



CHAPTER 21

Check Point Devices

The Check Point security product family can be distributed and tiered. As such, you must understand the deployment method, components, and release versions of this product family, their relationships, and how MARS interacts with them. You must also understand the many acronyms and abbreviations associated with this product family. [Table 21-1](#) lists the abbreviations and acronyms used in the topics that follow.

Table 21-1 Check Point Abbreviations and Acronyms

Abbreviation	Expansion	Additional Information
ASYMSSLCA	Secure Sockets Layer Certificate Authority using an asymmetric key cipher	Communications protocol used for establishing secure sessions.
CLM	Customer Log Modules	Standalone log server for collecting log data from the Check Point enforcement modules.
CMA	Customer Management Add-ons	A a virtual instance of SmartCenter and only exists within the context of a Provide-1/SiteManager-1 infrastructure.
CPMI	Check Point Management Interface	Communications protocol used for configuration discovery.
LEA	Log Export API	Communications protocol used for retrieving audit and firewall logs.
MDG	Multi Domain GUI	GUI used for managing Provider-1/ SiteManager-1 deployments. The MDG is the parent GUI that can launch specific SmartDashboard GUIs for a CMA.
MDS	Multi Domain Server	Is the umbrella manager for the CMA instances in a Provider-1/SiteManager-1 deployment.

Table 21-1 Check Point Abbreviations and Acronyms (Continued)

MLM	Multi Domain Log Module	Usually found in Provider-1/ SiteManager-1 deployments and provides the ability to create multiple instances of a CLM on a single logging server.
NG AI	Next Generation with Application Intelligence	All current trains of Check Point are released under the NG AI umbrella with specific release numbers, such as NG AI R55 and NG AI R60.
NG FP3	Next Generation Feature Pack 3	—
NGX	Next Generation eXtension	NGX is also NG AI R60
OPSEC	Open Platform for Security	An alliance, certification and integration methodology for products and solutions that integrate into a Check Point infrastructure.
P-1	Check Point Provider-1	—
SSLCA	Secure Sockets Layer Certificate Authority, using a symmetric key cipher (protocol)	—
SIC	Secure Internal Communication	—
SIC DN	SIC Distinguished Name	—
VIPs	Virtual IP Addresses	Usually used in a Provider-1/ SiteManager-1 deployment to assign unique IP addresses for CMA instances.
VPN-1	Check Point VPN-1 Pro and Edge	VPN-1 Pro is the Check Point enforcement gateway that does the inspection, firewalling, VPN encryption and QoS tagging. VPN-1 Edge is treated as a normal enforcement point.

To understand what MARS supports, we must first clarify the product terminology used by Check Point. NG refers to the 5.x product family, and it included three feature packs: FP1, FP2, and FP3. NG is different from NG AI in that NG AI improved upon, and renamed, the SmartDefense feature set that was introduced in NG FP2. NG AI also provides a larger number of application-aware inspections,; hence the name Application Intelligence. NG AI included releases R54 and R55. NGX refers to the 6.x product family and began with the R60 release.

MARS supports and has been tested with the following releases:

- NG FP3
- NG AI (R55)
- NGX (R60)

The different security platforms, Provider-1, SiteManager-1, SmartCenter, and SmartCenter Pro are bundles of the technologies released under the NG, NG AI, and NGX release trains. From this perspective, MARS works with any of the security platforms as long as it belongs to one of the supported release trains.

Check Point Provider-1 is a security management system for the managed security service providers (MSSP) and multi-site enterprises, respectively. Service providers are able to manage the Check Point gateways (firewall and VPN gateways) on their customer sites. The security policies and the system configurations are stored on the MDS. Each per-customer security policy is managed through a CMA, which also reside on the MDS. The Provider-1 system allows the service provider and the end customers to maintain separate log servers, using the MLM and CLM respectively. The user interface for Provider-1 is called the MDG. This system also supports a tiered fault-tolerant configuration via redundancy at the gateway, CMA, or MDS level.

The Provider-1 system ensures secure and private communication between its components and Check Point gateways. Each CMA has its own internal certificate authority that issues certificates for secure communication between the CMA, log servers, and its own network. All communication between MDSs is authenticated and secured, and every MDS communicates securely with the CMAs that it houses.

The SiteManager-1 system operates much the same as Provider-1; however, it is targeted toward large enterprise customers. The Check Point components are the same as those found in Provider-1.

SmartCenter and SmartCenter Pro are security management systems also targeted toward enterprise customers. They can support the Provider-1 system, serving as a backup server at the CMA level. However, their primary function is to provide centralized security and VPN policy and security event management through SmartDashboard, which is the user interface for both systems. From the MARS perspective, SmartCenter has the ability to extend the view of the network by managing the policies and events associated with gateway and desktop nodes:

- VPN-1 perimeter security gateways,
- InterSpect internal security gateways
- Connectra Web security gateways
- SecureClient, a personal firewall running on desktops and servers.

MARS monitors the primary management servers, such as the MDS in Provider-1 and SiteManager-1 and the SmartCenter Server in SmartCenter and SmartCenter Pro. These management servers are where the actual security and audit policies are centrally managed and stored. If the Check Point deployment requires, MARS also monitors those components managed by the management stations, such as individual firewalls, VPN gateways, and log servers. Whether you configure MARS to monitor these remote components depends on whether their security event logs are propagated to the centralized management servers (SmartCenter or CMA). If the logs are not forwarded to the primary management server, then you must define where the log repository exists, whether local to the enforcement module, or forwarded to a separate logging module (CLM).

In addition to understanding the components, it is important to understand how Check Point components use Secure Internal Communications (SIC) to securely communicate with each other and with third-party OPSEC applications. SIC is the process by which MARS Appliance authenticates to the SmartCenter Server and other Check Point components. SIC uses a shared secret as the seed for negotiating session keys. This shared secret is referred to as an activation key. The authentication and communication setup works as follows:

1. Using a username and password pair, MARS authenticates to the SmartCenter Server and other Check Point components, such as remote log servers, using TCP port 18210.
2. If authenticated, the peers swap the activation key and each other's SIC using TCP port 18190.

3. If each peer validates the authenticity of the other, the Check Point component establish an encrypted session over TCP port 18184 with the MARS Appliance. It is over this channel that the Check Point components to sends encrypted log data to MARS.

The following topics support the integration of MARS into a Check Point environment:

- [Determine Devices to Monitor and Restrictions, page 21-4](#)
- [Bootstrap the Check Point Devices, page 21-5](#)
- [Add and Configure Check Point Devices in MARS, page 21-18](#)
- [Troubleshooting MARS and Check Point, page 21-35](#)

Determine Devices to Monitor and Restrictions

To configure Check Point devices, you must identify the central management server and managed components, bootstrap them, and add and configure them in the MARS web interface. The Check Point product line and release, as well as the number of devices managed, determines which tasks you must perform to configure MARS to monitor your Check Point devices.

Representing a Check Point device in MARS involve two steps:

1. **Define a primary management station.** This primary management station represents the central management server that manages remote components, such as firewalls, VPN gateways, and log servers.
2. **Define one or more child enforcement modules.** Child enforcement modules are the remote components managed by the primary management station. They represent firewalls, VPN gateways, and log servers.

When managing SmartCenter and SmartCenter Pro, the primary management station is the SmartCenter server. When managing Provider-1/SiteManager-1 releases NG FP3, NG AI (R55), and NGX (R60), the primary management station is not the MDS, but each CMA defined under the MDS. In other words, you must define each CMA as a separate primary management station. The child enforcement modules are those gateways and logs servers (CLMs) managed as part of that customer or site as defined by the CMA.

Part of what you must determine is where the security event logs are stored. Two options exist:

- **Central Event Correlation.** The MLM or SmartCenter server pulls logs from all remote components.
- **Distributed Event Correlation.** In addition to the MLM or SmartCenter Server, one or more remote log servers exist where aggregation to the central management server does not occur. These servers, the CLMs, must also be represented and configure so that MARS can pull the events from them.

If the security events are stored in a distributed fashion, you must plan to define and establish SIC communication between the MARS Appliance and each Check Point log module. For SmartCenter and SmartCenter Pro, the server SIC DN is the one assigned to the primary management station. However, for Provider-1 and SiteManager-1, the server SIC DN varies based on release. For Provider-1 and SiteManager-1 NG FP3 and NG AI (R55), the server SIC DN is the one associated with the CMA. For Provider-1 and SiteManager-1 NGX (R60), you can use the SIC assigned to the MDS for all CMAs and CLMs that you define.

One other restriction exists with the Provider-1 and SiteManager-1 products. For Provider-1 and SiteManager-1 NG FP3 and NG AI (R55), you must define an OPSEC application representing the MARS Appliance in each CMA (using the CMAs SmartDashboard user interface). For Provider-1 and SiteManager-1 NGX (R60), you can define one OPSEC application representing the MARS Appliance and push that definition to all CMAs and CLMs managed by the MDS.

