



CHAPTER 10

Router Platform Policies

This chapter describes how to troubleshoot common problems that might occur when you configure router platform policies on Cisco IOS routers and includes the following topics:

- [Configuring Routers Running IOS Software Releases 12.1 and 12.2, page 10-1](#)
- [Managing Encrypted Passwords on IOS Routers, page 10-2](#)
- [Troubleshooting Device Interface Policies, page 10-2](#)
- [Troubleshooting NAT Policies, page 10-2](#)
- [Troubleshooting PVC Policies, page 10-4](#)
- [Troubleshooting Device Access Policies, page 10-4](#)
- [Troubleshooting DHCP Policies, page 10-5](#)
- [Troubleshooting SDP Policies, page 10-5](#)
- [Troubleshooting SNMP Policies, page 10-6](#)
- [Troubleshooting NAC Policies, page 10-6](#)
- [Troubleshooting Static Routing Policies, page 10-7](#)



Note

For more detailed information on working with routers, see the “Managing Routers” chapter in the [User Guide for Cisco Security Manager](#) for your release.

Configuring Routers Running IOS Software Releases 12.1 and 12.2

Security Manager provides limited support for routers running Cisco IOS Software Releases 12.1 and 12.2. You can configure the following policies on these routers:

- Access Rules (Layer 3 only).
- Access Rule Settings.
- Interfaces.
- FlexConfigs.

All other policies require Cisco IOS Software Release 12.3 or higher. For more information, see [Supported Devices and Software Versions for Cisco Security Manager](#) for your release.

Managing Encrypted Passwords on IOS Routers

The manner in which Security Manager discovers and manages encrypted passwords on Cisco IOS routers varies from policy to policy, as follows:

- **Accounts and Credentials**—The encrypted password is discovered and is displayed by the Security Manager interface as asterisks. Any change that you make to the password causes it to be deployed to the device as a clear-text password.
- **PPP**—The encrypted password is discovered and is displayed by the Security Manager interface as asterisks. If you make any changes, you have the option of deploying the modified password either as encrypted or as clear text.
- **SDP and Line Access (console and VTY)**—The encrypted password is not discovered. The password defined on the device is not removed from the configuration unless you define and deploy a new password in Security Manager.

Troubleshooting Device Interface Policies

This section describes how to troubleshoot the following problems that might occur when you configure device interface policies on Cisco IOS routers in Security Manager:

- [Deploying Layer 2 Interface Definitions, page 10-2](#)
- [Deleting an Interface Still in Use, page 10-2](#)

Deploying Layer 2 Interface Definitions

Problem Deployment fails if the interface policy includes a definition for a Layer 2 interface.

Solution Layer 2 interfaces do not support Layer 3 interface definitions, such as IP addresses. Make sure that you did not define a Layer 3 definition on the Layer 2 interface.

Deleting an Interface Still in Use

Problem Activity submission fails after you delete an entry on the Interfaces page.

Solution If an interface is referenced as part of a policy definition, deleting that interface causes activity submission to fail. You must first remove the interface from the policy definition, then delete the interface.

Troubleshooting NAT Policies

This section describes how to troubleshoot the following problems that might occur when you configure NAT policies on Cisco IOS routers in Security Manager:

- [VPN Traffic Sent Unencrypted, page 10-3](#)
- [Loss of Communication Between Security Manager and Device, page 10-3](#)
- [Discovering Dynamic NAT Rules Containing Route Maps, page 10-3](#)

VPN Traffic Sent Unencrypted

Problem Traffic that should be sent encrypted over a VPN is instead being sent unencrypted.

Solution Ensure that you are not performing NAT on VPN traffic. Performing address translation on VPN traffic prevents the traffic from being encrypted and sent through the VPN tunnel. When defining dynamic NAT rules, make sure that you do *not* deselect the Do Not Translate VPN Traffic check box, even when you perform NAT into IPsec. (This option does not interfere with the translation of addresses arriving from overlapping networks.)



Note

This option can be used only on site-to-site VPNs. For remote access VPNs, you need to create an ACL object that explicitly denies the flow containing VPN traffic and define this ACL as part of a dynamic rule in the NAT policy. For more information, see Defining Dynamic NAT Rules in the “Managing Routers” chapter of the [User Guide for Cisco Security Manager](#) for your release.

