



Quick Start for Cisco Security Monitoring, Analysis, and Response System

Revised: May 30, 2007, OL-12635-01

This guide summarizes key steps and procedures required to connect an installed MARS Appliance to the network, add a reporting device, and verify that MARS and the reporting device are communicating correctly.

This document contains the following sections:

- [Best Practice Recommendations, page 1](#)
- [Part 1: Configure the MARS Appliance for Access, page 2](#)
- [Part 2: Add Devices to Monitor, page 4](#)
- [Part 3: Additional Administrative Tasks, page 11](#)
- [Part 4: Frequently Asked Questions, page 12](#)
- [Related Documentation, page 14](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 14](#)

Best Practice Recommendations

The following best practices are recommended based on customer usage of MARS:

- Configure an NFS server for backup of each MARS Appliance. This backup archives the event data, but more importantly, it creates a backup copy of your configuration data. **This method is the only way to back up MARS configuration data.** For more information, see “Configuring and Performing Appliance Data Backups” in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.
- Configure NTP servers for your devices and the MARS Appliances. Using an NTP server ensures that events about the same activity, as reported by different reporting devices, can be correlated correctly. Proper correlation reduces the number of false positives and improves the accuracy of the



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

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

MARS Appliance in detecting suspicious activities. For more information on configuring NTP to work with MARS, see “Specify the Time Settings” in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

- Use SSH for administrative connections (access IP) to reporting devices. Cisco recommends SSH over Telnet and other unencrypted protocols.

Part 1: Configure the MARS Appliance for Access

This section summarizes the initial, required configuration. For a detailed instruction, see the “Checklist for Initial Configuration” section in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

Step 1 Access the command line interface of a MARS Appliance using one of the following methods:

- Monitor and keyboard
- Console cable
- Ethernet IP address and SSH client

192.168.0.100 and 192.168.0.101 are the default addresses assigned to eth0 and eth1, respectively. For more information on these options, see “Establishing a Console Connection” in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

Step 2 Log in to the CLI using the “pnadmin” username. The factory installed, default password is *pnadmin*.

Step 3 Change the password of the “pnadmin” account. You are prompted to change this password the first time you log in. Alternatively, you can use the following command:

```
passwd
```

Step 4 Specify the IP address for eth0 and optionally eth1. Add the appropriate default routes for each interface that you configure. Use the following commands:

```
gateway <gateway_address>
```

```
ifconfig eth0 <ip_address> <net_mask>
```

where:

- *gateway_address* is the IP address of the default gateway for the network to which you plan to attach eth0.
- *ip_address* is the IP address value for this interface in the appliance.
- *net_mask* is the netmask value for the IP address.

Step 5 Specify the following values:

- The hostname of the MARS Appliance. Use the **hostname** command. For syntax details, see “hostname” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.
- The domain name of the MARS Appliance. Use the **domainname** command. For syntax details, see “domainname” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

- The DNS servers used by the MARS Appliance to perform lookups. Use the **dns** command. For syntax details, see “dns” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

Step 6 Using Microsoft® Internet Explorer 6.0 SP1 or later, access the MARS web interface via `HTTPS://<ip_of_eth0>`.



Tip

Ensure that you’ve disabled caching in Internet Explorer. Select **Tools > Internet Options > Temporary Internet files > Settings**, and then click the **Every visit to the page** option.

Step 7 When prompted, install the necessary Adobe® SVG Viewer plug-in.

The SVG viewer plug-in is required to view the charts, graphs, and summary page data.

You can either wait for the SVG viewer to install itself when you access the Summary page for the first time, or you can download it from:

<http://www.adobe.com/svg/viewer/install/main.html>



Tip

If you declined to install the SVG Viewer plug-in when prompted, you can clear the cookies Internet Explorer and revisit the MARS login page to see the prompt again.

Step 8 Log in to the web interface using the “padmin” account.



Note

A valid license file is required for the login. Otherwise, you cannot proceed.

Step 9 Select **Admin > System Setup > Configuration Information**.

