



# Release Note for the Cisco DDoS MultiDevice Manager

---

August 10, 2006



**Note**

---

The most current Cisco documentation for released products is also available on Cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were released.

---

## Contents

This release note applies to the Cisco DDoS MultiDevice Manager (MDM), software version 1.0(1). The MDM remotely monitors and manages the following products:

- Cisco Traffic Anomaly Detector Module and Cisco Traffic Anomaly Detector appliance
- Cisco Anomaly Guard Module and Cisco Guard appliance

For information on configuring and maintaining the MDM software, refer to the *Cisco DDoS MultiDevice Manager Configuration Guide* located in <http://www.cisco.com>.

This release note contains the following sections:

- [The MultiDevice Manager Software](#)
- [Software Version 1.0 Open Caveats](#)
- [Obtaining Documentation](#)
- [Cisco Product Security Overview](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

# The MultiDevice Manager Software

The MDM software allows you to monitor and manage multiple Detector and Guard devices that protect your network against Distributed Denial of Service (DDoS) attacks. The MDM, which runs on a Linux server, has a web-based GUI that provides easy access to network and device status and statistical information. Using the MDM, you can also define and manage the network *zones*, or regions of your network that the devices protect. The MDM also enables you to perform the following tasks:

- Display a consolidated view of ongoing and past attacks on all zones
- Display consolidated statistical information related to all zones and devices
- Create aggregated reports
- Configure or modify zone information on one device and then synchronize the zone to copy the configuration information to the other zone devices
- Activate anomaly detection on all of the zone Detectors
- Activate zone protection (attack mitigation) on all of the zone Guards
- Activate the learning process on one, or all, of the zone devices

## Related Documentation

In addition to the *Cisco DDoS MultiDevice Manager Configuration Guide*, refer to the following documentation for information on configuring guard and detector modules and appliances.

The following documentation is available for the Cisco Anomaly Guard Module:

- *Cisco Anomaly Guard Module and Traffic Anomaly Detector Module Installation Note*
- *Cisco Anomaly Guard Module Configuration Guide*
- *Cisco Anomaly Guard Module Web-Based Manager Configuration Guide*

The following documentation is available for the Cisco Traffic Anomaly Detector Module:

- *Cisco Anomaly Guard Module and Traffic Anomaly Detector Module Installation Note*
- *Cisco Traffic Anomaly Detector Module Configuration Guide*
- *Cisco Traffic Anomaly Detector Module Web-Based Manager Configuration Guide*

The following documentation is available for the Cisco Guard appliance:

- *Cisco Guard and Traffic Anomaly Detector Hardware Installation and Configuration Note*
- *Cisco Guard Configuration Guide*
- *Cisco Guard Web-Based Manager Configuration Guide*

The following Detector documents are available:

- *Cisco Guard and Traffic Anomaly Detector Hardware Installation and Configuration Note*
- *Cisco Traffic Anomaly Detector Configuration Guide*
- *Cisco Traffic Anomaly Detector Web-Based Manager Configuration Guide*

# Software Version 1.0 Open Caveats

The following caveats apply to software version 1.0:

- **CSCse16985**—Synchronizing a zone overwrites any unique remote Guard lists that reside on the zone Detectors (synchronization configures each Detector with the remote Guard list that resides on the Detector master device). Workaround: If the zone Detectors are to operate using unique remote Guard lists, do not enable automatic synchronization or manually synchronize the zone (**Activation > Sync**).
- **CSCse31018**—The MDM may take up to 1 minute to load and display a requested page depending on the number devices associated with the page and the response time of each device. Workaround: none.
- **CSCse50797**—When a zone is active (Protect or Detect are enabled), you cannot change the zone operating state from INTERACTIVE to AUTOMATIC using the MDM. Workaround: Deactivate the zone, change the operating mode, and then reactivate the zone.
- **CSCse63597**—Because the MDM does not automatically delete the older historical reports it generates, the reports can eventually consume all of the available disk space on the MDM server hard drive. Workaround: Manually delete the reports folder to free disk space. The MDM saves all of the zone reports in the /Riverhead/logs/reports/generated/ directory. (You can use a cron job to automatically archive or delete the historical reports.)
- **CSCse63625**—When you delete a zone from the MDM zone list, the MDM does not delete the associated historical reports from the server hard drive. Workaround: Manually delete the directory that the MDM created for storing the zone-specific reports. The MDM saves all of the zone-specific reports in the /Riverhead/logs/reports/generated/*zone-name* directory. (You can use a cron job to automatically archive or delete the historical reports.)
- **CSCse63695**—When you have a zone defined on multiple Guards and you delete all of the zone reports from one of the Guards (using the device CLI), the MDM cannot properly consolidate future report information that it receives from that particular Guard. Workaround: Manually delete the reports in the /Riverhead/logs/reports/source// directory of the MDM server.
- **CSCse66096**—The MDM does not allow you to remove a Detector or Guard device from a zone when the communication state of the device (as shown in the device list (**Main > Device List**)) is in one of the following states:
  - Suspended—The device is not enabled.
  - Disconnected—The MDM is not able to establish a connection with the device.

