656 1272 S 0.0 0.0 0:00.00 initlog -c dbmirror.pl -m sensor-to-manager
    12629 root 15 0 27100 1664 1272 S 0.0 0.0 0:00.00 initlog -c dbmirror.pl -m manager-to-sensor
    12665 antura 16 0 228m 14m 13m S 0.0 0.4 0:17.30 postgres: sysd sysd 172.16.2.4 idle
    12668 antura 15 0 230m 10m 9152 S 0.0 0.3 0:00.90 postgres: sysd sysd 172.16.2.4 idle
    12492 root 15 0 27100 1484 1188 S 0.0 0.0 0:00.00 initlog -c /usr/counterstorm/bin/poisonarpd --no-
    seatbelts -p 2e:2e:2e:53:4a:52 -s :sysd-parpd-ext
    12514 root 16 0 52900 2732 2064 S 0.0 0.1 0:00.15 /usr/counterstorm/bin/poisonarpd --no-seatbelts -p
    2e:2e:2e:53:4a:52 -s :sysd-parpd-ext -i bond0
    12571 root 15 0 27096 1340 1080 S 0.0 0.0 0:00.00 initlog -c /usr/counterstorm/bin/rstd -i bond0 --no-
    seatbelts -s :sysd-rstd-ext -f "not ether dst 2
    12594 root 16 0 51784 2656 2012 S 0.0 0.1 0:00.15 /usr/counterstorm/bin/rstd -i bond0 --no-seatbelts -s
    :sysd-rstd-ext -f not ether dst 2e:2e:2e:53:4
    13174 root 17 0 47628 15m 3228 S 0.0 0.4 0:09.54 alarm-handler.pl
```

```
13176 antura 16 0 232m 17m 14m S 0.0 0.4 0:43.23 postgres: sysd sysd 127.0.0.1 idle
28899 root 16 0 216m 24m 4296 S 0.0 0.6 0:18.51 /usr/counterstorm/bin/worker --no-seatbelts --server-on-
stdin --one-shot --threads --log-stderr=/us
28913 root 16 0 138m 6884 4168 S 0.0 0.2 0:00.59 /usr/counterstorm/bin/worker --no-seatbelts --server-
on-stdin --one-shot --threads --log-stderr=/us
28927 root 16 0 139m 7168 4112 S 0.0 0.2 0:00.65 /usr/counterstorm/bin/worker --no-seatbelts --server-
on-stdin --one-shot --threads --log-stderr=/us
28941 root 16 0 104m 4440 3036 S 0.0 0.1 0:00.33 /usr/counterstorm/bin/worker --no-seatbelts --server-
on-stdin --one-shot --threads --log-stderr=/us
28959 root 16 0 104m 4436 3036 S 0.0 0.1 0:00.33 /usr/counterstorm/bin/worker --no-seatbelts --server-
on-stdin --one-shot --threads --log-stderr=/us
28973 root 16 0 104m 4440 3036 S 0.0 0.1 0:00.41 /usr/counterstorm/bin/worker --no-seatbelts --server-
on-stdin --one-shot --threads --log-stderr=/us
28987 root 16 0 104m 4436 3036 S 0.0 0.1 0:00.43 /usr/counterstorm/bin/worker --no-seatbelts --server-
on-stdin --one-shot --threads --log-stderr=/us
29087 root 15 0 27096 1340 1080 S 0.0 0.0 0:00.00 initlog -c /usr/counterstorm/bin/forensicsd --umask
022 --no-seatbelts --forensics-hdr-cache-patter
29110 root 17 0 71348 3072 2148 S 0.0 0.1 0:28.43 /usr/counterstorm/bin/forensicsd --umask 022 --no-
seatbelts --forensics-hdr-cache-pattern DISABLED
29170 antura 16 0 228m 9720 8024 S 0.0 0.2 0:00.08 postgres: sysd sysd 127.0.0.1 idle
29171 antura 16 0 229m 10m 8700 S 0.0 0.3 0:00.12 postgres: sysd sysd 127.0.0.1 idle
23015 root 18 0 2452 292 228 S 0.0 0.0 0:00.00 /usr/counterstorm/bin/timeout -t 20 -- /usr/counterstorm/
bin/jump.pl --raw --worker-status sysd-dhc
+---------------------------------------------------------------------+
Interface Status:
bond0 Link encap:Ethernet HWaddr 00:E0:81:2F:22:CA
inet6 addr: fe80::200:ff:fe00:0/64 Scope:Link
UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1
RX packets:234821 errors:492 dropped:0 overruns:0 frame:0
TX packets:2759 errors:0 dropped:0 overruns:0 carrier:0
collisions:3 txqueuelen:0
RX bytes:21495264 (20.4 MiB) TX bytes:179242 (175.0 KiB)

eth0 Link encap:Ethernet HWaddr 00:E0:81:2F:22:CA
inet6 addr: fe80::2e0:81ff:fe2f:22ca/64 Scope:Link
UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
RX packets:188634 errors:492 dropped:0 overruns:0 frame:0
TX packets:1380 errors:0 dropped:0 overruns:0 carrier:0
collisions:3 txqueuelen:1000
RX bytes:18516092 (17.6 MiB) TX bytes:89658 (87.5 KiB)
Interrupt:177

eth1 Link encap:Ethernet HWaddr 00:E0:81:2F:22:CA
inet6 addr: fe80::2e0:81ff:fe2f:22ca/64 Scope:Link
UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
RX packets:46187 errors:0 dropped:0 overruns:0 frame:0
TX packets:1379 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2979172 (2.8 MiB) TX bytes:89584 (87.4 KiB)
Interrupt:185

eth2 Link encap:Ethernet HWaddr 00:E0:81:2F:22:95
inet addr:172.16.2.4 Bcast:172.16.3.255 Mask:255.255.252.0
inet6 addr: fe80::2e0:81ff:fe2f:2295/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:67991 errors:0 dropped:0 overruns:0 frame:0
TX packets:53069 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:9869496 (9.4 MiB) TX bytes:9697378 (9.2 MiB)

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
```

Sample Status E-mail

```
RX packets:1256973 errors:0 dropped:0 overruns:0 frame:0
TX packets:1256973 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:282031902 (268.9 MiB) TX bytes:282031902 (268.9 MiB)

sit0 Link encap:IPv6-in-IPv4
NOARP MTU:1480 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

+---------------------------------------------------------------------+
Worker Summary Status:
sysd-dhcp-4_1 -Default- wumps://localhost:19001 RUNNING ws-sd2k4
sysd-dhcp-4_2 -Default- wumps://localhost:19002 RUNNING aw-emf-capture
sysd-dhcp-4_3 -Default- wumps://localhost:19003 RUNNING aw-emf-train
sysd-dhcp-4_4 -Default- wumps://localhost:19004 RUNNING aw-emf-detect
sysd-dhcp-4_5 -Default- wumps://localhost:19005 IDLE
sysd-dhcp-4_6 -Default- wumps://localhost:19006 IDLE
sysd-dhcp-4_7 -Default- wumps://localhost:19007 IDLE
sysd-dhcp-4_8 -Default- wumps://localhost:19008 IDLE
+---------------------------------------------------------------------+
Job Summary Status:
aw-emf-capture [Auto-Restart] [Priority 0] sysd-dhcp-4_2 RUNNING (From Worker) 2006-03-07 15:01:59 EST
aw-emf-detect [Auto-Restart] [Priority 0] sysd-dhcp-4_4 RUNNING (From Worker) 2006-03-07 15:02:08 EST
aw-emf-train [Auto-Restart] [Priority 0] sysd-dhcp-4_3 RUNNING (From Worker) 2006-03-07 15:02:03 EST
ws-sd2k4 [Auto-Restart] [Priority 0] sysd-dhcp-4_1 RUNNING (From Worker) 2006-03-07 15:01:52 EST
+---------------------------------------------------------------------+
Status of sysd-dhcp-4_1:
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/ws-sd2k4
Elapsed real time 1:05:43.23
Worker PID 28885
CPU time (this job) 0:02:36.25
CPU time (total) 0:02:36.36
Memory size 226062336
Memory heap size 8081920
Memory resident size 36073472
Bytes in 0
Bytes out 0
Events in 928
Events out 928
Alerts 0
Latest Input
pcap:bond0;promisc;snaplen=92?(ip%20and%20(tcp%20or%20udp%20or%20icmp)%20and%20(((ip%5b12%3a4%5d%20%3e%
3d%20167968768%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b12%3a4%5d%20%3c%3d%201680998
39)%20or%20(ip%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20((ip%5b16%3a4%5d%20%3e%3d%20167968768%20and%2
0ip%5b16%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4%5d%20%3c%3d%20168099839)%20or%20(ip%5b16%3a
4%5d%20%3e%3d%20169148416))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%20and%20
ip%5b8%5d%21%3d128%20and%20ip%5b8%5d%21%3d1))%20or%20(vlan%20and%20(ip%20and%20(tcp%20or%20udp%20or%20i
cmp)%20and%20(((ip%5b12%3a4%5d%20%3e%3d%20167968768%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)%20and%
20((ip%5b12%3a4%5d%20%3c%3d%20168099839)%20or%20(ip%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20((ip%5b1
6%3a4%5d%20%3e%3d%20167968768%20and%20ip%5b16%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4%5d%20%
3c%3d%20168099839)%20or%20(ip!
%5b16%3a4%5d%20%3e%3d%20169148416))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%
20and%20ip%5b8%5d%21%3d128%20and%20ip%5b8%5d%21%3d1)))
Wire bits 56509392
Recent Connection Pool Size 52101
Recent Source Pool Size 226
Input Thread Queue Length 0
Output Thread Queue Length 0
Number of targets being tracked 52101
Number of packets captured 52101
Number of packets dropped 0
```

