

Configuring and Troubleshooting E-mail Notifications for Cisco Secure IDS Director

Document ID: 13877

Cisco has announced the end-of-sales for the Cisco Secure IDS Director and the end-of-sales and end-of-life for Cisco IDS 3.x Sensor Software.

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure E-Mail Notifications
Troubleshoot E-mail Notifications
Related Information

Introduction

This document demonstrates how to configure an E-mail notification on the Cisco Intrusion Detection System (IDS) UNIX Director.

Note: This document does not cover how to use VPN/Security Management Solution (VMS) or Cisco Secure Policy Manager.

Prerequisites

Requirements

The instructions in this document are based on these conditions:

- The IDS UNIX Director communicates with the IDS Sensor and is able to see events.
- The operator has a basic knowledge of UNIX.
- This document is configured as a default installation.

Components Used

The information in this document is based on these software and hardware versions:

- IDS Sensor Appliance Model 4230 that runs software version 3.1(5)S62
- IDS UNIX Director that runs Solaris version 2.6, HP Openview version 6.1, IDS Director version 2.3(3)S62

Note: Version 2.3.3 is the latest release of IDS Director software. This release supports Cisco IDS Sensors that run versions 3 and earlier.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure E-Mail Notifications

Cisco Secure IDS (formerly Netranger) e-mail notification requires several configuration changes. Each change needs to be completed without error or the function does not work. These instructions demonstrate how to configure an e-mail notification.

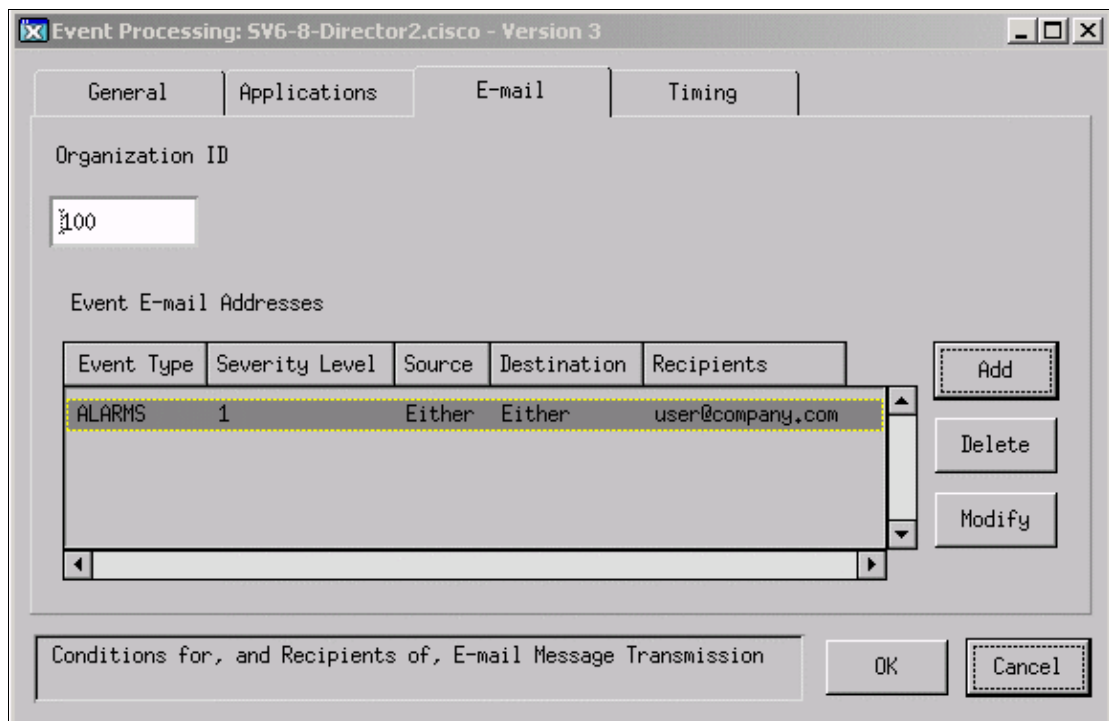
1. Log in to the Director system as user netranger.
2. Send a test e-mail to the user from the Director system command line interface (CLI).

