



CHAPTER 1

Deployment Planning Guidelines

Revised: September 11, 2008, OL-16776-01

This chapter presents information to assist you in deploying one or more MARS Appliances. It contains the following sections:

- [MARS Components, page 1-1](#)
- [Supporting Devices, page 1-1](#)
- [Required Traffic Flows, page 1-2](#)
- [Web Browser Client Requirements, page 1-4](#)

MARS Components

When planning a deployment, you must consider the ability of a MARS Appliance to process the traffic expected from reporting devices on your network. Which models you purchase and where you place them on your network depends on the anticipated, sustained events per second (EPS) and NetFlow flows per second (FPS) predicted for that network or segment.

For details on the supported EPS and FPS rates per model, see the [Cisco Security Monitoring, Analysis and Response System: Data Sheet](#). This datasheet also provides detailed technical specifications on the each appliance model, such as form factor, power consumption requirements, and disk type.

Supporting Devices

Supporting devices are network devices or hosts that provide network services used by MARS. The supporting devices, both optional and required, are listed in [Table 1-1](#) to help you plan your deployment.

Table 1-1 Supporting Devices and Their Role

Supporting Device Type	Is It Required?	Comment
E-mail Server	Yes	MARS uses e-mail servers to deliver administrative reports and notifications.
NTP Server	Not for single device deployment. Yes for any scenario involving a Global Controller.	You must specify the timezone and UTC settings on all appliances. The timestamps applied to received messages is critical to accurate incident correlation.
DNS Server	Yes	MARS uses DNS to resolve the hostnames for monitored devices, which improves the readability of reports and queries.
Internal Upgrade Server	No	For more information on configuring and using such a server, see Checklist for Upgrades of Appliance Software, page 5-3 .
GUI Client	Yes	This host is one from which you run the web interface that manages the appliance. See Web Browser Client Requirements, page 1-4 .

Required Traffic Flows

Required traffic flows identify traffic that must be allowed by gateways if they separate the MARS Appliance from a reporting device, mitigation device, or a supporting device (as listed in [Supporting Devices](#)). Also, traffic flows between a Global Controller and any monitored Local Controllers must be allowed.

The following table identifies categories of traffic flows, the protocols required, and how long they must be allowed:

Table 1-2 Required Traffic Flows and Ports

Category	Protocols	Allow Only As Needed?	Comments
Management GUI	HTTPS/SSL (TCP port 443)	No	You cannot effectively use the appliance and block GUI-based management traffic. This traffic must be enabled for Global Controller-to-Local Controller, as well as from the MARS Appliance to the computer you are using to manage the appliance.
Management CLI	SSH (TCP 22)	Yes	—

Table 1-2 Required Traffic Flows and Ports (continued)

Category	Protocols	Allow Only As Needed?	Comments
Support Servers and Services	DNS (TCP and UDP port 53) NTP (TCP/UDP port 123) SMTP (TCP port 25) ICMP (IP level service) NFS		SMTP is used for outgoing mail services. ICMP is useful for diagnostics and troubleshooting and is required by the dynamic vulnerability scanner. NFS is used for network-attached storage (NAS) servers to retain data archives for MARS. Because NFS ports are negotiated, it is recommended that the NAS server be located on the same network segment as the MARS Appliance.
Upgrade from GUI	HTTPS or FTP (TCP port 20 and 21)	Yes	Your options from within the GUI require that you
Upgrade from CLI	HTTPS, HTTP (TCP port 80), or FTP	Yes	At the command line, you can also upgrade from the DVD drive, which does not require any extra opened ports.
Discovery of reporting device or mitigation device	Telnet (TCP port 23) SSH FTP SNMP (TCP 161)	No	MARS Appliance periodically contacts the devices to ensure they are operational.
Monitoring of reporting device or mitigation device	HTTPS SSH SNMP Telnet FTP PostOffice (UDP port 45000) RDEP (SSL) SDEE (SSL) syslog (UDP port 514)	No	
Policy query to Cisco Security Manager	HTTPS	Yes	You must enable HTTPS access to the Common Services 3.0 server by the MARS Appliance..
Global Controller and Local Controller data synchronization.	Proprietary (port 8444)	No	This port must remain open on the outside and inside interfaces to ensure accurate data correlation operations of the Global Controller.

