



CHAPTER 19

Configuring Cisco Firewall Devices

Revised: July 31, 2008

This chapter describes how to bootstrap Cisco firewall devices and add them to MARS as reporting devices. Firewall devices come in several form factors: hardware appliances, software applications running on a host, modules that are installed in switches and routers, and modules that install in multifunction security devices.

Multifunction security devices, such as the Cisco Adaptive Security Appliance (ASA), also support non-firewall modules, such as intrusion detection or prevention systems (IDS/IPS) and Content Security and Control Security Services (CSC-SSM). This chapter does not focus on configuring non-firewalling modules. Instead, they are discussed in [Chapter 9, “Cisco IPS Modules”](#) and [Chapter 32, “Cisco CSC SSM”](#).

This chapter contains the following topics:

- [Cisco Firewall Devices \(PIX, ASA, and FWSM\), page 19-1](#)
- [Failover Considerations for PIX, ASA, and Modules in ASA, page 19-21](#)

Cisco Firewall Devices (PIX, ASA, and FWSM)

MARS support for Cisco firewall devices includes the following:

- PIX Security Appliance
- Cisco Adaptive Security Appliance (ASA)
- Cisco Firewall Services Modules (FWSM)

For the complete list of supported software releases by platform, refer to the latest [Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller](#) document.

Because this PIX software is mostly backward compatible, the commands required to bootstrap PIX security appliance remain consistent across the releases. In addition, Cisco ASA and FWSM have much in common with PIX command set.

The taskflow required to configure MARS to monitor a Cisco firewall device is as follows:

1. Configure the Cisco firewall device to accept administrative sessions from MARS (to discover settings).

For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types, you configure the admin context to accept these sessions.



Note To be monitored by MARS, the Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types have the following two requirements: each context requires a unique routable IP address for sending syslog messages to MARS, and each context must have a unique name (hostname+domain name).

2. Configure the Cisco firewall device to publish its syslog events to MARS.

For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types, you must configure the admin context and each security context.



Note MARS uses syslog events to discover information about the network topology. It uses SNMP to discover CPU utilization and related information.

3. Within MARS, define the Cisco firewall device by providing the administrative connection information.



Note Before you can add an FWSM module in a switch, you must add and configure the base module (the Cisco switch) in MARS. For more information, [Chapter 15, “Cisco Switch Devices”](#).

For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM, the basic device type represents the admin context. However you must also define or discover each security context and any installed Advanced Inspection and Prevention (AIP) modules running IPS 5.0.

To configure MARS to accept syslog event data and to pull device configurations settings from a Cisco firewall device, you must perform the following tasks:

- [Bootstrap the Cisco Firewall Device, page 19-2](#)
- [Add and Configure a Cisco Firewall Device in MARS, page 19-14](#)

Bootstrap the Cisco Firewall Device

You should configure your Cisco firewall devices to act as reporting devices and manual mitigation devices because they perform multiple roles on your network. MARS can benefit from the proper configuration of specific features:

- **IDS/IPS signature detection.** While it does not boast the most efficient or comprehensive set of signatures, the built-in IDS and IPS signature matching features of the Cisco firewall device can be critical in detecting an attempted attack.
- **Accept/Deny Logs.** The logging of accepted as well as denied sessions aids in false positive analysis.
- **Administrative Access.** Administrative access ensure MARS access to several key pieces of data:
 - *Route and ARP tables*, which aid in network discovery and MAC address mapping.
 - *NAT and PAT translation tables*, which aid in address resolution and attack path analysis, exposing the real instigator of attacks.
 - *OS Settings*, from which MARS determines the correct ACLs to block detected attacks, which paste into a management session with the Cisco firewall device.

To bootstrap the Cisco firewall device, you must identify the MARS Appliance as an administrative host. Enabling administrative access allows MARS to discover the Cisco firewall device configuration settings. To enable administrative access, you must make sure that the MARS Appliance is granted Telnet or SSH administrative access to the firewall device. If you use FTP access type, make sure that you have added its configuration file to an FTP server to allow MARS access to the FTP server.