This output is an example of a test e-mail.

```
netrangr@dir2:/usr/nr/var
>mail
This is a test
.

netrangr@dir2:/usr/nr/var
>
```

3. Open up the Netranger Configuration File Management Utility. Log in as user netranger and type **nrConfigure** from the Director system CLI.
4. Double-click the Director, select the **Event Processing** configuration under the installed version, and click **Open**.
5. Select the **E-mail** tab, and click **Add**.



6. Configure the e-mail settings.

◆ From the Event Type menu, select **ALARMS**.

- ◆ In the Severity Level field, type the severity level that triggers an e-mail. Only alarms of the *exact* severity trigger an e-mail. In order to test, use a low severity (1 is the lowest) so that you can ensure that the e-mail is sent.
- ◆ Leave the Source and Destination menu settings as **Either**.
- ◆ In the Recipients field, type the e-mail address where you send the notification. It is also possible to send the e-mail to user netrangr on the local machine in order to test.

Click **OK** when you are done.

Event E-mail Addresses - Add

Event Type: ALARMS

Source: Either

Recipients: user@company.com

Severity Level: 1

Destination: Either

Recipients: a comma separated list of email addresses. Ex: root@machine.com,sadm@unix.com

OK Cancel

7. Select the Applications tab, and click **Add**.

Event Processing: SV6-8-Director2.cisco - Version 3

General Applications E-mail Timing

Event Applications

Script ID	Severity Level	Script Name
1	1	/usr/bin/eventd/event

Add Delete Modify

Script(s) to Execute based on Event Severity Level

OK Cancel

8. Configure the application settings.

- ◆ In the Severity Level field, type the severity level that triggers an e-mail. Remember that this is the lowest severity level that triggers an e-mail message (1 is the lowest).
- ◆ In the Script Name field, type `/usr/nr/bin/eventd/event`.

Click **OK** when you are done.

Event Applications - Add

Script ID: 1

Severity Level: 1

Script Name: /usr/nr/bin/eventd/event

Script to run if event with severity greater than or equal the specified level is received.

OK Cancel

9. Select the Timing tab, and then configure the timing settings.

- ◆ In the Consolidation Interval field, type the interval time in seconds. In order to test, type **10**.
- ◆ In the Alarm Count Thresholds field, type **1,2,3,4,5**. This generates an e-mail on the first through fifth occurrence of each alarm in the consolidation interval.

Click **OK** when you are done.