Table 1-2 Required Traffic Flows and Ports (continued)

Category	Protocols	Allow Only As Needed?	Comments
	NetFlow (TCP port 2055)		You must enable Spanning Trees between switches (distribution and access switch, not the core). You can change the port on which the appliance listens for NetFlow traffic on the Admin > NetFlow Config page.
	OPSEC-LEA (TCP port 18184) OPSEC-CA (TCP 18210) SSLCA (TCP port 18184) OPSEC-CPMI (TCP port 18190)		Used by Check Point devices only. CA is used for pulling a certificate for the OPSEC application.
	Oracle Database Listener (TCP port 1521)		Used by Oracle only
	MS SQL (TCP port 1433)		Used by FoundStone and eEye.

Web Browser Client Requirements

The MARS web interface should be accessed *only* from a browser instance that was used to login to MARS. Avoid using browser instances spawned from the original login instance (for example, a new browser window launched with **Ctrl+N**, **File>New>New Window**, or **right-click** {link on MARS GUI}>**Open in New Window**).

Before running the user interface provided by MARS, you must prepare Microsoft® Internet Explorer 6.0 SP1 or later or Internet Explorer 7.0 to connect to the MARS Appliance. This section describes the properly configured and patched web browser.

- Configure the Browser
 - [Configuring Internet Explorer 7.0, page 1-4](#)
 - [Configuring Internet Explorer Settings 6.x, page 1-5](#)
- [Configuring Pop-Up Blockers, page 1-9](#)
- [Correcting Issues Caused by the 832894 \(MS04-004\) Security Update or the 821814 Hotfix \(IE 6.x only\), page 1-10](#)
- [Obtaining the Required Browser Plug-ins, page 1-10](#)
- [Web Browser Client Usage Guidelines and Notes, page 1-11](#)

Configuring Internet Explorer 7.0

You can use Microsoft® Internet Explorer 7.0 or later to connect to and configure the MARS Appliance. To run it with the MARS, you must configure your browser as follows:

- Set the browser's cache to check the page every visit.
- Set security level to medium (at least) to enable ActiveX controls and scripting or add the MARS Appliance URL to the Trusted sites zone with its default settings.

- Set privacy to medium (at least) to enable cookies.
- Allow pop-ups from the MARS Appliance (disable pop-up blockers for the MARS Appliance).
- Pop-up blocker must be disabled.
- Obtain the required plug-ins. For details, see [Obtaining the Required Browser Plug-ins, page 1-10](#).

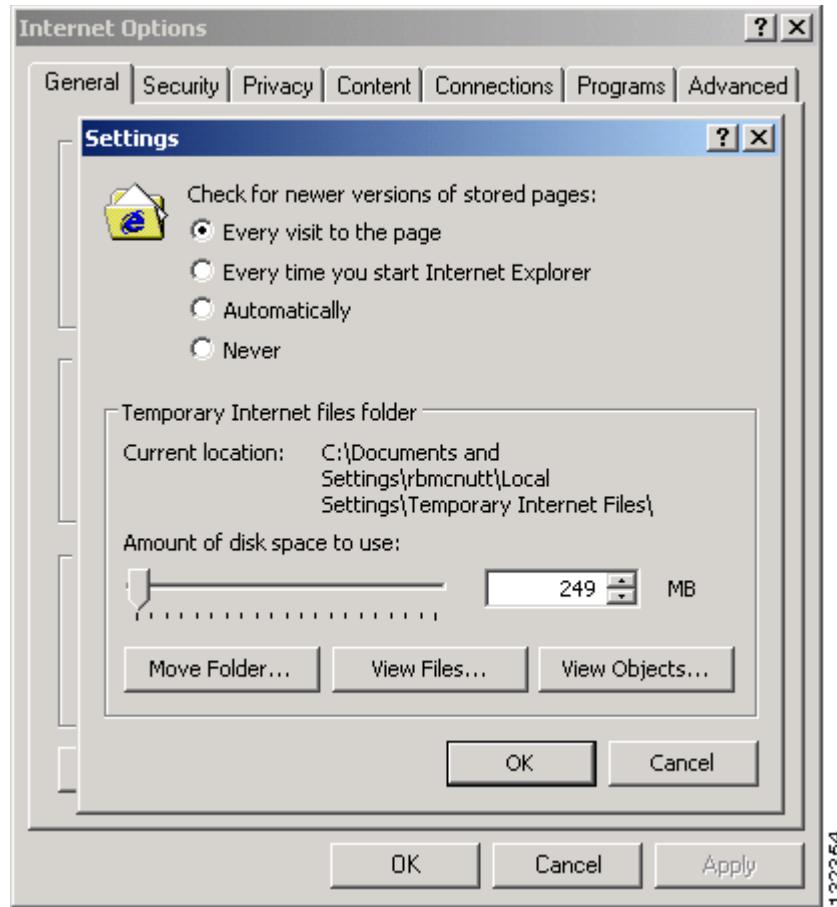
Configuring Internet Explorer Settings 6.x