CS-MARS Device Config

→ Name:

Interface Name	IP Address	Net Mask	Default Gateway
eth0	192.168.0.100	255.255.255.0	192.168.0.1
eth1	192.168.1.100	255.255.255.0	

→ Mail Gateway:

IP:Port :

Email domain name: (ex: Enter 'domain1' for user@domain1)

191874

Step 10 In the IP:Port field under Mail Gateway, enter the IP address and port on which your e-mail gateway listens. The port number is usually 25 for SMTP.

Step 11 Click **Submit** to save your changes.

The Submit action stores the details in the database. When you click Submit, your work is saved, even if you drop the administrative connection before clicking Activate.

Step 12 Click **Activate**.

The Activate action differs from Submit in that MARS begins to use the settings that you have defined.

**Tip**

You must click Activate whenever you add or modify rules, drop rules, reports, or add or modify any options or settings under in the Admin tab other than those on the User Management subtab. Otherwise, the changes that you make will not take effect.

Step 13 Continue with [Part 2: Add Devices to Monitor, page 4](#).

Part 2: Add Devices to Monitor

To add a device, you must prepare the reporting device to send events, enable MARS access for policy discovery, and then add the device to the MARS web interface. Events published by a reporting device to MARS are not inspected until the reporting IP address of the device is defined in the MARS web interface. However, the events are stored on the appliance and can be queried using the unknown device query.

This section summarizes how to add the following device type examples:

- IOS router
- PIX/ASA
- IPS sensor

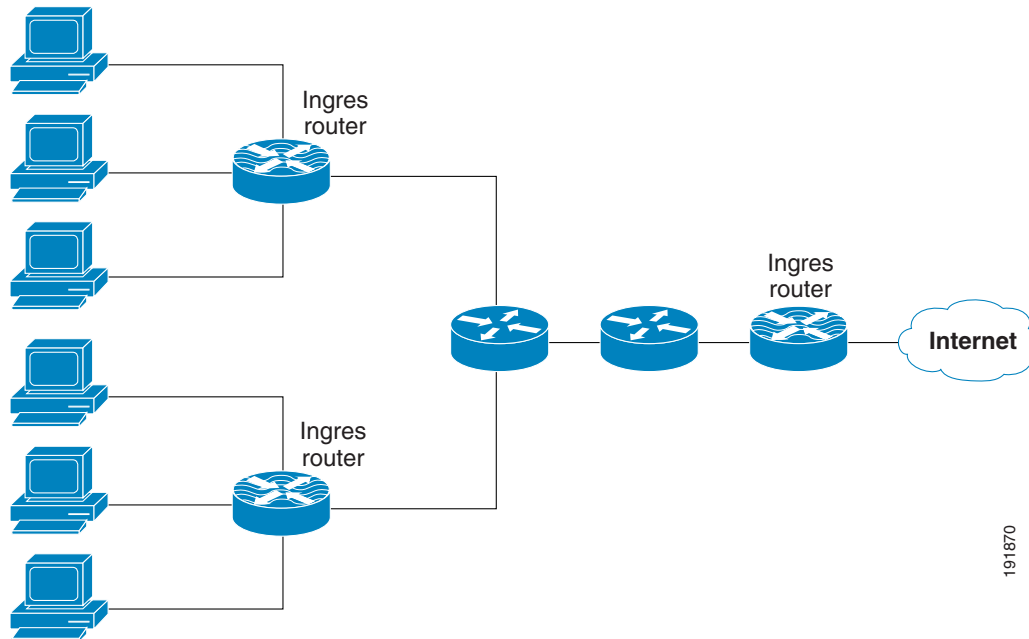
Configure an IOS Router for Syslog, SNMP, and NetFlow events

For detailed instructions on configuring an IOS router, refer to “Configuring Router and Switch Devices” in the *User Guide for Cisco Security MARS Local Controller*.