Loss of Communication Between Security Manager and Device

Problem Communication between Security Manager and a particular device is interrupted after you deploy a NAT policy to that device.

Solution Make sure that you are not using a local address on the device as the original address to be translated. Translating this address might result in translating the management traffic sent between Security Manager and the device, causing the interruption.

Discovering Dynamic NAT Rules Containing Route Maps

Problem After you discover dynamic NAT rules configured with route maps, you find that Security Manager creates new equivalent rules without route maps instead of reusing the existing configuration.

Solution Earlier versions of Security Manager, 3.0 and 3.0.1, defined dynamic NAT translations using route maps that reference access lists (ACLs). Security Manager 3.1 and forward defines these translations using direct references to the ACLs without using route maps. As a result, if you use Security Manager 3.2 to discover dynamic NAT rules that are configured with route maps, Security Manager creates new rules that are equivalent to the old ones (including new ACLs), without using route maps. The existing rules and ACLs are left intact on the device.

Troubleshooting DSL Policies

This section describes how to troubleshoot the following problem that might occur when you configure DSL policies on Cisco IOS routers in Security Manager:

- [Unable to Deploy ADSL Policy, page 10-4](#)

Unable to Deploy ADSL Policy

Problem Deployment fails for your ADSL policy.

Solution Make sure that you have selected the correct ATM interface card type in the policy definition. Security Manager cannot properly validate the policy definition without knowing the correct card type, which can lead to deployment failures.

Troubleshooting PVC Policies

This section describes how to troubleshoot the following problem that might occur when you configure PVC policies on Cisco IOS routers in Security Manager:

- [Unable to Deploy PVC Policy, page 10-4](#)
- [Unable to Deploy IP Protocol Mappings, page 10-4](#)

Unable to Deploy PVC Policy

Problem Deployment fails for your PVC policy.

Solution Make sure that you have selected the correct ATM interface card type in the policy definition. Security Manager cannot properly validate the policy definition without knowing the correct card type, which can lead to deployment failures.

Unable to Deploy IP Protocol Mappings

Problem Deployment fails when you select the None option in the Define Mapping dialog box. Mappings are required by the PVC to discover which IP address is reachable at the other end of a connection. The None option disables broadcast options for the map entry.

Solution This problem is known to occur when using Cisco IOS Software Releases 12.4(07.24)T01, 12.4(07.24)T02, and 12.4PI07, as described in CSCin99787 and CSCse05292. This problem is corrected in Cisco IOS Software Releases 12.4(09.10)T and 12.4(09)T01. Therefore, we recommend that you upgrade the Cisco IOS Software Release running on the device. If this is not possible, select one of the other options available in the Define Mapping dialog box (Broadcast or No Broadcast).

Troubleshooting Device Access Policies

This section describes how to troubleshoot the following problem that might occur when you configure device access policies on Cisco IOS routers in Security Manager:

- [Unable to Configure Device, page 10-5](#)

Unable to Configure Device

Problem Security Manager cannot configure a device after you unassign a device access policy from the device and redeploy it.

Solution Device access policies can be used to define the enable password for accessing the device. If you later unassign this policy and redeploy, the password is removed from the device. In such cases, the device typically reverts to the default password. However, in some cases, the device might contain an additional password that is unknown to Security Manager, such as a line console password. If this additional password exists, the device reverts to that password instead of the default password. If that happens, Security Manager cannot configure this device. Therefore, if you use a device access policy to configure the enable password or enable secret password on a device, make sure that you do not unassign the policy without assigning a new policy before the next deployment.

Troubleshooting DHCP Policies

This section describes how to troubleshoot the following problem that might occur when you configure DHCP policies on Cisco IOS routers in Security Manager:

- [DHCP Traffic Not Being Transmitted, page 10-5](#)

DHCP Traffic Not Being Transmitted

Problem DHCP traffic is not being transmitted even after you deploy a DHCP policy to the device.

Solution Check whether an access rule on the device blocks Bootstrap Protocol (BootP) traffic. Having such a rule prevents DHCP traffic from being transmitted.

