



FAQ and Troubleshooting Guide for Cisco Security Manager 3.3

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

FAQ and Troubleshooting Guide for Cisco Security Manager 3.3
© 2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface ix

Audience ix

Conventions ix

Product Documentation x

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

Security Manager Server 1-1

Collecting Server Troubleshooting Information 1-1

Security Manager Database 1-2

Restoring the Database Using Backed-Up Files 1-3

Restoring the Database from an Installation prior to Installing Service Packs 1-3

Unable to Launch the Security Manager Server 1-3

Restricting Access to the Security Manager Server 1-4

Installation, Uninstallation, or Reinstallation 1-4

CHAPTER 2

Security Manager Client 2-1

FAQs About the Security Manager Client 2-1

Resetting the Client Password 2-2

Using HTTP to Communicate with Server 2-3

Display Problems in Dual-Screen Setup 2-3

Wrong Message During Reinstallation of Client 2-5

Unable to Upgrade From a Previous Version of Client 2-5

Removing Another User's Locks in Non-Workflow Mode 2-6

Loading the Online Help 2-6

Preserving Search Results in Online Help 2-7

Unable to Display Activity Report 2-7

Installation, Uninstallation, or Reinstallation 2-7

CHAPTER 3

Security Manager and Cisco Secure ACS 3-1

Using Multiple Versions of Security Manager with Same ACS 3-1

Authentication Fails When in ACS Mode 3-2

System Administrator Granted Read-Only Access 3-2

ACS Changes Not Appearing in Security Manager 3-3

Devices Configured in ACS Not Appearing in Security Manager 3-3

Working in Security Manager after Cisco Secure ACS Becomes Unreachable 3-3

Restoring Access to Cisco Secure ACS 3-4

Authentication Problems with Multihomed Devices 3-4

Authentication Problems with Devices Behind a NAT Boundary 3-4

Updating Device Credentials via Cisco Secure ACS 3-4

CHAPTER 4

Cisco Security Agent 4-1

FAQs About the Cisco Security Agent 4-1

Installation, Uninstallation, or Reinstallation 4-2

CHAPTER 5

Device Management 5-1

Troubleshooting Device Communication Failures 5-1

FAQs About Device Communication 5-2

Security Certificate Rejected When Discovering Device 5-2

Invalid Certificate Error During Device Discovery 5-3

Deleting Configuration File When Deleting Security Context 5-3

Simultaneous Operations on the Same Device 5-3

Troubleshooting the Setup of Configuration Engine-Managed Devices 5-4

CHAPTER 6

Policy Discovery 6-1

FAQs About Policy Discovery 6-1

Performing Discovery in a Multi-User Environment 6-5

SSL VPN Policies Negated When Discovered From Configuration File 6-6

Undiscovered VPN Features 6-6

ACL Names Preserved by Security Manager 6-6

 ACL Naming Conventions 6-7

 Resolving Conflicts Between Policies 6-9

Resource Names Changed by Security Manager 6-9

 Name Changes in PIX/ASA Object Groups 6-10

 Name Changes in AAA Rules Policies 6-11

 Name Changes in Access Rules Policies 6-11

 Name Changes in Inspection Rules Policies 6-12

 Name Changes in Transparent Rules Policies 6-12

 Name Changes in Dynamic NAT Policies 6-13

 Name Changes in Service Policy Rules Policies 6-13

Name Changes in Dialer Policies	6-14
Name Changes in PPP Policies	6-15
Name Changes in AAA Policies	6-15
Name Changes in HTTP Policies	6-15
Name Changes in Line Access Policies	6-15
Name Changes in NAC Policies	6-17
Name Changes in Quality of Service Policies	6-17

CHAPTER 7**Firewall Services 7-1**

FAQs About Firewall Services	7-1
------------------------------	-----

CHAPTER 8**IPS 8-1**

Importing IPS 5.0 Sensors	8-1
Retrieving Signature Updates	8-1
Performing IPS Updates	8-2
Updating IOS IPS Crypto Configurations	8-2
Creating ACLs During IOS IPS Configuration	8-3
Performing IOS IPS Deployment	8-3
Provisioning Trusted Hosts	8-3
Managing Signature Updates	8-3

CHAPTER 9**VPNs 9-1**

Updating VPNs That Include Routing Processes	9-2
Loss of Communication with Spoke	9-2
Configuring PKI with AAA on IOS Devices	9-2
Defining Multiple CA Servers for Site-to-Site VPNs	9-2
Unneeded Policy in Easy VPN Topology	9-5
Discovering a VPN Already Configured in Security Manager	9-5
Enabling and Disabling VRF on Catalyst Switches and 7600 Devices	9-5
Commands That Cannot be Configured When Easy VPN is Enabled	9-6
Defining VPNs with Multiple Spoke Definitions	9-7
SSL VPN Limitations	9-8
SSL VPN Limitations Due to Device OS Defects	9-9
Removing Group Policy Attributes from SSL VPNs Defined on ASA 7.x Devices	9-9
VPN Policy Discovery Fails When Backup Servers Use Hostname	9-10
Provisioning GET VPN Using Security Manager Is Not Working	9-10

Preshared Key Policies Not Getting Discovered 9-11
 Edit Wizard of GETVPN Does Not Allow Editing of Key Servers or Group Members 9-11

CHAPTER 10

Router Platform Policies 10-1

Configuring Routers Running IOS Software Releases 12.1 and 12.2 10-1
 Managing Encrypted Passwords on IOS Routers 10-2
 Troubleshooting Device Interface Policies 10-2
 Deploying Layer 2 Interface Definitions 10-2
 Deleting an Interface Still in Use 10-2
 Troubleshooting NAT Policies 10-2
 VPN Traffic Sent Unencrypted 10-3
 Loss of Communication Between Security Manager and Device 10-3
 Security Manager Indicates Deployment Failed on an 83x Router 10-3
 Troubleshooting DSL Policies 10-3
 Unable to Deploy ADSL Policy 10-4
 Troubleshooting PVC Policies 10-4
 Unable to Deploy PVC Policy 10-4
 Unable to Deploy IP Protocol Mappings 10-4
 Troubleshooting Device Access Policies 10-4
 Unable to Configure Device 10-5
 Troubleshooting DHCP Policies 10-5
 DHCP Traffic Not Being Transmitted 10-5
 Troubleshooting SDP Policies 10-5
 Unable to Deploy SDP Policy with Local CA Defined 10-5
 Troubleshooting SNMP Policies 10-6
 Selected Traps Not Being Sent by Device 10-6
 Troubleshooting NAC Policies 10-6
 NAC Not Implemented on Router 10-6
 Deployment of NAC Policy Fails 10-7
 Troubleshooting Static Routing Policies 10-7
 Floating Route Not Inserted When Static Route Used as Backup 10-7

CHAPTER 11

Catalyst Switches and 7600 Devices 11-1

FAQs about Catalyst Switches and 7600 Devices 11-1
 Discovering Failover Pairs 11-2
 Deployment Fails for Interface Settings 11-2
 Deployment Fails for Internal VLANs 11-2

Deployment Fails When Changing the Running Mode of an ISDM Data Port VLAN 11-3

CHAPTER 12
Deployment 12-1

FAQs About Deployment 12-1

Changing How Security Manager Responds to Device Messages 12-8

Performing Rollback When Deploying to a File 12-9

Mixing Deployment Methods 12-9

SSL Handshake Failure When Deploying to PIX/ASA Devices 12-10

Deployment Failures to Devices Managed by AUS 12-10

Deployment Failures to FWSM Virtual Contexts After Changing Interface Policies 12-11

CHAPTER 13
**Interoperation of CS-MARS
and Security Manager 13-1**

FAQs about Policy Lookup from a CS-MARS Event 13-1

Policy Lookup for Events Generated by Devices with Multiple Contexts 13-12

FAQs about CS-MARS Events Lookup
from a Security Manager Policy 13-13

Changing the Association of the CS-MARS Appliance
with a Device 13-19

Configuring Required Browser Settings
for Policy and Events Lookup 13-19

Working with Cached Passwords in Internet Explorer 13-20

Setting Internet Explorer Security Options 13-20

Setting Internet Explorer to Allow Display of Nonsecure Content 13-21

INDEX



Preface

Revised: June 15, 2009, OL-19986-01

This document contains FAQs and troubleshooting information for Cisco Security Manager 3.3. The content contained herein is a collection of specific tips, and answers regarding particular situations, organized by topic area.



Note

This is not an operating manual. For comprehensive information on setting up and operating your Cisco Security Manager, select the [end-user guide](#) that matches your system.

Audience

This document is intended for the network administrator with expertise in network security, including the use and configuration of firewalls, VPNs, and IPS sensors.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Selecting a menu item	Option > Network Preferences

Product Documentation

For a list of available product documentation, see the appropriate *Guide to User Documentation for Cisco Security Manager* at the following URL on Cisco.com:

http://www.cisco.com/en/US/products/ps6498/products_documentation_roadmaps_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Security Manager Server

This chapter contains the following topics:

- [Collecting Server Troubleshooting Information, page 1-1](#)
- [Security Manager Database, page 1-2](#)
- [Restoring the Database Using Backed-Up Files](#)
- [Unable to Launch the Security Manager Server, page 1-3](#)
- [Restricting Access to the Security Manager Server, page 1-4](#)
- [Installation, Uninstallation, or Reinstallation, page 1-4](#)



Note

For detailed information on installing and uninstalling the Security Manager Server, see the [installation guide for Cisco Security Manager](#) for your release.

Collecting Server Troubleshooting Information

If you are experiencing problems with Security Manager, and you cannot resolve the problem after trying all the recommendations listed in the error message and reviewing this guide for a possible solution, use the Security Manager Diagnostics utility to collect server information.

The Security Manager Diagnostics utility collects server diagnostic information in a ZIP file (CSMDiagnostics.zip) that you overwrite with new information each time you run Security Manager Diagnostics. The information in your CSMDiagnostics.zip file can help a Cisco technical support engineer troubleshoot any problems that you might have with Security Manager or its related applications on your server.



Tip

Security Manager also includes an advanced debugging option that collects information about the configuration changes that have been made with the application. To activate this option, select **Tools > Security Manager Administration > Debug Options**, then select the **Capture Discovery/Deployment Debugging Snapshots to File** check box. Bear in mind that although the additional information saved to the diagnostics file may aid the troubleshooting effort, the file may contain sensitive information, such as passwords. You should change debugging levels only if the Cisco Technical Assistance Center (TAC) asks you to change them.

**Note**

There is no requirement to submit a CSMDiagnostics.zip file when you first submit a problem report. Your support engineer provides you with a method to submit the file if it is required.

You can run Security Manager Diagnostics in either of two ways.

From a Security Manager client system:	From a Security Manager server:
<ol style="list-style-type: none"> 1. On a client system from which you have established a Security Manager Client session to your server, click Tools > Security Manager Diagnostics. 2. Click OK to generate the diagnostics file. The resulting ZIP file (CSMDiagnostics.zip) is saved on your server in the <i>NMSROOT\MDC\etc\</i> directory, where <i>NMSROOT</i> is the directory where you installed Common Services (C:\Program Files\CSCOpX, for example). 3. Click Close to close the Security Manager Diagnostics dialog box. <p>Note We recommend that you rename this file so it does not get overwritten each time you run this utility.</p>	<ol style="list-style-type: none"> 1. Select Start > Run, then enter command. Alternatively, if your server keyboard includes a Windows key, press Windows-R, then enter command. 2. Enter C:\Program Files\CSCOpX\MDC\bin\CSMDiagnostics. Alternatively, to save the ZIP file in a different location than <i>NMSROOT\MDC\etc\</i>, enter CSMDiagnostics drive:\path. For example, CSMDiagnostics D:\temp.

Security Manager Database

This procedure describes the steps to take to back up the Security Manager database.

Procedure

- Step 1** Back up the database:
- a. Select **Tools > Backup**. The Backup Job page of CiscoWorks Common Services is displayed in a browser window.
 - b. Select a backup directory and schedule the operation.
 - c. Click **Apply**.

**Note**

Security Manager is shut down during the backup process. This is to prevent any inconsistency between different databases and data files. For complete details, click **Help** in the Common Services window to view the online help topic for “Scheduling a Backup”.

- Step 2** Send the database to TAC for troubleshooting.
- Step 3** After TAC corrects the problem and sends the database back to you, restore it in your system. For details, see “Backing up and Restoring the Security Manager Database” in the *Managing the Security Manager Server* chapter of the User Guide for your release:

http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html

Step 4 Change the database password.

For the procedure, see “Changing the Database Password” in the CiscoWorks Common Services online help. For quick results, access the online help and use the search function to find this topic.

Restoring the Database Using Backed-Up Files

Problem You want to restore a backup from a set of files that were not created using the backup mechanism in CiscoWorks Common Services.

Solution Restoring the Security Manager database directly from backed up files introduces a variety of potential problems, including hostname issues, file permission issues, database password issues, and file consistency issues. Therefore, we strongly recommend using the backup and restore mechanism in CiscoWorks Common Services to restore the Security Manager database.

Restoring the Database from an Installation prior to Installing Service Packs

Problem You want to restore a database that was backed up prior to installing service packs.

Solution If you have installed any service packs on your server and you restore a database that was backed up prior to installing those services packs, you must reapply the service packs after restoring the database.

