



Third Party Product Integration

Overview

The Management Center for Cisco Security Agents provides integration with other third party products. This section provides information on supported third party integration applications.

In most cases, you are referred to the third party documentation for configuration information.

This section contains the following topics.

- [Cisco VPN Client Support, page 13-2](#)
- [Cisco Security Monitor Integration Support, page 13-2](#)
- [netForensics Integration Support, page 13-2](#)
- [Check Point™ OPSEC™ Integration, page 13-3](#)
- [Configuration Prerequisites, page 13-3](#)
- [Integration Configuration, page 13-4](#)

Cisco VPN Client Support

The Cisco Security Agent is a supported configuration for the "Are You There?" feature of the Cisco VPN Client, Release 4.0. For configuration details, please refer to Chapter 1 of the Cisco VPN Client Administrator Guide, in the section entitled "Configuring VPN Client Firewall Policy -- Windows Only."

Cisco Security Monitor Integration Support

Cisco Security Monitor is a Security Information Management application that can receive security events from multiple devices. Security Monitor presents the information in a real-time, web-based console so that these events can be managed across the network. Security Monitor also provides event notification, event reporting, and event correlation.

To integrate events generated by the Cisco Security Agent with the Security Monitor application, refer to Chapter 3 of your Security Monitor documentation, "Configuring Devices to Monitor."

netForensics Integration Support

netForensics is a Security Information Management application that can receive security events from multiple devices. This gives the administrator the convenience of having a single point from which to manage events from heterogeneous sources. netForensics presents the information in a real-time, web-based console so that these events can be managed across the network.

To integrate events generated by the Cisco Security Agent with the netForensics application, refer to your netForensics documentation.

Check Point™ OPSEC™ Integration

The Check Point™ OPSEC™ (Open Platform for Security) provides a set of API's (Application Programming Interfaces) which allow integration of various network security components. The SCV (Secure Configuration Verification) API provides a mechanism by which the configuration of a machine running the VPN-1® SecureClient™ can be verified.

With its Cisco Security Agent product, Cisco provides an “SCV Check” which can be used to verify that the agent is running on machines connecting via the VPN-1 SecureClient. With such a configuration, machines which fail the “SCV Check” are not allowed to establish connections through the Firewall.

Configuration Prerequisites

The following components are required to integrate the Cisco Security Agent as an SCV check within the OPSEC framework:

- On Machine A, an installation of Management Center for Cisco Security Agents, version 4.0 or greater.
- On Machine B, an installation of the Check Point VPN-1 & Firewall-1®, along with the Management Client and Policy Server, all of which are components of Check Point NG FP1 (Next Generation Feature Pack 1). The Firewall should be configured for VPN-1 SecureClient use.
- On Machine C, an installation of the Check Point VPN-1 SecureClient which points to the Firewall on Machine B. Also on Machine C, an installation of the Cisco Security Agent, installed from the Management Center for Cisco Security Agents on Machine A. (See the *Caution* below.)



Caution

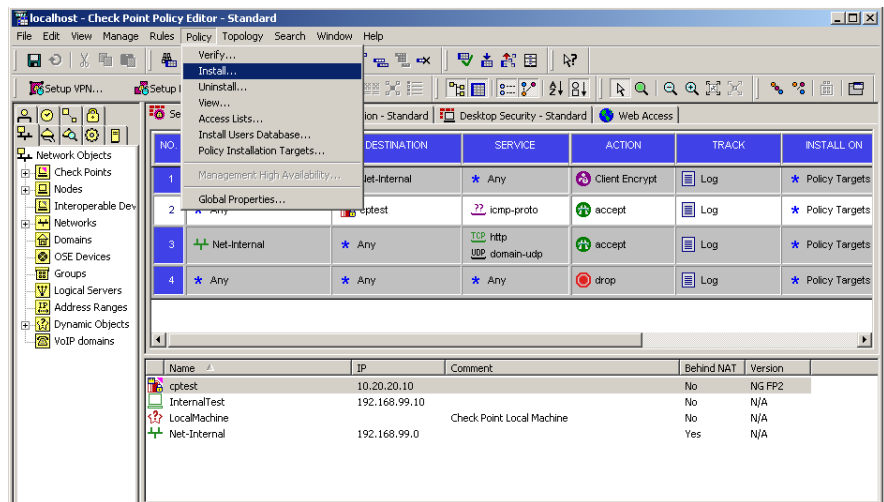
On Machine C, it is important that you install the SecureClient software before you install the Cisco Security Agent.

Integration Configuration

This section provides the procedure for deploying the SCV check. The following instructions assume the existence of (and refer to) the prerequisites described in the previous section. These instructions also refer to a file called `LOCAL.SCV`, which is accessible from the self-extracting executable located `ThirdParty\OpSec\SCV.exe` on the CSA MC product CD.

- Step 1** On Machine B, copy the `LOCAL.SCV` file from the CD to the `\winnt\fw1\ng\conf` directory. Note that any pre-existing versions of `LOCAL.SCV` should be renamed so that they are not overwritten.
- Step 2** Using the Check Point™ Policy Editor, perform a Policy->Install onto Machine C and on to any other SecureClient machines for which the SCV check “CSAgent” is to be enforced. (Configuration for enforcing SCV checks varies across Check Point™ Feature Packs. Please refer to the "Desktop Security Guide" for VPN-1 and SecureClient configuration details.)

Figure 13-1 Check Point Policy Editor



- Step 3** On Machine C (and other relevant SecureClient machines), the new policy will automatically be downloaded. With the SCV check now enforced, only machines with an installed (and running)

Cisco Security Agents are allowed to establish connections through the Firewall. Otherwise, the user receives a message box stating “Cisco Security Agent SCV Check Failed.”



Note No configuration is required on the client side. The Cisco Security Agent installation automatically installs and registers the relevant files.