Notes About NetFlow Configuration

- NetFlow affects the CPU utilization of a router. You need to understand the potential performance impact of enabling NetFlow before you deploy it. For more information, refer to “[NetFlow Performance Analysis](#).”
- By default, MARS stores statistics about the NetFlow events and those events that are identified as anomalous. However, you can configure the MARS Appliance to store all NetFlow events received. Storing all NetFlow events can degrade the performance of the appliance. Therefore, it is not recommended. For detailed instructions on configuring NetFlow and understanding the implications, refer to “Understanding NetFlow Anomaly Detection” in the *User Guide for Cisco Security MARS Local Controller*.
- As a best practice, enable NetFlow on as many supporting devices as possible while avoiding duplicate flows. MARS does not recognize that a flow has been duplicated by two devices. However, it does not affect anomaly detection as duplicated flows are used to established the baseline. At the bare minimum, enable NetFlow on those routers upstream of the assets you want to protect. You should only enable NetFlow on those devices where new packets are generated on your network. Do not enable it on transient gateways, which would generate flows that duplicate those on ingress gateways.

Figure 1 NetFlow Enabled on Ingress Routers



To add an IOS router to MARS and to configure the router correctly, perform the following steps:

-
- Step 1** At the CLI of the router, configure the following settings to define a user account in the local AAA database:
- a. Define a local username on the router:


```
username <username> privilege <priv_lvl> password <passwd>
```
 - b. Configure authentication and exec authorization to use the local database:


```
aaa authentication login default local
```

```
aaa authorization exec default local
```
 - c. Generate RSA key:


```
crypto key generate rsa general-keys modulus 1024
```
- Step 2** Enable SSH access for device discovery by the MARS Appliance
For information on configuring SSH access, see the following URL:
– http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml
- Step 3** To enable SNMP access by the MARS Appliance, enter the following command:
- ```
snmp-server community <community-string> ro <optional-acl>
```
- Step 4** To enable syslog and direct the output to the MARS Appliance, enter the following commands at the router CLI:
- ```
logging source-interface <interface>
```

logging trap *<level>*

logging *<mars_ip>*

logging on



Note

To be most effective, MARS must receive a high level of logging. This corresponds to a logging level of 6 (Informational) or higher.

Step 5 To enable NetFlow event generation, which MARS uses to detect attacks and other anomalous events in the network, enter the following commands:

ip flow-export version 5

ip flow-export destination *<mars_ip>* **2055**

ip flow-export source *<source_interface>*

The default NetFlow port is 2055.

Step 6 To enable flow caching on each interface so the router can track the flows traversing the interface, enter the following commands:

interface *<interface>*

ip route-cache flow



Note

You are not required to specify the source-interface in both the logging and flow-export commands. However, it is recommended on multi-interface routers where packets can originate from more than one interface and/or IP address. MARS associates received events with a specific reporting device based on the reporting IP address for which you can specify one value. Therefore, if events are published from different interfaces and addresses on the same device, MARS classifies any events not originating from the reporting IP as events reported by an unknown reporting device. Finally, as a security best practice, you should always specify the source interface and tie it to a loopback interface. Loopback is recommended as a source interface because it does not go down, whereas a physical interface can fail. Also a loopback ensures that the router has one access IP in the MARS.

Step 7 In the web interface of MARS, click **Admin > System Setup > Security and Monitor Devices, > Add**.

Step 8 Select **Cisco IOS 12.2** from the Device Type list for your router, if you are running 12.2 or later.

Step 9 Specify values for the following device access fields:

- Device name
- Access IP
- Reporting IP



Note

The access IP and the reporting IP are typically the same. The only time these addresses would differ is if, for example, an FTP server was used to provide access to the configuration data rather than the live device.

- Access Type

- Login
- Password
- Enable Password
- SNMP RO Community
- Monitor Resource Usage (requires SNMP RO)

Device Type:

→ *Device Name:

→ Access IP:

→ Reporting IP:

→ *Access Type:

Login:

Password:

Enable Password:

Config Path:

File Name:

SNMP RO Community:

→ Monitor Resource Usage:

191871

- Step 10** Click **Discover** to test connectivity, and then click **Submit** to save these settings.
- Step 11** Click **Activate**.
- Step 12** Click **Summary > Dashboard**.
- Step 13** Under the Hotspot Graph, click **Full Topology Graph**, and verify the device appears.

Add a Cisco ASA or PIX Security Appliance

Cisco ASA or PIX security appliance can be configured similarly. For detailed instructions on configuring these devices, refer to “Configuring Firewall Devices” in the [User Guide for Cisco Security MARS Local Controller](#).