In addition to configuring specific event types and administrative access, syslog messages should be sent to the MARS Appliance. To prepare the Cisco firewall device to send these messages to the MARS Appliance, you must configure the logging settings associated with each firewall device on your network. To prepare a firewall device to generate the syslog messages and direct them to a specific MARS Appliance, you must:

1. Enable logging on the firewall device.

Before a firewall device can generate syslog messages, you must enable logging for one or more interfaces. In addition, if you configured your firewall device in a failover pair, you can specify the standby firewall device to generate syslog messages as well. You can enable the device to ensure that the standby unit's syslog messages stay synchronized if failover occurs. However, this option results in twice as much traffic on the MARS Appliance.

2. Select the log facility and queue size.

To generate meaningful reports about the network activity of a firewall device and to monitor the security events associated with that device, you must select the appropriate logging level. The logging level generates the syslog details required to track session-specific data. After you select a logging level, you can define a syslog rule that directs traffic to the MARS Appliance.

3. Do one of the following:

- Select the log level to debug, or
- Change the severity level of required events to a level other than debug and select that log level.

The debug log level generates syslog messages that assist you in debugging. It also generates logs that identify the commands issued during FTP sessions and the URLs requested during HTTP sessions. It includes all emergency, alert, critical, error, warning, notification, and information messages. Alternatively, you can change the severity level of the required messages using the **logging message** command described in [Device-Side Tuning for Cisco Firewall Device Syslogs](#), page 19-6.



Note Full URLs, such as `www.cisco.com/foo.html`, are included in HTTP session logs and FTP command data is logged only if web filtering (N2H2\SecureComputing or WebSense) is enabled on the reporting device. If web filtering is not enabled, then the HTTP session log does not include the hostname (although the destination host's IP and the Request-URI are included, such as `192.168.1.1:/foo.htm`) and FTP command data is not logged at all. Caveats exist with HTTP session logging, such as if the HTTP session request is broken across packets, then the hostname data might not be included in the log data.

4. Identify the target MARS Appliance and the protocol and port pair that it listens on.

By directing syslog messages generated by a firewall device to MARS, you can process and study the messages.

**Tip**

When monitoring a failover pair of Cisco firewall devices, you should designate the primary Cisco firewall device as the device to be monitored. If failover occurs, the secondary device assumes the IP address of the primary, which ensures that session correlation is maintained after the failover. The same focus on the primary is true for performing any bootstrap operations. The secondary device will synchronize with the configuration settings of the primary.

To enable administrative connections to the firewall device, select from the following options:

- [Enable Telnet Access on a Cisco Firewall Device, page 19-4](#)
- [Enable SSH Access on a Cisco Firewall Device, page 19-4](#)
- [Send Syslog Files From Cisco Firewall Device to MARS, page 19-4](#)

To configure log settings, see [Send Syslog Files From Cisco Firewall Device to MARS, page 19-4](#).

Enable Telnet Access on a Cisco Firewall Device

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 Enter the command:

```
telnet <MARS IP address> <netmask of MARS IP address> <interface name>
```

where *interface name* can be inside, outside, DMZ.

Enable SSH Access on a Cisco Firewall Device

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 Enter the command:

```
ssh <MARS IP address> <netmask of the MARS IP address> <interface name>
```

where *interface name* can be inside, outside, DMZ.

Send Syslog Files From Cisco Firewall Device to MARS

To send syslog messages to the MARS Appliance, you must enable logging, select the log facility and queue size, and specify the log level to debug.