Bootstrap the Check Point Devices

Bootstrapping the Check Point devices involves preparing those devices to send data to the MARS Appliance, as well as enabling the MARS Appliance to discover the Check Point configuration settings. In addition to preparing the Check Point devices, you must gather the information required to represent the Check Point devices in the MARS web interface.

You bootstrap the central Check Point management server, whether it be a CMA or a SmartCenter server by defining the MARS Appliance as a target log host and OPSEC Application object.

1. Using Check Point SmartDashboard or the Check Point Provider-1/SiteManager-1 MDG, add the MARS Appliance as a host.
2. Create and install an OPSEC Application object for the defined host, import the authorization key, and generate the client SIC DN. This SIC DN is the one used by OPSEC applications, including the management server, to validate the MARS Appliance. You specify this client SIC DN in the MARS web interface. When a session is established between the MARS Appliance and the Check Point management server, the appliance publishes this SIC to the management server to ensure non-repudiation of the appliance.
3. Obtain the server SIC DN of the Check Point management server. You specify this sever SIC in the MARS web interface. The MARS Appliance validates the server SIC DN against the SIC published to the appliance by the management server during session setup. This validation ensures non-repudiation of the server.
4. Create the policies to permit SIC traffic between the defined host (MARS Appliance), the Check Point management server, and any remote servers. After you identify the devices, you must verify that the network services they use for SIC-based management and reporting are permitted on the reporting device. To enable these traffic flows, you must verify or update the policies that enable the SIC traffic to flow between each reporting device and the MARS Appliance. Once you have updated these policies, you must install the policies.
5. Define the log settings to push the correct events to the defined host. You must ensure that all of the security, firewall, user authentication, and audit events are logged and configured to be published to the MARS Appliance.
6. Install the policies. Once the policies are defined, you must update the Check Point components with the policies. Policy installation include an object database push that make the Check Point modules aware of the OPSEC Application representing the MARS Appliance. Without this step, the modules will not forward any log information via LEA.

To perform this task, you need a Check Point user account with administrative privileges. This account must be able to create a new host, define OPSEC application, define and install new policies, and access the settings of each managed Check Point component.

After completing this task, you should have collected the following information:

- The Client and server SIC DNs.
- If you are defining a CMA for Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), then you must have the virtual IP address (VIP) for each CMA and CLM managed by the MDS. Only Provider-1 and SiteManager-1 NGX (R60) requires the physical IP addresses of the MDS and MLM servers.
- Any CLMs, instead of CMAs, to which security logs are being sent. If logs are being sent to CLMs, LEA is only supported using clear text.

To bootstrap the Check Point devices, perform the following procedures:

- [Add the MARS Appliance as a Host in Check Point, page 21-6](#)
- [Define an OPSEC Application that Represents MARS, page 21-7](#)

- Obtain the Server Entity SIC Name, page 21-10
- Select the Access Type for LEA and CPMI Traffic, page 21-12
- Create and Install Policies, page 21-14
- Verify Communication Path Between MARS Appliance and Check Point Devices, page 21-15

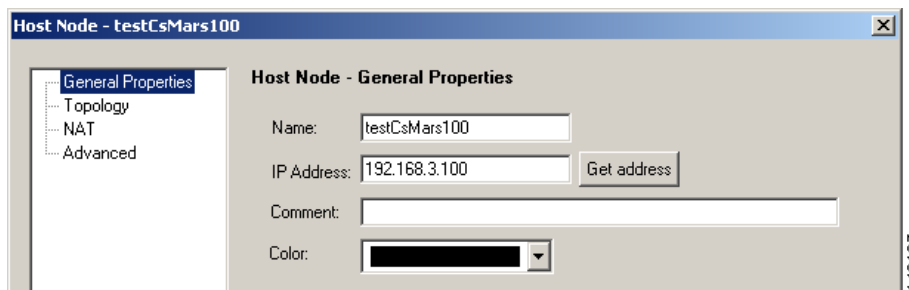
Add the MARS Appliance as a Host in Check Point

Representing the MARS Appliance in Check Point enables the following supporting tasks:

- Generate a client SIC DN for the MARS Appliance.
- Define policies to allow SIC and syslog traffic between the Check Point components and the MARS Appliance.
- Direct log traffic to the MARS Appliance.

To define the MARS Appliance as a host, follow these steps:

-
- Step 1** Log in to the correct Check Point user interface using an account with administrative privileges. If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.
- Step 2** Select **Manage > Network Objects** from the main menu. The Network Objects dialog box appears.
- Step 3** Click the **New** button, and then select **Node > Host** on the menu list. The Host Node dialog appears, with the General Properties settings selected.



- Step 4** Enter the name MARS Appliance in the Name field of the General Properties page. Any Check Point policies defined to enable access or send logs to this appliance will reference the appliance by this name. Cisco best practice recommends using the actual hostname of the MARS Appliance.
- Step 5** Enter the IP address of the monitoring interface in the MARS Appliance in the IP Address field. Typically, the monitoring interface is eth0. However, if one or more intermediate gateways are applying NAT rules to the physical IP address, enter the IP address that is exposed to the Check Point central management server.
- Step 6** Click **OK** to close the Host Node dialog box.

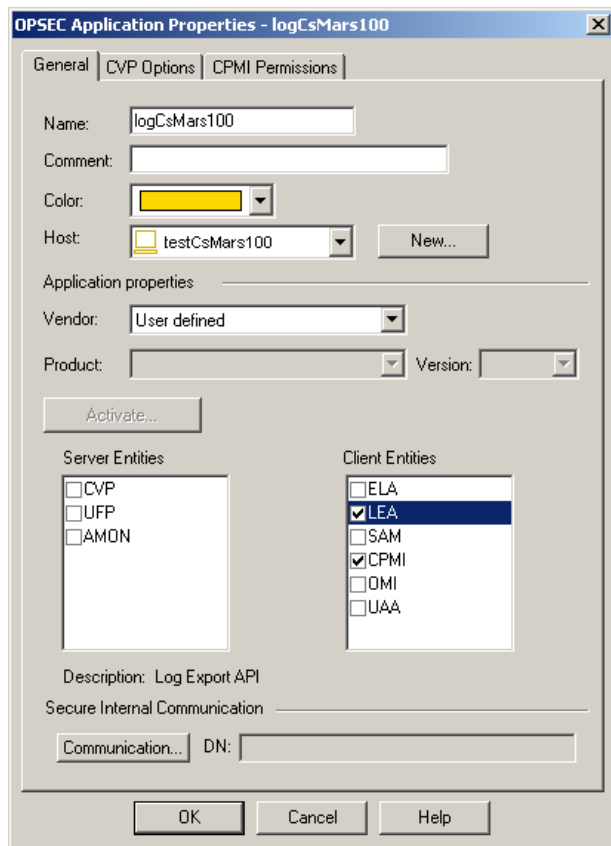
- Step 7** Click **Close** to close the Network Objects dialog box.
- The host representing the MARS Appliance is defined. You can now use this host when defining new policies in the Check Point user interface.
- Step 8** Continue with [Define an OPSEC Application that Represents MARS, page 21-7](#).
-

Define an OPSEC Application that Represents MARS

To integrate a third-party OPSEC application with Check Point components, you must define the application and associate it with the host on which the application is running. In addition to identifying this OPSEC application to the Check Point system, this procedure results in the generation of the client SIC DN for the MARS Appliance. Both the client SIC DN and the server SIC DN, obtained in [Obtain the Server Entity SIC Name, page 21-10](#), are required to enable secure communications between the appliance and Check Point components.

This procedure also involves selecting an activation key, or shared secret, that is also required to enable the secure communications. You must record both the activation key and the client SIC DN for use when defining the Check Point devices in the MARS web interface.

-
- Step 1** Log in to the correct Check Point user interface using an account with administrative privileges.
- If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.
- Step 2** Select **Manage > Servers and OPSEC Applications** from the main menu.
- The Servers and OPSEC Application dialog box appears.
- Step 3** Click the **New** button, and then click **OPSEC Application** on the menu list.
- The OPSEC Application Properties dialog box appears.



Step 4 Specify the name for this object in the Name field.

This value must be different from the name specified in ERROR: BROKEN STEPREF of [Add the MARS Appliance as a Host in Check Point, page 21-6](#). Best practice recommends using the actual hostname of the host object plus some other descriptor, which combines for a unique name.

Step 5 In the Host list, select the host that you specified in ERROR: BROKEN STEPREF of [Add the MARS Appliance as a Host in Check Point, page 21-6](#).

This OPSEC application definition is associated with the host that represents the MARS Appliance.