To add an ASA or PIX 7.x security appliance, perform the following steps:

- Step 1** Configure the Cisco security appliance so that MARS can discover the device’s settings. The following commands enable the MARS Appliance to discover via SSH:

```
crypto key generate rsa modulus <modulus>
```

```
ssh <mars_ip> 255.255.255.255 <interface>
```

Step 2 Configure the Cisco security appliance to publish its syslog events to MARS and enable the SNMP RO community string for the device. MARS uses syslog events to discover information about the network topology. It uses SNMP to discover CPU utilization and related information.

The commands needed to accomplish this are as follows:

```
snmp-server host <interface> <mars_ip> poll community <community>
```

```
logging host <interface> <mars_ip>
```

```
logging trap 7
```

```
logging enable
```

The log level should be debug (7) or you must configure the device to generate the required set of syslog messages, see “Device-Side Tuning for Cisco Firewall Device Syslogs” in the *User Guide for Cisco Security MARS Local Controller* for the required configuration.

Step 3 In the web interface of MARS, click **Admin > System Setup > Security and Monitor Devices > Add**.

Step 4 Select either Cisco ASA 7.0 or the correct version of Cisco PIX from the Device Type list:

Step 5 Specify values for the following device access fields:



Tip

For SSH discovery, the MARS Appliance must authenticate to the security appliance. The default username is “pix” and the password is the one specified by the passwd command, unless AAA is used.

- Device name
- Access IP (Access and Reporting IP should almost always be the same)
- Reporting IP
- Access Type
- Login
- Password
- Enable Password
- SNMP RO Community
- Monitor Resource Usage (requires SNMP RO)

Device Type:

→ *Device Name:

→ Access IP:

→ Reporting IP:

→ *Access Type:

Login:

Password:

Enable Password:

Config Path:

File Name:

SNMP RO Community:

→ Monitor Resource Usage:

191873

- Step 6** Click **Discover** to test connectivity, and then click **Submit** to save these settings.
- Step 7** Click **Activate**.
- Step 8** Click **Summary > Dashboard**.
- Step 9** Under the Hotspot Graph, click **Full Topology Graph**, and verify the device appears.

Add an IPS Sensor

To enable a Cisco IPS sensor running the IPS 5.x operating system, perform the following tasks:

- Ensure a self-signed x.509 Transport Layer Security (TLS) certificate exists on the IPS appliance.
- To display, in MARS, the payload of a packet that triggered an event, ensure that IPS events have the Produce Verbose Alert action. The default action is Produce Alert.

To add an IPS sensor, perform the following steps:

- Step 1** To add the IP address of the MARS Appliance to the permit list, enter the following command at the IPS CLI:

```
access-list ip_address/netmask
```

- Step 2** To verify HTTPS access is enabled, enter the following command:

```
show settings
```

The following results are desired:

```
enable-tls: true <defaulted>
port: 443 <defaulted>
server-id: HTTP/1.1 compliant <defaulted>
```

If the results differ, use the following procedure to perform the configuration:

<http://www.cisco.com/en/US/docs/security/ips/5.1/configuration/guide/idm/dmTS.html#wp151643>

- Step 3** To verify a self-signed x.509 Transport Layer Security (TLS) certificate exists on the IPS appliance, enter the following command:

show TLS fingerprint

If there is no value, you must enter the command `TLS generate-key`. This certificate should have been generated when the management interface was enabled. Use the setup command at the CLI to configure the management interface.

- Step 4** In the web interface of MARS, click **Admin > System Setup > Security and Monitor Devices > Add**.
Step 5 Select **Cisco IPS 5.x** from the Device Type list.

Device Type:

→ *Device Name:

→ Reporting IP:

→ *Access Type: **SSL**

 Login:

 Password:

 Port:

→ Monitor Resource Usage:

 Pull IP Logs:

[Optional: for attack path calculation and mitigation enter monitoring networks information]

→ Monitored Networks:

192.168.1.1/255.255.255.0

Select a Network:

Define a Network:

 Network IP:

 Mask:

191872

- Step 6** Enter the hostname of the sensor in the Device Name field.
 The Device Name value must be identical to the configured sensor name.
- Step 7** Enter the administrative IP address in the Access IP field.
- Step 8** Enter the administrative IP address in the Reporting IP field.
 The Reporting IP address is the same address as the administrative IP address.
- Step 9** In the Login field, enter the username associated with the administrative account of the IPS sensor.