Unable to Launch the Security Manager Server

Problem When you try to launch Security Manager, you receive a message that indicates you do not have permission to access /cwhp/LiaisonServlet on the Security Manager server.

Solution [Table 1-1](#) describes common causes and suggested workarounds for this problem.

Table 1-1 Causes and Workarounds for LiaisonServlet Error

Cause	Workaround
Anti-virus application installed on server	Uninstall the anti-virus application.
IIS installed on server	As stated in the <i>Installation Guide for Cisco Security Manager</i> , IIS is not compatible with Security Manager and must be uninstalled.

Table 1-1 Causes and Workarounds for LiaisonServlet Error (continued)

Cause	Workaround
Services required by Security Manager do not start in proper order	The only service that should be set to Automatic is the Cisco Security Manager Daemon Manager. All other CiscoWorks services should be set to Manual. Please note that it may take the Daemon Manager a few minutes to start up the other Ciscoworks services. These services must start up in the proper order; manually starting up the services can cause errors.
casuser password	The casuser login is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. Reset the casuser password as follows: <ol style="list-style-type: none"> 1. Open a command line. 2. Type <code>C:\Program Files\CSCOpX\setup\support\resetCasuser.exe</code>, then press Enter. 3. Choose option 1 (Randomly generate casuser password).

Restricting Access to the Security Manager Server

Problem You want to restrict access to the Security Manager server to a defined number of hosts based on the client IP address.

Solution Assuming that Security Manager is configured as part of a NOC (network operations center), you can configure ACLs on the firewall or router that acts as the perimeter device between the NOC and the other hosts. The ACLs should permit access to the Security Manager server over ports 443 and 1741 to specific IP addresses only. If Security Manager is managing the perimeter device, you can define these ACLs in an Access Rules policy and deploy the policy to the device.

Installation, Uninstallation, or Reinstallation

See the “Troubleshooting” chapter in the [installation guide for Cisco Security Manager](#) for your release, for information about troubleshooting problems that are related to the installation, uninstallation, or reinstallation of:

- Security Manager (including Common Services) software on a server.
- Security Manager Client.
- The standalone version of Cisco Security Agent that is installed on most Security Manager servers.



CHAPTER 2

Security Manager Client

This chapter contains the following topics:

- [FAQs About the Security Manager Client, page 2-1](#)
- [Resetting the Client Password, page 2-2](#)
- [Using HTTP to Communicate with Server, page 2-3](#)
- [Display Problems in Dual-Screen Setup, page 2-3](#)
- [Wrong Message During Reinstallation of Client, page 2-5](#)
- [Unable to Upgrade From a Previous Version of Client, page 2-5](#)
- [Removing Another User's Locks in Non-Workflow Mode, page 2-6](#)
- [Loading the Online Help, page 2-6](#)
- [Preserving Search Results in Online Help, page 2-7](#)
- [Installation, Uninstallation, or Reinstallation, page 2-7](#)
- [Unable to Display Activity Report, page 2-7](#)



Note

For detailed information on installing and uninstalling the Security Manager Client, see the “Installing or Uninstalling Security Manager Client” chapter in the [installation guide for Cisco Security Manager](#) for your release.

FAQs About the Security Manager Client

This section answers the following questions about the Security Manager client:

- [Q.Can I install the Security Manager client on the same machine as the Security Manager server?](#)
- [Q.How can I clean up the server list from the Server Name field in the Login window?](#)
- [Q.What do I do if I forget to enter the server name during installation?](#)
- [Q.The Security Manager client GUI did not load because of a version mismatch. What does this mean?](#)
- [Q.Where are the client log files located?](#)
- [Q.How do I know if Security Manager is running in HTTPS mode?](#)

- Q.** Can I install the Security Manager client on the same machine as the Security Manager server?
- A.** We recommend that you do *not* install both the Security Manager server software and Cisco Security Manager client on the same system. However, if you do install it on the same system, if the Cisco Security Agent asks if you want to allow a process to start, you must allow it or the Security Manager client might behave erratically and stop working.
- Q.** How can I clean up the server list from the Server Name field in the Login window?
- A.** Delete `csmsserver.txt` from the directory in which you installed the Security Manager client. The default location is `C:\Program Files\Cisco Systems\Cisco Security Manager Client`.
- Q.** What do I do if I forget to enter the server name during installation?
- A.** In the Server Name field in the Login window, enter the server name. Names of servers that you successfully logged in to are remembered and appear in the list the next time you login.
- Q.** The Security Manager client GUI did not load because of a version mismatch. What does this mean?
- A.** The Security Manager server version does not match the client version. To fix this, download and install the most recent client installer from the server.
- Q.** Where are the client log files located?
- A.** The client log files are located in `C:\Program Files\Cisco Systems\Cisco Security Manager Client\logs`. Each GUI session has its own log file.
- Q.** How do I know if Security Manager is running in HTTPS mode?
- A.** Do one of the following:
- Look at the HTTPS check box in the Login window. If it is selected, Security Manager is running in HTTPS mode.
 - After you log in, look at the URL in the address field. If the URL starts with `https`, Security Manager is running in HTTPS mode.
 - Go to **Common Services > Server > Security > Single Server Management > Browser-Server Security Mode Setup**. If you see **Current Setting: Enabled**, Security Manager is running in HTTPS mode.
- Q.** How can I enable the Client Debug log level?
- A.** In the file `client.info`, which is located by default in `C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars`, modify the `DEBUG_LEVEL` parameters to include `DEBUG_LEVEL=ALL` and then restart the Security Manager client.

Resetting the Client Password

If you cannot remember the password to the Security Manager client that was entered during installation, an administrator can reset the password using this procedure.



Caution

This procedure does not require knowledge of the old password; therefore, it is important to keep the Security Manager server physically secure from unauthorized users.

-
- Step 1** On the Security Manager server, shut down the Cisco Security Manager Daemon Manager service.
 - Step 2** Navigate to *NMSROOT*\bin. The default value for this location is C:\Program Files\CSCOpX\bin.
 - Step 3** Open a command line and enter the command: `resetpasswd [username]`.
 - Step 4** At the prompt, enter and confirm new password. Passwords can range from 5 to 256 characters in length and can include any printable character.
 - Step 5** Restart the Daemon Manager.
-

Using HTTP to Communicate with Server

Problem You want the Security Manager client to use HTTP to communicate with the Security Manager server, instead of HTTPS.

Solution Do the following:

-
- Step 1** In a web browser, enter `http://[Security_Manager_server]:1741`. This launches the web interface for the Security Manager server.
 - Step 2** Log in as an administrator, then click the **CiscoWorks** link in the upper-right corner.
 - Step 3** Under Common Services, select **Server > Security > Single-Server Management > Browser-Server Security Mode Setup**.
 - Step 4** Change the setting from Enable to Disable.
 - Step 5** Click **Apply**.
 - Step 6** Restart the Security Manager server.
 - Step 7** When you start the Security Manager client, be sure to deselect the **HTTPS** check box on the login screen.
-



Note For security reasons, we recommend that you use HTTPS instead of HTTP.

Display Problems in Dual-Screen Setup

Problem When working with a dual-screen setup, certain windows and popup messages always appear on the primary screen, even when the Security Manager client is running on the secondary screen. For example, with the client running on the secondary screen, windows such as the Policy Object Manager always open in the primary screen.

Solution This is a known issue with the way dual-screen support is implemented in certain operating systems. We recommend running the Security Manager client on the primary screen. You should launch the client after configuring the dual-screen setup.

**Tip**

If a window opens on the other screen, you can move it by pressing Alt+spacebar, followed by M; you can then use the arrow keys to move the window.

Wrong Message During Reinstallation of Client

Problem When you attempt to install the Security Manager client (or perform a reinstall, for example, after upgrading the operating system), the installer displays a message stating that a previous version of the client is installed on your system and that it will be uninstalled.

Solution During installation or reinstallation of the client, the installer might detect a previously installed client, even if no such client exists, and display an incorrect message that it will be uninstalled. This message is displayed because of the presence of certain old registry entries in your system. Although client installation proceeds normally when this message appears, do the following to delete old registry entries and prevent this message from being displayed during subsequent installations:

-
- Step 1** At the command line, type `regedit`, then press **Enter** to open the Registry Editor.
 - Step 2** Remove the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Cisco Security Manager Client
 - Step 3** Delete the previous installation directory.
 - Step 4** Navigate to the `..\Program Files\Zero G Registry` folder and rename the “.com.zerog.registry.xml” file located under this folder.
-

Unable to Upgrade From a Previous Version of Client

Problem When you attempt to install the Security Manager client (or perform an upgrade from a previous version to 3.3), you receive the “Could not find main class. Program will exit.” error message.

Solution This problem occurs because of the presence of old registry entries in your system. To correct this problem, do the following:

-
- Step 1** At the command line, type `regedit`, then press **Enter** to open the Registry Editor.
 - Step 2** Remove the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{427e21299b0dd254754c0d2778feec4-837992615}
 - Step 3** Delete the previous installation directory.
 - Step 4** Rename the following folder:
C:\Program Files\Common Files\InstallShield\Universal\common\Gen1
 - Step 5** Select **Start > Control Panel > Add or Remove Programs**. If the Cisco Security Manager Client is still listed, click **Remove**. If you receive the message, “Program already removed; do you want to remove it from the list?”, click **Yes**.

**Note**

If you are still unable to reinstall the Security Manager client, rename the C:\Program Files\Common Files\InstallShield directory, then try again.

After you complete the preceding steps, no error message is displayed when you retry the installation or upgrade operation.

Removing Another User's Locks in Non-Workflow Mode

Problem When working in non-workflow mode, you discover that certain devices and policies that you need to configure are locked by another user. The locks remain in place until the other user submits or discards the configuration changes.

Solution If you have administrative permissions, you can remove the locks placed by another user by taking over that user's session. Select **Tools > Security Manager Administration > Take Over User Session**, then select the session. You can then submit or discard the user's changes to remove the locks.

Loading the Online Help

Problem You cannot load the online help.

Solution

When using Internet Explorer as your default browser, try the following:

- Windows Server 2003, Windows XP, or Windows Vista—Select **Tools > Internet Options > Advanced > Security > Allow active content to run in files on My Computer**.
- When you access online help the first time using Internet Explorer 6.0 or 7.0, the page does not load right away and you are prompted to a series of warning or error messages before it can be displayed. These messages are displayed because of the default security settings of your browser. For detailed instructions on the actions to take when you access online help for the first time with default browser settings and to import the Security Manager certificate to the root certificate store in your browser, see the “Installing or Uninstalling Security Manager Client” chapter in the *Installation Guide for Cisco Security Manager 3.3*.

When using Firefox as your default browser, try the following:

- Add the following line to open \Mozilla Firefox\defaults\pref\firefox.js:

```
pref("dom.allow_scripts_to_close_windows", true);
```
- Enable Javascript.
- When you access online help the first time, two new browser windows might be opened: a blank page and a page with help contents. Also, existing browser windows might not be reused during subsequent attempts to access online help. To configure Firefox to display online help on a new tab in the most recently opened browser window and to reuse existing windows on later occasions, see the “Installing or Uninstalling Security Manager Client” chapter in the *Installation Guide for Cisco Security Manager 3.3*.

Some third-party popup blockers enable you to allow popups from a specific site or server without allowing popups universally. If your popup blocker does not allow you to configure exceptions to include in a white list, or if that option fails to meet your requirements, you must set your utility to allow all popups. The method for allowing popups from a trusted site varies according to the utility that you use. Please refer to the third-party product's documentation for more information.

Preserving Search Results in Online Help

Problem When you click the link for one of the topics displayed in the online help search results, clicking the Search tab again (for example, to try a different topic listed in the search results) erases the results.

Solution Use the Back button in the browser instead of clicking the Search tab. The results of the previous search will still be displayed.

Unable to Display Activity Report

Problem If you are using Internet Explorer as your default browser, Activity Change Report in PDF does not appear when you click View Changes from the Tools menu (nonWorkflow mode), or Activity Manager (Workflow mode).

Solution This problem occurs because of inaccuracies with the location of some of the dll files or invalid registry key values associated with Internet Explorer. For information on how to work around this problem, refer to the Microsoft Knowledge Base article 281679, which is available at this URL: <http://support.microsoft.com/kb/281679/EN-US>.

Installation, Uninstallation, or Reinstallation

See the [installation guide for Cisco Security Manager](#) for your release for information about troubleshooting problems that are related to the installation, uninstallation, or reinstallation of:

- Security Manager (including Common Services) software on a server.
- Security Manager Client.
- The standalone version of Cisco Security Agent that is installed on most Security Manager servers.