Troubleshooting SDP Policies

This section describes how to troubleshoot the following problem that might occur when you configure SDP policies on Cisco IOS routers in Security Manager:

- [Unable to Deploy SDP Policy with Local CA Defined, page 10-5](#)

Unable to Deploy SDP Policy with Local CA Defined

Problem You cannot deploy an SDP policy that uses the local CA server option to authenticate the identity of petitioners.

Solution The CA server was not configured locally on the router serving as the registrar. Enter the command `Crypto pki server [name]` using the CLI or FlexConfigs.

Troubleshooting SNMP Policies

This section describes how to troubleshoot the following problems that might occur when you configure SNMP policies on Cisco IOS routers in Security Manager:

- [Selected Traps Not Being Sent by Device, page 10-6](#)
- [Removing SNMP Traps Unintentionally from Device, page 10-6](#)

Selected Traps Not Being Sent by Device

Problem The device is not generating CPU and IP multicast traps, even though you selected these options in the assigned SNMP policy.

Solution The CPU and IP multicast traps require that you configure additional CLI commands to enable these traps on the router.

The CPU trap, which notifies users when a predefined threshold of CPU usage is crossed, requires that you define the rising and falling thresholds that determine when a trap is generated. For more information, go to:

http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455772.html

The IP multicast trap, which monitors the health of multicast deliveries and issues a trap when the delivery fails to meet certain parameters, requires you to define a multicast group address (Class D address, from 224.0.0.0 to 239.255.255.255) as well as other parameters related to the heartbeat. For more information, see the *Cisco IOS IP Multicast Command Reference*.

You can also use FlexConfigs to fully configure these traps.

Removing SNMP Traps Unintentionally from Device

Problem Disabling trap types in the SNMP policy removes additional traps on the device. For example, if you disable the IPSec tunnel trap, all IPSec-related traps are removed from the device.

Solution This is a known IOS issue documented in bug [CSCsg71381](#). The workaround is to reconfigure the unintentionally removed traps in Security Manager, then redeploy.

Troubleshooting NAC Policies

This section describes how to troubleshoot the following problems that might occur when you configure NAC policies on Cisco IOS routers in Security Manager:

- [NAC Not Implemented on Router, page 10-7](#)
- [Deployment of NAC Policy Fails, page 10-7](#)

NAC Not Implemented on Router

Problem Network admission control is not being implemented on the router, even though a NAC policy was deployed to it.

Solution Ensure that the default ACL on the router permits UDP traffic over the port defined in the NAC policy for EAP over UDP traffic. This is the protocol that NAC uses for communication between the Cisco Trust Agent (CTA), which is the NAC client that provides posture credentials for the endpoint device on which it is installed and the network access device (NAD; in this case, the router) that relays the posture credentials to the AAA server for validation. The default port used for EAP over UDP traffic is 21862, but you can change this port as part of the NAC policy. If the default ACL blocks UDP traffic, EAP over UDP traffic is likewise blocked, which prevents NAC from taking place.

Deployment of NAC Policy Fails

Problem Deployment fails after defining a NAC policy on a device that also has an authentication proxy.

Solution Make sure that the NAC policy and the authentication proxy use the same intercept ACL.

Troubleshooting Static Routing Policies

This section describes how to troubleshoot the following problems that might occur when you configure static routing policies on Cisco IOS routers in Security Manager:

- [Floating Route Not Inserted When Static Route Used as Backup, page 10-7](#)
- [Deployment Fails After Database Upgrade, page 10-7](#)

Floating Route Not Inserted When Static Route Used as Backup

Problem The static route you defined in Security Manager as a backup, “floating” route is not inserted in the routing table when the primary link fails.

Solution When using a static route as a floating route, you must specify the interface for the next hop instead of entering a specific IP address. For more information, go to:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800ef7b2.shtml

Deployment Fails After Database Upgrade

Problem Deployment and preview configuration fail for static routing policies after you upgrade to Security Manager 3.2 from version 3.0.1 or earlier.

Solution Delete the device from Security Manager, then add it back and perform discovery.



Note

This problem occurs only when the static routing policy was deployed or previewed in a version of Security Manager earlier than version 3.1. In addition, it affects only static routing policies that use the forwarding IP option rather than the forwarding interface option.