Event Processing: SV6-8-Director2.cisco - Version 3

General Applications E-mail Timing

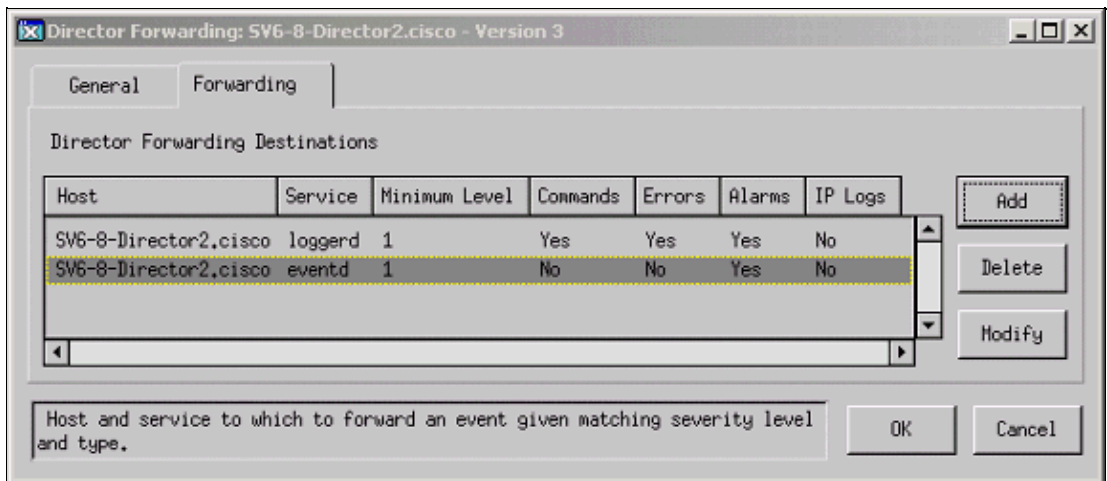
Consolidation Interval (s): 10

Alarm Count Thresholds: 1,2,3,4,5

Event Processing Timing Values

OK Cancel

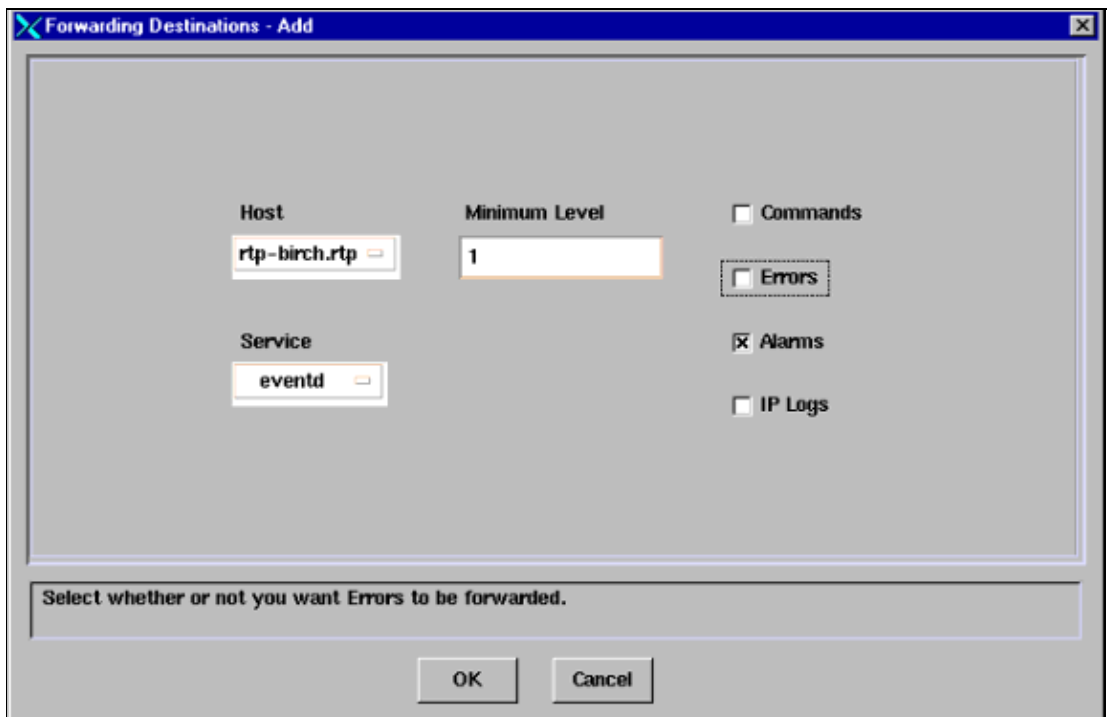
10. Double-click the Director, select the **Director Forwarding** configuration under the installed version, and click **Open**.
11. Select the Forwarding tab, and click **Add**.



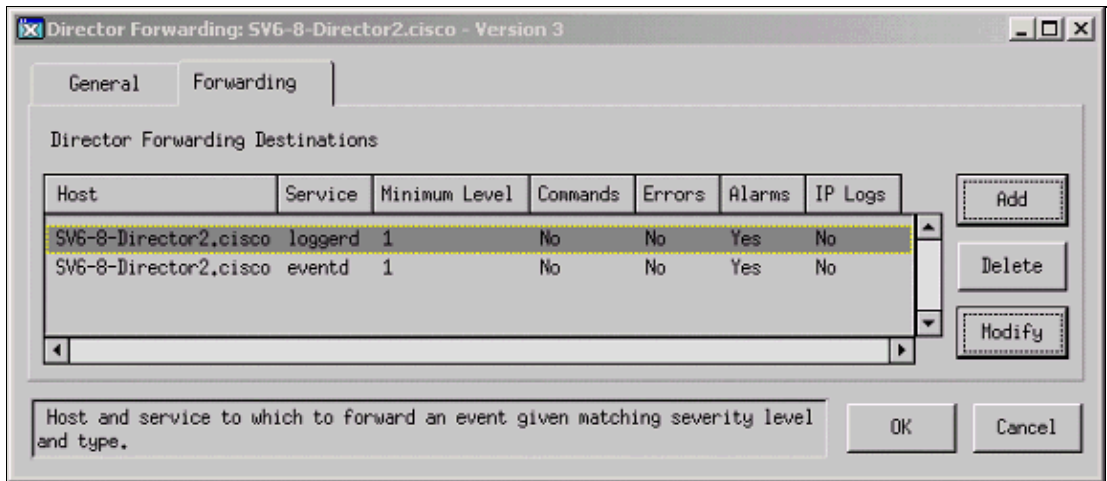
12. Configure the forwarding settings.