Before You Begin

When preparing a Cisco firewall device to publish syslog messages, consider the following restrictions:

- In releases prior to 4.2.1, do not customize the priority of any syslog messages. If you do, MARS fails to parse those messages.
- **Do not** configure EMBLEM format for syslog messages. Make sure that the format EMBLEM extension is not used on the following command in the configuration:

```
logging host <interface name> <PN-MARS's IP address> format EMBLEM
```

To configure the firewall device to forward syslog message to MARS, follow these steps:

-
- Step 1** Log in to the Cisco firewall device with administrator's privileges.
- Step 2** To enable logging, enter one of the following commands:
- (PIX and Cisco ASA) **logging enable**
 - (FWSM) **logging on**
- Step 3** To specify the MARS Appliance as a target logging host, enter the following command:
- ```
logging host <interface name> <MARS IP address>
```
- Step 4** To set the log level to debug, which ensures that HTTP and FTP session logs are generated, enter the following command:
- ```
logging trap debugging
```



Tip Alternatively, you can tune the event settings as defined in [Device-Side Tuning for Cisco Firewall Device Syslogs](#), page 19-6.

The debug messages contain the HTTP URL address information. Therefore, you can create keyword-based rules matching against the firewall message itself. For example, if the debug messages are enabled and users were logging to “http://mail.cisco.com”, you could create keyword-based rules that matched against “mail.yahoo.com.”



Note Full URLs, such as `www.cisco.com/foo.html`, are included in HTTP session logs and FTP command data is logged only if web filtering (N2H2\SecureComputing or WebSense) is enabled on the reporting device. If web filtering is not enabled, then the HTTP session log does not include the hostname (although the destination host's IP and the Request-URI are included, such as `192.168.1.1:/foo.htm`) and FTP command data is not logged at all. Caveats exist with HTTP session logging, such as if the HTTP session request is broken across packets, then the hostname data might not be included in the log data.

Debug messages are also preferred for troubleshooting. You can define inspection rules that match on on debug-level keywords, which send notifications to the appropriate group. Refer to PIX debug messages for interesting keywords.

Cisco recommends enabling debug for optimal use of your STM solution. If a Cisco firewall device is unable to sustain debug-level messages due to performance reasons, the informational level should be used. In non-debug mode, the URL information is not available; only the 5 tuple is available for queries and reports.

- Step 5** For FWSM, enter the following command:
- ```
logging rate-limit <eps rate desired> 1
```
- Step 6** For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM, repeat [Step 2](#) through [Step 5](#) for each context defined, admin and security.
- Step 7** (Cisco ASA only) If an Advanced Inspection and Prevention (AIP) module is installed, you need to prepare that module as you would any IPS 5.0 module. For more information, see [Chapter 9, “Cisco IPS Modules”](#).
-

## Device-Side Tuning for Cisco Firewall Device Syslogs

The default level for many of the events that are studied by MARS is the debug level, which can generate a high volume of additional events that are not used by MARS. If you are experiencing an influx of these other events, you can use the **logging message** command to either turn off events or change the severity level of the event to a level that generates required messages but not as many as debug.

This topic identifies the commands to use to change the log level from the command line, as well as identifies those messages consumed by MARS and their default severity level.

### Logging Message Command

The following references provide details for using the **logging message** command on the appropriate firewall device:

#### Cisco ASA and Cisco PIX

- “Changing the Severity Level of a System Log Message” in *Cisco Security Appliance Command Line Configuration Guide, Version 7.2*  
<http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/monitor.html#wp1065731>
- “Disabling a System Log Message” in *Cisco Security Appliance Command Line Configuration Guide, Version 7.2*  
<http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/monitor.html#wp1065706>
- “Logging Message Command” in *Cisco Security Appliance System Log Messages, Version 7.2*  
[http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/l2\\_72.html#wp1689570](http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/l2_72.html#wp1689570)
- *Cisco Security Appliance System Log Messages, Version 7.2*  
<http://www.cisco.com/en/US/docs/security/asa/asa72/system/message/logmsgs.html>