For information regarding the installation of the Security Manager License, see *Cisco Security Manager 3.x: Steps to Install the License for Various Options* on Cisco.com at:

http://www.cisco.com/en/US/products/ps6498/products_tech_note09186a0080849150.shtml



CHAPTER 3

Security Manager and Cisco Secure ACS

This chapter describes how to troubleshoot common problems that could occur because of the way Security Manager and Cisco Secure ACS interact. It contains the following topics:

- [Using Multiple Versions of Security Manager with Same ACS, page 3-1](#)
- [Authentication Fails When in ACS Mode, page 3-2](#)
- [System Administrator Granted Read-Only Access, page 3-2](#)
- [ACS Changes Not Appearing in Security Manager, page 3-3](#)
- [Devices Configured in ACS Not Appearing in Security Manager, page 3-3](#)
- [Working in Security Manager after Cisco Secure ACS Becomes Unreachable, page 3-3](#)
- [Restoring Access to Cisco Secure ACS, page 3-4](#)
- [Authentication Problems with Multihomed Devices, page 3-4](#)
- [Authentication Problems with Devices Behind a NAT Boundary, page 3-4](#)
- [Updating Device Credentials via Cisco Secure ACS](#)

Using Multiple Versions of Security Manager with Same ACS

You cannot use the same Cisco Secure ACS with two different versions of Security Manager. For example, if you have integrated Security Manager 3.2 with a Cisco Secure ACS and another part of your organization plans to use Security Manager 3.3 *without* upgrading the existing installation, you must integrate Security Manager 3.3 with a different ACS than the one used for Security Manager 3.2.

If you upgrade an existing Security Manager installation, you can continue to use the same Cisco Secure ACS. The permission settings will be updated as required.

Authentication Fails When in ACS Mode

If authentication keeps failing when you log in to Security Manager or CiscoWorks Common Services, even though you used Common Services to configure Cisco Secure ACS as the AAA server for authentication, do the following:

- Ensure that there is connectivity between the ACS servers and the server running Common Services and Security Manager.
- Ensure that the user credentials (username and password) you are using are defined in ACS and are assigned to the appropriate user group.
- Ensure that the Common Services server is defined as a AAA client on the Network Configuration page of ACS. Verify that the shared secret keys defined in Common Services (AAA Mode Setup page) and ACS (Network Configuration) match.
- Ensure that the IP address of each ACS server is correctly defined on the AAA Mode Setup page in Common Services.
- Ensure that the correct account is defined on the Administration Control page of ACS.
- Go to the AAA Mode Setup page in Common Services and verify that Common Services and Security Manager (as well as any other installed applications, such as AUS) are registered with Cisco Secure ACS.
- Go to Administration Control > Access Setup in ACS and ensure that the ACS is configured for HTTPS communication.
- If you receive “key mismatch” errors in the ACS log, check whether the Security Manager server is defined as a member of a network device group (NDG). If it is, be aware that if you defined a key for the NDG, that key takes precedence over the keys defined for the individual devices in the NDG, including the Security Manager server. Ensure that the key defined for the NDG matches the secret key of the Security Manager server.

System Administrator Granted Read-Only Access

Problem You have read-only access to all policy pages of Security Manager even after logging in as a System Administrator with full permissions.

Solution Do the following in Cisco Secure ACS:

- (When using network device groups (NDGs)) Click **Group Setup** on the Cisco Secure ACS navigation bar, then verify that the System Administrator user role is associated with all necessary correct NDGs for *both* CiscoWorks and Cisco Security Manager, especially the NDG containing the Common Services/Security Manager server.
- Click **Network Configuration** on the navigation bar, then:
 - Verify that the Common Services/Security Manager server is not assigned to the Not Assigned (default) group.
 - Verify that the Common Services/Security Manager server is configured to use TACACS+ not RADIUS. TACACS+ is the only security protocol supported between the two servers.



Note You can configure the network devices (routers, switches, firewalls, and so on) managed by Security Manager for either TACACS+ or RADIUS.

ACS Changes Not Appearing in Security Manager

When you are using Security Manager with Cisco Secure ACS 4.x, information from ACS is cached when you log into Security Manager or CiscoWorks Common Services on the Security Manager server. If you make changes in the Cisco Secure ACS Network Configuration and Group Setup while logged into Security Manager, the changes might not appear immediately or be immediately effective in Security Manager. You must log out of Security Manager and Common Services and close their windows, then log in again, to refresh the information from ACS.

If you need to make changes in ACS, it is best practice to first log out of and close Security Manager windows, make your changes, and then log back into the product.

**Note**

Although Cisco Secure ACS 3.3 is not supported, if you are using that version of ACS, you must open Windows Services and restart the Cisco Security Manager Daemon Manager service to get the ACS changes to appear in Security Manager.

Devices Configured in ACS Not Appearing in Security Manager

Problem The devices that you configured on the Cisco Secure ACS are not appearing in Security Manager.

Solution The device display names defined in Security Manager *must* match the names you configure in ACS when you add the devices as AAA clients. This is particularly important when you use domain names. If you intend to append a domain name to the device name in Security Manager, the AAA client hostname in ACS must be <device_name>.<domain_name>, for example, pixfirewall.cisco.com.

Working in Security Manager after Cisco Secure ACS Becomes Unreachable

Security Manager sessions are affected if the Cisco Secure ACS cannot be reached. Therefore, you should consider creating a fault-tolerant infrastructure that utilizes multiple Cisco Secure ACS servers. Having multiple servers helps to ensure your ability to continue work in Security Manager even if connectivity is lost to one of the ACS servers.

If your setup includes only a single Cisco Secure ACS and you wish to continue working in Security Manager in the event the ACS becomes unreachable, you can switch to performing local AAA authentication on the Security Manager server. To change the AAA mode, do the following:

-
- Step 1** Log in to Common Services using the *admin* CiscoWorks local account.
 - Step 2** Select **Server > Security > AAA Mode Setup**, then change the AAA mode back to Non-ACS/CiscoWorks Local. This enables you to perform authentication and authorization using the local Common Services database and its built-in roles. Bear in mind that you must create local users in the AAA database to make use of local authentication.
 - Step 3** Click **Change**.
-

Restoring Access to Cisco Secure ACS

If you cannot access Security Manager because the Cisco Secure ACS is down, do the following:

- Open up Windows Services on the ACS server and check whether the CSTacacs and CSRADIUS services are up and running. Restart these services, if required.
- Perform the following procedure in CiscoWorks Common Services:

-
- Step 1** Log in to Common Services as the Admin user.
- Step 2** Open a DOS window and run `NMSROOT\bin\perl ResetLoginModule.pl`.
- Step 3** Exit Common Services, then log in a second time as the Admin user.
- Step 4** Go to **Server > Security > AAA Mode Setup**, then change the AAA mode to Non-ACS > CW Local mode.
- Step 5** Open Windows Services and restart the Cisco Security Manager Daemon Manager service.
-

Authentication Problems with Multihomed Devices

Problem You cannot configure a multihomed device (a device with multiple network interface cards (NICs)) that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions.

Solution When you define a multihomed device as a AAA client of the Cisco Secure ACS, make sure to define the IP address of each NIC. Press **Enter** between each entry. For more information, see *Adding Devices as AAA Clients Without NDGs* in the installation guide. For more information, see the *Installation Guide for Cisco Security Manager* for your release at http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

Authentication Problems with Devices Behind a NAT Boundary

Problem You cannot configure a device with a pre-NAT or post-NAT IP address that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions.

Solution When a device is behind a NAT boundary, make sure to define all IP addresses, including pre-NAT and post-NAT, for the device in the AAA client configuration settings in Cisco Secure ACS. For more information on how to add AAA client settings to ACS, see *User Guide for Cisco Secure Access Control Server*.

Updating Device Credentials via Cisco Secure ACS

Problem You update the credentials of your managed devices on a regular basis and want your Cisco Secure ACS to automatically update Security Manager with these new credentials.

Solution Perform the following procedure in CiscoWorks Common Services:

-
- Step 1** Log in to Common Services as the Admin user.
- Step 2** Click the **Device and Credentials** tab, then click **Device Management**.
- Step 3** On the Device Management page, click **Bulk Import**.
- Step 4** In the Import Devices popup window, do the following:
- a. In the Select a Layer field, click **Remote NMS**.
 - b. From the NMS Type list, select **ACS**.
 - c. Enter the details of your Cisco Secure ACS, including the hostname, username, password, and port.
 - d. In the Conflict Resolution Option field, select **Use Data from Import Source**.
 - e. Set the schedule for performing the bulk import. For example, to update Security Manager with new device credentials once a month, select **Monthly** as the Run Type, then define a start date and time.
 - f. Click **Import**.
-



CHAPTER 4

Cisco Security Agent

This chapter contains the following topics:

- [FAQs About the Cisco Security Agent, page 4-1](#)
- [Installation, Uninstallation, or Reinstallation, page 4-2](#)



Note

For more detailed information, see the “Troubleshooting the Standalone Security Agent” section and the “Cisco Security Agent: Standalone Agent Overview” chapter in the [installation guide for Cisco Security Manager](#) for your release.

FAQs About the Cisco Security Agent

This section answers the following questions about the Cisco Security Agent:

- [Q.What if the Cisco Security Agent is already installed on the system on which I want to install Security Manager?](#)
 - [Q.Is it possible to reinstall the bundled Cisco Security Agent after uninstalling it?](#)
 - [Q.Does the Cisco Security Agent co-exist with other host IPS systems?](#)
 - [Q.Why does the following message appear in the Cisco Security Agent event log?](#)
- Q.** What if the Cisco Security Agent is already installed on the system on which I want to install Security Manager?
- A.** By default, a standalone version of the Cisco Security Agent is installed as part of Security Manager installation. However, if Security Manager detects a preexisting version of the full Cisco Security Agent that was *not* installed by Security Manager, that version of the Cisco Security Agent is left in place. In this case, we recommend that you import all of the policies that you find on the Security Manager installation DVD (in `\csm3_0_1_win_server\CSA\CSMCSA3.0.1_policies.export`) into your version of the full agent. Bear in mind that if you import these policies, you must reconcile them with any conflicting policies that your organization configures. To learn more, see the Cisco Security Agent documentation on Cisco.com.
- Q.** Is it possible to reinstall the bundled Cisco Security Agent after uninstalling it?
- A.** On the installation DVD, run `CSA\CSA-CSM-setup.exe` to reinstall the Cisco Security Agent. Be aware, however, that future upgrades of Security Manager will not treat this version of the Cisco Security Agent as having been installed by Security Manager. This could affect future upgrades. For

example, if an upgraded version of Security Manager contains a new version of the Cisco Security Agent, the new version will not be installed, because Security Manager does not overwrite versions of the Cisco Security Agent that it did not install (as described above).

The alternative method to reinstall the bundled Cisco Security Agent is to reinstall Security Manager.

- Q.** Does the Cisco Security Agent co-exist with other host IPS systems?
- A.** You may encounter problems with the Cisco Security Agent when other host IPS systems are already installed. Because the Cisco Security Agent is installed automatically with Security Manager, we recommend doing the following:
- Uninstalling the other host IPS.
 - Installing Security Manager (which automatically installs the Cisco Security Agent).
 - Uninstalling the Cisco Security Agent.
 - Reinstalling the other host IPS.



Note This procedure can also be used for other applications that might conflict with the Cisco Security Agent, such as personal firewalls. For more details, see the [installation guide for Cisco Security Manager](#) for your release.

- Q.** Why does the following message appear in the Cisco Security Agent event log?
- The process 'C:\apps\CSMServer\lib\vbroker\bin\osagent.exe' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on UDP port 42342 from <ip address of an external machine>. The operation was denied.
- A.** This messages represents a valid deny event. The only valid connection request to the CiscoWorks RME Gatekeeper daemon on the Security Manager server is from the co-located RME application. Because this connection request is considered to be an intraserver request, any connection request from an external machine to the CiscoWorks RME Gatekeeper daemon on the Security Manager server is denied.

Installation, Uninstallation, or Reinstallation

See the [installation guide for Cisco Security Manager](#) for your release for information about troubleshooting problems that are related to the installation, uninstallation, or reinstallation of:

- Security Manager (including Common Services) software on a server.
- Security Manager Client.
- The standalone version of Cisco Security Agent that is installed on most Security Manager servers.

For information regarding the installation of the Security Manager License, see *Cisco Security Manager 3.x: Steps to Install the License for Various Options* on Cisco.com at:

http://www.cisco.com/en/US/products/ps6498/products_tech_note09186a0080849150.shtml



CHAPTER 5

Device Management

Before you can manage devices in Security Manager, you must prepare the devices so that communication between Security Manager and the devices is enabled, then add those devices to the Security Manager inventory.

This chapter contains the following topics:

- [Troubleshooting Device Communication Failures, page 5-1](#)
- [FAQs About Device Communication, page 5-2](#)
- [Security Certificate Rejected When Discovering Device, page 5-2](#)
- [Invalid Certificate Error During Device Discovery, page 5-3](#)
- [Deleting Configuration File When Deleting Security Context, page 5-3](#)
- [Simultaneous Operations on the Same Device, page 5-3](#)
- [Troubleshooting the Setup of Configuration Engine-Managed Devices, page 5-4](#)

Troubleshooting Device Communication Failures

If Security Manager fails to communicate with a device, e.g. by failing to log into it, during discovery, deployment, or other actions, look at these areas to identify and resolve the problem.

- Ensure the device is operational.
- Check which transport protocol is selected. You must select a protocol that the device is configured to accept. For most devices, the protocol is selected on the Device Properties General page. For IPS devices, the IPS RDEP mode is selected on the Credentials page.

Some methods of adding devices also allow you to select a non-default transport protocol. To configure the default transport protocols for classes of devices, select **Tools > Security Manager Administration > Device Communications**.

- On the Device Properties General page, ensure that the hostname, domain name, and IP address are correct. Keep in mind that the Hostname and Accounts and Credentials policies for the device define the actual names and credentials that get configured on the device. However, the policies are not used for device communication. If you make changes to the policies that affect the credentials you are using for device communication, you must also manually update the device properties.
- Make sure DNS names can be resolved from the Security Manager server. You might need to fix the DNS settings on the server.