```
Format Input Thread Queue Length 1
Sensor detection status Running
Number of active SD keys in asymmetric holddown 0
+---------------------------------------------------------------------+
Status of sysd-dhcp-4_2:
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/aw-emf-capture
Elapsed real time 1:05:48.49
Worker PID 28899
CPU time (this job) 0:00:18.41
CPU time (total) 0:00:18.52
Memory size 226947072
Memory heap size 7922176
Memory resident size 25739264
Bytes in 0
Bytes out 0
Events in 36
Events out 36
Alerts 0
Latest Input
pcap:bond0;promisc;snaplen=92?(ip%20and%20tcp%20port%2025%20and%20(((ip%5b12%3a4%5d%20%3e%3d%2016796876
8%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b12%3a4%5d%20%3c%3d%20168099839)%20or%20(i
p%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20((ip%5b16%3a4%5d%20%3e%3d%20167968768%20and%20ip%5b16%3a4%
5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4%5d%20%3c%3d%20168099839)%20or%20(ip%5b16%3a4%5d%20%3e%3d
%20169148416))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%20and%20ip%5b8%5d%21%
3d128%20and%20ip%5b8%5d%21%3d1))%20or%20(vlan%20and%20(ip%20and%20tcp%20port%2025%20and%20(((ip%5b12%3a
4%5d%20%3e%3d%20167968768%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b12%3a4%5d%20%3c%3
d%20168099839)%20or%20(ip%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20((ip%5b16%3a4%5d%20%3e%3d%20167968
768%20and%20ip%5b16%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4%5d%20%3c%3d%20168099839)%20or%20
(ip%5b16%3a4%5d%20%3e%3d%2016!
9148416))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%20and%20ip%5b8%5d%21%3d128
%20and%20ip%5b8%5d%21%3d1)))
Wire bits 1312000
Recent Connection Pool Size 2000
Input Thread Queue Length 0
Output Thread Queue Length 0
Number of packets captured 2002
Number of packets dropped 0
Format Input Thread Queue Length 1
Number of sub-accumulator events 2000
Number of tracked accumulator keys 1
+---------------------------------------------------------------------+
Status of sysd-dhcp-4_3:
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/aw-emf-train
Elapsed real time 1:05:43.23
Worker PID 28913
CPU time (this job) 0:00:00.49
CPU time (total) 0:00:00.60
Memory size 145121280
Memory heap size 1917440
Memory resident size 7049216
Bytes in 19116
Bytes out 0
Events in 36
Events out 0
Alerts 0
Latest event 2006-03-07T21:55:51Z
Latest Input pipe:/usr/counterstorm/var/fifo/aw-emf-train-pipe
Input Thread Queue Length 0
Format Input Thread Queue Length 1
+---------------------------------------------------------------------+
Status of sysd-dhcp-4_4:
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/aw-emf-detect
Elapsed real time 1:05:43.24
Worker PID 28927
```

Sample Status E-mail

```
CPU time (this job) 0:00:00.56
CPU time (total) 0:00:00.66
Memory size 146612224
Memory heap size 2359808
Memory resident size 7340032
Bytes in 19116
Bytes out 0
Events in 36
Events out 0
Alerts 0
Latest event 2006-03-07T21:55:51Z
Latest Input pipe:/usr/counterstorm/var/fifo/aw-emf-detect-pipe
Input Thread Queue Length 0
Format Input Thread Queue Length 1
+--------------------------------------------------------------------+
Status of sysd-dhcp-4_5:
Status: IDLE
+--------------------------------------------------------------------+
Status of sysd-dhcp-4_6:
Status: IDLE
+--------------------------------------------------------------------+
Status of sysd-dhcp-4_7:
Status: IDLE
+--------------------------------------------------------------------+
Status of sysd-dhcp-4_8:
Status: IDLE
+--------------------------------------------------------------------+
Antura System Process Status:
postmaster (pid 23529 29180 29171 29170 13176 12668 12665 8901 4731 4730 4729) is running...
PostgreSQL is working.

Status of CounterStorm-1 arpd: arpd pids present
CounterStorm-1 arpd is running

Status of CounterStorm-1 forensicsd:
forensicsd pids present
CounterStorm-1 forensicsd is running

Status of CounterStorm-1 poisonarpd:
poisonarpd pids present
CounterStorm-1 poisonarpd is running
alarm="1" response="59" src_ip="10.21.2.24" uses="107"
alarm="2" response="59" src_ip="10.21.2.25" uses="0"
alarm="3" response="59" src_ip="10.21.2.26" uses="0"
alarm="15" response="59" src_ip="10.21.2.31" uses="0"
alarm="16" response="59" src_ip="10.21.2.32" uses="0"
alarm="17" response="59" src_ip="10.21.2.32" uses="0"
alarm="18" response="59" src_ip="10.21.2.33" uses="0"
alarm="19" response="59" src_ip="10.21.2.34" uses="0"
alarm="20" response="59" src_ip="10.21.2.35" uses="0"
alarm="21" response="59" src_ip="10.21.2.36" uses="0"
alarm="57" response="59" src_ip="10.21.2.71" uses="0"
alarm="58" response="59" src_ip="10.21.2.72" uses="0"
alarm="59" response="59" src_ip="10.21.2.72" uses="0"
alarm="60" response="59" src_ip="10.21.2.73" uses="0"
alarm="61" response="59" src_ip="10.21.2.74" uses="0"
alarm="62" response="59" src_ip="10.21.2.75" uses="0"
alarm="63" response="59" src_ip="10.21.2.76" uses="0"
alarm="71" response="59" src_ip="10.21.2.81" uses="0"
alarm="72" response="59" src_ip="10.21.2.82" uses="0"
alarm="73" response="59" src_ip="10.21.2.82" uses="0"
alarm="74" response="59" src_ip="10.21.2.83" uses="0"
alarm="75" response="59" src_ip="10.21.2.84" uses="0"
alarm="76" response="59" src_ip="10.21.2.85" uses="0"
```

```
alarm="77" response="59" src_ip="10.21.2.86" uses="0"
alarm="85" response="59" src_ip="10.21.2.91" uses="0"
alarm="86" response="59" src_ip="10.21.2.92" uses="0"
alarm="94" response="59" src_ip="10.21.4.11" uses="0"
alarm="95" response="59" src_ip="10.21.4.12" uses="0"
alarm="96" response="59" src_ip="10.21.4.12" uses="0"
alarm="97" response="59" src_ip="10.21.4.13" uses="0"
alarm="98" response="59" src_ip="10.21.4.14" uses="0"
alarm="99" response="59" src_ip="10.21.4.15" uses="0"
alarm="100" response="59" src_ip="10.21.4.16" uses="0"
alarm="112" response="59" src_ip="10.21.4.21" uses="0"
alarm="113" response="59" src_ip="10.21.4.22" uses="0"
alarm="114" response="59" src_ip="10.21.4.22" uses="0"
alarm="115" response="59" src_ip="10.21.4.23" uses="0"
alarm="116" response="59" src_ip="10.21.4.24" uses="0"
alarm="117" response="59" src_ip="10.21.4.25" uses="0"
alarm="118" response="59" src_ip="10.21.4.26" uses="0"
alarm="130" response="59" src_ip="10.21.4.31" uses="0"
alarm="131" response="59" src_ip="10.21.4.32" uses="0"
alarm="132" response="59" src_ip="10.21.4.32" uses="0"
alarm="133" response="59" src_ip="10.21.4.33" uses="0"
alarm="134" response="59" src_ip="10.21.4.34" uses="0"
alarm="135" response="59" src_ip="10.21.4.35" uses="0"
alarm="136" response="59" src_ip="10.21.4.36" uses="0"
alarm="148" response="59" src_ip="10.21.4.41" uses="0"
alarm="149" response="59" src_ip="10.21.4.42" uses="0"
alarm="150" response="59" src_ip="10.21.4.42" uses="0"
alarm="151" response="59" src_ip="10.21.4.43" uses="0"
alarm="152" response="59" src_ip="10.21.4.44" uses="0"
alarm="153" response="59" src_ip="10.21.4.45" uses="0"
alarm="154" response="59" src_ip="10.21.4.46" uses="0"
alarm="166" response="59" src_ip="10.21.4.51" uses="0"
alarm="167" response="59" src_ip="10.21.4.52" uses="0"
alarm="168" response="59" src_ip="10.21.4.52" uses="0"
alarm="169" response="59" src_ip="10.21.4.53" uses="0"
alarm="170" response="59" src_ip="10.21.4.54" uses="0"
alarm="171" response="59" src_ip="10.21.4.55" uses="0"
alarm="172" response="59" src_ip="10.21.4.56" uses="0"
alarm="184" response="59" src_ip="10.21.4.61" uses="0"
alarm="185" response="59" src_ip="10.21.4.62" uses="0"
alarm="186" response="59" src_ip="10.21.4.63" uses="0"
alarm="187" response="59" src_ip="10.21.4.64" uses="0"
alarm="188" response="59" src_ip="10.21.4.65" uses="0"
alarm="189" response="59" src_ip="10.21.4.66" uses="0"
alarm="200" response="59" src_ip="10.21.4.71" uses="0"
alarm="201" response="59" src_ip="10.21.4.72" uses="0"
alarm="202" response="59" src_ip="10.21.4.72" uses="0"
alarm="203" response="59" src_ip="10.21.4.73" uses="0"
alarm="204" response="59" src_ip="10.21.4.74" uses="0"
alarm="205" response="60" src_ip="10.21.4.75" uses="0"
alarm="206" response="60" src_ip="10.21.4.76" uses="0"
alarm="218" response="60" src_ip="10.21.4.81" uses="0"
alarm="219" response="60" src_ip="10.21.4.82" uses="0"
alarm="220" response="60" src_ip="10.21.4.82" uses="0"
alarm="221" response="60" src_ip="10.21.4.83" uses="0"

Status of CounterStorm-1 rstd:
rstd pids present
CounterStorm-1 rstd is running
alarm="1" response="57" src_ip="10.21.2.24" uses="0"
alarm="2" response="57" src_ip="10.21.2.25" uses="0"
alarm="3" response="57" src_ip="10.21.2.26" uses="0"
alarm="15" response="57" src_ip="10.21.2.31" uses="0"
alarm="16" response="57" src_ip="10.21.2.32" uses="0"
```

Sample Status E-mail