#### Cisco FWSM

- “Changing the Severity Level of a System Log Message” in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1*  
[http://www.cisco.com/en/US/docs/security/fwsm/fws32/configuration/guide/monitr\\_f.html#wp1099894](http://www.cisco.com/en/US/docs/security/fwsm/fws32/configuration/guide/monitr_f.html#wp1099894)
- “Disabling a System Log Message” in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1*  
[http://www.cisco.com/en/US/docs/security/fwsm/fws31/configuration/guide/monitr\\_f.html#wp1099869](http://www.cisco.com/en/US/docs/security/fwsm/fws31/configuration/guide/monitr_f.html#wp1099869)
- “Logging Message Command” in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference, 3.1*  
<http://www.cisco.com/en/US/docs/security/fwsm/fws31/command/reference/l2.html#wp1565791>
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages, 3.1*  
[http://www.cisco.com/en/US/docs/security/fwsm/fws31/system/message/fws\\_log.html](http://www.cisco.com/en/US/docs/security/fwsm/fws31/system/message/fws_log.html)

## List of Cisco Firewall Message Events Processed by MARS

The following list of events are processed by MARS. By changing the severity level for these events to ensure they are within the logging level you have selected, you can typically reduce the load on your firewall logging by 5-15%. However, the primary consumer of resources will remain the session detail events, which are processed and analyzed by MARS.

Starting with MARS version, the system can correctly parse syslogs at customized logging levels. Therefore, you can move the syslogs processed by MARS to a lower level and then set the log to that level, for example *logging level 6*. Use the command **logging message message-id level level** on the ASA, or PIX, to move a syslog message to a new level.

The following syslog message IDs are those required for proper sessionization. If you change the logging level of the firewall, ensure that the following messages IDs are generated at the new level so the MARS Appliance receives them.

**Note**

The syslog message IDs listed below are required for sessionization. However, other logs at the debug or informational levels may exist that you may require for other purposes. For example, a specific URL accessed by one user if you are doing URL filtering on the security appliance. Refer to the [Logging Message Command, page 19-6](#) for pointers to the full message list for each firewall device type.

- 101001-101005
- 102001
- 103001-103007
- 104001-104004
- 105001-105011
- 105020-105021
- 105031-105032
- 105034-105040
- 105042-105048
- 106001-106002
- 106006-106007
- 106010-106027
- 106100-106101
- 107001-107003
- 108002-108003
- 108005
- 108007
- 109001-109003
- 109005-109008
- 109010-109014
- 109016-109034
- 110001-110003
- 111001

- 111003-111005
- 111007-111009
- 111111
- 112001
- 113001
- 113003-113023
- 114001-114021
- 199001-199003
- 199005-199009
- 199011
- 199012
- 199907-199908
- 201002-201006
- 201008-201013
- 202001
- 202005
- 202011
- 208005
- 209003-209005
- 210001-210003
- 210005-210008
- 210010
- 210020-210022
- 211001
- 211003
- 212001-212006
- 213001-213006
- 214001
- 215001
- 216003
- 216004
- 217001
- 218001-218004
- 219002
- 302001
- 302003-302004
- 302007-302010
- 302012-302023

- 302033
- 302034
- 302302
- 303002-303005
- 304001-304009
- 305005-305012
- 308001-308002
- 311001-311004
- 312001
- 313001
- 313003-313005
- 313008
- 314001-314006
- 315004
- 315011
- 316001
- 316002
- 317001-317006
- 318001-318009
- 319001-319004
- 320001
- 321001-321004
- 322001-322004
- 323001-323006
- 324000-324007
- 324300-324301
- 325001-325003
- 326001-326002
- 326004-326017
- 326019-326028
- 327001-327003
- 328001
- 329001
- 331001-331002
- 332001-332004
- 333001-333010
- 334001-334009
- 335001-335014