Workaround: Change the device communication state to connected. If the current device communication state is suspended, perform the following steps:

1. From the Network Summary menu, choose **Main > Device List**. The Device List appears.
2. Click on the suspended device. The Device Form appears.
3. Check the Enable check box.
4. Click **OK**. The device is enabled and the communication state changes to connected.

If the current device communication state is disconnected, check the device configuration or your network connections to correct any problems that are preventing the MDM from communicating with the device.

If you cannot change the communication state to connected, the only other alternative is to remove the device from all of the zones by deleting it from the MDM device list.

- **CSCse68324**—When you deactivate a zone that is handling an attack, the MDM does not reset the number of Dynamic filters that displays in the Zone status screen to zero (0). Workaround: none.
- **CSCse69139**—The MDM incorrectly allows you to add a Detector or Guard device to a zone when the device communication state is suspended or disconnected. Workaround: Only add a device to a zone when its communication state is connected.
- **CSCse70536**—After you complete the required steps to resolve a conflict, the MDM does not always update the Conflict Resolution screen to show that the operation was successful. Workaround: Use the browser Refresh function to force a screen update.
- **CSCse70628**—When a current report shows that there is a zombie attack in progress, the report may not show the zombies list. Workaround: None. The MDM displays the zombies list after the attack is over. To view the zombies list while the attack is occurring, you can view the report from a zone Detector or Guard device using the device CLI or Web-Based Manager (WBM).
- **CSCse72914**—When you delete a single Dynamic filter from a Detector or Guard, the MDM displays the following error message even though the error does not exist: Received error from all devices. Workaround: none. Regardless of the reported error condition, the MDM does delete the Dynamic filter. The message does not display when you use the **delete all** option.
- **CSCse72934**—The MDM does not synchronize clocks with the Detector or Guard device after the MDM initially connects to the device. Workaround: To initiate a clock synchronizing with a single device, you must disable and then enable the device by performing the following steps:
  1. From the Network Summary menu, choose **Main > Device List**. The Device List appears.
  2. Click on the device. The Device Form appears.
  3. Uncheck the Enable check box.
  4. Click **OK**. The device is disabled.
  5. Click on the same device. The Device Form appears.
  6. Check the Enable check box.
  7. Click **OK**. The device is enabled and the MDM synchronizes the device clock.

To initiate a clock synchronization with all of the Detector and Guard devices, you must restart the MDM back-end service by entering the **service backend restart** command from the server prompt.

- **CSCse74586**—The MDM duplicates the historical data in a zone consolidated report when you remove a device from the device list and then add the device back onto the list. When you add the device back onto the device list, the MDM considers the device to be a new device and treats the device's historical data accordingly. New reports and events are not affected. Workaround: Before you add the device back onto the device list, clear the historical reports from the device using the device CLI.
- **CSCse75858**—The MDM can take up to 1 minute to display a change in the zone status that was not initiated by the MDM. For example, if a Detector detects an attack and initiates a zone status change by activating Protect, the MDM may take up to 1 minute to display this status change. Workaround: none.
- **CSCse75943**—If you have the automatic reports export function enabled, you cannot disable this function through the MDM interface. Workaround: To disable the automatic reports export function, log into the MDM server as root and manually delete the `/Riverhead/conf/RepFTP.conf` file.

- **CSCse77349**—When the MDM experiences a problem exporting reports due to connectivity issues with the FTP server, it may take several minutes for the MDM to report the problem. Workaround: Ensure that you define the FTP server configuration correctly prior to exporting the reports. If the connectivity issues with your FTP server continue and you have the automatic reports export function enabled, disable this function until you can resolve the connectivity issues.
- **CSCse80955**—When all of the Detector and Guard devices are communicating with the MDM, an application error popup window appears in the Network Summary screen with the following error message: Received error from all devices. This condition occurs only when a sub-zone has expired but the MDM user interface has not received the information. Workaround: none.
- **CSCsf00254**—Microsoft Internet Explorer fails intermittently when five or more MDM sessions are open on the same PC and the sessions are looking at the Network Summary screen for two days. This problem is the result of the PC running low on virtual memory. Workaround: none. Use the browser Refresh function to reestablish a session with the MDM or open a new browser window and establish a new session.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

---

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://cisoiq.texterity.com/cisoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.