- Check the credentials for the device in Security Manager and ensure that they are correct and that there is a route between the server and device. Right-click the device, select **Device Properties**, select the Credentials tab, and click the **Test Connectivity** button. If the connection fails, check error messages to determine whether the problem is connectivity or credentials. Update the credentials in the device properties if necessary.

When adding new devices the credentials are defined within the New Device wizard if your method of adding the device requires credentials. Keep the following in mind:

- The primary credentials are used for SSH and Telnet connections.
- The HTTP/HTTPS credentials are used for HTTP and SSL connections unless you select **Use Primary Credentials**, in which case the primary credentials are also used for these connections.

FAQs About Device Communication

This section answers the following questions about device communication:

- [Q.How does Security Manager connect to a Cisco IOS router that does not have a K8 or K9 crypto image?](#)
 - [Q.Why cannot Security Manager connect to a Cisco IOS router after configuration rollback?](#)
- Q.** How does Security Manager connect to a Cisco IOS router that does not have a K8 or K9 crypto image?
- A.** By default, Security Manager connects to Cisco IOS routers using SSL. However, a device running IOS version 12.3 or later without a K8 or K9 crypto image will not be able to support SSL. Therefore, after you add the device to Security Manager, you must select **Tools > Device Properties**, then change the default transport protocol to Telnet.
- Q.** Why cannot Security Manager connect to a Cisco IOS router after configuration rollback?
- A.** This could occur because of one of the following reasons:
- At rollback, for some versions of Cisco IOS software and when necessary, the configurations are copied from the TFTP server to startup-config, then the Cisco IOS router is reloaded. This reload causes a temporary loss in device connectivity. Wait for the device to be reloaded completely, then try to connect to it again.
 - The configuration contains a nonexisting or unauthorized username and password.

Security Certificate Rejected When Discovering Device

If an error occurs when you attempt to discover a device, and the error message states that the security certificate received from the device was rejected, you need to update the certificate. You can do this using one of the following methods:

- Manually enter the thumbprint required by the certificate by doing one of the following:
 - Select **Tools > Security Manager Administration > Device Communication**. Click **Add Certificate**, enter the IP address of the device, then copy and paste the thumbprint displayed in the error message into the Certificate Thumbprint field.
 - Right-click the device and select **Device Properties > Credentials**. Copy and paste the thumbprint displayed in the error message into the Authentication Certificate Thumbprint field.

You must manually enter the thumbprint whenever you add a new device using the Add New Device or Add From Configuration File options and when you perform rediscovery. It is not required when you add a new device using the Add New Device From Network or Add Device From File options.

- Configure the SSL certificate settings to automatically retrieve the certificate when adding devices. You can select different settings for IPS, router, and ASA/PIX/FWSM devices. To configure these settings, select **Tools > Security Manager Administration > Device Communication**, and look at the **SSL Certificate Parameters** group.

Invalid Certificate Error During Device Discovery

Problem If the time settings on the device and Security Manager are not in synchronization, an error message is displayed stating that the certificate is not yet valid when you try to discover a device.

Solution When the time set on the Security Manager server is lagging behind the time set on the device, Security Manager cannot validate the device certificate as the start time of the validity period is ahead of the Security Manager time setting. Even if the time zones configured on the device and Security Manager are the same, the invalid certificate error occurs if the daylight saving time (summertime) settings are different. To resolve this problem, make sure that the daylight saving time settings are the same on the device and Security Manager, regardless of whether the time zone is the same. After setting the daylight saving time, synchronize the clock on the device with Security Manager so that both of them display the same time.

To obtain best results, we recommend that you set the same time zone on the device and Security Manager, and modify the time zone after you discover the certificates at a later time, if necessary.

Deleting Configuration File When Deleting Security Context

Problem Deleting a security context from an FWSM device in Security Manager removes the security context from the running configuration of the device, but it does not delete the associated configuration file. This can create problems if you later add another security context with the same name as the one that you previously deleted.

Solution This is a known issue for this type of device and is not connected to the behavior of Security Manager. The workaround is to use the CLI to delete the configuration file from the device.

Simultaneous Operations on the Same Device

Problem Simultaneous operations performed on the same device (that is, devices with the same IP address) produce inconsistent results. For example, deployment to the first device succeeds, but deployment to the second device fails. These simultaneous operations may be a combination of jobs executed by Security Manager, such as a deployment job, and user-initiated operations, such as discovering a live device. Problems can occur whether the operations are contained in the same job or in multiple jobs that are executed at the same time.

Solution The device locking mechanism in Security Manager is based on the device name, not the IP address. As a result, operations such as discovery and deployment can run into problems if two devices share the same IP address. This is especially true if you attempt one of these operations on both devices at the same time.

For example, if a deployment job contains two devices with the same IP address, deployment will be executed to both devices because the names are different. However, doing so is not recommended, as it might result in an incomplete or failed deployment. To ensure consistent results, we recommend against defining more than one device with the same IP address.

Troubleshooting the Setup of Configuration Engine-Managed Devices

The following topics describe issues that might arise when you set up a device managed by a Cisco Configuration Engine (also known as CNS) and how to solve them:

- [Q. Why does Configuration Engine deployment fail?](#)
- [Q. Why do I receive an InvalidParameterException when I click on an IOS device on the Configuration Engine web page?](#)
- [Q. Why am I getting the following error:
com.cisco.netmgmt.ce.websvc.exec.ExecServiceException: \[002-01003\]\]deviceName does not exists?](#)
- [Q. Why am I getting the following error:
com.cisco.netmgmt.ce.websvc.config.ConfigServiceException: \[002-01003\]\]Device device id is not connected](#)
- [Q. Why is deployment to my Configuration Engine-managed PIX device not working?](#)
- [Q. Why was I able to deploy successfully to a Configuration Engine-managed PIX device the first time, but subsequent deployments were unsuccessful?](#)
- [Q. How do I debug Configuration Engine on a PIX device?](#)
- [Q. How do I debug Configuration Engine on an IOS device?](#)
- [Q. Why did I fail to discover an IOS device and acquire its configuration through Configuration Engine?](#)
- [Q. Why does not the event mode router appear on the Configuration Engine Discover Device page or appear in green on the Configuration Engine web page?](#)

Q. Why does Configuration Engine deployment fail?

A. Not all versions of Configuration Engine function in a compatible manner. Because Security Manager does not verify the software version running on a Configuration Engine when you add it to the device inventory, you can add unsupported versions to the inventory. Then, when you try to deploy, you can run into unpredictable errors. Ensure that you are running a supported version of Configuration Engine, such as 3.0. For support information, see the supported devices information at http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Q. Why do I receive an InvalidParameterException when I click on an IOS device on the Configuration Engine web page?

A. This is the expected behavior. For IOS devices, Security Manager uses deployment jobs to deploy configurations to Configuration Engine instead of associating a configuration to the IOS device in Configuration Engine. Therefore, you do not see an associated configuration when you click the device name on the Configuration Engine web page. For PIX devices, Security Manager associates the configuration to the device in Configuration Engine. Therefore, clicking the device name displays the associated configuration.

- Q.** Why am I getting the following error: `com.cisco.netmgmt.ce.websvc.exec.ExecServiceException: [002-01003]]deviceName does not exists?`
- A.** This error indicates that the device has not been added to Configuration Engine. It appears if you have not performed rollback or deployment in Security Manager (both of which add the device automatically), and have not manually added the device to Configuration Engine.
- Q.** Why am I getting the following error:
`com.cisco.netmgmt.ce.websvc.config.ConfigServiceException: [002-01003]]Device device id is not connected`
- A.** The answer depends on the type of setup you are performing:
- Event mode setup—Make sure that the Configuration Engine device ID defined in the Device Properties window in Security Manager matches the device ID configured on the router (using the **`cns id string`** command).
 - Call home mode setup—The device is not connected to Configuration Engine in this mode; therefore, all Security Manager operations that require the retrieval of the device configuration using Configuration Engine are not supported. This includes discovery, preview configuration, display running configuration, and connectivity tests (and rollback, for IOS devices).
- Q.** Why is deployment to my Configuration Engine-managed PIX device not working?
- A.** There are several possibilities:
- The configuration contains invalid commands. You can test this by copying the configuration associated with the PIX device in Configuration Engine and pasting it directly into the device.
 - The **`auto-update server`** command contains an invalid username and password.
 - You did not wait long enough for the configuration to be polled into the PIX device. Use the **`show auto`** command to verify when the next polling cycle will occur.
 - If you previously used the Configuration Engine server for the same PIX device and did not delete the PIX from the Configuration Engine server before you started the current task, it is possible that the PIX device received the previous configuration from the server before you deployed the new configuration to it.
 - If none of the suggestions above solves the problem, turn on Configuration Engine debug mode (see [Q.How do I debug Configuration Engine on a PIX device?](#)) on the PIX device and check the log for errors after the next polling cycle.
- Q.** Why was I able to deploy successfully to a Configuration Engine-managed PIX device the first time, but subsequent deployments were unsuccessful?
- A.** This can happen if the configuration pushed during the first deployment contains incorrect CLI commands for the auto-update feature. Check the following:
- Make sure the username and password of the Configuration Engine server is defined correctly in the **`auto-update`** command.
 - Make sure that you have defined a FlexConfig that contains the necessary **`name`** commands. A FlexConfig is necessary because Security Manager does not support this command directly. As a result, even though the command was discovered, it does not appear in the full configuration.

Q. How do I debug Configuration Engine on a PIX device?

A. Enter the following CLI commands:

```
logging monitor debug
terminal monitor
logging on
```



Tip You can also find relevant information in the PIX log on the Configuration Engine server.

Q. How do I debug Configuration Engine on an IOS device?

A. Enter the following CLI commands:

```
debug cns all
debug kron exec-cli
terminal monitor
```



Tip When working in event mode, you can also find relevant information in the event log on the Configuration Engine server. When working in call home mode, check the config server log on the Configuration Engine server.

Q. Why did I fail to discover an IOS device and acquire its configuration through Configuration Engine?

A. If you see the following errors in debug mode:

```
*Feb 23 21:42:15.677: CNS exec decode: Unknown hostname cnsServer-lnx.cisco.com ...
474F6860: 72726F72 2D6D6573 73616765 3E584D4C error-message>XML 474F6870: 5F504152
53455F45 52524F52 3C2F6572 _PARSE_ERROR</er
```

Verify the following:

- The CNS commands use a fully-qualified host name (host name and domain name).
- The device contains **ip domain name** *your domain name*.
- The device contains **ip host** *fully-qualified-cns-hostname cns-ip-address*.

Q. Why does not the event mode router appear on the Configuration Engine Discover Device page or appear in green on the Configuration Engine web page?

A. Check the following:

- Make sure that the router and the Configuration Engine server can ping each other.
- Make sure that the event gateway on the Configuration Engine server is up and running by using one of the following commands:

Status for plain text mode: **/etc/init.d/EvtGateway**

Status for SSL encrypted mode: **/etc/init.d/EvtGatewayCrypto**

- Clear the **cns event** command, then re-enter it without specifying a port number.



CHAPTER 6

Policy Discovery

This chapter contains the following topics:

- [FAQs About Policy Discovery, page 6-1](#)
- [Performing Discovery in a Multi-User Environment, page 6-5](#)
- [SSL VPN Policies Negated When Discovered From Configuration File, page 6-6](#)
- [Undiscovered VPN Features, page 6-6](#)
- [ACL Names Preserved by Security Manager, page 6-6](#)
- [Resource Names Changed by Security Manager, page 6-9](#)

FAQs About Policy Discovery

This section answers the following questions about policies:

- [Q.How does policy discovery work?](#)
- [Q.When should I discover policies?](#)
- [Q.How can I determine the results of the discovery?](#)
- [Q.Does Security Manager show which commands are not discovered and what can I do about them?](#)
- [Q.How are discovered policies reflected in the user interface?](#)
- [Q.I am using Auto Update Server for my PIX or ASA devices. How do I discover policies?](#)
- [Q.I am using a Cisco Secure Access Control Server \(ACS\) to manage authentication and authorization to Security Manager. How does this affect policy discovery?](#)
- [Q.What should I do after discovering VPN or router platform policies?](#)
- [Q.If I discover policies on a device and then deploy the policies from Security Manager without changing them, what is the difference between the original configuration on the device and the one that exists after deployment?](#)
- [Q.How does Security Manager handle my current CLI naming schemes for ACLs and object groups?](#)
- [Q.Are all configuration commands discovered and brought into Security Manager?](#)
- [Q.If I rediscover policies on a device already in Security Manager, what happens to the policies assigned to the device?](#)
- [Q.Does Security Manager use existing policies and objects during policy discovery?](#)

REVIEW DRAFT – CISCO CONFIDENTIAL

- Q.What do I need to know about security contexts on PIX 7.0+ and ASA devices in terms of policy discovery?
 - Q.What do I need to know about security contexts for Firewall Services Modules (FWSMs) on Catalyst switches when I add them and discover policies?
 - Q.After adding a device and discovering policies, I cannot submit my changes to the database; instead I get warnings such as “Connection Policies Not Set.” What must I do to complete the device addition?
 - Q.Why does the AAA policy not show the AAA configuration that I discovered on the router?
 - Q.Why are parts of the AAA method list definitions configured on my router not discovered?
 - Q.Can I discover AAA servers on devices running IOS software that were configured using the server-private command?
 - Q.What do I need to know about discovery and device hostnames?
- Q.** How does policy discovery work?
- A.** After you select the device whose policies, settings, and interfaces (inventory) you want to discover, Security Manager obtains the running configuration (from live devices) or the supplied configuration (when discovering from configuration files) and translates the CLI into Security Manager policies and objects. The imported configuration is added to the Configuration Archive as the initial configuration for the device. After discovery, you can review the resulting policies and objects and decide whether to commit them to the database or discard them. Please note that when discovering policies on multiple devices, commit and discard affect all the devices as a group and cannot be implemented on a per-device basis.
- Q.** When should I discover policies?
- A.** Typically, you should discover policies when you add devices to Security Manager. However, if you are creating devices in Security Manager (instead of importing live devices or configuration files), you must perform policy discovery after adding the device. You should also perform policy discovery to synchronize Security Manager with any out-of-band changes that have been made to the device, for example through the CLI.
- Q.** How can I determine the results of the discovery?
- A.** When you initiate a discovery task, a window opens that shows you the discovery status and results. You can also view a history of discovery task results on the Policy Discovery Status page (select **Tools > Policy Discovery Status**).
- Q.** Does Security Manager show which commands are not discovered and what can I do about them?
- In the discovery status window, go to the Message Summary section, then select **Commands Not Discovered**. Any undiscovered commands are listed in the Description field. You can either remove the command from the device and repeat the discovery process, or continue. If the latter, Security Manager will remove the unsupported command in the next deployment.
- If Security Manager does not support a command found on a device (for example, object groups in IOS devices), the discovery is generally not aborted; however, if the device has any ACEs that refer to object groups, the discovery is aborted.
- Other error messages, such as “User groups not supported,” might also provide details about undiscovered commands. Read the information in the Action box for suggestions.