- 336001-336011
- 400000-400050
- 401001-401005
- 402101-402103
- 402106
- 402114-402120
- 402121-402127
- 403101-403104
- 403106-403110
- 403500-403507
- 404101-404102
- 405001-405002
- 405101-405107
- 405201
- 405300-405301
- 406001-406002
- 407001-407003
- 408001-408003
- 409001-409013
- 409023
- 410001-410004
- 411001-411004
- 412001-412002
- 413001-413006
- 414001-414002
- 415001-415020
- 416001
- 417001
- 417004
- 417006
- 417008-417009
- 418001
- 419001-419002
- 420001-420006
- 421001-421007
- 422004-422006
- 423001-423005
- 424001-424002

- 425001-425006
- 428001
- 431001-431002
- 446001
- 450001
- 500001-500004
- 501101
- 502101-502103
- 502111-502112
- 503001
- 504001-504002
- 505001-505016
- 506001
- 507001-507002
- 508001-508002
- 509001
- 602101-602104
- 602201-602203
- 602301-602304
- 603101-603109
- 604101-604104
- 605004-605005
- 606001-606004
- 607001-607002
- 608001-608005
- 609001-609002
- 610001-610002
- 610101
- 611101-611104
- 611301-611323
- 612001-612003
- 613001-613003
- 614001-614002
- 615001-615002
- 616001
- 617001-617004
- 620001-620002
- 621001-621003

- 621006-621010
- 622001
- 622101-622102
- 634001
- 701001-701002
- 702201-702212
- 702301-702303
- 702305
- 702307
- 703001-703002
- 709001-709007
- 710001-710006
- 711001-711002
- 713004
- 713006
- 713008-713010
- 713012
- 713014
- 713016-713018
- 713020
- 713022
- 713024-713037
- 713039-713043
- 713047-713052
- 713056
- 713059-713063
- 713065-713066
- 713068
- 713072-713076
- 713078
- 713081-713086
- 713088
- 713092
- 713094
- 713098-713099
- 713102-713105
- 713107
- 713109

- 713112-713124
- 713127-713149
- 713152
- 713154-713172
- 713174
- 713176-713179
- 713182
- 713184-713187
- 713189-713190
- 713193-713199
- 713203-713206
- 713208-713226
- 713228-713251
- 713254
- 713900-713906
- 714001-714007
- 714011
- 715001
- 715004-715009
- 715013
- 715019-715022
- 715027-715028
- 715033-715042
- 715044-715072
- 715074-715079
- 716001-716056
- 717001-717049
- 718001-718081
- 718082-718088
- 719001-719026
- 720001-720073
- 721001-721019
- 722001-722041
- 723001-723014
- 724001-724002
- 725001-725015
- 726001
- 730001

- 730002-730005
- 730010
- 731001-731003
- 732001-732003
- 733100
- 733102
- 733103
- 734002-734004

## Add and Configure a Cisco Firewall Device in MARS

The process of adding a PIX security appliance, Cisco ASA, or FWSM to MARS involves many of the same steps, regardless of the version of software that is running. The process is exactly the same for PIX software versions 6.0, 6.1, 6.2, and 6.3. However, Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM provide the ability to define multiple security contexts, or virtual firewalls.

Adding a Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM to MARS has two distinct steps. First, you must define the settings for the admin context. Then, if multiple context mode is enabled, you define or discover the settings for its security contexts. These Cisco firewall device have two type of contexts: one admin context, which is used for configuration of the device itself, and one or more security contexts. For Cisco ASA, you can also define or discover any modules that are installed in the appliance.

To be monitored by MARS, the Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types have the following additional requirements:

- each context requires a unique routable IP address for sending syslog messages to MARS
- each context must have a unique name (hostname+ domain name)



### Note

The Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM can run in single context mode, which means that the system context acts as both the admin context and a security context.