- ◆ Verify that the name of the Director is in the Host field.
- ◆ From the Service menu, select **eventd**.
- ◆ In the Minimum Level field, type the same severity level that you entered in step 5. In this test example, the severity level is 1.
- ◆ Select the **Alarms** option.
- ◆ De-select the **Commands**, **Errors**, and **IP Logs** options.

Click **OK** when you are done.



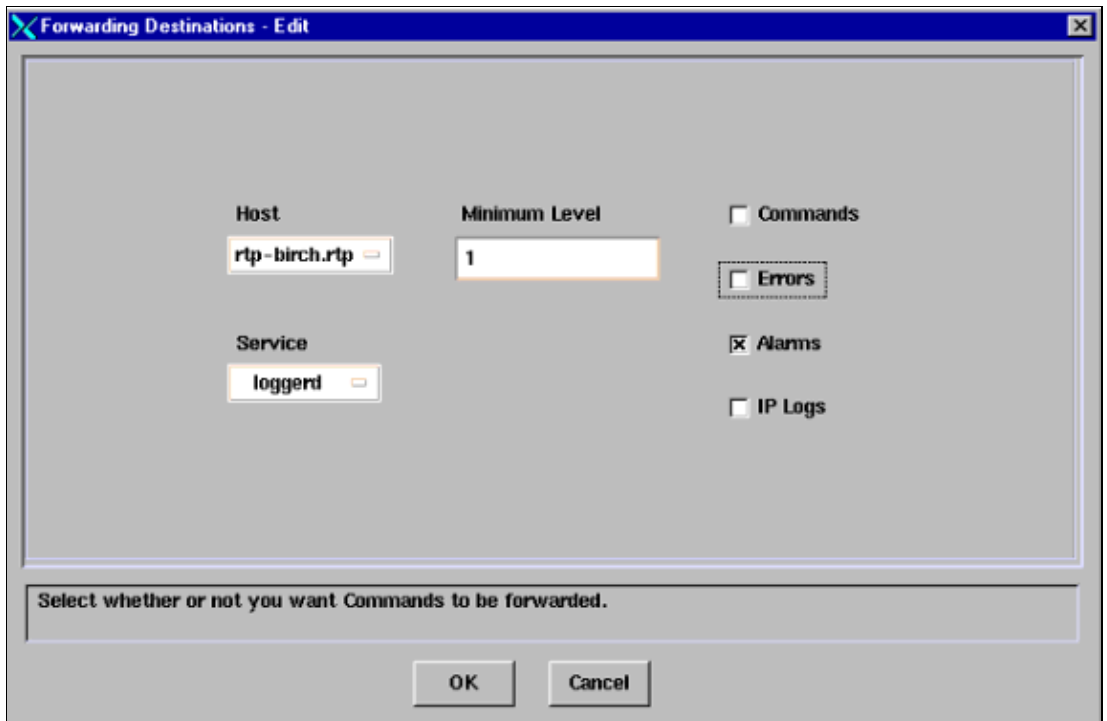
13. On the Forwarding tab, check to see if the service called loggerd is listed. If so, click **Modify**. If not, click **Add**.



14. Configure the settings for the loggerd service.

- ◆ Verify that the name of the Director is in the Host field.
- ◆ From the Service menu, select **loggerd**.
- ◆ In the Minimum Level field, type the same severity level that you entered in step 5. In this test example, the severity level is 1.
- ◆ Select the **Alarms** option.
- ◆ De-select the **Commands**, **Errors**, and **IP Logs** options.