REVIEW DRAFT – CISCO CONFIDENTIAL

- Q.** How are discovered policies reflected in the user interface?
- A.** Security Manager converts device commands into policies. There is no difference between a policy discovered from a device configuration and one defined in Security Manager.
- Q.** I am using Auto Update Server for my PIX or ASA devices. How do I discover policies?
- A.** If a device has a static IP address, you can discover policies from the device. If it has a dynamic IP address, you must discover policies from the device's configuration file.
- Q.** I am using a Cisco Secure Access Control Server (ACS) to manage authentication and authorization to Security Manager. How does this affect policy discovery?
- A.** You must add all managed devices to the ACS, including security contexts on PIX, ASA, and FWSM devices, before you can perform policy discovery and manage these devices in Security Manager.
- Q.** What should I do after discovering VPN or router platform policies?
- A.** Due to the way these features are discovered, Security Manager does not assume management of discovered VPN and router platform policies until after it deploys them. This means that if you discover a router, unassign one of its policies and deploy, no commands are removed from the router's configuration. We recommend, therefore, that you perform deployment to a file immediately after discovering VPN or router platform policies, *before* you make any changes to those policies. After this initial deployment, you can reconfigure these policies and deploy your changes as required.
- Q.** If I discover policies on a device and then deploy the policies from Security Manager without changing them, what is the difference between the original configuration on the device and the one that exists after deployment?
- A.** Typically, there are no differences between the new configuration and your original one, assuming you set up FlexConfigs for any unsupported CLI commands (because they are not displayed in Security Manager). However, in certain cases minor changes might occur in your ACL or object-group naming schemes. For more information, see "How Policy Objects are Provisioned as PIX Object Groups" in the Security Manager online help. In addition, any discovered objects that are not being used by a policy are removed from the configuration. There can also be instances where the new configuration is functionally equivalent to the old one but does not use the same commands.
- Q.** How does Security Manager handle my current CLI naming schemes for ACLs and object groups?
- A.** When you discover policies from a device, Security Manager tries to use the same names you have used. However, depending on your naming scheme, some minor differences might occur between what you defined on your device and the policies created through discovery. For more information, see [ACL Names Preserved by Security Manager, page 6-6](#) and [Name Changes in PIX/ASA Object Groups, page 6-10](#). Additionally, it is possible that a naming conflict can occur between an existing ACL or object on the device and the name required for the new policy; in this case, Security Manager generates a different name so as not to misconfigure the device.
- Q.** Are all configuration commands discovered and brought into Security Manager?
- A.** No. Security Manager does not discover all device configuration commands. Instead, it discovers commands that are related to security policies. For any commands that are not discovered, use the FlexConfig feature to include the commands that Security Manager does not support.

REVIEW DRAFT – CISCO CONFIDENTIAL

- Q.** If I rediscover policies on a device already in Security Manager, what happens to the policies assigned to the device?
- A.** If you rediscover policies on a device that you are already managing with Security Manager, the newly discovered policies replace the ones assigned to the device. All policies within the selected policy domain (firewall services, platform settings, or both) are replaced, not just the ones that are different on the device compared to the ones in the Security Manager database. If you assigned shared policies to the device, the assignment is removed and the shared policy is left unchanged (so that other devices that use the shared policy are not affected). After policy discovery, all policies assigned to the device are local to that device; none of them are shared with other devices. If you want to use shared policies with the device, you must redo the assignments after policy discovery.
- Q.** Does Security Manager use existing policies and objects during policy discovery?
- A.** During policy discovery, Security Manager uses existing policy objects (ones that you already defined in Security Manager) when creating policies for the device. However, Security Manager does not reuse existing policies; all policies created during discovery are local to the device being discovered. Thus, you might find it beneficial to define your policy objects (such as network objects) before adding devices to Security Manager.
- Q.** What do I need to know about security contexts on PIX 7.0+ and ASA devices in terms of policy discovery?
- A.** On devices running PIX 7.0+ or ASA software, you can create security contexts, which act like independent firewalls. When you add a device that has security contexts, you should discover all contexts and policies at the same time; otherwise, you will have to discover policies for each context separately. When you add the device, select **MULTI** for Context and do not select Security Context of Unmanaged Device. (If you select this option, only the admin context is imported, and it has no relationship to other security contexts on the device; select this option only if you want to manage the security context independently from the parent device.) Depending on how you add the device, you might need to select the option to discover security contexts. During discovery, Security Manager identifies each security context and adds it as a separate device to the device list, appending the security context name to the end of the parent's name; for example, if the parent is pix_141, the admin context would be pix_141_admin. When managing PIX 7.0 and ASA devices in Security Manager, you can create security contexts or delete contexts, as well as create and delete policies for those contexts.
- Q.** What do I need to know about security contexts for Firewall Services Modules (FWSMs) on Catalyst switches when I add them and discover policies?
- A.** On FWSMs, you can create security contexts, which act like independent firewalls. If you use this feature and are running IOS software on the chassis, add the chassis device using the SSH credentials for the chassis. Then Security Manager can identify each FWSM on the chassis, and give you the option to add each of them. During FWSM discovery, Security Manager discovers the security contexts for each FWSM, including the policies for the FWSM and for each context. In the device list, each security context is listed separately and the name of the context is appended to the name of the FWSM on which it is defined. (For example, Cat6K_FW_4 might be the FWSM, and Cat6K_FW_4_context1 would be the context1 security context.) You should always perform policy discovery on the chassis, not on the individual FWSM, so that Security Manager can discover the inventory. However, if you are running the Catalyst OS on the device, you must add the FWSM as a standalone device instead of adding the chassis, because Security Manager does not support the Catalyst OS.

REVIEW DRAFT – CISCO CONFIDENTIAL

- Q.** After adding a device and discovering policies, I cannot submit my changes to the database; instead I get warnings such as “Connection Policies Not Set.” What must I do to complete the device addition?
- A.** When you add a device and discover policies (particularly when you add devices from configuration files), Security Manager warns you if the resulting configuration is incomplete in ways that will prevent it from successfully managing the device. Connection policies, for example, are simply the device credentials (usernames and passwords) required to log in to the device and other connection-related configuration settings (such as HTTP settings). Because these missing settings result in an invalid configuration or prevent Security Manager from contacting and managing the device, you are prevented from submitting the changes to the database. Ensure that you have complete and valid configurations for these settings, then resubmit your changes to the database.
- Q.** Why does the AAA policy not show the AAA configuration that I discovered on the router?
- A.** The AAA policy contains the default configurations for authentication, authorization, and accounting. Other AAA commands that specify a particular list name are mapped to the policies that reference them. If the list name is not referenced by a policy, it is not discovered.
- Q.** Why are parts of the AAA method list definitions configured on my router not discovered?
- A.** Security Manager does not support certain keywords, such as `if-needed`. Method lists containing these keywords are discovered without the keyword. If the default AAA definitions on the device contain unsupported keywords, the entire CLI command is not discovered.
- Q.** Can I discover AAA servers on devices running IOS software that were configured using the `server-private` command?
- A.** Yes, you can discover these servers. However, Security Manager converts them into standard AAA servers that can be used globally or in multiple AAA server groups. The `server-private` command is not supported.
- Q.** What do I need to know about discovery and device hostnames?
- A.** When you discover a device, the hostname policy is populated with the hostname discovered on the device. However, the hostname listed in Device Properties is not updated with this value. Therefore, if you want to specify the DNS hostname for the device, you must specify it manually when you add the device to Security Manager or on the Device Properties page.

Performing Discovery in a Multi-User Environment

Problem You receive inconsistent discovery results on a live device when working in a multi-user environment.

Solution Security Manager does not lock devices across operations. Therefore, it is possible for one user to discover a device while another user is deploying to the same device. To ensure consistent discovery results, make sure that no other users are deploying to the device while you are performing discovery.

REVIEW DRAFT – CISCO CONFIDENTIAL

SSL VPN Policies Negated When Discovered From Configuration File

One of the ways you can add devices to Security Manager is to use the device's configuration file. This method adds the device without Security Manager contacting the device. However, if you add a device using a configuration file, and discover security policies while adding the device, Security Manager cannot successfully discover policies that require that files be downloaded from the discovered device. This especially affects devices that include the **svc image** command in a web VPN configuration. Because Security Manager does not have the referenced file in its database, the **no** form of the command is generated for the discovered configuration.

If a device configuration includes any command that references another file, you should not discover policies for that device from an off-line configuration file. Instead, use the add from network option, or alternatively, add the device using the configuration file without discovering policies, then discover policies from the live device after it is in the device inventory.

Undiscovered VPN Features

The following VPN features are supported by Security Manager, but cannot be discovered:

- Large-scale DMVPN (high-concentration hub)
- VRF-Aware IPsec
- Dial backup
- IPsec and ISAKMP profiles for Easy VPN

If you define and deploy policies of these types using the Security Manager interface, your policies overwrite the device configurations that were not discovered. Therefore, if you want Security Manager to manage existing configurations, you should define policies that match the existing configurations as closely as possible. (Use the Preview Configuration feature to examine the results before deploying.) The VPN provisioning mechanism leverages the content of the existing configuration as much as possible (assuming the content matches the policies configured in Security Manager), but does not retain the naming conventions used in the CLI commands. For more information, see [Resource Names Changed by Security Manager, page 6-9](#).

**Note**

Under certain circumstances, an SSL VPN group-policy is removed from the device configuration even if you do not define an SSL VPN user group policy. See [Removing Group Policy Attributes from SSL VPNs Defined on ASA 7.x Devices, page 9-9](#).

ACL Names Preserved by Security Manager

Security Manager tries to preserve user-defined ACL names as they appear in device configurations. Security Manager can preserve the ACL names configured on a device in the following circumstances:

- If the ACL name is specified in Security Manager.
 - For firewall Access Rules policies, you can specify ACL names in **Firewall > Settings > Access Control**. You can specify a given name for a single interface and direction, but the name is used for any other interfaces and directions that use the same ACL. Keep in mind that you cannot use the same name as an ACL policy object that you assign to other policies on the device.

REVIEW DRAFT – CISCO CONFIDENTIAL

- If a policy uses an ACL policy object, the name of the policy object is used for the ACL name. ACL policy objects created during discovery use the name of the ACL defined on the device whenever possible. Behavior depends on an administrative setting:
 - If you select **Allow Device Override for Policy Objects** in **Tools > Security Manager Administration > Discovery**, if a policy object with the same name exists in Security Manager, but it has different content, the name is reused and a device-level override is created.
 - If you do not select that option, a new policy object is created with the same name but with a number appended to it, for example, ACLobject_1. This is the default behavior.
- If you select **Reuse Existing Names** for the **Firewall Access List Names** setting in **Tools > Security Manager Administration > Deployment**, names defined on the device are reused for AAA, NAT, and firewall access rules.
- If the ACL is unshared, even if you change the content of the ACL in Security Manager.
- If the ACL is shared, but the policies that share the ACL are defined identically in Security Manager. If you change the content of the ACL, one ACL retains the name and the others are assigned generated names.



Note

On ASA devices and on PIX devices not running version 6.3(x), Security Manager does not reuse the ACL name if it is used by a policy static and contains an object-group. The ACL is deployed with the contents of the object-group defined as the source. This is because the device requires that all ACEs in the ACL have the same source.