To add and configure a Cisco firewall device, follow these steps:

### Step 1

Do one of the following:

- If you are adding an FWSM, you must be on the main page of the Cisco switch to which you are adding it. On that page, click **Add Module**, and select one of the following options from the Device Type list:
  - Cisco FWSM 1.1
  - Cisco FWSM 2.2
  - Cisco FWSM 2.3
  - Cisco FWSM 3.1
  - Cisco FWSM 3.2
- If you are adding a PIX security appliance or a Cisco ASA, an Select **Admin > System Setup > Security and Monitor Devices > Add**, and select one of the following options from the Device Type list:

- Cisco ASA 7.0
- Cisco ASA 7.2
- Cisco ASA 8.0
- Cisco PIX 6.0
- Cisco PIX 6.1
- Cisco PIX 6.2
- Cisco PIX 6.3
- Cisco PIX 7.0
- Cisco PIX 7.2
- Cisco PIX 8.0

Device Type:

|                    |                                                                    |
|--------------------|--------------------------------------------------------------------|
| → *Device Name:    | <input type="text" value="Admin"/>                                 |
| → *Access IP:      | <input type="text" value="10.1.1.23"/>                             |
| → *Reporting IP:   | <input type="text" value="10.1.1.23"/>                             |
| → *Access Type:    | <input type="text" value="SSH"/> <input type="text" value="3DES"/> |
| Login:             | <input type="text" value="pix"/>                                   |
| Password:          | <input type="password" value="....."/>                             |
| Enable Password:   | <input type="password" value="....."/>                             |
| Config Path:       | <input type="text"/>                                               |
| File Name:         | <input type="text"/>                                               |
| SNMP RO Community: | <input type="text" value="public"/>                                |

143178

**Step 2** Enter the name of the firewall device in the Device Name field.

MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and in the Security and Monitoring Device list. For devices that support the discovery operation, such as routers and firewalls, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the *hostname.domain* format. For devices that cannot be discovered, such as Windows and Linux hosts and host applications, MARS uses the provided value.

**Step 3** (Optional) To enable MARS to discover settings from this firewall device, enter the administrative IP address in the Access IP field.



**Note** If the device is running Cisco ASA, PIX 7.0, 7.2, and 8.0, or FWSM, this address corresponds to IP address from which the syslog messages of the admin context are sent.

To learn more about the access IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

**Step 4** Enter the IP address of the interface that publishes syslog messages or SNMP notifications, or both in the Reporting IP field.




---

**Note** If the device is running Cisco ASA, PIX 7.0, 7.2, and 8.0, or FWSM, this address corresponds to the address from which the admin context syslog messages are published.

---

To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings](#), page 1-10.

**Step 5** If you entered an address in the Access IP field, select **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- [Configure Telnet Access for Devices in MARS](#), page 1-13
- [Configure SSH Access for Devices in MARS](#), page 1-13
- [Configure FTP Access for Devices in MARS](#), page 1-14




---

**Note** If you select the FTP access type and you are defining a Cisco ASA, PIX 7.0, 7.2, and 8.0, or FWSM, you cannot discover the non-admin context settings. Therefore, this access type is not recommended.

---

For more information on determining the access type, see [Selection of the Access Type](#), page 1-11.

**Step 6** (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the device's read-only community string in the SNMP RO Community field.

Before you can specify the SNMP RO string, you must define an access IP address. MARS uses the SNMP RO string to read MIBs related to a reporting device's CPU usage, network usage, and device anomaly data and to discover device and network settings.

**Step 7** (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see [Configuring Resource Usage Data](#), page 1-21.

**Step 8** (Cisco ASA, FWSM, and PIX 7.0, 7.2, and 8.0 Only) do one of the following:

- Click **Discover** to let MARS contact the device and conduct a topology and context configuration discovery. Information about the security contexts is presented in the Context section of the main page. To edit discovered contexts, continue with [Edit Discovered Security Contexts](#), page 19-20.
- Click **Next** to commit your changes and allow for manual definition of security contexts or modules. Continue with [Add Security Contexts Manually](#), page 19-17, [Add Discovered Contexts](#), page 19-19, or [Add an IPS Module to a Cisco Switch or Cisco ASA](#), page 9-2.