```
    alarm="17" response="57" src_ip="10.21.2.32" uses="0"
    alarm="18" response="57" src_ip="10.21.2.33" uses="0"
    alarm="19" response="57" src_ip="10.21.2.34" uses="0"
    alarm="20" response="57" src_ip="10.21.2.35" uses="0"
    alarm="21" response="57" src_ip="10.21.2.36" uses="0"
    alarm="57" response="57" src_ip="10.21.2.71" uses="0"
    alarm="58" response="57" src_ip="10.21.2.72" uses="0"
    alarm="59" response="57" src_ip="10.21.2.72" uses="0"
    alarm="60" response="57" src_ip="10.21.2.73" uses="0"
    alarm="61" response="57" src_ip="10.21.2.74" uses="0"
    alarm="62" response="57" src_ip="10.21.2.75" uses="0"
    alarm="63" response="57" src_ip="10.21.2.76" uses="0"
    alarm="71" response="57" src_ip="10.21.2.81" uses="0"
    alarm="72" response="57" src_ip="10.21.2.82" uses="0"
    alarm="73" response="57" src_ip="10.21.2.82" uses="0"
    alarm="74" response="57" src_ip="10.21.2.83" uses="0"
    alarm="75" response="57" src_ip="10.21.2.84" uses="0"
    alarm="76" response="57" src_ip="10.21.2.85" uses="0"
    alarm="77" response="57" src_ip="10.21.2.86" uses="0"
    alarm="85" response="57" src_ip="10.21.2.91" uses="0"
    alarm="86" response="57" src_ip="10.21.2.92" uses="0"
    alarm="94" response="57" src_ip="10.21.4.11" uses="0"
    alarm="95" response="57" src_ip="10.21.4.12" uses="0"
    alarm="96" response="57" src_ip="10.21.4.12" uses="0"
    alarm="97" response="57" src_ip="10.21.4.13" uses="0"
    alarm="98" response="57" src_ip="10.21.4.14" uses="0"
    alarm="99" response="57" src_ip="10.21.4.15" uses="0"
    alarm="100" response="57" src_ip="10.21.4.16" uses="0"
    alarm="112" response="57" src_ip="10.21.4.21" uses="0"
    alarm="113" response="57" src_ip="10.21.4.22" uses="0"
    alarm="114" response="57" src_ip="10.21.4.22" uses="0"
    alarm="115" response="57" src_ip="10.21.4.23" uses="0"
    alarm="116" response="57" src_ip="10.21.4.24" uses="0"
    alarm="117" response="57" src_ip="10.21.4.25" uses="0"
    alarm="118" response="57" src_ip="10.21.4.26" uses="0"
    alarm="130" response="57" src_ip="10.21.4.31" uses="0"
    alarm="131" response="57" src_ip="10.21.4.32" uses="0"
    alarm="132" response="57" src_ip="10.21.4.32" uses="0"
    alarm="133" response="57" src_ip="10.21.4.33" uses="0"
    alarm="134" response="57" src_ip="10.21.4.34" uses="0"
    alarm="135" response="57" src_ip="10.21.4.35" uses="0"
    alarm="136" response="57" src_ip="10.21.4.36" uses="0"
    alarm="148" response="57" src_ip="10.21.4.41" uses="0"
    alarm="149" response="57" src_ip="10.21.4.42" uses="0"
    alarm="150" response="57" src_ip="10.21.4.42" uses="0"
    alarm="151" response="57" src_ip="10.21.4.43" uses="0"
    alarm="152" response="57" src_ip="10.21.4.44" uses="0"
    alarm="153" response="57" src_ip="10.21.4.45" uses="0"
    alarm="154" response="57" src_ip="10.21.4.46" uses="0"
    alarm="166" response="57" src_ip="10.21.4.51" uses="0"
    alarm="167" response="57" src_ip="10.21.4.52" uses="0"
    alarm="168" response="57" src_ip="10.21.4.52" uses="0"
    alarm="169" response="57" src_ip="10.21.4.53" uses="0"
    alarm="170" response="57" src_ip="10.21.4.54" uses="0"
    alarm="171" response="57" src_ip="10.21.4.55" uses="0"
    alarm="172" response="57" src_ip="10.21.4.56" uses="0"
    alarm="184" response="57" src_ip="10.21.4.61" uses="0"
    alarm="185" response="57" src_ip="10.21.4.62" uses="0"
    alarm="186" response="57" src_ip="10.21.4.63" uses="0"
    alarm="187" response="57" src_ip="10.21.4.64" uses="0"
    alarm="188" response="57" src_ip="10.21.4.65" uses="0"
    alarm="189" response="57" src_ip="10.21.4.66" uses="0"
    alarm="200" response="57" src_ip="10.21.4.71" uses="0"
    alarm="201" response="57" src_ip="10.21.4.72" uses="0"
```

```
alarm="202" response="57" src_ip="10.21.4.72" uses="0"
alarm="203" response="57" src_ip="10.21.4.73" uses="0"
alarm="204" response="57" src_ip="10.21.4.74" uses="0"
alarm="205" response="58" src_ip="10.21.4.75" uses="0"
alarm="206" response="58" src_ip="10.21.4.76" uses="0"
alarm="218" response="58" src_ip="10.21.4.81" uses="0"
alarm="219" response="58" src_ip="10.21.4.82" uses="0"
alarm="220" response="58" src_ip="10.21.4.82" uses="0"
alarm="221" response="58" src_ip="10.21.4.83" uses="0"

Status of CounterStorm-1 Worker 1:
UMP/1.0 200 Your status, sir.
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/ws-sd2k4
Content-Type: text/plain
Content-Length: 2336

<statistics generated="2006-03-07T22:05:08Z">
<param name="Elapsed real time">1:05:48.98</param>
<param name="Worker PID">28885</param>
<param name="CPU time (this job)">0:02:36.50</param>
<param name="CPU time (total)">0:02:36.61</param>
<param name="Memory size">226062336</param>
<param name="Memory heap size">8081920</param>
<param name="Memory resident size">36081664</param>
<param name="Bytes in">0</param>
<param name="Bytes out">0</param>
<param name="Events in">930</param>
<param name="Events out">930</param>
<param name="Alerts">0</param>
<param name="Latest
Input">pcap:bond0;promisc;snaplen=92?(ip%20and%20(tcp%20or%20udp%20or%20icmp)%20and%20(((ip%5b12%3a4%5d
%20%3e%3d%20167968768%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b12%3a4%5d%20%3c%3d%20
168099839)%20or%20(ip%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20((ip%5b16%3a4%5d%20%3e%3d%20167968768%
20and%20ip%5b16%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4%5d%20%3c%3d%20168099839)%20or%20(ip%
5b16%3a4%5d%20%3e%3d%20169148416))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%2
0and%20ip%5b8%5d%21%3d128%20and%20ip%5b8%5d%21%3d1))%20or%20(vlan%20and%20(ip%20and%20(tcp%20or%20udp%2
0or%20icmp)%20and%20(((ip%5b12%3a4%5d%20%3e%3d%20167968768%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)
%20and%20((ip%5b12%3a4%5d%20%3c%3d%20168099839)%20or%20(ip%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20(
(ip%5b16%3a4%5d%20%3e%3d%20167968768%20and%20ip%5b16%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4
%5d%20%3c%3d%20168099839)%20or%20(ip%5b16!
%3a4%5d%20%3e%3d%20169148416))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%20and
%20ip%5b8%5d%21%3d128%20and%20ip%5b8%5d%21%3d1)))</param>
<param name="Wire bits">56540880</param>
<param name="Recent Connection Pool Size">52149</param>
<param name="Recent Source Pool Size">226</param>
<param name="Input Thread Queue Length">0</param>
<param name="Output Thread Queue Length">0</param>
<param name="Number of targets being tracked">52149</param>
<param name="Number of packets captured">52149</param>
<param name="Number of packets dropped">0</param>
<param name="Format Input Thread Queue Length">1</param>
<param name="Sensor detection status">Running</param>
<param name="Number of active SD keys in asymmetric holddown">0</param>
</statistics>

Status of CounterStorm-1 Worker 2:
UMP/1.0 200 Your status, sir.
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/aw-emf-capture
Content-Type: text/plain
Content-Length: 2186

<statistics generated="2006-03-07T22:05:08Z">
<param name="Elapsed real time">1:05:53.36</param>
<param name="Worker PID">28899</param>
```

Sample Status E-mail

```
<param name="CPU time (this job)">0:00:18.42</param>
<param name="CPU time (total)">0:00:18.53</param>
<param name="Memory size">226947072</param>
<param name="Memory heap size">7922176</param>
<param name="Memory resident size">25755648</param>
<param name="Bytes in">0</param>
<param name="Bytes out">0</param>
<param name="Events in">36</param>
<param name="Events out">36</param>
<param name="Alerts">0</param>
<param name="Latest
Input">pcap:bond0;promisc;snaplen=92?(ip%20and%20tcp%20port%2025%20and%20(((ip%5b12%3a4%5d%20%3e%3d%201
67968768%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b12%3a4%5d%20%3c%3d%20168099839)%20
or%20(ip%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20((ip%5b16%3a4%5d%20%3e%3d%20167968768%20and%20ip%5b
16%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4%5d%20%3c%3d%20168099839)%20or%20(ip%5b16%3a4%5d%2
0%3e%3d%20169148416))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%20and%20ip%5b8
%5d%21%3d128%20and%20ip%5b8%5d%21%3d1))%20or%20(vlan%20and%20(ip%20and%20tcp%20port%2025%20and%20(((ip%
5b12%3a4%5d%20%3e%3d%20167968768%20and%20ip%5b12%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b12%3a4%5d%
20%3c%3d%20168099839)%20or%20(ip%5b12%3a4%5d%20%3e%3d%20169148416)))%20or%20((ip%5b16%3a4%5d%20%3e%3d%2
0167968768%20and%20ip%5b16%3a4%5d%20%3c%3d%20169279487)%20and%20((ip%5b16%3a4%5d%20%3c%3d%20168099839)%
20or%20(ip%5b16%3a4%5d%20%3e%3d%201691484!
16))))%20and%20not%20(net%20169.254.0.0%2f16%20and%20ip%5b8%5d%21%3d255%20and%20ip%5b8%5d%21%3d128%20an
d%20ip%5b8%5d%21%3d1)))</param>
<param name="Wire bits">1312000</param>
<param name="Recent Connection Pool Size">2000</param>
<param name="Input Thread Queue Length">0</param>
<param name="Output Thread Queue Length">0</param>
<param name="Number of packets captured">2002</param>
<param name="Number of packets dropped">0</param>
<param name="Format Input Thread Queue Length">1</param>
<param name="Number of sub-accumulator events">2000</param>
<param name="Number of tracked accumulator keys">1</param>
</statistics>

Status of CounterStorm-1 Worker 3:
UMP/1.0 200 Your status, sir.
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/aw-emf-train
Content-Type: text/plain
Content-Length: 831