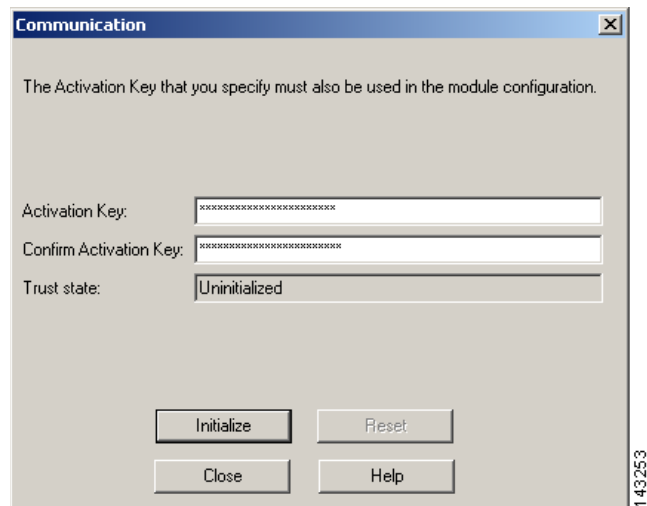
Step 6 Verify that **User defined** is selected in the Vendor field.

Step 7 Select the **LEA** and **CPMI** check boxes under Client Entities.

These values identify the OPSEC services required by the MARS Appliance.

Step 8 Click the **Communication** button under Secure Internal Communication.

The Communication dialog box appears.



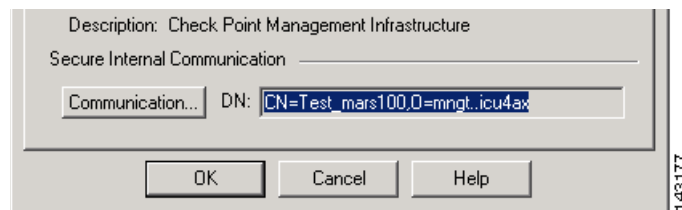
- Step 9** Enter the activation key in the **Activation Key** and **Confirm Activation Key** fields of the Communication dialog box.



Note Remember this key for future use with MARS.

- Step 10** Click **Initialize** to generate the client SIC DN.

The client SIC DN is generated and the Communication dialog box closes, returning to the OPSEC Application Properties dialog box. The new SIC appears in the DN field.



- Step 11** Click **Close** to close the Communication dialog box.

- Step 12** Record the contents of the DN field that appears under Secure Internal Communication.

This value is used to populate the Client Entity SIC Name field of MARS in [Add a Check Point Primary Management Station to MARS, page 21-19](#).



Tip If possible, you should cut and paste the **Secure Internal Communication DN** field value into an application, such as Notepad, for later use. Transcribing this field is error prone. Use a mouse to select the contents of read-only field, and then use **Ctrl+Insert** to copy the field to memory. You can paste the value using **Shift+Insert**. Be careful to avoid trailing spaces when you paste the value into MARS.

- Step 13** Select the **CPMI Permissions** tab and verify that either **Administrator's credentials** or a permissions profile with administrative credentials is selected under Login to SmartCenter with.

- Step 14** Click **OK** to close the OPSEC Application Properties dialog box.

Step 15 Click **Close** to close the Servers and OPSEC Application dialog box.

The OPSEC Application that represents MARS is defined and associated to the correct host. You also have obtained the activation key and client SIC DN for later use in [Add a Check Point Primary Management Station to MARS, page 21-19](#).

Step 16 Select **Policy > Install Database** on the main menu.

This operation updates the remote Check Point components (child enforcement modules), such as CMAs, CLMs, log servers, and firewalls. It provides them with the authorization and credentials of the MARS Appliance, as an OPSEC component and SIC client.



Tip Using the Check Point log viewer, you can verify that the OPSEC object was pushed successfully.

Step 17 Continue with [Obtain the Server Entity SIC Name, page 21-10](#).

Obtain the Server Entity SIC Name

The server SIC DN is one of the shared secrets used to provide non-repudiation during a secure communication between a Check Point component and the MARS Appliance. This value is used when defining a primary management station in MARS as defined in [Add a Check Point Primary Management Station to MARS, page 21-19](#).

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX (R60), use the MDG.

Step 2 Select **Manage > Network Objects** on the main menu.

Step 3 Select **Check Points** in the Show list.

Step 4 Select the correct Check Point component in the Network objects list.

Which Check Point component you select depends on which SIC you need and what Check Point system you are using. Specifically, you want to obtain SICs for:

- Each management server to discover configuration settings via CPML.
- Each management server to which logs are forwarded by remote components.
- Each remote log server that does not forward logs to a central management server, either the MDS or a SmartCenter.

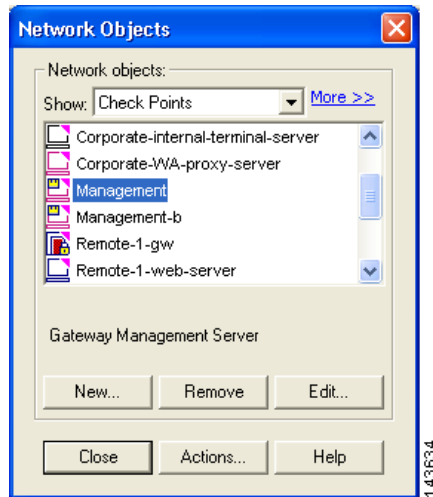
Management servers are the following devices:

- SmartCenter server for standalone SmartCenter and SmartCenter Pro installations.
- Each CMA of a Provider-1 or SiteManager-1 NG FP3 or NG AI (R55) installation.
- The MDS of a Provider-1 or SiteManager-1 NGX (R60) installation.

Log servers are the following devices:

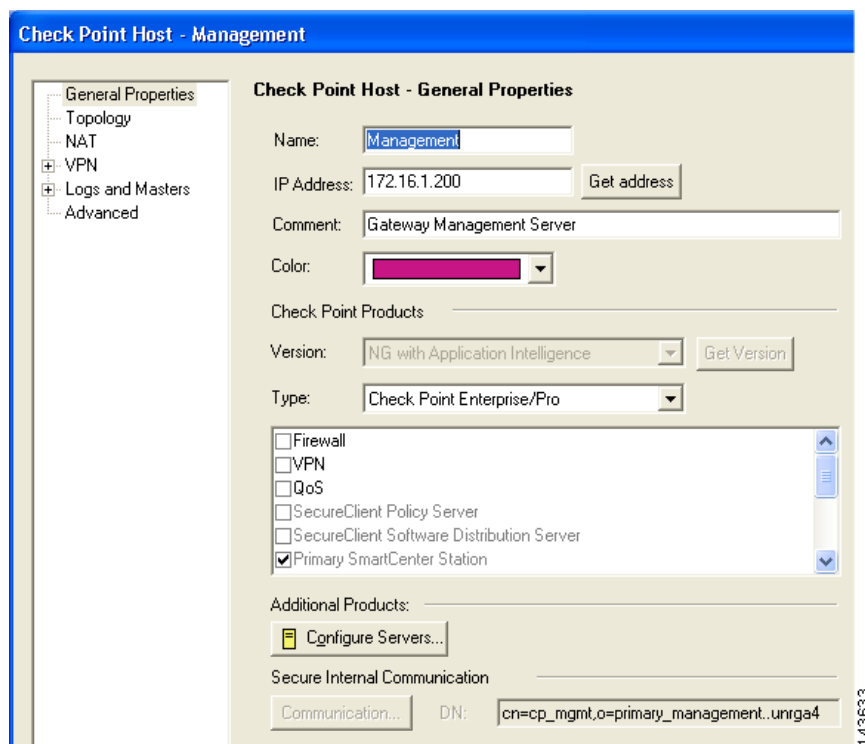
- SmartCenter server for standalone SmartCenter and SmartCenter Pro installations.
- Each CLM of a Provider-1 or SiteManager-1 NG FP3 or NG AI (R55) installation.

- The MLM of a Provider-1 or SiteManager-1 NGX (R60) installation.



Step 5 Click **Edit**.

The Check Point Host - Management dialog box appears, with the General Properties page selected.



Step 6 Record the value defined in the DN field under Secure Internal Communication.

This value is used to populate the Server Entity SIC Name field of MARS in either [Add a Check Point Primary Management Station to MARS, page 21-19](#), [Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23](#), or [Edit Discovered Firewall on a Check Point Primary Management Station, page 21-29](#).

- Step 7** Click **OK** to close the Check Point Host dialog box.
- Step 8** For each additional management or log server in this Check Point installation, select that device in the Network Objects list, and repeat [Step 5](#) through [Step 7](#).
- Step 9** Click **Close** to close the Network Objects dialog box.
- Step 10** Continue with [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).