- Step 10** In the Password field, enter the password associated with the username specified in the Login field.
- Step 11** The access type default is SSL and cannot be changed.
- Step 12** In the Port field, enter the TCP port on which the webserver running on the sensor listens. The default SSL port is 443.
- Step 13** Select **Yes** to activate monitor resource usage.
- Step 14** Select **Yes** in the Pull IP Logs box to pull the IP logs from the sensor.
- Step 15** For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:
- To manually define the networks, click the **Define a Network** radio button.
- Enter the network address in the Network IP field.
 - Enter the corresponding network mask value in the Mask field.
 - Click **Add** to move the specified network into the Monitored Networks field.
 - Repeat as needed.
- To select the networks that are attached to the device, click the **Select a Network** radio button.
- Select a network from the Select a Network list.
 - Click **Add** to move the selected network into the Monitored Networks field.
 - Repeat as needed.
- Step 16** To verify the configuration, click **Test Connectivity**.
- Step 17** Click **Submit**.
- Step 18** Click **Activate**.

Part 3: Additional Administrative Tasks

The following administrative checklists and links can assist you in operating your MARS Appliance:

- “Installation Quick Reference” in [Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System](#)
Provides an overview of the full install process.
- “Checklist for Initial Configuration” in [Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System](#)
In-depth walkthrough the required initial configuration.
- “Checklist for Upgrading the Appliance Software” in [Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System](#)
Describes how to keep the appliance up-to-date, how to perform the upgrades, and where to download upgrades.
- “Checklist for Provisioning Phase” in the [User Guide for Cisco Security MARS Local Controller](#)
Provisioning involves planning, setting up, and configuring the hardware, software, and networks that provide the MARS Appliance with access to data and network resources. This phase occurs after a successful installation and initial configuration.
- “Checklist for Monitoring Phase” in the [User Guide for Cisco Security MARS Local Controller](#)

Following the provisioning phase, you must configure MARS to realize your broader security goals and requirements. Your primary goal of the monitoring phase is to effectively realize your monitoring, mitigation, and remediation policies. This process involves defining the strategies, rules, reports, and other settings required to achieve this goal.

- Archiving: See “Configuring and Performing Appliance Data Backups” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*
 1. Ensure that you have a high-speed, low-latency connection. For example, enable eth1 as an out-of-band management interface. See “Specify IP Address and Default Gateway of Eth1” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*
 2. Define a route on MARS to the NFS server (if using eth1). See “Set Up Additional Routes” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*
 3. Enable NFS traffic on intermediate gateways.
 4. Configure the NFS server.
 5. Configure MARS to archive to the NFS server.
- “Specify the Time Settings” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*

Enable NTP on your network to ensure the consistency of log data by multiple device and to improve the probability of correct correlation to same events
- “Specify DNS Settings” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*

Configure DNS settings so MARS can resolve IP addresses to hostnames in the reports
- “User Management and Roles” in the *User Guide for Cisco Security MARS Local Controller*

Enable selective access to and control of the MARS Appliance.

Part 4: Frequently Asked Questions

- Q.** How can I determine the status and health of the MARS (status, event rate, and so on)?
- A.** You can use a combination of CLI commands and web interface reporting to determine the status of your MARS Appliance. At the CLI, the **diskusage** and **pndbusage** commands provide details on the current state of the disks and database. In the web interface, the graphs on the Summary page and the statistics for the past 24 hours (in comparison to your model's event rate) helps determine how busy the appliance is. In addition, MARS creates and stores a variety of status events on which you can query.
- Q.** How can I verify the MARS is receiving events?
- A.** Use the following methods to verify that MARS is receiving events:
 - Verify that the device is defined as a reporting device and that the reporting IP address field is populated with the address from which events are published to MARS.
 - Run a user-defined query for events being reported by that IP address. Any events published by a device to MARS before adding and activating the device in the web interface can be queried using the reporting IP address of the device as a match criterion.
- Q.** What does it mean when I get events from an “Unknown Reporting Device”?

