



ForeScout Technologies

**CheckPoint OPSEC
Component Management
for ActiveScout**



Legal Notice

Copyright © ForeScout Technologies, 2001. All rights reserved.

The copyright and proprietary rights in the guide belong to ForeScout Technologies. It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this guide in any way, shape or form without the prior consent of ForeScout Technologies.

This product is based on software developed by ForeScout Technologies.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use, acknowledge that the software was developed by ForeScout Technologies.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

All other trademarks used in this document are the property of their respective owners.

Copyright © 2000 Check Point Software Technologies Ltd. All rights reserved.

Check Point Software, the Check Point Software logo and FireWall-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. The products described in this document are protected by U. S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U. S. Patents , foreign patents , or pending applications.

P.N.R1-02/03

Table of Contents

CheckPoint OPSEC Component Management	2
Registering the Scout with the CheckPoint SmartCenter Management Station	2
Sending Events to the SmartCenter (AMON Server)	4
Configuring the SAM Client	5
Configure the ELA Client	6


CheckPoint OPSEC Component Management

This document presents instructions for managing the following OPSEC components:

- CheckPoint Smart Center Management Station — Scout registration with the CheckPoint Smart Center Management Station. See *Registering the Scout with the CheckPoint SmartCenter Management Station* for more information.
- Amon Server — Run the AMON server, which is responsible for transmitting status messages from the Scout to the SmartCenter. See *Sending Events to the SmartCenter (AMON Server)* for more information.
- SAM server — Configure the SAM server if you are blocking offensive sources using Check Point's FireWall-1® and the Scout. See *Configuring the SAM Client* for more information.
- ELA server — Configure the ELA server if you are working with the FireWall-1® ELA external logging system. See *Configure the ELA* for more information.

Registering the Scout with the CheckPoint SmartCenter Management Station

You can register the Scout with the CheckPoint SmartCenter Management Station. Once registered and connected to the AMON server, status messages regarding the Scout will appear in the SmartView Status window of the SmartCenter.

 *You will be required to register the Scout to the SmartCenter to enable sslca communication from a SAM client and ELA client.*

To register the Scout:

1. Log in to the Scout machine.
2. Run the following command: *fstool opsec*. The OPSEC configuration menu appears.

OPSEC Configuration Menu:

- 1) Add ActiveScout object to SmartCenter Server*
- 2) Configure SAM client*
- 3) Configure ELA client*
- 4) Start AMON server*
- 5) Quit*

Choice :

- 3.** Select option 1, and press Enter. The following strings appears:

SmartCenter Management Server IP address :

SmartCenter Management Server at (X.X.X.X) user [admin] :

SmartCenter Management Server password :

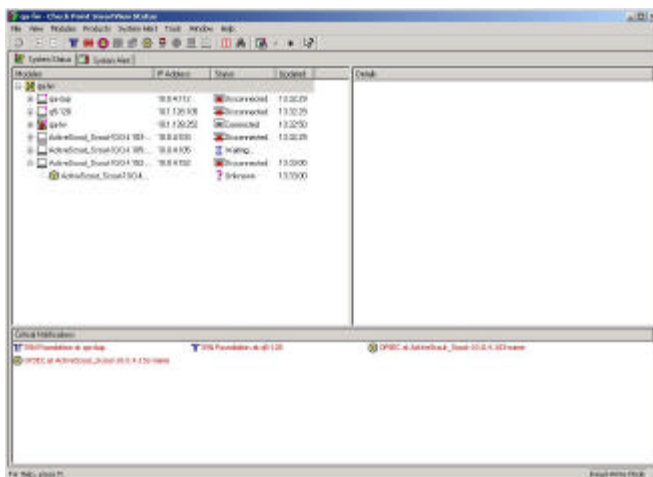
Make sure all SmartDashboard client connections, any other RA tools or CPMI client applications that might have a lock on the Check Point objects repository are closed.

Press ENTER to continue

- 4.** Enter the required information and press Enter. A series of registration messages appear. After the registration is complete, the following message appears:

Press ENTER to return to main menu.

The ActiveScout module is registered with SmartView and appears in the SmartView Status Window.



ActiveScout registered with the SmartCenter – SmartView Status Window

After you have registered the Scout, you must connect the Scout to the AMON Server. The server is responsible for sending Scout status messages to the SmartCenter.

Sending Events to the SmartCenter (AMON Server)

After you have registered the Scout with the SmartCenter, you must run the AMON server, which is responsible for transmitting status messages from the Scout to the SmartCenter. These message appear in the SmartView Status window.