Select the Access Type for LEA and CPMI Traffic

Check Point devices use special access types for configuration discovery and event log queries. For configuration discovery, the protocol is CPMI. For event log queries, the protocol is LEA. Each of these protocols has specific configurable attributes, including whether to use bulk encryption, what cipher to use, and what port to use for communications.

You must understand what the supported settings are so that you can verify the Check Point devices are configured correctly. MARS supports only three of the available Check Point authentication mode:

- **CLEAR**—Indicates that the traffic is neither authenticated nor encrypted.
- **SSLCA**—Indicates that the communications need to be authenticated and encrypted using an symmetric key cipher.
- **ASYMSSLCA**—Indicates that the communications need to be authenticated and encrypted using an asymmetric key cipher.

These access protocols are configured as follows:



Note

Typically, the default values should be used unless your Check Point deployment includes CLMs.

- `<service> auth_port <port_number>`

This line is required in the `fwpsec.conf` file. The `service` value is either **LEA_SERVER** or **CPMI_SERVER**. Two possible values exist for `port_number`: **0**, which indicates that the server is not listening for authenticated session requests, and the port number of an authenticated and/or encrypted protocol. If the `port_number` value is 0, you must configure the server to listen for session requests in CLEAR mode on a valid port using the settings.

- `<service> auth_type <cipher>`

The `service` value is either **LEA_SERVER** or **CPMI_SERVER**. Two possible values are supported for `cipher`: **sslca** for authentication and encryption using a symmetric key cipher, or **asym_sslca** for authentication and encryption using an asymmetric key cipher. If the `auth_port` setting is set to 0 (zero) for this service, then you do not need to specify the `auth_type` in the `fwpsec.conf` file. You can comment out this line.

- `<service> port <port_number>`

This line is required in the `fwpsec.conf` file. The `service` value is either **LEA_SERVER** or **CPMI_SERVER**. The value for `port_number` must match the port number on which the desired network service listens. A `port_number` of **0** (zero) indicates that the log server is not listening in CLEAR mode.

If it is some other number, then any service can come pull the logs without authenticating. For **LEA_SERVER**, you cannot use port 18184, as it is used for encrypted log communications. For **CPMI_SERVER**, you cannot use port 18190. When CLEAR is enabled, authentication is disabled

for this port. Any host with access to the Check Point component at this port can pull logs. If you chose to enable CLEAR, which is less expensive in terms of overall transaction costs, you define policies that restrict access to the MARS Appliance and other know management hosts.

**Note**

Prior to MARS 4.1 and when using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), you could not use SSLCA mode for log retrieval by the MARS Appliance. Instead, you were required to configure each CMA and CLM to accept LEA session requests using CLEAR mode. It was unnecessary to configure the LEA settings for the MLM.

The following example indicates that LEA is using ASYMSSLCA-based authentication connecting over port 18184 (default), the traffic is encrypted via SSL, and the log server is not listening for requests in cleartext.

```
LEA_SERVERauth_port18184
LEA_SERVERauth_typeasym_sslca
LEA_SERVERport0
```

The following example indicates that the log server is listening for requests in cleartext at port 18187. Such requests will be serviced and the sessions will be neither authenticated nor encrypted.

```
LEA_SERVERport18187
```

Check Point uses the following default settings:

- For LEA, SSLCA is the authentication method and communications occur over TCP 18184.
- For CPMI, SSLCA is the authentication method and communications occur over TCP 18190.

To review or change the access type settings, follow these steps:

Step 1 Log on to the Check Point server.

For Provider-1 and SiteManager-1, this server is the MDS, MLM, or CLM. Otherwise, it is the SmartCenter server.

Step 2 Open the fwopsec.conf file found in the subdirectory for each CMA and CLM.

The following example uses the find command to locate the file. Customer1 identifies the CLM.

```
[Expert@logger]# find . -name "fwopsec.conf" -print
./var/opt/CPfw1-R55/conf/fwopsec.conf
./var/opt/CPmds-R55/customers/Cust1Log/CPfw1-R55/conf/fwopsec.conf
[Expert@logger]# cd /var/opt/CPmds-R55/customers/Cust1Log/CPfw1-R55/conf
```

Step 3 Using a text editor, such as vi or Notepad, edit the fwopsec.conf file and modify the LEA and CPMI communication settings as needed.

Step 4 Save your changes to the file.

Step 5 Repeat [Step 2](#) through [Step 4](#) for each CLM and CMA.

Step 6 Restart the Check Point server after the changes are made.

The CPMI and LEA servers are restarted, which reloads their configuration information, and ensures they are listening to the correct ports for session requests.

Step 7 Continue with [Create and Install Policies](#), page 21-14.

Create and Install Policies

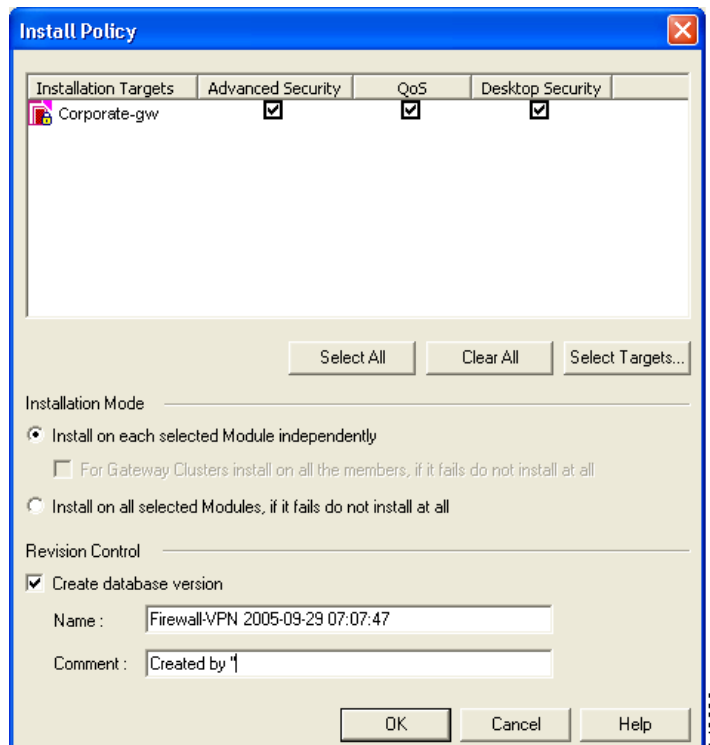
You must create firewall policies that permit the MARS Appliance to access the relevant ports of the Check Point central management server and any remote log servers. The default ports are as follows:

- **TCP port 18190**—Used by CPMI to discover configuration settings.
- **TCP port 18210**—Used to retrieve the certificate from the Certificate Authority on the SmartCenter, MDS, MLM, CMA, or CLM.
- **TCP port 18184**—Used to pull security event logs from the log servers, such as the MLM or CLM.

However, you must use the CPMI and LEA servers settings specified in [Select the Access Type for LEA and CPMI Traffic, page 21-12](#). When the policies are defined, you must install them on any firewall modules that inspect traffic between the Check Point components and the MARS Appliance.

If the management server has a Check Point firewall installed, follow these steps:

-
- Step 1** Log in to the correct Check Point user interface using an account with administrative privileges. If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.
- Step 2** If Check Point firewall components reside between the Check Point components (central management and log server) and the MARS Appliance monitoring those components, define the security policies that allow management and log traffic between those devices. If you have enabled CPMI discovery, the service condition must include CMPI. To enable the log access, the service list must include FW1_lea.
- Step 3** Verify that the security policies are set to log. The Track column of each rule should display the Log action. To enable logging, right-click the **Track** field of a rule and select **Log** on the shortcut menu.
- Step 4** Once you have defined the security policies that enable traffic flows between the Check Point and MARS components, select **Policy > Install** on the main menu.



Step 5 In the Install Policy dialog box, verify the **Advanced Security** check box is selected for each selected installation target.

The target devices should be those firewalls that reside between the Check Point components and the MARS Appliance.

Step 6 Click **OK** to install the policies on the selected devices.

The security policies on the target firewall devices are updated, enabling CPMI and LEA traffic flows between the Check Point components and the MARS Appliance.



Tip Using the Check Point log viewer, you can verify that the policies were installed successfully.

Verify Communication Path Between MARS Appliance and Check Point Devices

You should verify that the MARS Appliance can reach the Check Point devices, including the SmartCenter server and the remote log servers. Use the **telnet** command at CLI of the MARS Appliance to verify access to the SmartCenter server and log servers. The ports to check are defined in For more information on accessing the CLI, see [Establishing a Console Connection](#) of the *Cisco Security MARS Initial Configuration and Upgrade Guide*.