<statistics generated="2006-03-07T22:05:08Z">
<param name="Elapsed real time">1:05:49.28</param>
<param name="Worker PID">28913</param>
<param name="CPU time (this job)">0:00:00.51</param>
<param name="CPU time (total)">0:00:00.62</param>
<param name="Memory size">145121280</param>
<param name="Memory heap size">1917440</param>
<param name="Memory resident size">7049216</param>
<param name="Bytes in">19116</param>
<param name="Bytes out">0</param>
<param name="Events in">36</param>
<param name="Events out">0</param>
<param name="Alerts">0</param>
<param name="Latest event">2006-03-07T21:55:51Z</param>
<param name="Latest Input">pipe:/usr/counterstorm/var/fifo/aw-emf-train-pipe</param>
<param name="Input Thread Queue Length">0</param>
<param name="Format Input Thread Queue Length">1</param>
</statistics>

Status of CounterStorm-1 Worker 4:
UMP/1.0 200 Your status, sir.
Status: RUNNING:postgres://sysd:XEmvzUjl@localhost:5432/sysd/antura/file/jobs/aw-emf-detect
Content-Type: text/plain
Content-Length: 832
```

```
<statistics generated="2006-03-07T22:05:08Z">
<param name="Elapsed real time">1:05:49.45</param>
<param name="Worker PID">28927</param>
<param name="CPU time (this job)">0:00:00.57</param>
<param name="CPU time (total)">0:00:00.68</param>
<param name="Memory size">146612224</param>
<param name="Memory heap size">2359808</param>
<param name="Memory resident size">7340032</param>
<param name="Bytes in">19116</param>
<param name="Bytes out">0</param>
<param name="Events in">36</param>
<param name="Events out">0</param>
<param name="Alerts">0</param>
<param name="Latest event">2006-03-07T21:55:51Z</param>
<param name="Latest Input">pipe:/usr/counterstorm/var/fifo/aw-emf-detect-pipe</param>
<param name="Input Thread Queue Length">0</param>
<param name="Format Input Thread Queue Length">1</param>
</statistics>

Status of CounterStorm-1 Worker 5:
UMP/1.0 200 Your status, sir.
Status: IDLE


Status of CounterStorm-1 Worker 6:
UMP/1.0 200 Your status, sir.
Status: IDLE


Status of CounterStorm-1 Worker 7:
UMP/1.0 200 Your status, sir.
Status: IDLE


Status of CounterStorm-1 Worker 8:
UMP/1.0 200 Your status, sir.
Status: IDLE


Status of CounterStorm-1 alarmer:
alarmer pids present
CounterStorm-1 alarmer is running
expires | response | ip | proto | ports
----------+-------------------+------------+-------+---------
22:21:49 | ARP Host Blocking | 10.21.2.24 | 17 | 22
22:21:50 | TCP Host Blocking | 10.21.2.24 | 17 | 22
22:22:04 | TCP Host Blocking | 10.21.2.25 | 6 | 22
22:22:04 | ARP Host Blocking | 10.21.2.25 | 6 | 22
22:22:18 | TCP Host Blocking | 10.21.2.26 | 17 | 22
22:22:19 | ARP Host Blocking | 10.21.2.26 | 17 | 22
22:25:52 | TCP Host Blocking | 10.21.2.31 | 6 | 23
22:25:53 | ARP Host Blocking | 10.21.2.31 | 6 | 23
22:26:21 | TCP Host Blocking | 10.21.2.32 | 17 | 23,110
22:26:22 | ARP Host Blocking | 10.21.2.32 | 17 | 23,110
22:26:34 | ARP Host Blocking | 10.21.2.33 | 6 | 23
22:26:34 | TCP Host Blocking | 10.21.2.33 | 6 | 23
22:26:49 | ARP Host Blocking | 10.21.2.34 | 17 | 23
22:26:49 | TCP Host Blocking | 10.21.2.34 | 17 | 23
22:27:03 | ARP Host Blocking | 10.21.2.35 | 6 | 23
22:27:04 | TCP Host Blocking | 10.21.2.35 | 6 | 23
22:29:29 | ARP Host Blocking | 10.21.2.36 | 17 | 23
22:29:30 | TCP Host Blocking | 10.21.2.36 | 17 | 23
22:45:06 | TCP Host Blocking | 10.21.2.71 | 6 | 143
```

Sample Status E-mail

```
    22:45:06 | ARP Host Blocking | 10.21.2.71 | 6 | 143
    22:45:35 | ARP Host Blocking | 10.21.2.72 | 17 | 143,110
    22:45:35 | TCP Host Blocking | 10.21.2.72 | 17 | 143,110
    22:45:49 | TCP Host Blocking | 10.21.2.73 | 6 | 143
    22:45:49 | ARP Host Blocking | 10.21.2.73 | 6 | 143
    22:46:04 | TCP Host Blocking | 10.21.2.74 | 17 | 143
    22:46:04 | ARP Host Blocking | 10.21.2.74 | 17 | 143
    22:46:16 | ARP Host Blocking | 10.21.2.75 | 6 | 143
    22:46:16 | TCP Host Blocking | 10.21.2.75 | 6 | 143
    22:46:31 | ARP Host Blocking | 10.21.2.76 | 17 | 143
    22:46:31 | TCP Host Blocking | 10.21.2.76 | 17 | 143
    22:49:24 | TCP Host Blocking | 10.21.2.81 | 6 | 161
    22:49:24 | ARP Host Blocking | 10.21.2.81 | 6 | 161
    22:49:50 | ARP Host Blocking | 10.21.2.82 | 17 | 161,110
    22:49:51 | TCP Host Blocking | 10.21.2.82 | 17 | 161,110
    22:50:04 | ARP Host Blocking | 10.21.2.83 | 6 | 161
    22:50:04 | TCP Host Blocking | 10.21.2.83 | 6 | 161
    22:50:18 | TCP Host Blocking | 10.21.2.84 | 17 | 161
    22:50:18 | ARP Host Blocking | 10.21.2.84 | 17 | 161
    22:50:32 | ARP Host Blocking | 10.21.2.85 | 6 | 161
    22:50:32 | TCP Host Blocking | 10.21.2.85 | 6 | 161
    22:50:48 | ARP Host Blocking | 10.21.2.86 | 17 | 161
    22:50:48 | TCP Host Blocking | 10.21.2.86 | 17 | 161
    22:53:37 | ARP Host Blocking | 10.21.2.91 | 6 | 3306
    22:53:37 | TCP Host Blocking | 10.21.2.91 | 6 | 3306
    22:53:52 | TCP Host Blocking | 10.21.2.92 | 17 | 3306
    22:53:53 | ARP Host Blocking | 10.21.2.92 | 17 | 3306
    23:01:18 | TCP Host Blocking | 10.21.4.11 | 6 | 21
    23:01:19 | ARP Host Blocking | 10.21.4.11 | 6 | 21
    23:01:52 | TCP Host Blocking | 10.21.4.12 | 17 | 21,110
    23:01:53 | ARP Host Blocking | 10.21.4.12 | 17 | 21,110
    23:02:10 | ARP Host Blocking | 10.21.4.13 | 6 | 21
    23:02:10 | TCP Host Blocking | 10.21.4.13 | 6 | 21
    23:02:26 | ARP Host Blocking | 10.21.4.14 | 17 | 21
    23:02:26 | TCP Host Blocking | 10.21.4.14 | 17 | 21
    23:02:43 | TCP Host Blocking | 10.21.4.15 | 6 | 21
    23:02:43 | ARP Host Blocking | 10.21.4.15 | 6 | 21
    23:03:01 | ARP Host Blocking | 10.21.4.16 | 17 | 21
    23:03:02 | TCP Host Blocking | 10.21.4.16 | 17 | 21
    23:06:26 | ARP Host Blocking | 10.21.4.21 | 6 | 22
    23:06:27 | TCP Host Blocking | 10.21.4.21 | 6 | 22
    23:06:58 | TCP Host Blocking | 10.21.4.22 | 17 | 22,110
    23:06:58 | ARP Host Blocking | 10.21.4.22 | 17 | 22,110
    23:07:15 | ARP Host Blocking | 10.21.4.23 | 6 | 22
    23:07:15 | TCP Host Blocking | 10.21.4.23 | 6 | 22
    23:07:32 | TCP Host Blocking | 10.21.4.24 | 17 | 22
    23:07:33 | ARP Host Blocking | 10.21.4.24 | 17 | 22
    23:07:50 | TCP Host Blocking | 10.21.4.25 | 6 | 22
    23:07:50 | ARP Host Blocking | 10.21.4.25 | 6 | 22
    23:08:07 | ARP Host Blocking | 10.21.4.26 | 17 | 22
    23:08:07 | TCP Host Blocking | 10.21.4.26 | 17 | 22
    23:11:30 | TCP Host Blocking | 10.21.4.31 | 6 | 23
    23:11:30 | ARP Host Blocking | 10.21.4.31 | 6 | 23
    23:12:04 | ARP Host Blocking | 10.21.4.32 | 17 | 23,110
    23:12:04 | TCP Host Blocking | 10.21.4.32 | 17 | 23,110
    23:12:20 | ARP Host Blocking | 10.21.4.33 | 6 | 23
    23:12:20 | TCP Host Blocking | 10.21.4.33 | 6 | 23
    23:12:38 | ARP Host Blocking | 10.21.4.34 | 17 | 23
    23:12:38 | TCP Host Blocking | 10.21.4.34 | 17 | 23
    23:12:54 | TCP Host Blocking | 10.21.4.35 | 6 | 23
    23:12:54 | ARP Host Blocking | 10.21.4.35 | 6 | 23
    23:13:12 | TCP Host Blocking | 10.21.4.36 | 17 | 23
    23:13:13 | ARP Host Blocking | 10.21.4.36 | 17 | 23
    23:16:35 | TCP Host Blocking | 10.21.4.41 | 6 | 25
```