For PIX and FWSM, you can add one or more security contexts. For Cisco ASA, you can add one or more security contexts or Advanced Inspection and Prevention (AIP) modules, running the Cisco IPS 5.x software.

Device Type: Cisco PIX 7.0

|                    |                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|
| → *Device Name:    | <input type="text" value="Admin"/>                                                                                            |
| → *Access IP:      | <input type="text" value="10"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="23"/> |
| → *Reporting IP:   | <input type="text" value="10"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="23"/> |
| → *Access Type:    | <input type="text" value="SSH"/> <input type="text" value="3DES"/>                                                            |
| Login:             | <input type="text" value="pix"/>                                                                                              |
| Password:          | <input type="password" value="....."/>                                                                                        |
| Enable Password:   | <input type="password" value="....."/>                                                                                        |
| Config Path:       | <input type="text"/>                                                                                                          |
| File Name:         | <input type="text"/>                                                                                                          |
| SNMP RO Community: | <input type="text" value="public"/>                                                                                           |

  

|                                            |                                             |                                               |                                                      |
|--------------------------------------------|---------------------------------------------|-----------------------------------------------|------------------------------------------------------|
| <input type="button" value="Add Context"/> | <input type="button" value="Edit Context"/> | <input type="button" value="Remove Context"/> | <input type="button" value="Add Available Context"/> |
|--------------------------------------------|---------------------------------------------|-----------------------------------------------|------------------------------------------------------|

  

|                                     |                                         |                                       |
|-------------------------------------|-----------------------------------------|---------------------------------------|
| <input type="button" value="Back"/> | <input type="button" value="Discover"/> | <input type="button" value="Submit"/> |
|-------------------------------------|-----------------------------------------|---------------------------------------|

143182

**Step 9** (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings, including any security contexts and their settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the “Discovery is done.” dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see [Scheduling Topology Updates, page 1-18](#).

**Step 10** To add this device to the MARS database, click **Submit**.

The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

**Step 11** Click **Activate**.

MARS begins to sessionize events generated by this device and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see [Activate the Reporting and Mitigation Devices, page 1-15](#).

## Add Security Contexts Manually

You can manually define security contexts in PIX 7.0, 7.2, and 8.0, Cisco ASA, or FWSM.

**Step 1** Do one of the following:

- (PIX 7.0, 7.2, and 8.0 and FWSM) Click **Add Context**.
- (Cisco ASA) Click **Add Module**.

Device Type: Cisco PIX 7.0 ▼

→ \*Device Name:

→ \*Context Name:

→ \*Reporting IP:

SNMP RO Community:

Discover
Cancel
Submit

143179

**Step 2** In the Device Type list, do one of the following:

- For Cisco ASA, select **Cisco ASA 7.0**, **Cisco ASA 8.0**, or **Cisco ASA 8.1**.
- For PIX, select **Cisco PIX 7.0**, **Cisco PIX 7.2**, or **Cisco PIX 8.0**.
- For FWSM, select **Cisco FWSM x.y**, where *x.y* is the version number of the software running on the module.

**Step 3** Enter the name of the firewall device in the Device Name field.

MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and in the Security and Monitoring Device list. For devices that support the discovery operation, such as routers and firewalls, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the *hostname.domain* format. For devices that cannot be discovered, such as Windows and Linux hosts and host applications, MARS uses the provided value.

**Step 4** Enter the name of the security context in the Context Name field.

This name must exactly match the context name defined on the device.

**Step 5** Enter the IP address of the security context from which syslog messages or SNMP notifications, or both are published in the Reporting IP field.

To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

**Step 6** (Optional) To enable MARS to retrieve MIB objects for this security context, enter the device's read-only community string in the SNMP RO Community field.