The command syntax is as follows

```
telnet <ip_address> <port_number>
```

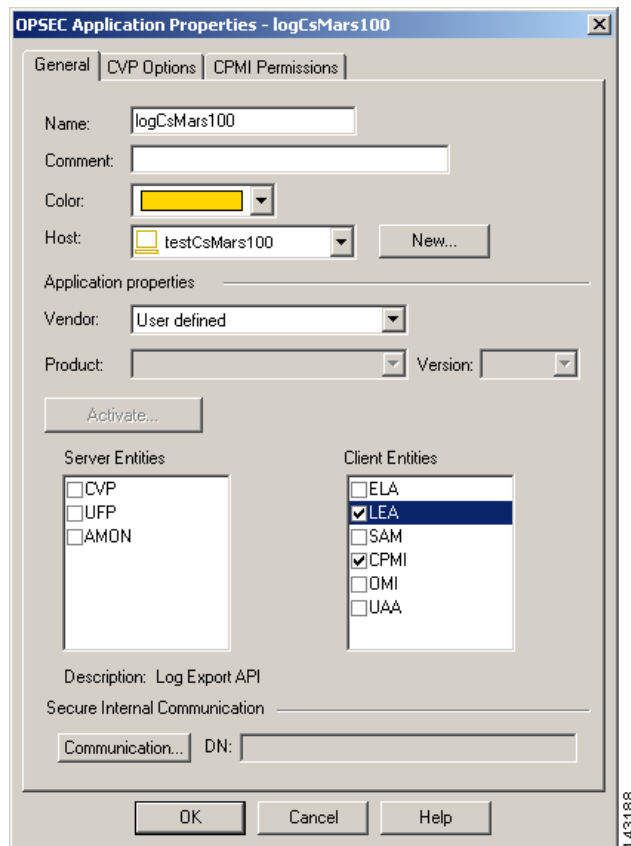
If you are unsuccessful, verify the settings of the ports for each Check Point component and verify that no firewalls are blocking the traffic. For more information on [Telnet](#) of the *Cisco Security MARS Command Reference*.

Reset the OPSEC Application Certificate of the MARS Appliance

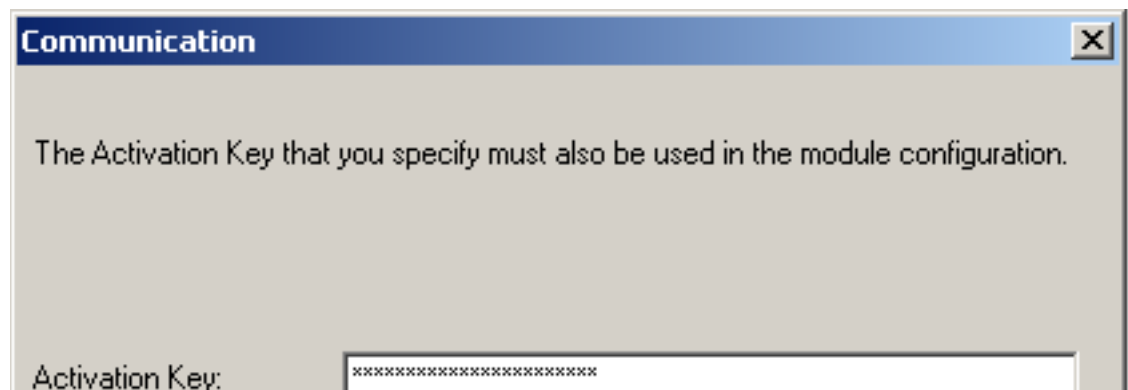
If you encounter an error when pulling the certificate as part of defining the Check Point devices in the MARS web interface, you must reset the certificate before you can attempt to pull it again. This procedure details how to reset the certificate, or SIC, associated with the OPSEC Application that is associated with the host that represents the MARS Appliance.

To reset the OPSEC application certificate, follow these steps:

-
- Step 1** Log in to the correct Check Point user interface using an account with administrative privileges. If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.
- Step 2** Select **Manage > Servers and OPSEC Applications** from the main menu. The Servers and OPSEC Application dialog box appears.
- Step 3** Select **OPSEC Applications** in the Show list.
- Step 4** Select the OPSEC application that represents the MARS Appliance in the Servers and OPSEC Applications list, and click **Edit**. The OPSEC Application Properties dialog box appears.



- Step 5** Click the **Communication** button under Secure Internal Communication. The Communication dialog box appears.



- Step 6** Click **Reset** to reset the certificate.

- Step 7** Click **Close** to close the Communication dialog box.

The client SIC DN is generated and the Communication dialog box closes, returning to the OPSEC Application Properties dialog box. The new SIC appears in the DN field.

- Step 8** Click **OK** to close the OPSEC Application Properties dialog box.

- Step 9** Click **Close** to close the Servers and OPSEC Application dialog box.

The OPSEC Application that represents MARS is defined and associated to the correct host. You also have obtained the activation key and client SIC DN for later use in [Add a Check Point Primary Management Station to MARS, page 21-19](#).

Add and Configure Check Point Devices in MARS

After you identify and bootstrap the Check Point reporting devices and install the policies that enable the required traffic flows, you must represent those devices in MARS, which uses this information to communicate with the devices. When adding a Check Point device, you add two types of devices:

- **Primary management station.** The primary management station represents the SmartCenter server or CMA that manages other Check Point components. In the web interface, the bases module is defined as a software application (Check Point Management Console application) running on a host.
- **Child enforcement module.** A child enforcement module is a Check Point component, a firewall or log server, that is managed by a primary management station. When viewing the Security and Monitoring Devices list, child enforcement modules appear as children of the hosts that are running the primary management station.

With these definitions in mind, adding and configuring the Check Point device involves the following:

1. Define a host that represents the Check Point primary management station, specifying the hostname and management and reporting IP addresses.
2. Define all of the interfaces of the host.
3. Add the correct Check Point software application to the host. This application represents the primary management station.
4. Specify the communication settings for the primary management station. These settings include identifying which access types are allowed (CPMI, LEA or both) and the authentication type and port to use for each supported access type.
5. (Optional) Define the settings for secure communications. If the access communication are not conducted in CLEAR, then you must specify the client and server SIC DNs and identify the certificate authority.
6. (Optional) Define the routes used by the firewall running on the primary management station. If a firewall is running on the primary management station, the route information is required to enable the path analysis and mitigation features of MARS.
7. Discover the child enforcement modules and the configuration settings of the primary management station. Discovery of child enforcement modules includes any log servers and firewalls managed by the primary management station. MARS discovers configuration settings, such as policies, NAT, modules, and clusters, as well as event information, such as traffic logs, SmartDefense events, and user authentication events.
8. Configure the discovered log servers. To configure these log servers, select the Self option from the Log Info page associated with each server, and specify the access type settings.
9. Define any log servers not managed by the primary management station. These servers are used by one or more of the firewalls that were discovered or by the primary management station.
10. Edit each firewall child enforcement module to select a log server.
11. (Optional) Specify an SNMP RO community string for each firewall child enforcement module for which resource utilization monitoring is desired.

12. (Optional) Define the routes used by each firewall child enforcement module. Route information is required to enable the path analysis and mitigation features of MARS.
13. Click Activate in MARS.

To add a Check Point device in MARS, you must perform the following procedures:

- [Add a Check Point Primary Management Station to MARS, page 21-19](#)
- [Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23](#)
- [Edit Discovered Log Servers on a Check Point Primary Management Station, page 21-27](#)
- [Edit Discovered Firewall on a Check Point Primary Management Station, page 21-29](#)
- [Verify Connectivity Between MARS and Check Point Devices, page 21-34](#)

If discovery of Check Point configuration settings is not enabled for MARS, you must perform the following manual configuration procedures:

- [Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23](#)
- [Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31](#)

Before You Begin

To perform this procedure, you need the following information:

- A MARS account with Administrative privileges.
- A Check Point CMA or SmartCenter username and password that has READ access (minimum requirement).
- The client and server SIC DNSs.
- If you are defining a CMA for Provider-1 or SiteManager-1, you must have the virtual IP address (VIP) for each CMA and CLM managed by the MDS.

Add a Check Point Primary Management Station to MARS

The primary management station represents one of the following:

- The SmartCenter server in a SmartCenter or SmartCenter Pro installation.
- A CMA of a Provider-1 or SiteManager-1 installation.



Note

Check Point 4.1, NG FP1, and NG FP2 devices are not officially supported. They cannot be configured to retrieve configuration information using CPMI. However, they can be configured to retrieve logs using LEA. To configure one of these devices to work with the MARS, leave the Access IP field blank on the host that represents the base platform.

You must define each individual CMA of a Provider-1 or SiteManager installation, regardless of the release and version.

Step 1 Select **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2 Do one of the following:

- Select **Add SW Security apps on a new host** from the Device Type list, and continue with [Step 3](#)

- Select **Add SW security apps on existing host** from the Device Type list. Select the device to which you want to add the software application and click **Add**. Continue with [Step 7](#).