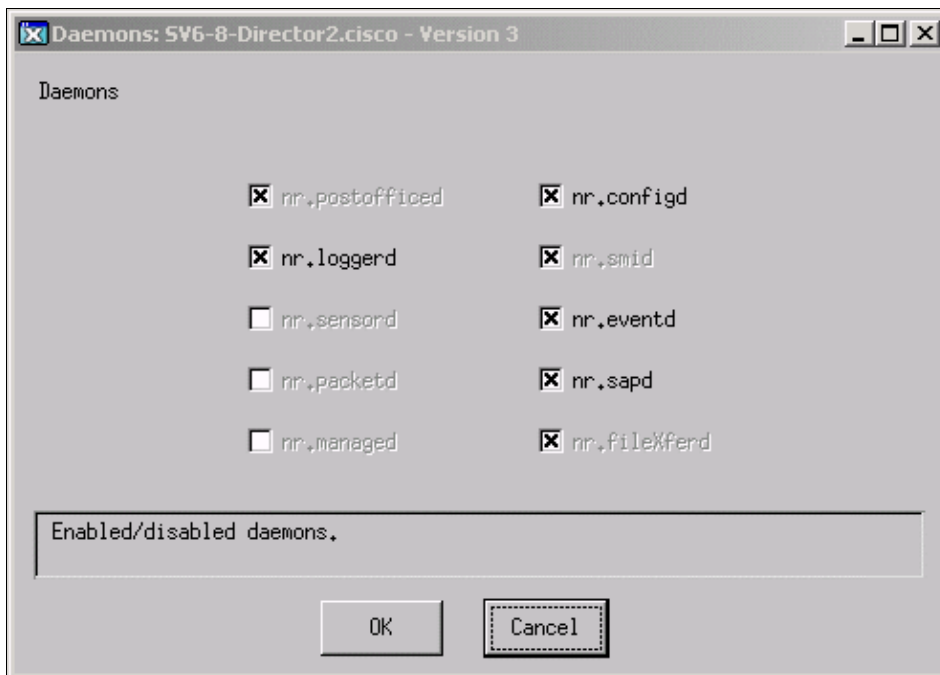
Click **OK** when you are done.



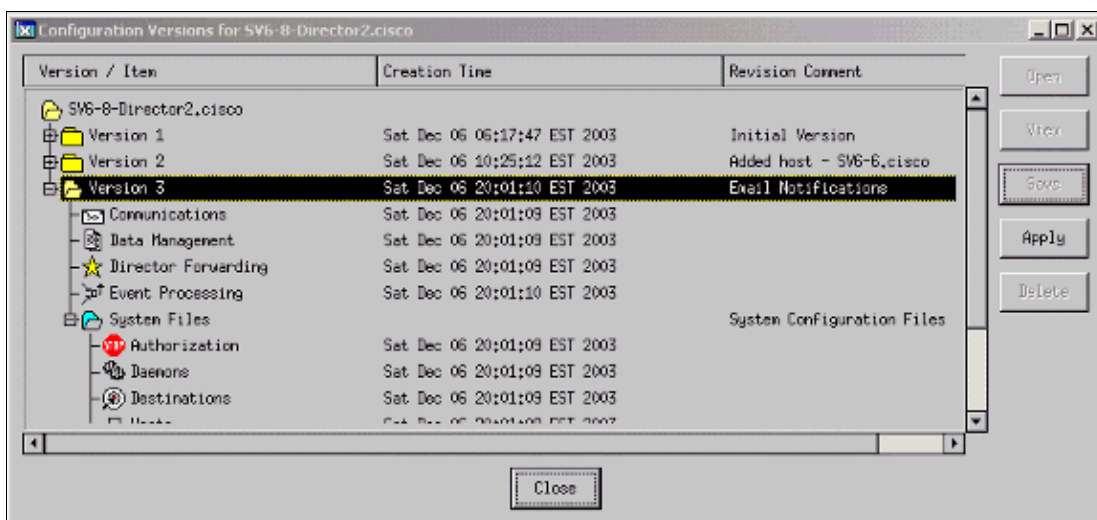
15. Click **OK** in order to close the Director Forwarding configuration.