Tips

- If you use an ACL policy object that uses a name also used by an ACL already defined on the device, and the existing ACL is for a command that Security Manager does not support, you will get a deployment error asking you to choose a different name. If this happens, rename the policy object.
- ACLs named <number>_<number> are not valid on Cisco IOS Software devices. Security Manager strips off the suffix prior to deployment. This also means that you cannot assign an IOS device more than one ACL object with the same numbered prefix. However, named ACLs that have a numbered suffix are allowed, for example, ACLname_1.
- Numbered ACLs must use the correct number ranges for IOS devices. Standard ACLs must be in the range 1-99 or 1300-1999. Extended ACLs must be in the range 100-199 or 2000-2699.
- ACL names for IOS devices cannot begin with an underscore (_).
- Policies that do not preserve user-defined names include SSL VPN policies, transparent firewall rules, AAA rules (for IOS devices), service policy rules (for ASA/PIX devices).

ACL Naming Conventions

When the name for the ACL is generated by Security Manager, the name is derived from the type of rule or platform being defined and certain configuration settings that make it unique. All newly created ACLs are given a name based on the naming conventions shown in [Table 6-1](#).

REVIEW DRAFT – CISCO CONFIDENTIAL**Tip**

During deployment, sometimes a suffix *.n* (where *n* is an integer) might get added to an ACL name if the existing ACL cannot be edited in place. For example, if an ACL named `acl_mdc_outside_10` already exists on the device, a new ACL with the name `acl_mdc_outside_10.1` is created if you do not remove the old ACL before you deploy the new ACL.

Table 6-1 ACL Naming Conventions

Policy Type	Naming Convention
Access ACLs	<ul style="list-style-type: none"> Inbound: CSM_FW_ACL_InterfaceName Outbound: CSM_FW_ACL_OUT_InterfaceName
Inspection Rules	<ul style="list-style-type: none"> For ASA 7.0+/PIX 7.0+: CSM_CMAP_ACL_n where n is an integer beginning with 1. For IOS devices, a numbered ACL.
NAT0 ACLs	<ul style="list-style-type: none"> Inbound: CSM_nat0_InterfaceName_in Outbound: CSM_nat0_InterfaceName
NAT ACLs	<ul style="list-style-type: none"> Inbound: CSM_nat_InterfaceName_poolID_in Outbound: CSM_nat_InterfaceName_poolID <p>Note For PIX 6.3(x) devices, the following is added to the ACL name: add <code>_dns</code> for dns, <code>_nrseq</code> for norandomseq, <code>_emb##</code> for embryonic limit and <code>_tcp##</code> and <code>_udp##</code> for tcp and udp max connection limits.</p>
NAT Policy Static Translation Rules ACLs	<ul style="list-style-type: none"> For PIX 6.3(x) devices: <ul style="list-style-type: none"> For IP: CSM_static_globalIP_LocalInterfaceName_globalInterfaceName For other protocols: CSM_static_globalIP_LocalInterfaceName_globalInterfaceName_protocol_globalPort For devices running other OS versions, the localIP string is added: <ul style="list-style-type: none"> For IP: CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName For other protocols: CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName_protocol_globalPort

REVIEW DRAFT – CISCO CONFIDENTIAL**Table 6-1 ACL Naming Conventions (continued)**

Policy Type	Naming Convention
AAA ACLs	<p>For PIX/ASA/FWSM: CSM_AAA_{AUTHO ATHEN ACCT}_InterfaceName_ServerGroupName</p> <p>Authentication Proxy for IOS devices:</p> <ul style="list-style-type: none"> On an interface without NAC: CSM_AUTH-PROXY_InterfaceName_traffic type_ACL, where InterfaceName is the interface in which the rule is applied and traffic type is HTTP, Telnet, or FTP. AuthProxy and NAC on the same interface: CSM_ADMISSION_ID_ACL, where ID is an internal identifier of the interface role within Security Manager to which NAC is applied.
Web Filter Rules ACLs	<p>For ASA 7.0+/PIX 7.0+: devices correspond to a filter command.</p> <p>For IOS devices, a numbered ACL.</p>

Resolving Conflicts Between Policies

If an ACL is shared, but the policies that share the ACL are *not* defined identically in Security Manager, one policy uses the original name of the ACL and the other policies uses a new name generated by Security Manager. The order of preference for determining which policy uses the original name is as follows:

- Access list ACLs
- AAA ACLs
- Static ACLs
- NAT0 ACLs
- NAT ACLs

For example, if an access ACL and a NAT0 ACL try to reuse the same ACL, the access ACL uses the original name as configured on the device and the NAT0 ACL is renamed by Security Manager.

Resource Names Changed by Security Manager

When you discover a device, Security Manager translates the CLI commands contained in the device configuration into their corresponding policies and policy objects. In most cases, no changes are made to the device configuration if you deploy without modifying these discovered values in Security Manager.

In certain cases, however, Security Manager changes the name of resources that are discovered on the device. These resources are configured on the device at the global level and are referred to by other CLI commands as part of the configuration of a specific feature.

The name changes performed by Security Manager are described in the following sections:

- [Name Changes in PIX/ASA Object Groups, page 6-10](#)
- [Name Changes in AAA Rules Policies, page 6-11](#)
- [Name Changes in Access Rules Policies, page 6-11](#)

REVIEW DRAFT – CISCO CONFIDENTIAL

- Name Changes in Inspection Rules Policies, page 6-12
- Name Changes in Transparent Rules Policies, page 6-12
- Name Changes in Dynamic NAT Policies, page 6-13
- Name Changes in Service Policy Rules Policies, page 6-13
- Name Changes in Dialer Policies, page 6-14
- Name Changes in PPP Policies, page 6-15
- Name Changes in AAA Policies, page 6-15
- Name Changes in HTTP Policies, page 6-15
- Name Changes in Line Access Policies, page 6-15
- Name Changes in NAC Policies, page 6-17
- Name Changes in Quality of Service Policies, page 6-17

Name Changes in PIX/ASA Object Groups

When Security Manager discovers object-group definitions on PIX/ASA devices, it converts those object groups into policy objects that can be managed using the Policy Object Manager. The conversions work as follows:

- The command **object-group network** generates network/host objects.
- The command **object-group service** generates port list objects.

For example, if the device contains the following:

```
object-group services myService udp
port-object eq 789
port-object eq 333
```

Security Manager creates a port list object called myService that contains ports 333 and 789.

The naming conventions when moving between policy objects in Security Manager and the object groups defined on PIX/ASA devices is described in detail in the section “How Policy Objects are Provisioned as PIX/ASA Object Groups,” which can be found in the *User Guide for Cisco Security Manager*.



Tip

To have Security Manager delete unused object groups from a device during deployment, select **Tools Security Manager Administration > Deployment**, then select **Remove Unreferenced Object Groups from Device**.

REVIEW DRAFT – CISCO CONFIDENTIAL**Name Changes in AAA Rules Policies**

Table 6-2 describes the changes that are made to resource names in AAA rules policies discovered by Security Manager.

Table 6-2 AAA Rules Resource Name Changes

Resource	Sample Name on Device	Security Manager Naming Format
ip admission name	test-auth	CSM_[INTERFACE_NAME]
acl-name	101	CSM_AUTH-PROXY_[INTERFACE_NAME]

When you deploy to the device, Security Manager adds these new resources to the existing resources in the device configuration. As a result, the device configuration will contain two identical ip admission name statements. Although Cisco IOS routers can use either standard or extended access lists (ACLs) in AAA rules, the AAA rules policy in Security Manager uses only extended ACLs. Therefore, if Security Manager discovers a AAA rule in the device configuration that uses a standard ACL, it creates an equivalent extended ACL using the naming format, CSM_AUTH-PROXY_[INTERFACE_NAME].

Name Changes in Access Rules Policies

As a general rule, Security Manager preserves the names of user-defined ACLs on PIX, ASA, and FWSM devices, provided you have selected the “Reuse existing names” option in the Firewall Access-List Names field under **Tools > Security Manager Administration > Deployment**. A user-defined ACL is one that does not have a name that begins CSM_FW_ACL.

If an ACL does not have a user-defined name (for example, an ACL created in Security Manager without specifying a name), Security Manager generates a name using the following format:

CSM_FW_ACL_[INTERFACE_NAME]_[DIRECTION]

For example:

```
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
deny icmp any any log
deny tcp any any eq ftp log
permit ip any any log
```

If Security Manager discovers a standard ACL on an IOS device, it converts it into an extended ACL.



Tip

To have Security Manager delete unused ACLs from a device during deployment, select **Tools > Security Manager Administration > Deployment**, then select the **Remove Unreferenced Access-lists on Device** check box.

REVIEW DRAFT – CISCO CONFIDENTIAL**Name Changes in Inspection Rules Policies**

Table 6-3 describes the changes that are made to resource names in inspection rule policies discovered on a firewall device (PIX/ASA 7.0+, FWSM 3.1+).

Table 6-3 *Inspection Rules Resource Name Changes*

Resource	Sample Name on Device	Security Manager Naming Format
acl-name	allowtcp	CSM_CMAP_ACL_#
class-map	cmtcp	CSM_CLASS_MAP_ftp_#
policy-map	inspectmap	(Globally applied rules) CSM_POLICY_MAP_GLOBAL_0 (Rules applied to specific interface) CSM_POLICY_MAP_[INTERFACE_NAME]

When you deploy to the device, Security Manager creates an access list with the same definition as the one it replaces. A new class-map points to the new access list. A new policy-map replaces the one in the original configuration.

```
access-list CSM_CMAP_ACL_1 extended permit tcp 10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
class-map CSM_CLASS_MAP_ftp_1
  match access-list CSM_CMAP_ACL_1
exit
policy-map CSM_POLICY_MAP_global_1
  class CSM_CLASS_MAP_ftp_1
    inspect ftp
  exit
exit
no service-policy inspectmap global
service-policy CSM_POLICY_MAP_global_1 global
```

Name Changes in Transparent Rules Policies

Security Manager takes the number of the extended ACL configured in a transparent rule and creates an ACL using the first free number available on the device.

For example, if Security Manager discovers a transparent rule that includes the following:

```
access-list 700 permit 0x0000 0xFFFF
```

It changes the name of the ACL, as follows:

```
access-list 214 permit 0x0000 0xFFFF
```

REVIEW DRAFT – CISCO CONFIDENTIAL**Name Changes in Dynamic NAT Policies**

Table 6-4 describes the changes that are made to resource names in dynamic network address translation (NAT) policies discovered on a Cisco IOS router.

Table 6-4 NAT Resource Name Changes

Resource	Sample Name on Device	Security Manager Naming Format
ip access-list	myNatAcl	CSM_IP_NAT_DYNAMIC_ACL_1
ip nat pool	myNatPool	CSM_IP_NAT_POOL_1

When you deploy to the device, Security Manager adds these new resources to the existing resources in the device configuration. As a result, the device configuration will contain two identical ACLs and two identical NAT address pools with different names. In addition, the dynamic NAT rule is duplicated and points to the new resources.

```
ip nat pool myNatPool 1.1.1.2 1.1.1.100 prefix-length 24
ip nat pool CSM_IP_NAT_POOL_1 1.1.1.2 1.1.1.100 prefix-length 24
ip nat inside source list CSM_IP_NAT_DYNAMIC_ACL_1 pool CSM_IP_NAT_POOL_1
ip nat inside source list myNatAcl pool myNatPool
ip access-list extended CSM_IP_NAT_DYNAMIC_ACL_1
 permit ip 192.168.102.0 0.0.0.255 192.168.0.0 0.0.255.255
ip access-list extended myNatAcl
 permit ip 192.168.102.0 0.0.0.255 192.168.0.0 0.0.255.255
```

As can be seen in this example, the device configuration now contains duplicate NAT pools and ACLs. In addition, the dynamic NAT rule itself has been duplicated.

**Note**

We recommend that you remove the original NAT rule from the device after Security Manager has created and deployed the new rule. Otherwise, Security Manager will continue duplicating the original NAT rule during each subsequent deployment, which adds unnecessary commands to the device configuration.

Name Changes in Service Policy Rules Policies

Table 6-6 describes the changes that are made to resource names in service policy rule policies discovered on a firewall device (PIX/ASA 7.0+, FWSM 3.1+).

Table 6-5 Service Policy Rules Resource Name Changes

Resource	Sample Name on Device	Security Manager Naming Format
acl-name	allowudp	CSM_TF_ACL_allowudp_#
policy-map	svemap	(Globally applied rules) CSM_POLICY_MAP_GLOBAL_0 (Rules applied to specific interface) CSM_POLICY_MAP_[INTERFACE_NAME]

REVIEW DRAFT – CISCO CONFIDENTIAL

The ACLs refer to class-maps used by service policy rules (which are represented by traffic flow objects in Security Manager).

When you deploy to the device, Security Manager creates an access list with the same definition as the one it replaces. The class-map points to the new access list. (The name of the class-map itself remains unchanged.) A new policy-map replaces the one in the original configuration.

```
access-list CSM_TF_ACL_allowudp_1 extended permit udp 30.30.30.0 255.255.255.0
40.40.50.0 255.255.255.0
class-map cmudp
  no match access-list allowudp
  match access-list CSM_TF_ACL_allowudp_1
exit
policy-map CSM_POLICY_MAP_inside_1
  class isakmp-tfbb
    set connection timeout embryonic 0:00:40 half-closed 0:10:40 tcp 1:00:40
    priority
  exit
  class cmudp
    police output 20000
  exit
exit
no service-policy svcmap interface inside
service-policy CSM_POLICY_MAP_inside_1 interface inside
```

Name Changes in Dialer Policies

Table 6-6 describes the changes that are made to resource names in dialer policies discovered on a Cisco IOS router.