Step 3 Specify values for the following fields:

- **Device Name**—Enter the name of the device. This name must exactly match the hostname shown in the Check Point user interface. MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and as the primary management station in the Security and Monitoring Device list.
- **Access IP**—(Optional) This address is used to pull from a Check Point device using CPML, enabling MARS to discover settings from this device. This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. To learn more about the access IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).
- **Reporting IP**—Enter the IP address of the interface in the Check Point server from which MARS will pull traffic and audit logs. Check Point audit logs save information regarding user interaction with Check Point devices, such as log in and out of the Check Point user interface, initialize or revoke certificate, install or uninstall policy, create, modify, and delete objects, etc. No additional configuration is needed to turn on audit log on Check Point device.

This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. 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 4 Under Enter interface information, enter the interface name, IP address, and netmask value of each interface in the Check Point server from which configuration information will be discovered and from which security event logs will be pulled.

This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. To learn more about the interface settings, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

Step 5 (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 6 Click **Apply** to save these settings.

Step 7 Click **Next** to access the Reporting Applications tab.

Step 8 Select the appropriate version of Check Point Opsec from the Select Application list, and click **Add**.

The following options are available:

- **CheckPoint Opsec NG FP3**—Select this option for Check Point NG FP3 devices.
- **CheckPoint Opsec NG AI**—Select this option for Check Point NG AI (R55) devices.
- **CheckPoint Opsec NGx**—Select this option for Check Point NGX (R60) devices.

↓

General	Reporting Applications	Vulnerability Assessment
---------	------------------------	--------------------------

Enter reporting application:

→ Device Name: Softie II

→ Select application: Select one

Select one

CheckPoint Opsec NG AI

CheckPoint Opsec NG FP3

Cisco ACS 3.x

Cisco CSA 4.x

Cisco ICS 1.x

Enterasys Dragon 6.x

Entercept Entercept 2.5

Entercept Entercept 4.0

Foundstone FoundScan 3.0

Generic Web Server Generic

ISS RealSecure 6.5

ISS RealSecure 7.0

IntruVert IntruShield 1.5

McAfee ePO 3.5

NetScreen IDP 2.1

Oracle Database Server Generic

Snort Snort 2.0

Symantec Anti Virus 9.x

Copyright © 2003, 2005 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Manag 3/202

Step 9 If you are in a state:

Access Information
[Optional: for NAT-related session correlation, attack path calculation, and mitigation enter access information]

→ * Access Type: SSLCA

→ * Access Port: 18190 (Default:18190)

* Login:

* Password:

Reporting Information

→ * LEA Access Type: SSLCA

* LEA Port: 18184 (Default:18184)

Secure Internal Communication Information

* Certificate: Select Certificate

* Client Entity SIC Name:


* Server Entity SIC Name:

SNMP RO Community:

- **Login**—Identifies the Check Point administrative account to be used to discover configuration settings.
- **Password**—Identifies the password associated with the Login account.

Step 10 Specify values for the following fields:

- **LEA Access Type**—If a log server is running on this primary management station select **ASYMSSLC**, **CLEAR**, or **SSLCA**. You must have entered an address in the Reporting IP field on the host that represents this primary management station. This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. For more information on the access type, see [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).
- **LEA Port**—Verify that the port number corresponds to the value specified in the LEA_SERVER auth_port line of the fwopsec.conf file. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).

- Step 11** If this device uses SSLCA or ASYMSSLCA as an authentication method, specify values for the following fields (Otherwise, the authentication method is CLEAR. Skip to [Step 12](#)):
- **Certificate**—Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with [Add a Check Point Certificate Server, page 21-26](#).
 - **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in [Define an OPSEC Application that Represents MARS, page 21-7](#).
 - **Server SIC Name**—Enter the SIC DN for this primary management station. This value was obtained in [Obtain the Server Entity SIC Name, page 21-10](#). Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.
- Step 12** (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 on host that represents the primary management station and you must configure the Access Information settings on the primary management station. MARS uses the SNMP RO string to perform resource utilization monitoring. Currently, it is not used for configuration or log discovery.
- Step 13** (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.
- Before you can enable this feature, you must provide a SNMP RO Community string.
- 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 14** (Optional) To specify the route information for a firewall running on this primary management station, continue with [Define Route Information for Check Point Firewall Modules, page 21-29](#).
- Step 15** (Optional) If you defined an access IP and selected and configured an access type, click Discover to determine the device 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](#).
-  **Note** Sometimes, the discovery operation times out, in which case you should try again. At other times, a message appears that states the discovery is taking a long time and that you should proceed to performing other tasks in MARS.
- Step 16** To add this device to the MARS database and continue adding firewall modules manually, 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 17** Do one of the following:
- To manually define the child enforcement modules that are managed by this primary management station, continue with [Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23](#).
 - To edit the settings of the discovered child enforcement modules, continue with [Edit Discovered Firewall on a Check Point Primary Management Station, page 21-29](#).

Step 18 Click **Activate**.

Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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](#).

Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station

If you have not enabled configuration discovery on the primary management station or if one or more of the managed firewalls uses a log server that is not managed by the primary management station, you can manually define firewalls or log servers. Your goal should be to represent all of the firewalls managed by this primary management station and all log servers used by those firewalls and the primary management station. While MARS does not discover configuration settings of the firewalls, it uses the defined information to discover topology, calculate attack paths, and identify preferred mitigation points in the network.

For example, if you are defining a primary management station that represents a CMA, you must define the CLM associated with that CMA. Any firewalls managed under that CMA may either act as their own log servers, publish information to the CLM, or publish information to a MLM. In the case of the later, you must define that relationship by defining the firewalls and then specifying which log servers pull their traffic and audit logs. First, however, must also define the MLM settings, as it is a log server that external to the perspective of the CMA, and it cannot be referred by a firewall until it has been defined. The CLM, however, would be considered part of the CMA (assuming the reporting IP and LEA settings are specified), so you would not define a separate child enforcement module to represent it. Instead, you would select the Management option in the Log Info dialog for firewalls that use the CLM as their log server. For more information on selecting the log server option, see [Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31](#).

To manually define a child enforcement module that is managed by the primary management station or a log server to which either the primary management station or a child enforcement module publishes its audit and security logs, follow these steps:

-
- Step 1** Select **Admin > System Setup > Security and Monitor Devices**.
- Step 2** From the Security and Monitor Devices list, select the host that represents the primary management station and click **Edit**.
- Such devices have CheckPoint Management Console as an entry in the Device Type column.
- Step 3** Click **Next** to access the Reporting Applications tab.

General Reporting Applications Vulnerability Assessment Info

Enter reporting application:

→ Device Name: DEV-CMA

→ Select application: Select one Add

Edit Remove

Device Type

CheckPoint Management Console

Done

143632

- Step 4** Select the **CheckPoint Management Console** check box in the Device Type list and click **Edit**. The Access Information page appears.

Access Information
[Optional: for NAT-related session correlation, attack path calculation, and mitigation enter access information]

→ * Access Type: SSLCA
→ * Access Port: 18190 (Default:18190)
* Login: eng
* Password: *****

Secure Internal Communication Information

* Certificate: testServer Add Edit
* Client Entity SIC Name: testServer
* Server Entity SIC Name: testServer
SNMP RD Community:

Reporting Information

→ * LEA Access Type: SSLCA
* LEA Port: 18184 (Default:18184) Route Info

Firewall & Log Server Settings

Add Edit Delete Log Info Route Info

Info Discover Cancel Submit

143627

- Step 5** Click **Add** under Firewall & Log Server Settings.

The list of available hosts appears.

- Step 6** Do one of the following:

- Select the host on which the child enforcement module is running, click **Change Existing**, and continue with [Step 7](#)

Result: A page with a read-only device name appears, prompting you to specify the SNMP RO Community string.

→ *Device Name: Test host

→ SNMP RO Community:

Name:	IP Address:	Network Mask:
<input type="checkbox"/> ether0	192.168.3.13	255.255.255.255

143623

- Click **Add New** to define a new host, and continue with [Step 7](#)
Result: A page appears, prompting you to specify device name and SNMP RO Community string.