```
23:16:35 | ARP Host Blocking | 10.21.4.41 | 6 | 25
23:17:09 | TCP Host Blocking | 10.21.4.42 | 17 | 25,110
23:17:10 | ARP Host Blocking | 10.21.4.42 | 17 | 25,110
23:17:27 | ARP Host Blocking | 10.21.4.43 | 6 | 25
23:17:28 | TCP Host Blocking | 10.21.4.43 | 6 | 25
23:17:43 | ARP Host Blocking | 10.21.4.44 | 17 | 25
23:17:44 | TCP Host Blocking | 10.21.4.44 | 17 | 25
23:18:01 | ARP Host Blocking | 10.21.4.45 | 6 | 25
23:18:02 | TCP Host Blocking | 10.21.4.45 | 6 | 25
23:18:17 | TCP Host Blocking | 10.21.4.46 | 17 | 25
23:18:17 | ARP Host Blocking | 10.21.4.46 | 17 | 25
23:21:44 | ARP Host Blocking | 10.21.4.51 | 6 | 53
23:21:44 | TCP Host Blocking | 10.21.4.51 | 6 | 53
23:22:16 | ARP Host Blocking | 10.21.4.52 | 17 | 53,110
23:22:16 | TCP Host Blocking | 10.21.4.52 | 17 | 53,110
23:22:32 | TCP Host Blocking | 10.21.4.53 | 6 | 53
23:22:32 | ARP Host Blocking | 10.21.4.53 | 6 | 53
23:22:49 | ARP Host Blocking | 10.21.4.54 | 17 | 53
23:22:50 | TCP Host Blocking | 10.21.4.54 | 17 | 53
23:23:06 | TCP Host Blocking | 10.21.4.55 | 6 | 53
23:23:07 | ARP Host Blocking | 10.21.4.55 | 6 | 53
23:23:24 | ARP Host Blocking | 10.21.4.56 | 17 | 53
23:23:24 | TCP Host Blocking | 10.21.4.56 | 17 | 53
23:26:47 | TCP Host Blocking | 10.21.4.61 | 6 | 110
23:26:48 | ARP Host Blocking | 10.21.4.61 | 6 | 110
23:27:05 | TCP Host Blocking | 10.21.4.62 | 17 | 110
23:27:05 | ARP Host Blocking | 10.21.4.62 | 17 | 110
23:27:37 | ARP Host Blocking | 10.21.4.63 | 6 | 110
23:27:38 | TCP Host Blocking | 10.21.4.63 | 6 | 110
23:27:56 | TCP Host Blocking | 10.21.4.64 | 17 | 110
23:27:56 | ARP Host Blocking | 10.21.4.64 | 17 | 110
23:28:11 | ARP Host Blocking | 10.21.4.65 | 6 | 110
23:28:12 | TCP Host Blocking | 10.21.4.65 | 6 | 110
23:28:30 | ARP Host Blocking | 10.21.4.66 | 17 | 110
23:28:30 | TCP Host Blocking | 10.21.4.66 | 17 | 110
23:31:53 | ARP Host Blocking | 10.21.4.71 | 6 | 143
23:31:53 | TCP Host Blocking | 10.21.4.71 | 6 | 143
23:32:27 | TCP Host Blocking | 10.21.4.72 | 17 | 143,110
23:32:27 | ARP Host Blocking | 10.21.4.72 | 17 | 143,110
23:32:44 | TCP Host Blocking | 10.21.4.73 | 6 | 143
23:32:44 | ARP Host Blocking | 10.21.4.73 | 6 | 143
23:33:00 | ARP Host Blocking | 10.21.4.74 | 17 | 143
23:33:01 | TCP Host Blocking | 10.21.4.74 | 17 | 143
23:33:17 | ARP Host Blocking | 10.21.4.75 | 6 | 143
23:33:18 | TCP Host Blocking | 10.21.4.75 | 6 | 143
23:33:35 | TCP Host Blocking | 10.21.4.76 | 17 | 143
23:33:35 | ARP Host Blocking | 10.21.4.76 | 17 | 143
23:37:00 | TCP Host Blocking | 10.21.4.81 | 6 | 161
23:37:01 | ARP Host Blocking | 10.21.4.81 | 6 | 161
23:37:33 | TCP Host Blocking | 10.21.4.82 | 17 | 161,110
23:37:33 | ARP Host Blocking | 10.21.4.82 | 17 | 161,110
23:37:48 | ARP Host Blocking | 10.21.4.83 | 6 | 161
23:37:49 | TCP Host Blocking | 10.21.4.83 | 6 | 161

Status of CounterStorm-1 batcher:
-Default- [none]
Save [none]
sysd-dhcp-4_1 -Default- wumps://localhost:19001 RUNNING ws-sd2k4
sysd-dhcp-4_2 -Default- wumps://localhost:19002 RUNNING aw-emf-capture
sysd-dhcp-4_3 -Default- wumps://localhost:19003 RUNNING aw-emf-train
sysd-dhcp-4_4 -Default- wumps://localhost:19004 RUNNING aw-emf-detect
sysd-dhcp-4_5 -Default- wumps://localhost:19005 IDLE
sysd-dhcp-4_6 -Default- wumps://localhost:19006 IDLE
sysd-dhcp-4_7 -Default- wumps://localhost:19007 IDLE
```

Sample Status E-mail

```
sysd-dhcp-4_8 -Default- wumps://localhost:19008 IDLE
Temp [none]
Trash [none]
CounterStorm-1 batcher is running
dbmirror.pl -m manager-to-sensor is running
dbmirror.pl -m sensor-to-manager is running
+--------------------------------------------------------------------+
Database Summary:
stat | int_value | real_value | time
------+-----------+------------+------
(0 rows)

+--------------------------------------------------------------------+
Rows in worm-sd:
1168 (last was 0 for an increase of 1168)
+--------------------------------------------------------------------+
Rows in aw-upad-emf:
0 (last was 0 for an increase of 0)
+--------------------------------------------------------------------+
Rows in aw-emf-records-private:
36 (last was 0 for an increase of 36)
+--------------------------------------------------------------------+
Hardware Sensor Report:
eeprom-i2c-1-55
Adapter: SMBus AMD8111 adapter at 50e0
Memory type: DDR SDRAM DIMM
Memory size (MB): 1024

eeprom-i2c-1-54
Adapter: SMBus AMD8111 adapter at 50e0
Memory type: DDR SDRAM DIMM
Memory size (MB): 1024

eeprom-i2c-1-51
Adapter: SMBus AMD8111 adapter at 50e0
Memory type: DDR SDRAM DIMM
Memory size (MB): 1024

eeprom-i2c-1-50
Adapter: SMBus AMD8111 adapter at 50e0
Memory type: DDR SDRAM DIMM
Memory size (MB): 1024

adm1027-i2c-1-2e
Adapter: SMBus AMD8111 adapter at 50e0
ERROR: Can't get alarm mask data!
V1.5: +2.594 V (min = +1.42 V, max = +1.58 V) ALARM
VCore: +1.307 V (min = +0.00 V, max = +0.00 V) ALARM
V3.3: +3.321 V (min = +3.13 V, max = +3.47 V)
V5: +5.078 V (min = +4.74 V, max = +5.26 V)
V12: +12.063 V (min = +11.38 V, max = +12.62 V)
CPU_Fan: 9490 RPM (min = 4000 RPM)
CPU: +50.75 C (low = +10 C, high = +50 C) ALARM
Board: +46.50 C (low = +10 C, high = +35 C) ALARM
Remote: +44.75 C (low = +10 C, high = +35 C) ALARM
ERROR: Can't get PWM1 data!
ERROR: Can't get PWM2 data!
ERROR: Can't get PWM3 data!

+--------------------------------------------------------------------+
vmstat:
procs -----------memory---------- ---swap-- -----io---- --system-- ----cpu----
r b swpd free buff cache si so bi bo in cs us sy id wa
0 0 0 2973808 168244 517116 0 0 12 67 529 192 3 2 95 1
```

```
+--------------------------------------------------------------------+
/proc/stat (for expert diagnostics):
cpu 110110 3869 46363 3210576 17019 1093 5093 0
cpu0 56992 2055 21622 1604952 8505 529 2404 0
cpu1 53117 1814 24741 1605624 8514 563 2688 0
intr 17965710 16976393 299 0 11 11 0 3 0 0 0 0 0 3 0 110653 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 517069 0 0 0 0 0 0 0 180854 0 0 0 0 0 0 0 55731
0 0 0 0 0 0 0 124683 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0
ctxt 6510439
btime 1141752132
processes 88703
procs_running 1
procs_blocked 0
+--------------------------------------------------------------------+
/proc/meminfo (for expert diagnostics):
MemTotal: 4058776 kB
MemFree: 2973816 kB
Buffers: 168244 kB
Cached: 517116 kB
SwapCached: 0 kB
Active: 592332 kB
Inactive: 252776 kB
HighTotal: 0 kB
HighFree: 0 kB
LowTotal: 4058776 kB
LowFree: 2973816 kB
SwapTotal: 8388600 kB
SwapFree: 8388600 kB
Dirty: 340 kB
Writeback: 0 kB
Mapped: 230828 kB
Slab: 134536 kB
CommitLimit: 10417988 kB
Committed_AS: 603188 kB
PageTables: 6508 kB
VmallocTotal: 34359738367 kB
VmallocUsed: 10328 kB
VmallocChunk: 34359727955 kB
HugePages_Total: 0
HugePages_Free: 0
Hugepagesize: 2048 kB
+--------------------------------------------------------------------+
/proc/net/softnet_stat (for expert diagnostics):
0015a8d3 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000061
001573a9 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000016
+--------------------------------------------------------------------+
/proc/net/sockstat (for expert diagnostics):
sockets: used 152
TCP: inuse 46 orphan 0 tw 28 alloc 49 mem 0
UDP: inuse 16
RAW: inuse 1
FRAG: inuse 0 memory 0
+--------------------------------------------------------------------+
/proc/net/netstat (for expert diagnostics):
TcpExt: SyncookiesSent SyncookiesRecv SyncookiesFailed EmbryonicRsts PruneCalled RcvPruned OfoPruned
OutOfWindowIcmps LockDroppedIcmps ArpFilter TW TWRecycled TWKilled PAWSPassive PAWSActive PAWSEstab
DelayedACKs DelayedACKLocked DelayedACKLost ListenOverflows ListenDrops TCPPrequeued
TCPDirectCopyFromBacklog TCPDirectCopyFromPrequeue TCPPrequeueDropped TCPHPHits TCPHPHitsToUser
TCPPureAcks TCPHPAcks TCPRenoRecovery TCPSackRecovery TCPSACKReneging TCPFACKReorder TCPSACKReorder
TCPRenoReorder TCPTSReorder TCPFullUndo TCPPartialUndo TCPDSACKUndo TCPLossUndo TCPLoss
TCPLostRetransmit TCPRenoFailures TCPSackFailures TCPLossFailures TCPFastRetrans TCPForwardRetrans
```

Sample Status E-mail