You can use Microsoft® Internet Explorer 6.0 SP1 or later to connect to and configure the MARS Appliance. To run it with the MARS, you must configure your browser as follows:

- Set the browser's cache to check the page every visit.
- Set security level to medium (at least) to enable ActiveX controls and scripting or add to the Trusted sites zone with its default settings.
- Set privacy to medium (at least) to enable cookies.
- Allow pop-ups from the MARS Appliance (disable pop-up blockers for the MARS Appliance).

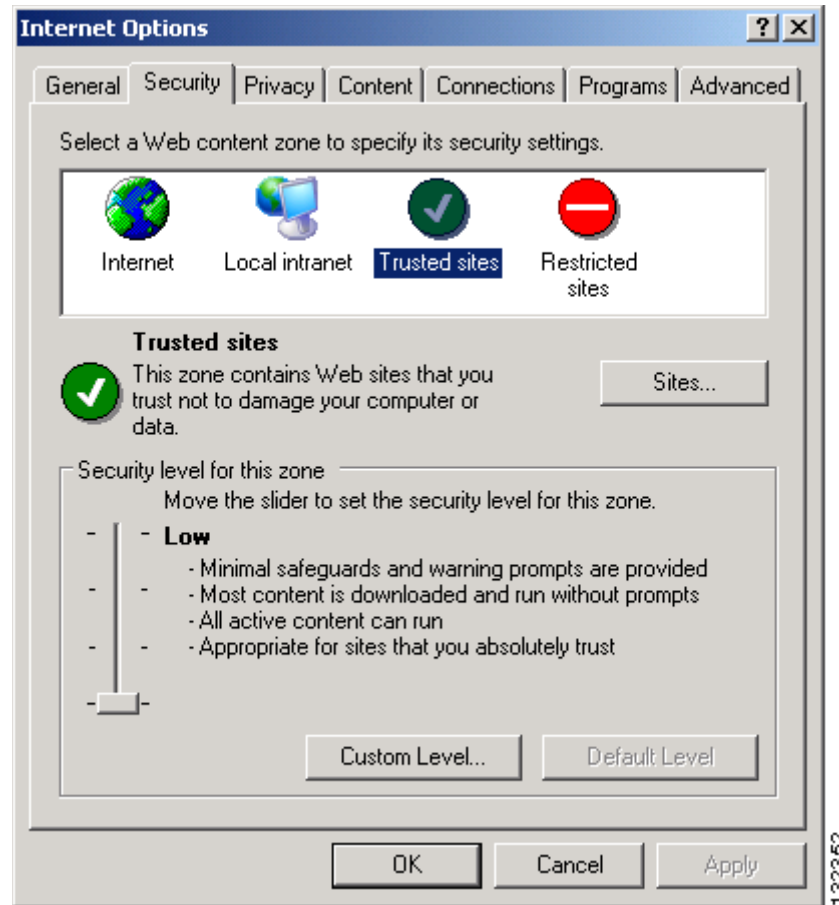
To configure Internet Explorer 6.x to meet these requirements, follow these steps:

-
- Step 1** Start Internet Explorer.
 - Step 2** Click **Tools > Internet Options**.
 - Step 3** On the General tab under Temporary Internet Settings, click **Settings**.