→ *Device Name:

→ SNMP RO Community:

Name:	IP Address:	Network Mask:
<input type="checkbox"/> ether0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

143787

- Step 7** Enter the name of the child enforcement module or log server in the **Device Name** field.
MARS maps this name to the IP address specified in the interfaces. This name is used in topology maps, queries, and appears in the Children column of the base Check Point module in the Security and Monitoring Device list.
- Step 8** (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the child enforcement module’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 on host that represents the primary management station. 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 9** Under Enter interface information, enter the interface name, IP address, and netmask value of each interface installed in the child enforcement module or log server.
- These interfaces include the ones from which the configuration information will be discovered and security event logs will be pulled. To learn more about the interface settings, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).
- Step 10** Click **Submit** to add this module to the primary management station.
- Step 11** (Optional) To specify the route information for a firewall child enforcement module, continue with [Define Route Information for Check Point Firewall Modules, page 21-29](#).
- Step 12** If the child enforcement module does not propagate its logs to the primary management station or if you are defining a log server that is not managed by this primary management station, you must specify where its logs are stored. Continue with [Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31](#).
- Step 13** Repeat [Step 5](#) through [Step 12](#) for each child enforcement module that is managed by this primary management station and each log server that is used by the primary management station or child enforcement modules.
- Step 14** 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 15** Click **Done** to close the Reporting Applications tab and return to the Security and Monitoring Devices list.
- Step 16** Click **Activate**.
- Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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 a Check Point Certificate Server

When defining a Check Point module that uses secured communications, you must identify the certificate sever that authenticates the SICs provided by the client and the server. Typically, a SmartCenter server or the CMA has its own certificate server, however, your configuration may use a central server. If that is the case, you must define the certificate server as part of a defining a base or child enforcement module.

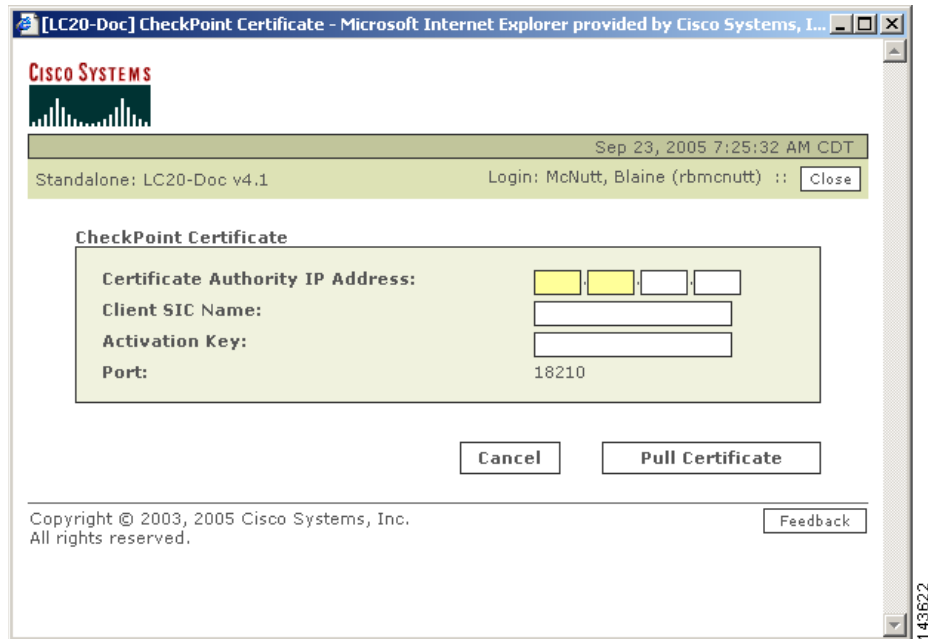


Note

This procedure assumes you have been refer to it, and that you are in the middle of defining a primary management station or child enforcement module.

To define a certificate server, follow these steps:

- Step 1** Click **Add** to define the settings for the certificate authority.



Step 2 Specify values for the following fields:

- **Certificate Authority IP Address**—Typically, this IP address is the physical IP address of the SmartCenter server or the virtual IP address of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this IP address represents the physical IP address of the MDS that manages the CMA.
- **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in [Define an OPSEC Application that Represents MARS, page 21-7](#).
- **Activation Key**—This value was also provided in [Define an OPSEC Application that Represents MARS, page 21-7](#).

Step 3 Click **Pull Certificate**.

A message box appears stating “Discovery is done.”

A certificate can be pulled only once for an OPSEC Application. If for any reason the pull operation fails, you must reset the certificate using the CheckPoint SmartDashboard. For more information, see [Reset the OPSEC Application Certificate of the MARS Appliance, page 21-16](#).

Step 4 Click **Close**.

Edit Discovered Log Servers on a Check Point Primary Management Station

After performing a discovery operation, you must edit each discovered log servers. The purpose of editing this log server is to identify that it is its own log server and to provide the SIC communication settings.

To edit a discovered log server, follow these steps:

Step 1 Under Firewall & Log Server Settings, select the check box next to the desired log server, and click **Log Info**.

Step 2 Select **Self**.

The screenshot shows a configuration window for a log server. It has three radio buttons: 'Management', 'Log Server', and 'Self'. The 'Self' radio button is selected. The configuration fields are as follows:

- *Reporting IP:** Four empty input boxes.
- Certificate:** A dropdown menu showing 'Select Certificate', with 'Add' and 'Edit' buttons to its right.
- Client SIC Name:** An empty text input field.
- Server SIC Name:** An empty text input field.
- *Logging Access Type:** A dropdown menu with 'SSLCA' selected.
- *Logging Access Port:** A text input field containing '18184', with '(Default:18184)' displayed to its right.

At the bottom right of the window are 'Cancel' and 'Submit' buttons. A small number '143626' is visible to the right of the 'Submit' button.

Step 3 Specify values for the following fields:

- **Reporting IP**—Enter the IP address of the interface in the log server from which MARS will pull security event logs. This address represents either a virtual IP address associated with a CLM, an MLM, or another log server. To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).
- **Logging Access Type**—This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. Select ASYMSSLCA, CLEAR, or SSLCA. For more information on the access type, see [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).
- **Logging Port**—Verify that the port number in the corresponds to the value specified in the LEA_SERVER auth_port line of the fwopsec.conf file on this log server. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).

Step 4 If this log server uses SSLCA or ASYMSSLCA as an authentication method, specify values for the following fields (Otherwise, the authentication method is CLEAR. Skip to [Step 5](#)):

- **Certificate**—Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with [Add a Check Point Certificate Server, page 21-26](#).
- **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in [Define an OPSEC Application that Represents MARS, page 21-7](#).
- **Server SIC Name**—Enter the SIC DN for the child enforcement module. This value was obtained in [Obtain the Server Entity SIC Name, page 21-10](#). Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 5 Click **Submit** to save your changes to this log server.

Step 6 Repeat [Step 1](#) through [Step 5](#) for each discovered log server.

Edit Discovered Firewall on a Check Point Primary Management Station

After performing a discovery operation, you must edit any discovered firewalls. You must specify which log server the firewall uses, define the route information, and if you want to monitor resource utilization, you must specify the SNMP RO community string.

**Note**

When editing a Check Point Firewall, never select a Check Point Firewall from the Security and Monitoring Devices list. Instead, select the Check Point Management Console that acts as the primary management station for that firewall.

**Note**

You must configure the discovered log servers and define any log servers not managed by the primary management station before editing the discovered firewalls. To configure the discovered log servers, see [Edit Discovered Log Servers on a Check Point Primary Management Station, page 21-27](#). To manually define log servers, see [Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23](#).

To edit a discovered firewall, follow these steps:

- Step 1** Under Firewall & Log Server Settings, select the check box next to the desired firewall.
- Step 2** Click **Edit**.
- Step 3** (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the child enforcement module'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 on host that represents the primary management station. 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** Click **Submit**.
- Step 5** To define the route settings for this firewall, continue with [Define Route Information for Check Point Firewall Modules, page 21-29](#).
- Step 6** To select the log server used by this firewall, continue with [Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31](#).
- Step 7** Repeat [Step 1](#) through [Step 6](#) for each discovered firewall.

Define Route Information for Check Point Firewall Modules

To perform attack path analysis and to provide suggested mitigation configurations, MARS must understand the static routes that are defined on a firewall module. This requirement is true for firewalls running on the primary management station as well as for each firewall child enforcement module managed by the primary management station. To provide this information, you must define the routes manually in the MARS web interface. You will need a list of the routes for all interfaces in the firewall before you attempt to enter this information.

**Note**

You do not need to specify which interface the route is associated with. MARS derives this information based on the interface settings you have specified for the host.

To define the static routes used by a firewall, follow these steps:

Step 1 Do one of the following:

- To specify the route information for the primary management station, click **Route Info** on the primary management station page.
- To specify the route information for a firewall child enforcement module, select the server under Device Type, click **Route Info**.

The Route Information dialog box appears.

Step 2 Specify values for the following fields:

- **Destination Address**—Enter the internal or external destination network address.
- **Destination Mask**—Enter the corresponding network mask value.
- **Next Hop Address**—Enter the IP address of the default gateway.
- **Metric**—Identifies the priority for using a specific route. When routing network packets, a gateway device uses the rule with the most specific network within the rule's definition. Only in cases where two routing rules have the same network is the metric used to determine which rule is applied. If they are the same, the lowest metric value takes priority. If no routing rule exists, the network packet is dropped, and if the gateway is not detected (dead), the network packet is dropped.