Before you can specify the SNMP RO string, you must define an access IP address. MARS uses the SNMP RO string to read MIBs related to a security context's CPU usage, network usage, and device anomaly data and to discover device and network settings.

**Step 7** To discover the settings of the defined context click **Discover**.

This discovery collects all of the route, NAT, and ACL-related information. In addition, the name of the device may change to the *hostname.domain* format if it was not already entered as such.

**Step 8** To save your changes, click **Submit**.

## Add Discovered Contexts

When you select Discover on a Cisco ASA, PIX 7.0, 7.2, and 8.0 or FWSM, MARS discovers the contexts that are defined for that firewall device. However, you must still manually add discovered contents.



### Note

You cannot discover a module install in a Cisco ASA; you must manually define IPS modules. However, the discovered contexts do appear under the Module area on the main page.

**Step 1** Do one of the following:

- (PIX 7.0, 7.2, and 8.0 and FWSM) Click **Add Available Context**.
- (Cisco ASA) Click **Add Available Module**.

| Module Name                          | Module Type   |
|--------------------------------------|---------------|
| <input type="checkbox"/> asa context | Cisco ASA 7.0 |
| <input type="checkbox"/> ips context | Cisco IPS 5.x |

143173

**Step 2** Select a security context from the Select list.

143174

**Step 3** Click **Add**.

**Step 4** Repeat for other contexts.

**Step 5** To save your changes, click **Submit**.

After you add discovered contexts, you must edit them to provide the contact information required by MARS. Continue with [Edit Discovered Security Contexts](#), page 19-20.

## Edit Discovered Security Contexts


**Note**

You must edit all discovered contexts to specify the reporting IP address and the SNMP RO community string.

**Step 1** From the list of discovered contexts, select the one that you want to edit and select the action appropriate to the device type:

- (PIX 7.0, 7.2, and 8.0) Click **Edit Context**.
- (Cisco ASA and FWSM) Click **Edit Module**.

Device Type: Cisco ASA 7.0

|                    |                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------|
| → *Device Name:    | <input type="text" value="qa.protegonetworks.co"/>                                                                           |
| → *Context Name:   | <input type="text" value="qa"/>                                                                                              |
| → *Reporting IP:   | <input type="text" value="10"/> <input type="text" value="4"/> <input type="text" value="2"/> <input type="text" value="9"/> |
| SNMP RO Community: | <input type="text" value="public"/>                                                                                          |




143211

**Step 2** Enter the IP address from which the syslog messages of the security context are sent in the Reporting IP field.

**Step 3** (Optional) To enable MARS to retrieve MIB objects for this context, enter the device's read-only community string in the SNMP RO Community field.

Before you can specify the SNMP RO string, you must define an access IP address. MARS uses the SNMP RO string to read MIBs related to a reporting device's CPU usage, network usage, and device anomaly data and to discover device and network settings.

**Step 4** (Optional) To enable MARS to monitor this context for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see [Configuring Resource Usage Data, page 1-21](#).

**Step 5** To save your changes, click **Submit**.

**Step 6** Repeat for each discovered context.

## Failover Considerations for PIX, ASA, and Modules in ASA

When monitoring a failover pair of Cisco firewall devices (PIX or ASA), you should designate the primary Cisco firewall device as the device to be monitored. If failover occurs, the secondary device assumes the IP address of the primary, which ensures that session correlation is maintained after the failover. The same focus on the primary is true for performing any bootstrap operations. The secondary device will synchronize with the configuration settings of the primary.

While this is true for the actual firewalls, it is not true for AIP-SSM modules. AIP-SSM modules do not swap IP addresses in the event of a failover. Therefore, to ensure that MARS receives uninterrupted IPS event data, you must configure both the primary and secondary AIP-SSM modules as child modules of the same ASA device that represents the Active/Standby pair. In this configuration, MARS will likely generate "Inactive Reporting Device" messages on the hour for the non-active AIP-SSM module.