Table 6-6 Dialer Resource Name Changes

Resource	Sample Name on Device	Security Manager Naming Format
dialer-list access-list-number	101	CSM_EXT_101

Although Cisco IOS routers can use either standard or extended ACLs in dialer configurations, the dialer policy in Security Manager uses only extended ACLs. Therefore, if Security Manager discovers a dialer configuration that uses a standard ACL, it creates an equivalent extended ACL using the naming format, CSM_EXT_[ACL#]. The standard ACL is removed from the device if it is not being referenced by the device configuration and the option to remove unreferenced ACLs is selected in Security Manager.

REVIEW DRAFT – CISCO CONFIDENTIAL

Name Changes in PPP Policies

Security Manager does not change the resource names in PPP configurations that use their own customized method lists for AAA authentication and authorization.

However, if the AAA configuration on the device contains an unsupported keyword, the method list is not discovered. Instead, you must create a policy in Security Manager.

Table 6-7 describes the naming conventions used by Security Manager for AAA services configured on the PPP connections of a Cisco IOS router.

Table 6-7 PPP Resource Naming Conventions

Resource	Naming Convention for PPP
Global configuration commands	
aaa authentication ppp <i>list-name</i>	CSM_PPP_AUTHENTICATION_#
aaa authorization network <i>list-name</i>	CSM_PPP_AUTHORIZATION_#
Interface configuration commands	
ppp authentication <i>protocols list-name</i>	CSM_PPP_AUTHENTICATION_#
ppp authorization <i>list-name</i>	CSM_PPP_AUTHORIZATION_#

Name Changes in AAA Policies

In AAA policies, the only resource name used by Security Manager is the name of the method lists used by each AAA service, such as login authentication and EXEC authorization. In each case, the AAA policy uses the name “default” and does not change the name during discovery.

There are some keywords that are unsupported in Security Manager. If you try to discover a method list containing an unsupported keyword, Security Manager displays a warning indicating that this method list cannot be discovered. Because all method lists in the AAA policy use the name “default,” any method list that you configure in Security Manager overwrites the method list on the device for the same AAA service, including a method list containing an unsupported keyword.

Name Changes in HTTP Policies

Security Manager does not change the resource names in HTTP policies that use their own customized method lists. It can also reuse the method lists in an HTTP policy that uses the default lists configured in the device’s AAA policy.

However, if the AAA configuration on the device contains an unsupported keyword, the method list is not discovered. Instead, Security Manager creates a new method list using the naming format: CSM_HTTP_AAA_1.

Name Changes in Line Access Policies

Security Manager does not change the resource names in line access configurations (console and VTY) that use their own customized method lists. It can also reuse the method lists in a line access configuration that uses the default lists configured in the device’s AAA policy.

REVIEW DRAFT – CISCO CONFIDENTIAL

However, if the AAA configuration on the device contains an unsupported keyword, the method list is not discovered. Instead, you must create a policy in Security Manager.

Table 6-9 describes the naming conventions used by Security Manager for AAA services configured on the console port and VTY lines of a Cisco IOS router.

Table 6-8 Line Access Resource Naming Conventions

Resource	Naming Convention for VTY	Naming Convention for Console
Global configuration commands		
aaa authentication login <i>list-name</i>	CSM_VTY_AUTHENTICATION_#	CSM_CON_AUTHENTICATION_#
aaa authorization exec <i>list-name</i>	CSM_VTY_EXEC_AUTHORIZATION_#	CSM_CON_EXEC_AUTHORIZATION_#
aaa authorization commands <i>level list-name</i>	CSM_VTY_COMM_AUTHORIZATION_#	CSM_CON_COMM_AUTHORIZATION_#
aaa accounting exec <i>list-name</i>	CSM_VTY_EXEC_ACCOUNTING_#	CSM_CON_EXEC_ACCOUNTING_#
aaa accounting connection <i>list-name</i>	CSM_VTY_CONN_ACCOUNTING_#	CSM_CON_CONN_ACCOUNTING_#
aaa accounting commands <i>list-name</i>	CSM_VTY_COMM_ACCOUNTING_#	CSM_CON_COMM_ACCOUNTING_#
Line configuration commands		
login authentication <i>list-name</i>	CSM_VTY_AUTHENTICATION_#	CSM_CON_AUTHENTICATION_#
authorization exec <i>list-name</i>	CSM_VTY_EXEC_AUTHORIZATION_#	CSM_CON_EXEC_AUTHORIZATION_#
authorization commands <i>level list-name</i>	CSM_VTY_COMM_AUTHORIZATION_#	CSM_CON_COMM_AUTHORIZATION_#
accounting exec <i>list-name</i>	CSM_VTY_EXEC_ACCOUNTING_#	CSM_CON_EXEC_ACCOUNTING_#
accounting connection <i>list-name</i>	CSM_VTY_CONN_ACCOUNTING_#	CSM_CON_CONN_ACCOUNTING_#
accounting commands <i>level list-name</i>	CSM_VTY_COMM_ACCOUNTING_#	CSM_CON_COMM_ACCOUNTING_#

For example, if the device contains:

```
aaa authentication login CSM_CON_AUTHENTICATION_1 group tacacs+ local
```

REVIEW DRAFT – CISCO CONFIDENTIAL

And the console policy in Security Manager uses this AAA method list for authentication, the following CLI command is deployed:

```
line con 0
login authentication CSM_CON_AUTHENTICATION_1
```

Name Changes in NAC Policies

Table 6-9 describes the changes that are made to resource names in Network Admission Control (NAC) policies discovered on a Cisco IOS router.

Table 6-9 NAC Resource Name Changes

Resource	Sample Name on Device	Security Manager Naming Format
ip admission name	myAdmission	CSM_[INTERFACE_NAME]

When you deploy to the device, Security Manager adds the new ip admission name definition to the existing resource in the device configuration, as shown below. It reuses the access lists that are configured for the intercept ACL and the identity action ACL.

```
ip admission name MY_ADMISSION_NAME eapoudp inactivity-time 60 list MY_ADMISSION_ACL
ip admission name CSM_Group-Async4 eapoudp inactivity-time 60 list MY_ADMISSION_ACL
identity profile eapoudp
  device authorize type cisco ip phone policy MY_IDENTITY_POLICY
identity policy MY_IDENTITY_POLICY
  access-group MY_IDENTITY_ACL
interface Group-Async4
  ip admission CSM_Group-Async4
!
ip access-list extended MY_ADMISSION_ACL
  permit ospf any any
ip access-list extended MY_IDENTITY_ACL
  permit ip host 2.2.2.2 host 3.3.3.3
```

As can be seen in this example, the new **ip admission** definition is identical to the original resource except for the name.

Name Changes in Quality of Service Policies

Table 6-10 describes the changes that are made to resource names in quality of service (QoS) policies discovered on a Cisco IOS router.

Table 6-10 QoS Resource Name Changes

Resource	Sample Name on Device	Security Manager Naming Format
class-map	myClassMap	CSM_CLASS_MAP_0
policy-map	myPolicyMap	CSM_POLICY_MAP_0

REVIEW DRAFT – CISCO CONFIDENTIAL

When you deploy to the device, Security Manager adds these new resources to the existing resources in the device configuration. As a result, the device configuration will contain two identical class maps and two identical policy maps with different names.

As can be seen in the following example, the original policy map (myPolicyMap) continues to reference the original class map (myClassMap) even after the addition of the new resources configured in Security Manager. The service policy configured on the interface also points to the new policy map.

```
class-map match-any myClassMap
  match access-group name myAcl
  match protocol arp
class-map match-any CSM_CLASS_MAP_0
  match access-group name myAcl
  match protocol arp
!
policy-map myPolicyMap
  class myClassMap
policy-map CSM_POLICY_MAP_0
  class CSM_CLASS_MAP_0
!
interface GigabitEthernet0/0
  ip address 10.56.12.22 255.255.255.128
  duplex auto
  speed auto
  service-policy output CSM_POLICY_MAP_0
```



CHAPTER 7

Firewall Services

This chapter contains the following topic:

- [FAQs About Firewall Services, page 7-1](#)



Note

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

FAQs About Firewall Services

This section answers the following questions about firewall services:

- [Q. Why do I lose my connection after I deploy my firewall rules to a device?](#)
- [Q. Why does the Hit Count report not show standard ACLs for my IOS device?](#)
- [Q. Why does the CLI supporting HTTP for authentication proxy remain on the device after I unassign the policy?](#)
- [Q. Why can I not deploy my access rules policies for the BGP routing protocol to 87x routers?](#)
- [Q. Why is an ACE removed from the ACL even though it is bound to the interface?, page 7-2](#)
- [Q. How do I create an firewall rule that permits a range of addresses, as defined in a network/host object, but negates selected addresses within that range?](#)
- [Q. How do I configure the management IP of a security context in transparent mode without going to the device to configure it?](#)

Q. Why do I lose my connection after I deploy my firewall rules to a device?

A. Security Manager does not check whether the firewall rules that you configured in Security Manager permit management traffic (SSH and HTTPS) to the device being managed. As a result, after you deploy firewall rules to the device, connection to the device might be lost. Therefore, we strongly recommend that your access rules policies contain a global rule that permits Security Manager to access the device. Keep in mind that when you create an access rule policy, the device creates an implicit **deny any** rule at the end of your explicit rules.

- Q.** Why does the Hit Count report not show standard ACLs for my IOS device?
- A.** The purpose of the Hit Count tool is to show statistics related to the access rules defined in Security Manager and deployed to the device. Do not use the Hit Count tool until after you use Security Manager to deploy the configuration to the device. Because Security Manager deploys only extended ACLs for the access rules policy, results are displayed only for extended ACLs.
- Q.** Why does the CLI supporting HTTP for authentication proxy remain on the device after I unassign the policy?
- A.** IOS devices require that HTTP be used as the traffic type for authentication proxy, which generates the command **ip http server**. Security Manager does not remove the CLI after you unassign the authentication proxy policy from the device in Security Manager. If you do not require HTTP access for other purposes to the IOS device, you can manually remove the CLI or create a FlexConfig object to remove the CLI from the device.
- Q.** Why can I not deploy my access rules policies for the BGP routing protocol to 87x routers?
- A.** IOS 87x ISR routers do not support BGP as a routing protocol or as a service in ACLs if the device has only 24 MB of memory; however, BGP is supported if the device has more than 24 MB of memory. Security Manager does not detect the amount of memory available on the device and cannot enforce any restrictions. As a result, deploying a job containing an access rule for BGP fails. If you create an ACL with a single ACE containing BGP, an empty ACL is created on the device, which you can remove manually.
- Q.** Why is an ACE removed from the ACL even though it is bound to the interface?
- A.** If you import or discover a PIX 6.3 device that has an ACE with the “interface” keyword, then you deploy to the same device without making any changes, the ACE might be removed from the ACL even though it is bound to the interface by the **access-group** command. This can occur if the ACL has other ACEs, or the ACL contains only the ACEs using the “interface” keyword. The **access-group** command for the ACL is removed from the device.
- Q.** How do I create an firewall rule that permits a range of addresses, as defined in a network/host object, but negates selected addresses within that range?
- A.** It is not possible to create a network object that includes a range but excludes certain addresses within that range. Instead, create two rules. The first rule should define those addresses that you want to deny. You can create a network/host object for that purpose. The second rule, which should immediately follow the first, should define the range of permitted addresses, as defined in the other network/host object.
- Q.** How do I configure the management IP of a security context in transparent mode without going to the device to configure it?
- A.** This requires a two-step process. First, you must configure and deploy a management IP policy to the security context. You can then configure the device properties of the security context so that Security Manager uses the management IP to communicate directly with the security context.

-
- Step 1** In the Device selector, select the security context, then select **Platform > Bridging > Management IP** in the Policy selector.
- Step 2** Enter the management IP address and network mask, then click **Save**.
- Step 3** Submit and deploy your changes. Deployment to the security context is performed through the system execution space. The management IP is now configured on the device.
- Step 4** In the Device selector, right-click the security context and select **Device Properties**.

- Step 5** On the General page, enter the management IP address in the IP Address field.
 - Step 6** Click **Credentials** to display the Credentials page.
 - Step 7** Enter the credentials for the security context, then click **Save**. Security Manager can now communicate directly with the security context.
-



CHAPTER 8

IPS

This chapter contains the following topics:

- [Importing IPS 5.0 Sensors, page 8-1](#)
- [Retrieving Signature Updates, page 8-1](#)
- [Performing IPS Updates, page 8-2](#)
- [Updating IOS IPS Crypto Configurations, page 8-2](#)
- [Creating ACLs During IOS IPS Configuration, page 8-3](#)
- [Performing IOS IPS Deployment, page 8-3](#)
- [Provisioning Trusted Hosts, page 8-3](#)
- [Managing Signature Updates, page 8-3](#)



Note

For more detailed information see the “Managing IPS Devices” chapter in the [User Guide for Cisco Security Manager](#) for your release.

Importing IPS 5.0 Sensors

Problem You cannot import IPS 5.0 (or earlier) sensors into Security Manager.