```
TCPSlowStartRetrans TCPTimeouts TCPRenoRecoveryFail TCPSackRecoveryFail TCPSchedulerFailed
TCPRcvCollapsed TCPDSACKOldSent TCPDSACKOfoSent TCPDSACKRecv TCPDSACKOfoRecv TCPAbortOnSyn
TCPAbortOnData TCPAbortOnClose TCPAbortOnMemory TCPAbortOnTimeout TCPAbortOnLinger TCPAbortFailed
TCPMemoryPressures
TcpExt: 0 0 0 0 0 0 0 0 0 0 3044 9 0 0 0 0 22435 42 0 0 0 373747 17240 2464104 0 120425 3942 19137 148173
0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 5 0 0 0 1 0 0 4594 4633 0 0 0 0 0
+--------------------------------------------------------------------+
/proc/slabinfo (for expert diagnostics):
slabinfo - version: 2.1
# name <active_objs> <num_objs> <objsize> <objperslab> <pagesperslab> : tunables <limit> <batchcount>
<sharedfactor> : slabdata <active_slabs> <num_slabs> <sharedavail>
ip_conntrack_expect 0 0 136 29 1 : tunables 120 60 8 : slabdata 0 0 0
ip_conntrack 176 176 344 11 1 : tunables 54 27 8 : slabdata 16 16 0
fib6_nodes 9 61 64 61 1 : tunables 120 60 8 : slabdata 1 1 0
ip6_dst_cache 13 24 320 12 1 : tunables 54 27 8 : slabdata 2 2 0
ndisc_cache 1 15 256 15 1 : tunables 120 60 8 : slabdata 1 1 0
RAWv6 4 4 960 4 1 : tunables 54 27 8 : slabdata 1 1 0
UDPv6 1 8 960 4 1 : tunables 54 27 8 : slabdata 1 2 0
TCPv6 4 10 1600 5 2 : tunables 24 12 8 : slabdata 2 2 0
ip_fib_alias 10 119 32 119 1 : tunables 120 60 8 : slabdata 1 1 0
ip_fib_hash 10 122 64 61 1 : tunables 120 60 8 : slabdata 2 2 0
reiser_inode_cache 70420 70420 712 5 1 : tunables 54 27 8 : slabdata 14084 14084 0
dm-snapshot-in 128 164 96 41 1 : tunables 120 60 8 : slabdata 4 4 0
dm-snapshot-ex 0 0 32 119 1 : tunables 120 60 8 : slabdata 0 0 0
ext3_inode_cache 19867 19880 800 5 1 : tunables 54 27 8 : slabdata 3976 3976 0
ext3_xattr 0 0 88 45 1 : tunables 120 60 8 : slabdata 0 0 0
journal_handle 17 156 24 156 1 : tunables 120 60 8 : slabdata 1 1 0
journal_head 49 82 96 41 1 : tunables 120 60 8 : slabdata 2 2 0
revoke_table 4 225 16 225 1 : tunables 120 60 8 : slabdata 1 1 0
revoke_record 0 0 32 119 1 : tunables 120 60 8 : slabdata 0 0 0
dm_tio 1253 1404 24 156 1 : tunables 120 60 8 : slabdata 9 9 120
dm_io 1304 1309 32 119 1 : tunables 120 60 8 : slabdata 11 11 180
scsi_cmd_cache 63 63 512 7 1 : tunables 54 27 8 : slabdata 9 9 0
sgpool-128 32 32 4096 1 1 : tunables 24 12 8 : slabdata 32 32 0
sgpool-64 32 34 2048 2 1 : tunables 24 12 8 : slabdata 16 17 0
sgpool-32 36 36 1024 4 1 : tunables 54 27 8 : slabdata 9 9 0
sgpool-16 32 40 512 8 1 : tunables 54 27 8 : slabdata 4 5 0
sgpool-8 90 90 256 15 1 : tunables 120 60 8 : slabdata 6 6 0
UNIX 76 88 704 11 2 : tunables 54 27 8 : slabdata 8 8 0
ip_mrt_cache 0 0 128 31 1 : tunables 120 60 8 : slabdata 0 0 0
tcp_tw_bucket 49 60 192 20 1 : tunables 120 60 8 : slabdata 3 3 0
tcp_bind_bucket 119 119 32 119 1 : tunables 120 60 8 : slabdata 1 1 0
tcp_open_request 31 31 128 31 1 : tunables 120 60 8 : slabdata 1 1 0
inet_peer_cache 0 0 64 61 1 : tunables 120 60 8 : slabdata 0 0 0
secpath_cache 0 0 192 20 1 : tunables 120 60 8 : slabdata 0 0 0
xfrm_dst_cache 0 0 384 10 1 : tunables 54 27 8 : slabdata 0 0 0
ip_dst_cache 40 60 384 10 1 : tunables 54 27 8 : slabdata 6 6 0
arp_cache 7 15 256 15 1 : tunables 120 60 8 : slabdata 1 1 0
RAW 4 5 768 5 1 : tunables 54 27 8 : slabdata 1 1 0
UDP 35 35 768 5 1 : tunables 54 27 8 : slabdata 7 7 0
TCP 75 75 1472 5 2 : tunables 24 12 8 : slabdata 15 15 0
flow_cache 0 0 128 31 1 : tunables 120 60 8 : slabdata 0 0 0
cfq_ioc_pool 2475 2511 48 81 1 : tunables 120 60 8 : slabdata 31 31 0
cfq_pool 74 88 176 22 1 : tunables 120 60 8 : slabdata 4 4 0
crq_pool 722 722 104 38 1 : tunables 120 60 8 : slabdata 19 19 120
deadline_drq 0 0 96 41 1 : tunables 120 60 8 : slabdata 0 0 0
as_arq 0 0 112 35 1 : tunables 120 60 8 : slabdata 0 0 0
mqueue_inode_cache 1 4 896 4 1 : tunables 54 27 8 : slabdata 1 1 0
isofs_inode_cache 0 0 632 6 1 : tunables 54 27 8 : slabdata 0 0 0
hugetlbfs_inode_cache 1 6 600 6 1 : tunables 54 27 8 : slabdata 1 1 0
ext2_inode_cache 0 0 752 5 1 : tunables 54 27 8 : slabdata 0 0 0
ext2_xattr 0 0 88 45 1 : tunables 120 60 8 : slabdata 0 0 0
dnotify_cache 1 96 40 96 1 : tunables 120 60 8 : slabdata 1 1 0
dquot 0 0 256 15 1 : tunables 120 60 8 : slabdata 0 0 0
```

```
eventpoll_pwq 2 54 72 54 1 : tunables 120 60 8 : slabdata 1 1 0
eventpoll_epi 2 20 192 20 1 : tunables 120 60 8 : slabdata 1 1 0
kioctx 0 0 384 10 1 : tunables 54 27 8 : slabdata 0 0 0
kiocb 0 0 256 15 1 : tunables 120 60 8 : slabdata 0 0 0
fasync_cache 0 0 24 156 1 : tunables 120 60 8 : slabdata 0 0 0
shmem_inode_cache 379 385 792 5 1 : tunables 54 27 8 : slabdata 77 77 0
posix_timers_cache 0 0 184 21 1 : tunables 120 60 8 : slabdata 0 0 0
uid_cache 6 31 128 31 1 : tunables 120 60 8 : slabdata 1 1 0
blkdev_ioc 51 162 48 81 1 : tunables 120 60 8 : slabdata 2 2 0
blkdev_queue 153 160 720 5 1 : tunables 54 27 8 : slabdata 32 32 0
blkdev_requests 772 795 264 15 1 : tunables 54 27 8 : slabdata 53 53 81
biovec-(256) 260 260 4096 1 1 : tunables 24 12 8 : slabdata 260 260 0
biovec-128 264 264 2048 2 1 : tunables 24 12 8 : slabdata 132 132 0
biovec-64 272 272 1024 4 1 : tunables 54 27 8 : slabdata 68 68 0
biovec-16 272 285 256 15 1 : tunables 120 60 8 : slabdata 19 19 0
biovec-4 272 305 64 61 1 : tunables 120 60 8 : slabdata 5 5 0
biovec-1 648 900 16 225 1 : tunables 120 60 8 : slabdata 4 4 240
bio 620 620 128 31 1 : tunables 120 60 8 : slabdata 20 20 180
file_lock_cache 5 25 160 25 1 : tunables 120 60 8 : slabdata 1 1 0
sock_inode_cache 190 190 704 5 1 : tunables 54 27 8 : slabdata 38 38 0
skbuff_head_cache 534 564 320 12 1 : tunables 54 27 8 : slabdata 47 47 0
acpi_operand 1040 1134 72 54 1 : tunables 120 60 8 : slabdata 21 21 0
acpi_parse_ext 0 0 64 61 1 : tunables 120 60 8 : slabdata 0 0 0
acpi_parse 0 0 40 96 1 : tunables 120 60 8 : slabdata 0 0 0
acpi_state 0 0 88 45 1 : tunables 120 60 8 : slabdata 0 0 0
proc_inode_cache 750 750 616 6 1 : tunables 54 27 8 : slabdata 125 125 54
sigqueue 23 23 168 23 1 : tunables 120 60 8 : slabdata 1 1 0
radix_tree_node 17703 17703 536 7 1 : tunables 54 27 8 : slabdata 2529 2529 0
bdev_cache 15 16 832 4 1 : tunables 54 27 8 : slabdata 4 4 0
sysfs_dir_cache 2965 2989 64 61 1 : tunables 120 60 8 : slabdata 49 49 0
mnt_cache 28 60 192 20 1 : tunables 120 60 8 : slabdata 3 3 0
inode_cache 2177 2177 584 7 1 : tunables 54 27 8 : slabdata 311 311 0
dentry_cache 118269 118269 232 17 1 : tunables 120 60 8 : slabdata 6957 6957 0
filp 1854 2205 256 15 1 : tunables 120 60 8 : slabdata 147 147 30
names_cache 24 24 4096 1 1 : tunables 24 12 8 : slabdata 24 24 0
avc_node 12 54 72 54 1 : tunables 120 60 8 : slabdata 1 1 0
key_jar 10 40 192 20 1 : tunables 120 60 8 : slabdata 2 2 0
idr_layer_cache 91 91 528 7 1 : tunables 54 27 8 : slabdata 13 13 0
buffer_head 113400 113400 88 45 1 : tunables 120 60 8 : slabdata 2520 2520 0
mm_struct 112 112 1152 7 2 : tunables 24 12 8 : slabdata 16 16 12
vm_area_struct 6087 7329 184 21 1 : tunables 120 60 8 : slabdata 349 349 480
fs_cache 183 183 64 61 1 : tunables 120 60 8 : slabdata 3 3 0
files_cache 126 126 832 9 2 : tunables 54 27 8 : slabdata 14 14 0
signal_cache 165 165 704 11 2 : tunables 54 27 8 : slabdata 15 15 0
sighand_cache 135 135 2112 3 2 : tunables 24 12 8 : slabdata 45 45 12
task_struct 160 160 1808 2 1 : tunables 24 12 8 : slabdata 80 80 12
anon_vma 2058 2496 24 156 1 : tunables 120 60 8 : slabdata 16 16 180
shared_policy_node 0 0 56 69 1 : tunables 120 60 8 : slabdata 0 0 0
numa_policy 27 225 16 225 1 : tunables 120 60 8 : slabdata 1 1 0
size-131072(DMA) 0 0 131072 1 32 : tunables 8 4 0 : slabdata 0 0 0
size-131072 0 0 131072 1 32 : tunables 8 4 0 : slabdata 0 0 0
size-65536(DMA) 0 0 65536 1 16 : tunables 8 4 0 : slabdata 0 0 0
size-65536 3 3 65536 1 16 : tunables 8 4 0 : slabdata 3 3 0
size-32768(DMA) 0 0 32768 1 8 : tunables 8 4 0 : slabdata 0 0 0
size-32768 5 5 32768 1 8 : tunables 8 4 0 : slabdata 5 5 0
size-16384(DMA) 0 0 16384 1 4 : tunables 8 4 0 : slabdata 0 0 0
size-16384 20 20 16384 1 4 : tunables 8 4 0 : slabdata 20 20 0
size-8192(DMA) 0 0 8192 1 2 : tunables 8 4 0 : slabdata 0 0 0
size-8192 30 30 8192 1 2 : tunables 8 4 0 : slabdata 30 30 0
size-4096(DMA) 0 0 4096 1 1 : tunables 24 12 8 : slabdata 0 0 0
size-4096 189 189 4096 1 1 : tunables 24 12 8 : slabdata 189 189 0
size-2048(DMA) 0 0 2048 2 1 : tunables 24 12 8 : slabdata 0 0 0
size-2048 658 658 2048 2 1 : tunables 24 12 8 : slabdata 329 329 0
size-1024(DMA) 0 0 1024 4 1 : tunables 54 27 8 : slabdata 0 0 0
```

Sample Status E-mail