To send events to the SmartCenter:

1. Log in to the Scout machine.
2. Run the following command: `fstool opsec`. The OPSEC configuration menu appears.

OPSEC Configuration Menu:

- 1) Add ActiveScout object to SmartCenter Server
- 2) Configure SAM client
- 3) Configure ELA client
- 4) Start AMON server
- 5) Quit

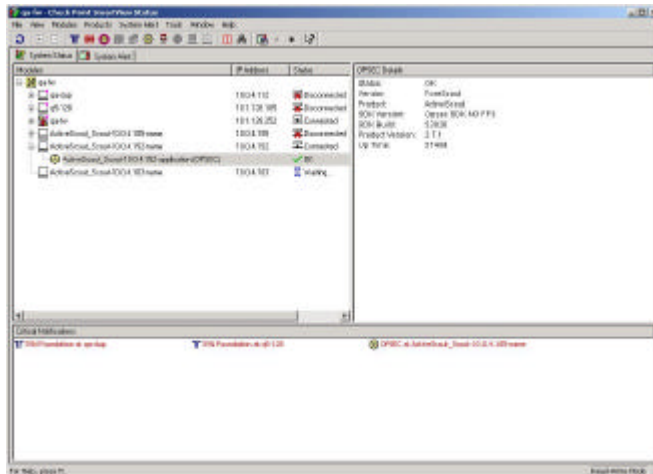
Choice :

3. Select Option 4 and press Enter. The following message appears:

Starting AMON server...

Press ENTER to return to main menu

Basic Information about the Scout appears in the CheckPoint SmartView Status window.



ActiveScout registered with the SmartCenter – Connected to AMON Server

Configuring the SAM Client

Configure the SAM client if you are blocking offensive sources using the CheckPoint firewall and the Scout. In addition, if the SAM client is configured using the sslca authentication method, you will be required to register the Scout at the SmartCenter Management Station. Messages regarding sslca communication are displayed at the SmartCenter in the SmartView status window.

To configure the SAM client:

1. Log in to the Scout machine.
2. Run the following command: `fstool opsec`. The OPSEC configuration menu appears.

OPSEC Configuration Menu:

- 1) Add ActiveScout object to SmartCenter Server
- 2) Configure SAM client
- 3) Configure ELA client
- 4) Start AMON server
- 5) Quit

Choice :

3. Select Option 2 and press Enter. The following message appears:

SAM server IP address :

SAM server port [18183] :

Choose SAM server (X.X.X.X) communication type:

1) clear No authentication (use for debugging only)

2) sslca: Certificate based authentication (recommended)

Choice :

4. Select an option. It is recommended to choose option 2. If you choose option 2, your Scout must be registered at the Check Point SmartCenter Management Station. See *Registering the Scout with the CheckPoint SmartCenter Management Station* for more information.

After selecting an option, the following message appears:

Scout should be restarted for changes to be applied.

Restart Scout? (yes/no) [yes] :

5. Select *yes* to apply the configuration.
6. If you have not already done so, you must select the block with Scout and Firewall option from the Block Method tab in the Policy dialog box of your Site or Enterprise Manager. See the ActiveScout Site or Enterprise Manager User's Guide for more information.

Configure the ELA Client

If you are working with the FireWall-1® ELA external logging system, you must configure the ELA logger. In addition, if the ELA client is configured using the sslca authentication method, you will be required to register the Scout at the SmartCenter Management Station. Messages regarding sslca communication are displayed at the SmartCenter in the SmartView status window.

To configure the ELA client:

1. Log in to the Scout machine.
2. Run the following command: *fstool opsec*. The OPSEC configuration menu appears.

OPSEC Configuration Menu:

1) Add ActiveScout object to SmartCenter Server

2) Configure SAM client

3) Configure ELA client

4) *Start AMON server*

5) *Quit*

Choice :

3. Select Option 3 and press Enter. The following message appears:

ELA server IP address:

ELA server port [18183] :

Choose ELA server (X.X.X.X) communication type:

1) *clear No authentication (use for debugging only)*

2) *sslca: Certificate based authentication (recommended)*

Choice :

4. Select an option. It is recommended to choose option 2. If you choose option 2, your Scout must be registered at the Check Point SmartCenter Management Station. See *Registering the Scout with the CheckPoint SmartCenter Management Station* for more information.

After selecting an option, the following message appears:

Scout should be restarted for changes to be applied.

Restart Scout? (yes/no) [yes] :

5. Select *yes* to apply the configuration.