Figure 1-1 Internet Explorer Page Cache Settings

- Step 4** Click the **Every Visit to the Page** radio button.
- Step 5** Click **OK** to close the Settings dialog box and to save your changes.
- Step 6** On the Security tab under Select a Web content zone to specify its security settings, select **Trusted Sites**.

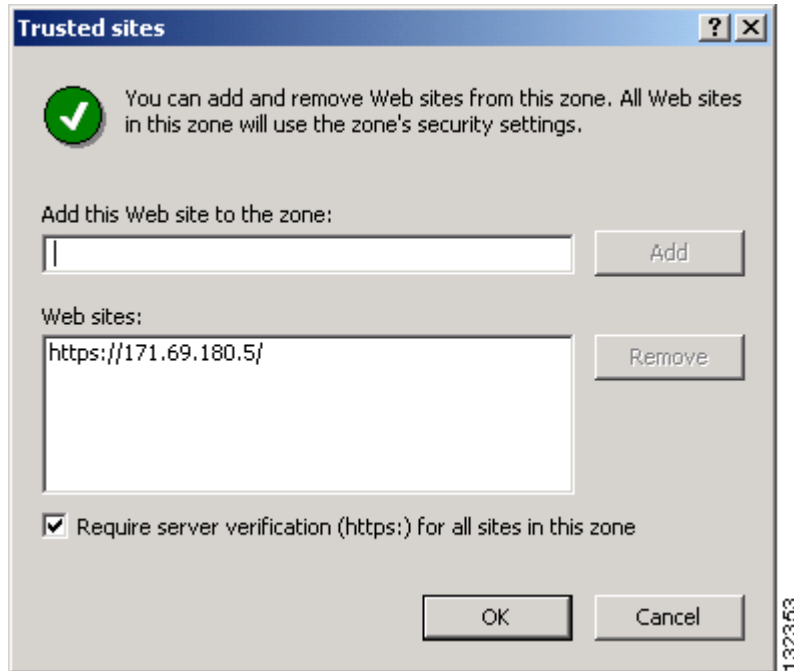
Figure 1-2 Internet Explorer Security Settings



The default security level settings for Trusted Sites is Low. If this value is not Low or Medium, use the Custom Level settings to ensure that ActiveX controls and scripting are allowed.

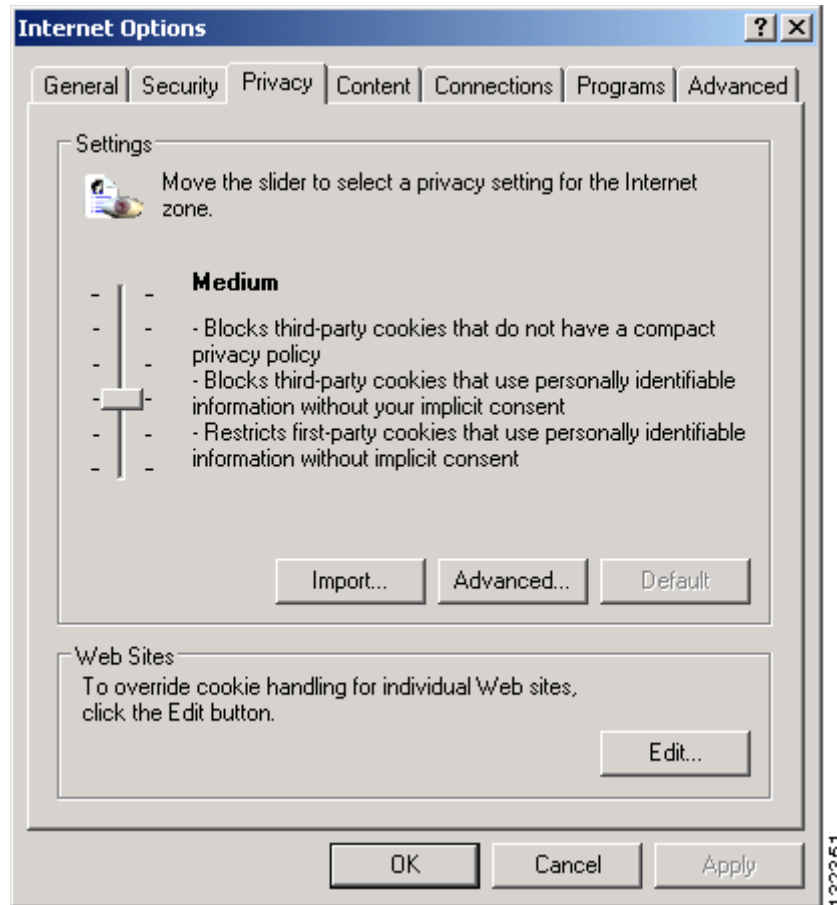
Step 7 With Trusted sites selected, click **Sites**.