- A.** The term, unknown reporting device, refers to a device from which MARS has received events, but that device has not been formally defined in MARS. You must define the device, including the device type and reporting IP address, before MARS can properly process the events from that device. In addition, it will only correctly parse those events from the time you apply the definition forward. Previously received events will remain associated with the unknown reporting device.

To display all devices that are either added incorrectly or not activated in MARS, you can define one of two queries:

- Select “Unknown Reporting Device” in the Devices field. This query returns the events only for those devices that are reporting events that do not match the one of the reporting IPs defined in MARS. When MARS receives events, it first determines if the IP from which the events are received matches one of the reporting IPs identified in the Reporting and Monitor Devices page. Only if MARS finds a match does it attempt to parse the events. Therefore, if the Reporting IP is defined incorrectly for a reporting device, the events from that device are not parsed. This query essentially identifies events that are not parsed.
- Select the “Unknown Device Event Type” in the Events field. This query returns events from known devices that for some reason the event is not parsed by MARS (for example, if the MARS signature list is not current with the device event lists), and it returns events reported by unknown devices.

- Q.** Which devices should I add to the MARS?

- A.** Cisco Best Practices, refer to SAFE blueprint.

- Q.** What is the difference between an event, session, and an incident?

- A.** *Events* are logs generated about events and activities that occur on or are detected by the reporting devices. Events include information such as IPS alarms, authentication event records, and session accept/reject logs.

A *session* is a collection of events that all share a common source and destination, which were reported within a given time period. For example, usually the events in a session map well to the events generated between the opening and closing of a TCP/IP connection.

In MARS, *sessionization* refers to the combining of event data from multiple reporting devices to reconstruct the occurrence of a session. Sessionizing takes two forms:

- reconstructing a session-oriented protocol, such as TCP, where the initial handshake and the session tear down and
- reconstructing a sessionless protocol, such as UDP, where the initial start and session end times are defined more based on first and last packets tracked within a restricted time period. In other words, packets that fall outside of the time period are considered part of different sessions.

Inspection rules correlate events and sessions from disparate devices into meaningful collections that reflect the end-to-end activities of an attack or other suspicious network operation. When an inspection rule is matched, a notification is created in MARS that is called an *incident*.

- Q.** What is the best way to back up my configuration?

- A.** Currently archiving is the only available option. For more information, see “Configuring and Performing Appliance Data Backups” in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

- Q.** What the difference between pulled versus pushed events with respect to Windows events, IPS, firewall syslogs, etc.)?

- A.** *Push* and *pull* refer to the two event retrieval methods that MARS uses to obtain events from reporting devices. When an event occurs, a pushed event is published by the reporting device to consumers of that network service, such as MARS. However, a pulled event is stored locally on the reporting device. Periodically, MARS connect to the reporting device to retrieve the data any events that occurred. As a result, events may have occurred in the pulled scenario about which MARS is unaware until the next time it pulls data.

Most reporting devices supported by MARS use only one event retrieval method. Windows hosts are the exception. You can configure MARS to parse events logs pushed by the Snare agent as well as to pull event logs from the Windows host. The selection is a trade off between installing the Snare agents and acceptable latency in processing events from those hosts.

- Q.** What is the maximum size of a stored event in the MARS?
- A.** As of 5.2.4, the maximum event size is 1.5 MB. In releases 4.2.6 and earlier, the event size was restricted to 500 bytes.
- Q.** Which reports are applicable to the Sarbanes/Oxley requirements?
- A.** MARS includes pre-packaged report groups for both COBIT and SOX compliance standards. The group names include the identifiers COBIT and SOX. You can find these report groups in the Groups drop-down list on the Query/Reports > Reports subtab of the web interface.

Related Documentation

- *Cisco Secure MARS Documentation Guide and Warranty*. The document roadmap presents the full list of publications and URLs available in support of Cisco Secure MARS.

http://www.cisco.com/en/US/products/ps6241/products_documentation_roadmaps_list.html

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>

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, GigaStack, 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, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, 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. (0612R)

© 2007 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.