



# Release Note for the Cisco DDoS MultiDevice Manager

---

March 24, 2008



Note

---

The most current Cisco documentation for released products is available on [cisco.com](http://cisco.com)

---

## Contents

This release note applies to the Cisco DDoS MultiDevice Manager (MDM), software version 1.5(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 on [cisco.com](http://cisco.com).

This release note contains the following sections:

- [The MDM Software](#)
- [Related Documentation](#)
- [New Features in Software Version 1.5\(1\)](#)
- [MDM System Requirements for Software Version 1.5\(1\)](#)
- [Upgrading to Software Version 1.5\(1\)](#)
- [Software Version 1.5\(1\) Open and Resolved Caveats](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)



---

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

© <year> Cisco Systems, Inc. All rights reserved.

# The MDM Software

The MDM software allows you to monitor and manage multiple Detector and Guard devices (modules and appliances) 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

For information about obtaining any of the documents listed here, see the [“Obtaining Documentation, Obtaining Support, and Security Guidelines”](#) section.

## New Features in Software Version 1.5(1)

The new features in software version 1.5(1) are as follows:

- Ability to modify the configuration of a zone while it is active (learning traffic, detecting traffic anomalies (Detector), or protecting the zone from an attack (Guard))
- Ability to exclude zone policies and remote Guard lists (Detector only) from the synchronization process
- New threshold tuning features are as follows:
  - Ability to allow each device to learn zone traffic and maintain its own unique set of policies and policy thresholds
  - Ability to merge the results of the learning process (policies and policy thresholds) when each device is allowed to perform the learning process
- Full TACACS AAA support
- Ability to manage the customer portal to restrict access to specific devices and zones
- Ability to display device utilization information
- Ability to create a zone with an IP address list
- Ability to configure remote Guard lists per zone
- Improvements to Time Diff management
- Ability to view the Replied IP summarization information in an attack report that a Guard compiles as part of the new Guard software version 6.1

## MDM System Requirements for Software Version 1.5(1)

Table 1-1 lists the MDM system requirements.

**Table 1-1** MDM System Requirements

Item	Requirements
Linux Server Software	
Linux Operating System	English language version only of Red Hat Enterprise Linux 5 (see the Caution below), 4, or 3.
Preinstalled Applications	MDM Red Hat Package Manager (RPM) requires a Linux server that was installed with a minimum RPM selection and has no preinstalled Tomcat, Java Virtual Machine (JVM), or MySQL applications. The MDM RPM loads these applications as part of the MDM installation process.
Linux Server Hardware	
CPU	2 GHz recommended (1 GHz minimum).
RAM	1 GB recommended (512 MB minimum).
Free disk space	40 G.

**Table 1-1 MDM System Requirements (continued)**

Item	Requirements
Client	
Browser	Microsoft Internet Explorer 6.0 or higher (must support HTML, tables, cookies, Javascript, and frames).
Monitor	Recommend 1024 x 768 pixels minimum.
Detector and Guard operating software	Version 6.1 or higher.



**Caution**

When using the Red Hat Enterprise Linux 5 operating system on your Linux server, you must install the following Red Hat package after installing the MDM software to ensure that the MDM software operates properly:

```
xorg-x11-deprecated-libs-6.8.1-23.EL.i386.rpm
```

You can download this Red Hat package, which is part of the Red Hat Enterprise Linux 4 distribution, from [www.redhat.com](http://www.redhat.com). After downloading the package, install it on the MDM server using the following command:

```
rpm -U xorg-x11-deprecated-libs-6.8.1-23.EL.i386.rpm
```

## Upgrading to Software Version 1.5(1)

When you upgrade the MDM software from version 1.0(1) to version 1.5(1), you must also upgrade all of the Cisco Guard and Detector devices on your MDM network to software version 6.1.

After upgrading the MDM software to software version 1.5(1), you must use the device CLI to restore the MDM remote agent stub on each of the Guard and Detector devices. To restore the MDM remote agent stub, enter the following command in configuration mode:

**mdm restore**

For example:

```
user@DETECTOR# configure
user@DETECTOR-conf# mdm restore
```

# Software Version 1.5(1) Open and Resolved Caveats

The following sections contain the open caveats and resolved caveats in software version 1.5(1):

- [Open Caveats for Software Version 1.5\(1\)](#)
- [Resolved Caveats for Software Version 1.5\(1\)](#)

## Open Caveats for Software Version 1.5(1)

The following open caveats apply to software version 1.5(1):

- **CSCse31018**—The MDM may take up to 1 minute to load and display a requested page depending on the number of devices associated with the page and the response time of each device.  
Workaround: None.
- **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.
- **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.
- **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 to the list again. 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.
- **CSCsf00254**—Microsoft Internet Explorer fails intermittently when five or more MDM sessions are open on the same PC and the sessions display the Network Summary screen for two days. This problem is the result of the PC running low on virtual memory. Workaround: Use the browser Refresh function to reestablish a session with the MDM or open a new browser window and establish a new session.
- **CSCsm53406**—The policy template modification screens do not contain a device drop-down list that allows you to select the policy templates of a specific zone device. The device drop-down list should be available when you exclude zone policies from the MDM synchronization process. The MDM performs the following operations on the master device only from the policy template screens (**Configuration > Policy Templates**): view policy templates, add a service, and delete a service. Workaround: To modify the services of a device other than the master device, use the policy view screen (**Configuration > Policies > View**). This screen allows you to select a specific device and then add or delete a service from the device policy templates.
- **CSCso30648**—The following sequence of events causes the Detector and Guard devices (modules and appliances) to incorrectly measure the traffic rate of a policy and produce dynamic filters even though the traffic rate does not exceed the policy threshold and there is no attack on the zone:
  1. You modify a specific policy using the MDM Config Policy screen.
  2. You activate anomaly detection (Detector) or zone protection (Guard).
  3. The device detects traffic packets associated with the modified policy.

Workaround: If you can apply the policy change to more than one policy, configure the policies using the MDM Config Policy Group screen, which you access by selecting multiple policies to configure. If you need to apply the change to one policy only, use the device CLI.

If the problem exists already, use the one of the following methods to correct it:

- Use the device CLI to export the zone configuration and then import it back under a different zone name (do not use the "copy-from" operation).
- Use the MDM or device CLI to remove the service associated with the policy and then add it back to the zone configuration. For example, if the problem exists with the `http/80/analysis/syns/src_ip` policy, remove the `http/80` service and then add it back to the zone

configuration. After you add the service, you must allow the device to perform the threshold tuning phase of the learning process. This method does not work for services that are built in, such as the tcp\_services/any and dns\_udp/53 services, because these services cannot be removed.

## Resolved Caveats for Software Version 1.5(1)

The following closed caveats apply to software version 1.5(1):

- **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**).
- **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 display the contents of the zombies list while the attack is occurring, access a zone Detector or Guard device directly using the device CLI or Web-Based Manager (WBM).
- **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.

- **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.

- **CSCsj78279**—When you add a new user the MDM server using the Linux **adduser** command, the user receives incorrect privileges.

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.