16. Under the System Files folder, open the Daemons configuration.

17. Select **nr.eventd**, and click **OK**.



18. Click **OK** in order to close the Daemons configuration.
19. Click **Apply** in order to use the new version, and then click **Close** in order to exit nrConfigure.



Troubleshoot E-mail Notifications

Try these suggestions if you have problems with e-mail notifications.

- Run **nrstatus** from the Director system CLI. This shows that eventd runs and that user netrangr is the owner.

This is an example of the expected output.

```
netrangr@dir2:/usr/nr
>nrstatus
netrangr 4541 1 2 14:01:09 ? 0:01 /usr/nr/bin/nr.sapd
netrangr 4287 1 0 14:00:55 ? 0:00 /usr/nr/bin/nr.postofficed
-r 100 200 111
netrangr 4513 1 0 14:01:08 ? 0:00 /usr/nr/bin/nr.smid
netrangr 4531 1 0 14:01:08 ? 0:00 /usr/nr/bin/nr.eventd
netrangr 4553 1 0 14:01:09 ? 0:00 /usr/nr/bin/nr.fileXferd
```

```

netrangr  4497      1  0 14:01:07 ?           0:00 /usr/nr/bin/nr.configd -r 111
netrangr  4482      1  0 14:01:07 ?           0:00 /usr/nr/bin/nr.loggerd

```

If the service is not owned by netrangr or does not run, as user netrangr, run **nrstop** then **nrstart** from the Director system CLI. Next, run the **nrstatus** command again in order to recheck the daemon.

- Ensure that you see new events that come in. Issue the **su - root** command and then enter the **tail -f /usr/nr/var/log.*** command in order to log in as user root. Press Ctrl-C to exit. For more information on how to read the log, refer to Cisco Secure IDS Version 3.1 and Earlier Raw Log Files.

This is an example of the expected output.

```

netrangr@dir2:/usr/nr/var
>su - root
Password:
Sun Microsystems Inc. SunOS 5.6 Generic August 1997
You have new mail.
# tail -f /usr/nr/var/log.*
4,1000002,2003/12/07,02:31:31,2003/12/07,13:31:31,10008,198,100,OUT,OUT,
  4,2156,0,TCP/IP,10.66.190.59,10.66.79.198,0,0,0.0.0.0,Nachi ICMP
4,1000003,2003/12/07,02:31:31,2003/12/07,13:31:31,10008,198,100,OUT,OUT,
  4,2156,0,TCP/IP,10.66.79.198,10.66.190.59,0,0,0.0.0.0,Nachi ICMP
^C#

```

- Issue the **mail** command in order to see why e-mails are sent.

This is an example of a failed mail message.

```

# mail
From Mailer-Daemon Sun Dec 7 01:52:33 2003
Date: Sun, 7 Dec 2003 01:52:33 +1100
From: Mailer-Daemon (Mail Delivery Subsystem)
Subject: Returned mail: Host unknown
      (Name server: mailhost: host not found)
Message-Id: <200312061452.BAB00585@dir2.>
To: Postmaster
Content-Length: 671

The original message was received at Sun, 7 Dec 2003 01:52:33 +1100
from netrangr@localhost

----- The following addresses had delivery problems -----
<user @company.com> (unrecoverable error)

----- Transcript of session follows -----
550 <user @company.com>... Host unknown
      (Name server: mailhost: host not found)

----- Message header follows -----
Return-Path: <netrangr>
Received: by dir2. (SMI-8.6/SMI-SVR4)
id BAA00584; Sun, 7 Dec 2003 01:52:33 +1100
Date: Sun, 7 Dec 2003 01:52:33 +1100
From: netrangr
Message-Id: <200312061452.BAA00584@dir2.>
Content-Type: text
Apparently-To: <user @company.com>
content-length: 34

----- Message body suppressed -----

?

```

Once the e-mail works, you can adjust the e-mail settings so that the e-mail can be sent less frequently, and are sent only on severe events.

Related Information

- [Cisco Secure IDS Director End-of-Sales](#)
 - [Cisco IDS 3.x Sensor Software End-of-Sales End-of-Life](#)
 - [Cisco Secure Intrusion Detection Support Page](#)
 - [Documentation for Cisco Secure Intrusion Detection System](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 22, 2008

Document ID: 13877