```
size-1024 368 368 1024 4 1 : tunables 54 27 8 : slabdata 92 92 0
size-512(DMA) 0 0 512 8 1 : tunables 54 27 8 : slabdata 0 0 0
size-512 648 648 512 8 1 : tunables 54 27 8 : slabdata 81 81 0
size-256(DMA) 0 0 256 15 1 : tunables 120 60 8 : slabdata 0 0 0
size-256 1485 1485 256 15 1 : tunables 120 60 8 : slabdata 99 99 0
size-128(DMA) 0 0 128 31 1 : tunables 120 60 8 : slabdata 0 0 0
size-128 2601 2697 128 31 1 : tunables 120 60 8 : slabdata 87 87 0
size-64(DMA) 0 0 64 61 1 : tunables 120 60 8 : slabdata 0 0 0
size-64 3777 3904 64 61 1 : tunables 120 60 8 : slabdata 64 64 0
size-32(DMA) 0 0 32 119 1 : tunables 120 60 8 : slabdata 0 0 0
size-32 1551 4046 32 119 1 : tunables 120 60 8 : slabdata 34 34 7
kmem_cache 135 135 448 9 1 : tunables 54 27 8 : slabdata 15 15 0
+----------------------------------------------------------------------+
Forensicsd Pcap Statistics:
Packets received: 118325
Packets dropped: 0
+----------------------------------------------------------------------+
Database Mirror Progress:
dir | min | count
-----+-----+-------
0 | 1 | 12
(1 row)