A *metric* is a measurement of the cost of a route based on the number of hops (hop count) to the network on which a specific host resides. Hop count refers to the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination.

Because the hop count includes the destination network, all directly connected networks have a metric of 1. For the metric value, specify a number between 1 and 15.

Step 3 Click **Submit** to add the route to the list of routes**Step 4** Repeat [Step 1](#) through [Step 3](#) for each route defined on the firewall.**Step 5** Click **Close** to return to the Access Information page.

Specify Log Info Settings for a Child Enforcement Module or Log Server

There are two occasions when you must define the log settings manually:

- If you do not discover the settings of the primary management station, which does discover the log settings.
- If the child enforcement module does not propagate its logs up to the primary management station.

Three options exist for manually specifying the log settings:

- **Management**—Identifies that the child enforcement module propagates its logs up to the primary management station, the MLM or the SmartCenter server. You do not specify these settings; they are derived from the settings on the primary management station. However, the option is available if the configuration of a child enforcement module changes. If the primary management station is the log server for a child enforcement module, the log server information is populated when you perform the test connectivity operation.

<input checked="" type="radio"/> Management	Reporting IP	10.1.1.17
	Certificate:	testServer
	Client SIC Name:	testServer
<input type="radio"/> Log Server	Server SIC Name:	testServer
	Logging Access Type:	SSLCA
	Logging Access Port:	18184
<input type="radio"/> Self		

143625

- **Log Server**—Identifies that another log server, such as a CLM, is acting as the log server for this child enforcement module. You must either select a pre-defined log server or define the settings for a new one and select it.
- **Self**—Identifies that the child enforcement module is acting as its own log server. In this case, you must specify the communication settings required to pull the logs from that module or server.

To specify the log server settings of a child enforcement module manually, follow these steps:

Step 1 (Firewall only) If a child enforcement module does not propagate its log information to the primary management station, then select that child enforcement module under Device Type, click **Log Info**, and do one of the following:

- To specify that the child enforcement module is acting as its own log server, select **Self** and continue with [Step 3](#), omitting the Device Name field.

Figure 21-1 Log Information Published to Self

<input type="radio"/> Management	*Reporting IP:	<input type="text"/>
	Certificate:	<input type="text" value="Select Certificate"/> <input type="button" value="Add"/> <input type="button" value="Edit"/>
<input type="radio"/> Log Server	Client SIC Name:	<input type="text"/>
	Server SIC Name:	<input type="text"/>
<input checked="" type="radio"/> Self	*Logging Access Type:	<input type="text" value="SSLCA"/>
	*Logging Access Port:	<input type="text" value="18184"/> (Default:18184)

143626

- To specify an alternate log server, select **Log Server**, and continue with [Step 2](#).

The Log Information dialog box appears, and the desired option is selected.

Step 2 Do one of the following:

- Select a predefined log server from the Select list, click **Submit**, and continue with [Step 5](#).

<input type="radio"/> Management	<input type="text" value="Select"/>	<input type="button" value="Add"/>	<input type="button" value="Edit"/>
<input checked="" type="radio"/> Log Server			
<input type="radio"/> Self			

143624

- Click **Add** to define a new log server.

*Device Name:	<input type="text"/>
*Reporting IP:	<input type="text"/>
Certificate:	<input type="text" value="Select Certificate"/> <input type="button" value="Add"/> <input type="button" value="Edit"/>
Client SIC Name:	<input type="text"/>
Server SIC Name:	<input type="text"/>
*Logging Access Type:	<input type="text" value="SSLCA"/>
*Logging Access Port:	<input type="text" value="18184"/> (Default:18184)

143623

Step 3 Specify values for the following fields:

- Device Name**—Enter the name of the log server. MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and as the primary management station 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.

- **Reporting IP**—Enter the IP address of the interface in the log server from which MARS will pull security event logs. This address represents either a virtual IP address associated with a CLM, an MLM, or another log server. To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).
- **Logging Access Type**—This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. Select **ASYMSSLCA**, **CLEAR**, or **SSLCA**. For more information on the access type, see [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).
- **Logging Port**—Verify that the port number in the corresponds to the value specified in the LEA_SERVER auth_port line of the `fwopsec.conf` file on this log server. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).

Step 4 If this log server uses SSLCA or ASYMSSLCA as an authentication method specify values for the following fields (Otherwise, CLEAR is the authentication method for Access Type and LEA Access Type, and you should skip to [Step 5](#)):

- **Certificate**—Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with [Add a Check Point Certificate Server, page 21-26](#).
- **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in [Define an OPSEC Application that Represents MARS, page 21-7](#).
- **Server SIC Name**—Enter the SIC DN for the child enforcement module. This value was obtained in [Obtain the Server Entity SIC Name, page 21-10](#). Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 5 To add this child enforcement module to the primary management station, click **Submit**.

Step 6 To add the primary management station 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 7 Click **Done** to close the Reporting Applications tab and return to the Security and Monitoring Devices list.

Step 8 Click **Activate**.

Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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](#).

Verify Connectivity Between MARS and Check Point Devices

After defining the Check Point device and clicking **Activate** in the MARS web interface, the MARS Appliance connects to the log servers and pulls the traffic and audit logs stored on them. You can verify that these transactions are successful using the following method:

- Perform an ad hoc query for Event Types/Sessions specify to the Check Point primary management station.

Remove a Firewall or Log Server from a Check Point Primary Management Station

If the configuration of your network changes so that a firewall or log server is no longer managed by the primary management station under which it is defined, you must remove the child enforcement module.

To remove a child enforcement module from the primary management station, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices**.

Step 2 From the Security and Monitor Devices list, select the host that represents the primary management station of the Check Point server and click **Edit**.

Such devices have CheckPoint Management Console as an entry in the Device Type column.

Step 3 Click **Next** to access the Reporting Applications tab.

↓

General	Reporting Applications	Vulnerability Assessment Info
---------	------------------------	-------------------------------

Enter reporting application:

→ Device Name: DEV-CMA

→ Select application:

Device Type

CheckPoint Management Console

143632

Step 4 Select **CheckPoint Management Console** from the Device Type list and click **Edit**.

The Access Information page appears.

Step 5 Under Firewall & Log Server Settings, check the box next to the child enforcement module that you want to remove.

Step 6 Click **Remove**.

The Confirmation screen appears.

- Step 7** Click **Submit** to remove the child enforcement module from the primary management station.
-

Troubleshooting MARS and Check Point

The following information can be used to troubleshoot communicate issues between the MARS Appliance and Check Point components.

- To view attack information by user, run a query where the device is a Check Point device.
- If you attempt to discover the certificate and it returns to the CheckPoint Certificate screen instead of displaying the "Discovery done." message box, then the discover operation failed. The likely cause is an incorrect SIC value.



Note A certificate can be pulled only once for an OPSEC Application. If for any reason the pull operation fails, you must reset the certificate using the CheckPoint SmartDashboard. For more information, see [Reset the OPSEC Application Certificate of the MARS Appliance, page 21-16](#).

- If the device discovery operation fails, click the **View Error** button for a detailed error message.

Common reasons for failure of device discovery are as follows:

- client SIC DN name or server SIC DN name is incorrect. Use copy and paste from SmartDashboard to avoid erroneous entry.
- Invalid Certificate used.
- Invalid user name, password, or both used. Verify that the credentials provided for the Access IP match an Check Point account with administrative privileges.
- Unsupported version of Check Point. (Discovery works only with NG FP3 and above. Internally we have tested up to Version R60)
- Invalid authentication method used. The default method is SSLCA. Check the fwopsec.conf file to determine which method is used. CS-MARS currently support only three authentication methods for CPMI communication: SSLCA, ASYM_SSLCA and CLEAR. For more information on specifying these settings, see [Select the Access Type for LEA and CPMI Traffic, page 21-12](#).
- Invalid access port. Default port for secured CPMI-based communication is TCP 18180. Check the fwopsec.conf to verify the configured port.
- The MARS Appliance does not have access to port 18190, or an alternate specified in fwopsec.conf for CPMI. At the CLI of the MARS Appliance, use the **telnet** command to test the access port. For more information on **telnet**, see [Verify Communication Path Between MARS Appliance and Check Point Devices, page 21-15](#).
- The policy database was not installed after creating OPSEC Application in the SmartDashboard.
- Firewall policies were not created and installed that permitted the MARS Appliance to connect to the Check Point primary management station. For information, see [Create and Install Policies, page 21-14](#).

For additional Check Point discovery-related debug information, use the **pnlog** command at the CLI of the MARS Appliance. You can use the *cpdebug* attribute to specify appropriate debug level. Level 9 presents all debug messages. You can view the debug messages using the **pnlog showlog cpdebug** command at the CLI. For more information on **pnlog**, see [pnlog](#) of the *Cisco Security MARS Command Reference, 6.X*.