Figure 1-3 Internet Explorer Trusted Sites



- Step 8** Enter the URL used to connect to the MARS Appliance in the Add this Web site to the zone box and click **Add**.
- Specify the full URL, preceded by `https://`; you can use either the DNS name or the IP address, such as `https://192.168.0.1/`, in the URL.
- Step 9** Click **OK** to close the Trusted sites dialog box and to save your changes.
- Step 10** On the Privacy tab under Settings, verify the selected value is **Medium**.

Figure 1-4 Internet Explorer Privacy Settings



If the selected value is not Medium, slide the bar to Medium or click Advanced to define custom settings that will enable first-party cookies.

Step 11 Click **Apply**.

Step 12 Click **OK** to close the Internet Options dialog box and to save your changes.

Configuring Pop-Up Blockers

This procedure describes how to allow access to the MARS Appliance for users running Windows XP SP2, which includes a pop-up blocker.

For information on configuring a different popup blocker to allow access to the MARS Appliance, refer to the documentation provided with the pop-up blocker product.

To enable pop-up for Internet Explorer running on Windows XP SP2, follow these steps:

Step 1 Click **Options > Toolbar Options** on the MSN toolbar.

Step 2 Select **Pop-up Blocker** under Toolbar.

In the Allow list box, enter the host ID of the MARS prefixed by https://. For example, `https://171.69.180.5/`.

**Note**

For later versions of the MSN Toolbar, you can access the Allow Lists tab by clicking the Popup Guard Settings button on Toolbar Buttons tab.

- Step 3** Click **Add** to add the host to the list of sites for which pop-ups are allowed.
- Step 4** Click **OK** to close the MSN Toolbar Options dialog box and to save your changes.

Correcting Issues Caused by the 832894 (MS04-004) Security Update or the 821814 Hotfix (IE 6.x only)

An issue introduced in one Internet Explorer security update, 832894, and in the 821814 hotfix can cause a “page cannot be displayed” error when you post to a site that requires authentication. If you have installed either of these updates, you must take corrective action to ensure proper operation with MARS. The following steps verify whether you have installed either update and points you to instructions provided by Microsoft to resolve the issue:

- Step 1** Start Internet Explorer.
- Step 2** Click **Help > About Internet Explorer**.
- Step 3** Under Updated Version, look for Q832894.
If the Q832894 entry appears, you have the IE bug installed.
- Step 4** If Q832894 entry appears, visit the Microsoft support web site to resolve the issue. The following knowledge base article provides specific instructions on resolving this issue:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;831167>

Obtaining the Required Browser Plug-ins

The following plug-ins are required for use with MARS:

- Adobe® SVG Viewer plug-in 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>
- Adobe Reader® to view the MARS documentation
You can download the latest Acrobat Reader plug-in from:
<http://www.adobe.com/products/acrobat/readermain.html>

Web Browser Client Usage Guidelines and Notes

Familiarize yourself with the following usage guidelines and notes before using the MARS web interface:

- Avoid using the Refresh, Back, and Forward buttons in the browser. Using these buttons can lead to unpredictable behavior.
- Some pages, such as the Summary page, automatically refresh. Other pages do not. If you are viewing a page that is not automatically refreshed, you will be logged out of the user interface after a period of inactivity.
- Do not open multiple instances of the browser under the same login session. In other words, do not perform any of the following actions when viewing a page in the MARS web interface:
 - Click **File > New > Window** on the menu bar of the browser.
 - Enter **Ctrl+N**.
 - Right-click a link on the page and select **Open in New Window** on the shortcut menu.