+----------------------------------------------------------------------+
```

Appendix B: Troubleshooting Health Messages

Message	Detail	Meaning	Action
$fields[0] currently not responding	Currently Not Responding	A component of the CounterStorm detection engine has died or is very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.
$fields[0] restart detected through event progress reset	Job Restarted	Someone may have performed maintenance on a CS-1 system, such as applying a patch, rebooting (including via physical access), or running Restart Core Programs.	Contact technical support if maintenance was not performed.
$fields[0] restart detected through wire bits reset	Job Restarted	Someone may have performed maintenance on a CS-1 system, such as applying a patch, rebooting (including via physical access), or running Restart Core Programs.	Contact technical support if no-one performed maintenance.
A response action failed	Please contact technical support for more information	An action taken (either automatically or manually) in response to an alarm has failed to properly operate.	Validate switch or VPN connectivity as well as authentication and permissions. Contact technical support.
Arpd is initializing	Long message explaining the purpose of ARP monitoring and the possible resolutions	A component of the CounterStorm detection engine has either just restarted or is unable to operate properly.	Verify that switch configuration has ingress enabled. Disable arpd.
Connectivity Test Database Problems	Cannot Connect To Database: $cmdout	Database failure on sensor.	Verify that the system is not undergoing maintenance. Restart core programs or reboot.
Could not gather progress of $fields[0]	Could Not Gather Progress: $?: $cmdout	A component of the CounterStorm detection engine has died or it is very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.
Could not gather status of $fields[0]	Could Not Gather Status: $?: $jcmdout	A component of the CounterStorm detection engine has died or it is very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.
Could not gather Worker Detailed Status	Could Not Gather Status: $?: $cmdout	A component of the CounterStorm detection engine has died or it is very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.

Message	Detail	Meaning	Action
Could not remove an active response multiple times	N/A	A currently operational active response (such as switch or VLAN blocking) could not be removed upon its expiration time.	Validate switch or VPN connectivity and authentication and permissions. Contact technical support.
CounterStorm-1 Installation Time Synchronization	Host $host has (serious|""|minor) clock drift relative to me of x minutes/seconds (plus long message describing problem)	Sensor and CC have different ideas of the current time.	Configure NTP, disable NTP filtering between sensor and CC and wait at least 10 minutes between booting CC and sensor.
CounterStorm version information: Failed	Could not obtain my own CounterStorm version: $?: $my_version	The CounterStorm detection engine has encountered an internal error. Detection and alarming are impacted and possibly not working at all.	Contact CounterStorm support.
CounterStorm version information: Failed	Could not obtain my CounterStorm role: $?: $my_role	The CounterStorm detection engine has encountered an internal error. Detection and alarming are impacted and possibly not working at all.	Contact CounterStorm support.
CounterStorm version information: Failed	Could not obtain list of sensors: $?: $sensors	The CounterStorm detection engine has encountered an internal error.	Contact CounterStorm support.
CounterStorm version information: Mismatch detected	Listing of sensor and CC version information	A sensor or sensors do not have the same software revision installed as the CC, or the systems are unreachable.	Validate sensor connectivity and health. Apply patches to get the CC and sensors at the same patch revision.
CounterStorm-1 Installation Connectivity Problems	Could not contact and retrieve data from $host within 15 seconds	The sensor or CC was unable to successfully validate that the CC or sensors were operational within 15 seconds. The peer system may be unreachable through the network or unhealthy.	Verify that the system is not undergoing maintenance. Verify that all CS-1 devices, including CC and all sensors, are otherwise healthy. Verify that the peer systems cabled and powered on. Attempt to ping or ssh to between each device. Reboot CS-1 devices. Fix network problems.
CounterStorm-1 Installation Connectivity Problems	Could not successfully contact $host, it may be very sick	The command center attempted to connect to a host to retrieve its status update, but was unable to do so.	Verify system is not undergoing maintenance. Verify that all CS-1 devices, including CC and all sensors, are otherwise healthy. Verify that the peer systems are cabled and powered on. Attempt to ping or ssh to between each device. Reboot CS-1 devices. Fix network problems.
CounterStorm-1 Installation Connectivity Problems	Host $host contacted, but did not have a recent health report	Remote host does not have critical programs running or is (or has recently been) undergoing maintenance.	Verify that the system is not undergoing maintenance. Reboot remote host.

Message	Detail	Meaning	Action
Counterstorm-1 System Processes Not Fully Operational	One or more CounterStorm-1 processes are not running:\n$cmdout	A component of the CounterStorm detection engine has died or is very busy and hasn't responded.	If the detailed error message says "pids not present," reboot or restart core programs. If the detailed error messages say "pids present," the system may be overloaded and you should see troubleshooting for high load average. If this error message appears several times without successful status in between, reboot or restart core programs.
Database Mirror Backlogged Progress	Count of items to be mirror appear too high, is mirroring stuck?	The normal CS communications between the CC and the sensors have potentially encountered errors or have slowed down. This may be due to the remote system recently becoming unavailable, or the network link between the sensor and CC being slow, or the CS-1 devices being very busy.	Verify that all CS-1 devices, including CC and all sensors, are otherwise healthy. Verify that the network links between the sensor and CC is not slow. Contact technical support.
Database Mirror Has No Progress	No progress mirroring! Minimum item to mirror still $min. Is mirroring stuck?\n\nInformation for technical support: [lotsa data]	The normal CS communications between the CC and the sensors has encountered errors. This may be due to the remote system being unreachable or unhealthy.	Verify that thesystem is not undergoing maintenance. Verify that all CS-1 devices, including CC and all sensors, are otherwise healthy. Make sure that the sensor and the CC are running the same patch version. Contact technical support.
Database Mirror Progress DB Failure	Cannot Connect To Database: $cmdout	Database failure on system.	Verify that the system is not undergoing maintenance. Restart core programs or reboot.
Database Tagset Size DB Initialization Failure	Database not initialized--no tagset_directory: $dbh->errstr	The CounterStorm detection engine has encountered an internal error. Detection and alarming are impacted and possibly not working at all.	Contact CounterStorm support.
Database Tagset Size Missing Table Failure	Could not retrieve number of rows! $dbh->errstr	The CounterStorm detection engine has encountered an internal error. Detection and alarming are impacted and possibly not working at all.	Contact CounterStorm support.
Degraded RAID Status	N/A	The CounterStorm Command Center has experienced a failed or severely impacted disk. The CC will continue to run, but its performance will be degraded. You may disable the RAID alarm via the admin menu.	Perform a backup. Contact CounterStorm for replacement hardware and detailed replacement instructions.
Excessive output backlog of $fields[0]	Waiting to write $workerinfo{$fields[0]}->{'params'}->{'Output Thread Queue Length'} events	System has encountered an extremely high volume of bad traffic.	Often caused by high load. See high load average on B-4. Adjustments to segment definitions and/or whitelisting may be needed.

Message	Detail	Meaning	Action
Extremely High Load Average	N/A	The CounterStorm appliance is running with excessive load, and is likely dropping packets and otherwise failing to timely notify properly on malicious traffic.	Check for and resolve any intense worm outbreaks. Check for and resolve any asymmetric traffic. Check for specific clients or servers or connections which can be filtered out (contact technical support for more information about super filters) or excluded from segments. Consider deploying more sensors to handle individual high-traffic segments. Check for excess forensicsq processes (packet dumping).
Forensicsd Not Responding	Cannot Retrieve Forensics Pcap Statistics	A component of the CounterStorm detection engine has died or is very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.
High Load Average	N/A	The CounterStorm appliance is running under a slightly higher load than normal, and could drop packets or otherwise fail to timely notify properly on malicious traffic.	Check for and resolve any intense worm outbreaks. Check for and resolve any asymmetric traffic. Check for specific clients or servers or connections which can be filtered out (contact technical support for more information about super filters) or excluded from segments. Consider deploying more sensors to handle individual high-traffic segments. Check for excess forensicsq processes (packet dumping).
Job Status Test Failed	Could Not Gather Status: $?: $cmdout	A component of the CounterStorm detection engine has died or it is very busy and hasn't responded.	Often caused by high load, see troubleshooting for high load average. If this error message appears several times without successful status in between, reboot or restart core programs.
Job Status Test Failed	Worker Summary Status: Missing Worker Jobs	This sensor has not been fully configured.	If the sensor has very recently been installed, this may be a transitory problem. If this error message appears several times, contact technical support.
Machine Check Exceptions	Long message explaining what an MCE is	A hardware error has been detected.	Check environment (temperature, power) of system. Reboot to clear any potential problems. Replace system if problem continues.
No event progress of $fields[0]	No New Events (remains $workerinfo{$fields[0]}->{'params'}->{'Events in'})	Sensor has not monitored e-mail in 24 hours.	Check segment configuration for the IPs which are assigned to this sensor. Check cables. Check that the span is properly configured. Check power to taps, if installed. Consider disabling e-mail sensor health check if this is not unusual.
No wire bits progress of $fields[0] seen	No Traffic Observed (remains $workerinfo{$fields[0]}->{'params'}->{'Wire bits'} bits))	The CS sensor isn't seeing any traffic on the monitoring interface.	Check segment configuration for the IPs which are assigned to this sensor. Get segment suggestions to see what traffic may have been seen previously. Check interface packet counts. Check cables. Check that the span is properly configured. Check power to taps, if installed.

Message	Detail	Meaning	Action
Number of sources declared asymmetric by $fields[0] increased!	SD2k4 Scan detection sensor has seen new IP addresses with apparently asymmetric TCP connection traffic (only one direction of traffic observed, but going beyond the initial three-way handshake)	Sensor detected asym traffic.	Traceroute between the two listed IPs--from src to dst or to the immediate upstream routers of each--and check intermediate switches/ routers for proper span config. This may require adding ports to a span configuration, changing the span configuration to monitor "both" input and output traffic, or creating a span on a different switch and also sending that traffic to the same CounterStorm-1 sensor.
S.M.A.R.T. Hard Drive Warnings	N/A	A hard drive in the CounterStorm-1 appliance is failing.	Perform a backup. Contact CounterStorm for replacement hardware and detailed replacement instructions. Sensors will need to be unregistered and the new sensor re-registered, or a restore performed.
Summary Status: Failed Worker Jobs	Listing of failed jobs	A component of the CounterStorm detection engine has died.	Reboot or Restart core programs. If this happens subsequent to a reboot/restart, contact technical support.
Switch Connectivity Test Failure	Contact All Switches: $cmdout	The CounterStorm appliance is unable to connect to one or more of the configured switches.	Check to ensure that you have entered the switch information properly, that the appliance can reach the switch over the network, and that the proper login account exists and is working on the switch.
Very High Load Average	N/A	The CounterStorm appliance is running under a heavy load, and may be dropping packets or otherwise failing to timely notify properly on malicious traffic.	Check for and resolve any intense worm outbreaks. Check for and resolve any asymmetric traffic. Check for specific clients or servers or connections which can be filtered out (contact technical support for more information about super filters) or excluded from segments. Consider deploying more sensors to handle individual high-traffic segments. Check for excess forensicsq processes (packet dumping).
VPN Connectivity Test Failure	Cannot Contact All VPNs: $cmdout	The CounterStorm appliance is unable to connect to one or more of the configured VPN concentrators.	Check to ensure that you have entered the concentrator and LDAP information properly, that the appliance can reach the concentrator and LDAP server over the network, and that the proper login account exists and is working on the concentrator and LDAP server.
Worker dropped %d packets	Waiting to write $workerinfo{$fields[0]}->{'params'}->{'Output Thread Queue Length'} events	Sensor is dropping packets. May be due to load, asym traffic.	Check for and resolve any intense worm outbreaks. Check for and resolve any asymmetric traffic. Check for specific clients or servers or connections which can be filtered out (contact technical support for more information about super filters) or excluded from segments. Consider deploying more sensors to handle individual high-traffic segments. Check the load (though see below).
Worker Progress Retrieval Failure	Could Not Gather Status: $?: $cmdout	A component of the CounterStorm detection engine has died or is very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.

Message	Detail	Meaning	Action
Worker Status Test Failed	Could Not Gather Status: $?: $cmdout	A component of the CounterStorm detection engine has died or iis very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.
Worker Summary Status: Hung Worker Jobs	N/A	A component of the CounterStorm detection engine has died or is very busy and hasn't responded.	Often caused by high load. See high load average on B-4. If this error message appears several times without successful status in between, reboot or restart core programs.

Appendix C: Detection Reason Explanation

The following table describes the detection reasons listed in the activity table's expanded row for a specific activity.

Detection Reason	Explanation
Excessive DNS connections	An unusually large number of domain name lookups to different resolvers may indicate a spambot or other malware that is attempting to locate targets.
Excessive DNS volume	An unusually high level of domain lookup traffic may indicate a spambot or other malware that is attempting to locate targets.
Excessive e-mail connections	An unusually large number of outbound e-mail connections to different mail recipients may indicate a spambot or e-mail worm.
Excessive e-mail volume	An unusually high level of e-mail traffic may indicate a spambot or e-mail worm.
Fast ICMP scanning	An extremely high level of failed pings may indicate a worm or other malware, but is more likely to be a network mapping tool or vulnerability scanner.
Fast scanning	An extremely high level of bad TCP connections may indicate a worm or other malware, but can also be a network mapping tool or vulnerability scanner.
Fast UDP scanning	An extremely high level of unanswered UDP requests may indicate a worm or other malware, but can also be a network mapping tool or vulnerability scanner.
Internet (inbound) ICMP scanning	A high level of failed pings from an external (Internet) source may indicate a targeted attack or reconnaissance attempt.
Internet (inbound) scanning	A high level of bad TCP connections from an external (Internet) source may indicate a targeted attack, worm, or other malware, and may be an indication of a problem with firewall configuration and/or coverage.
Internet (inbound) UDP scanning	A high level of unanswered UDP requests from an external (Internet) source may indicate a targeted attack, worm, or other malware, and is often an indication of a problem with firewall configuration and/or coverage.
Intranet (inbound) ICMP scanning	A high level of failed pings from other systems within the enterprise may indicate a worm or other malware that is attempting to locate vulnerable systems, but can also be a network mapping tool.
Intranet (inbound) scanning	A high level of bad TCP connections from other systems within the enterprise may indicate a worm or other that is malware attempting to spread to other systems.
Intranet (inbound) UDP scanning	A high level of unanswered UDP requests from other systems within the enterprise may indicate a worm or other malware that is attempting to spread to other systems.
Intranet ICMP scanning	A high level of failed pings to systems within the enterprise may indicate a worm or other malware that is attempting to locate vulnerable systems, but can also be a network mapping tool.

Detection Reason	Explanation
Intranet scanning	A high level of bad TCP connections to systems within the enterprise may indicate a worm or other malware that is attempting to spread to other systems.
Intranet UDP scanning	A high level of unanswered UDP requests to systems within the enterprise may indicate a worm or other malware that is attempting to spread to other systems.
Local-segment ICMP scanning	A high level of failed pings to systems in the same segment may indicate a worm or other malware that is attempting to locate vulnerable systems, but can also be a network mapping tool.
Local-segment scanning	A high level of bad TCP connections to systems in the same segment may indicate a worm or other malware attempting to spread to other systems.
Local-segment UDP scanning	A high level of unanswered UDP requests to systems in the same segment may indicate a worm or other malware that is attempting to spread to other systems.
Outbound ICMP scanning (public internet)	A high level of failed pings to external systems on the Internet may indicate a worm or other malware that is attempting to locate vulnerable systems.
Outbound scanning (public internet)	A high level of bad TCP connections to external systems on the Internet may indicate a worm or other malware that is attempting to spread to other systems, or a bot participating in a distributed denial of service attack.
Outbound UDP scanning (public internet)	A high level of unanswered UDP requests to external systems on the Internet may indicate a worm or other malware that is attempting to spread to other systems.
Unrecognized DNS client	A system performing domain lookups on a segment where none were previously observed may indicate malware, but can also be a newly installed system.
Unrecognized DNS server/relay	A system handling domain lookups on a segment where no DNS servers were previously observed may indicate malware, but may just be a newly installed DNS server that should be placed in its own segment.
Unrecognized e-mail server/relay	A system accepting e-mail on a segment where no SMTP servers were previously observed may indicate malware, but is more likely to be a newly installed e-mail server that should be placed in its own segment.
Unrecognized e-mail source	A system sending e-mail via SMTP on a segment where this was never previously observed may indicate a spambot or e-mail worm, but can also be a new installation of an e-mail server that should be placed in its own segment.

Index