Solution Security Manager supports IPS 5.1, IPS 6.0, IPS 6.2, IPS 7.0, and IPS-enabled IOS 12.4(11)T2 and above only. When you import a sensor on which virtual sensors are configured, you must submit your changes (or approve your activity when working in Workflow mode) after discovery in order to view the virtual sensors in the Device selector. A warning message that explains this is displayed after discovery.

Retrieving Signature Updates

Problem You cannot connect to the Update Server or CCO to retrieve signature updates into Security Manager.

Solution Make sure that you have specified the location from which Security Manager should download signature updates. Select **Tools > Security Manager Administration > IPS Updates**, then click **Edit Settings** under Update Server to enter this information. After updating the server information, make sure you click **Save** at the bottom of the page.

Performing IPS Updates

Problem You cannot update your IPS sensor with patches, service packs, or signature updates.

Solution Check the time on your IPS sensor. If the time on the sensor is ahead of the time on the associated certificate, the certificate is rejected and the update may fail. Use the Network Time Protocol (NTP) to maintain accurate time on an IPS sensor.

The following procedures describes how to identify an NTP server.



Caution

If your sensors already have an NTP server configuration, you must identify the NTP server by performing the relevant procedure. Otherwise, your NTP server settings are lost.



Note

Signature updates are available for IPS 5.1(4) and above.

- Step 1** In Device view, select the IPS sensor for which you want to identify an NTP server.
- Step 2** Select **Platform > Device Admin > Server Access > NTP**. The Network Time Protocol page appears.
- Step 3** In the NTP Server IP Address field, enter the address of the NTP server.
- Step 4** In the Key field, enter the key value of the NTP server.
- Step 5** In the Key ID field, enter the key ID value of the NTP server. Valid values are 1 through 4294967295.



Note

For detailed information on how to set the time on a sensor, refer to [Configuring the Sensor to Use an NTP Time Source](#) in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0*, which is available on Cisco.com. You will be prompted for your CCO username and password.

Updating IOS IPS Crypto Configurations

Problem You cannot update your IOS IPS Crypto configuration.

Solution Check whether the TFTP server is running on your Cisco Security Manager server. Make sure your TFTP directory has the required permissions to enable IOS IPS to download the certificate from it. The default TFTP directory for Windows 2000 and 2003 is `<install-dir>\tftpboot`. In addition, you must have a user account with adequate privileges to update IOS IPS crypto configurations.

Creating ACLs During IOS IPS Configuration

Problem ACL creation during IOS IPS configuration is not producing the expected results.

Solution Entering the name or number of an ACL on the following IPS Manager pages does not actually create the ACL:

- IOS IPS Rules page
- IOS IPS Filters page
- IOS IPS Port Mapping page

To create the ACL, use the command line on the IOS IPS device that you are configuring. If you enter an ACL number and deploy the configuration while no corresponding ACL exists in the router, this command has no effect.

Performing IOS IPS Deployment

Problem You receive an error message during initial deployment of an IOS IPS device.

Solution You may have exceeded the memory available on the IOS IPS device. To work around this problem, select a reduced set of signatures to be deployed and then redeploy the IOS IPS device.

Provisioning Trusted Hosts

Problem You cannot provision a Management Center for Cisco Security Agent (CSA MC) server as a trusted host to an IPS sensor.

Solution You must use CLI commands or the IPS Device Manager (IDM). When you add a CSA MC server to an IPS sensor in IDM, a message appears that asks whether to add the server as a trusted host to the sensor. (There is a separate option in IDM for adding a list of IP addresses as trusted hosts to the sensor.)

Managing Signature Updates

Problem You cannot obtain signature updates for a sensor running IPS 5.1.

Solution Although Security Manager supports IPS 5.1 and above, signature updates are available only for IPS 5.1(4) and higher.



CHAPTER 9

VPNs

This chapter contains the following topics:

- [Updating VPNs That Include Routing Processes, page 9-2](#)
- [Loss of Communication with Spoke, page 9-2](#)
- [Configuring PKI with AAA on IOS Devices, page 9-2](#)
- [Defining Multiple CA Servers for Site-to-Site VPNs, page 9-2](#)
- [Unneeded Policy in Easy VPN Topology, page 9-5](#)
- [Discovering a VPN Already Configured in Security Manager, page 9-5](#)
- [Enabling and Disabling VRF on Catalyst Switches and 7600 Devices, page 9-5](#)
- [Commands That Cannot be Configured When Easy VPN is Enabled, page 9-6](#)
- [Defining VPNs with Multiple Spoke Definitions, page 9-7](#)
- [SSL VPN Limitations, page 9-8](#)
- [SSL VPN Limitations Due to Device OS Defects, page 9-9](#)
- [Removing Group Policy Attributes from SSL VPNs Defined on ASA 7.x Devices, page 9-9](#)
- [Provisioning GET VPN Using Security Manager Is Not Working, page 9-10](#)
- [Preshared Key Policies Not Getting Discovered, page 9-11](#)
- [Edit Wizard of GETVPN Does Not Allow Editing of Key Servers or Group Members, page 9-11](#)



Note

For information about VPN features that are not discovered by Security Manager, see [Undiscovered VPN Features, page 6-6](#).



Note

For more detailed information on employing VPNs with Security Manager, see the [User Guide for Cisco Security Manager](#) for your release.

Updating VPNs That Include Routing Processes

Problem When you define and deploy changes to a routing process that is being used by a VPN topology (using either the Site-to-Site VPN Manager or the routing policies), the changes that you make are not reflected in the CLI commands configured on the device.

Solution When you discover a VPN topology that includes routing processes, such as GRE full mesh, Security Manager populates the GRE Modes policy in the Site-to-Site VPN Manager, as well as the relevant routing policies. However, changes made to one of these policies in Security Manager are not automatically reflected in the other policy, which can lead to unexpected results after deployment.

Therefore, if you make changes to the secured IGP in the Site-to-Site VPN Manager, be sure to go to Platform > Routing in Device view to make the necessary changes in the device's routing policies. Likewise, if you make changes directly to the routing policy, be sure to make the necessary changes in the Site-to-Site VPN Manager as well.

Loss of Communication with Spoke

Problem You lose communication with a spoke in the VPN.

Solution This problem can occur when the Security Manager server communicates with an external interface on the spoke from within the hub's protected network. We recommend that when you add the hub device to Security Manager that you define a management IP address that is located outside of the hub's protected network.

Configuring PKI with AAA on IOS Devices

Problem You cannot configure PKI with AAA authorization that uses the entire subject name on an IOS router.

Solution You can create this configuration using the predefined FlexConfig object named IOS_PKI_WITH_AAA. Please note that this FlexConfig is not supported on PIX/ASA devices.

Defining Multiple CA Servers for Site-to-Site VPNs

Problem You can select only one CA server when defining a Public Key Infrastructure (PKI) policy on a site-to-site VPN. This creates a problem when the devices in the VPN enroll with different CA servers. For example, the spoke devices might enroll with a different CA server than the hub, or the spokes in one part of the VPN might enroll with a different CA server than the spokes in another part of the VPN.

Solution To define a PKI policy, you select a PKI enrollment object that specifies the CA server to which the devices should enroll. Although by default the policy object refers globally to a single CA server, you can use device-level overrides to have the object refer to a different CA server on selected devices.

For example, if PKI enrollment object PKI_1 refers to a CA server named CA_1, you can create a device-level override for selected devices that has PKI_1 refer to a different CA server, for example, CA_2. Theoretically, you can use overrides to define a different CA server for each device in the VPN.

This procedure describes the basic steps for creating overrides for PKI enrollment objects.

**Note**

All topics that are referenced in the procedure can be found in the *User Guide for Security Manager*.

Procedure

-
- Step 1** To create the PKI enrollment object, open the PKI Enrollment dialog box. You can access this dialog box in two ways:
- From the Public Key Infrastructure policy—Click the **Add** button beneath the Selected field. See *Configuring Public Key Infrastructure Policies*.
 - From the Policy Object Manager—Select **PKI Enrollments** from the Object Type selector, then click the **New Object** button. See *Understanding the Policy Object Manager Window*.
- Step 2** Define the global definition of the PKI enrollment object, including the CA server to which the object refers. Be sure to select the **Allow Value Override per Device** check box. This option makes the object overridable on individual devices. For more information, see *Creating PKI Enrollment Objects*.



Note We recommend that you base the global definition of the object on the CA server that is used by the most devices in the VPN. Doing this reduces the number of device-level overrides that are required.

- Step 3** When you finish defining the PKI enrollment object, click **OK**. As a result:
- If you accessed the dialog box via the PKI policy, the new object appears in the Selected field of the policy page.
 - If you accessed the dialog box via the Policy Object Manager, the new object appears in the work area of the Policy Object Manager window. A green check mark in the Overridable column indicates that device-level overrides *may* be created for this object. (The check mark does *not* indicate whether any overrides actually exist.)

- Step 4** Create the device-level overrides for the PKI enrollment object. You can do this in one of two ways:
- From Device Properties—This option is recommended when you want to create a device-level override for a single device. Select **Policy Object Overrides > PKI Enrollments**, select the PKI enrollment object that you want to override, then click the **Create Override** button. You can then define the content of the override, including the CA server defined by the object.
For more information, see *Creating Object Overrides for a Single Device*.
 - From the Policy Object Manager—This option is recommended when you want to create a device-level override for multiple devices at the same time. Double-click the green check mark in the Overridable column, select the devices to which the override should apply, then define the content of the override, including the CA server defined by the object.
For more information, see *Creating Object Overrides for Multiple Devices*.
-



Note You can also use device-level overrides when the CA servers are arranged in a PKI hierarchy beneath a common, trusted CA server. To do this, you must ensure that both the global definition of the object and the device-level override specify the trusted CA server in the Trusted CA Hierarchy tab of the PKI Enrollment dialog box. See *Defining the Trusted CA Hierarchy*.

Unneeded Policy in Easy VPN Topology

Problem According to the Site-to-Site VPN Manager, your Easy VPN topology contains a policy that is not relevant to the types of devices contained in the topology.

Solution When you configure an Easy VPN topology, IOS routers, Catalyst 6500/7600 devices, and PIX 6.3 devices require you to define a user group policy. PIX 7.0+ and ASA devices, however, require a tunnel group policy instead. To streamline the process, the Create VPN wizard automatically configures both policies with default values, including matching keys and group names.

If your topology contains both devices that require the user group policy and devices that require the tunnel group policy, each policy receives the relevant policy during deployment. If your topology consists entirely of devices that require the same policy (either the user group policy or the tunnel group policy), the unneeded policy is simply ignored during deployment.

**Note**

If you make any changes to the user group or tunnel group policies, you must make sure that the group name and the key match in both policies. Otherwise, deployment will fail.

Discovering a VPN Already Configured in Security Manager

Problem After you perform discovery, you see duplicate VPN topologies configured in the Site-to-Site VPN Manager. This situation can occur if you discover a VPN that you have already configured manually in Security Manager. If the VPN topology you discover matches the one you configured, the discovered VPN is imported into Security Manager without overwriting the VPN that you configured manually.

Solution When you add existing site-to-site VPNs to Security Manager, you should either:

- Use discovery to import the VPN into Security Manager *instead* of configuring the topology manually.
- Perform rediscovery *after* configuring the VPN manually. Performing rediscovery after configuring the VPN does not result in duplicate topologies. To perform rediscovery, right-click the VPN in the Site-to-Site VPN Manager, then select **Re-Discover Site-To-Site VPN**.

**Note**

Rediscovery discovers the VPN endpoints only; it does not discover the policies configured for the VPN.

Enabling and Disabling VRF on Catalyst Switches and 7600 Devices

Problem Deployment fails when you change the virtual routing and forwarding (VRF) mode on the Catalyst switches and 7600 hub of an existing site-to-site VPN. For example, if you initially configured VRF in the Create VPN wizard and deployed, but later return to the Peers policy and deselect the Enable VRF Settings check box, deployment fails. (This setting is found in the VRF Aware IPsec tab of the Edit Endpoints dialog box.) Deployment likewise fails if you try to enable VRF on a VPN that was not initially configured with it.

Solution You cannot change the VRF mode during operation. Therefore, you must do the following:

Procedure

-
- Step 1** Delete the VPN topology from Security Manager.
 - Step 2** Deploy your changes.
 - Step 3** Reload (restart) the Catalyst 6500/7600 device.
 - Step 4** Right-click the device and select **Discover Policies on Device**.
 - Step 5** Open the Create VPN wizard and redefine the VPN topology. At this point, you can select a different VRF mode.

**Note**

- This restriction applies only to Catalyst 6500/7600 hubs, not other device types.
 - This restriction does not apply to changes made to the VRF settings themselves. For example, if VRF is configured on the VPN topology, you can return to the Peers policy and change the VRF name or route distinguisher.
-

Commands That Cannot be Configured When Easy VPN is Enabled

Problem You cannot modify the configuration of a VPN client, including interface settings, on an ASA device when Easy VPN is enabled.

Solution The following commands (including their ‘no’ form) cannot be modified when Easy VPN is enabled:

- `aaa authentication listener`
- `aaa mac-exempt`
- `clear configure aaa`
- `clear configure crypto`
- `clear configure crypto isakmp`
- `clear configure crypto map`
- `clear configure nat`
- `clear configure sysopt`
- `clear configure tunnel-group`
- `crypto isakmp`
- `crypto map`
- `interface name-if`
- `interface security-level`
- `isakmp keepalive`
- `nat...access list`
- `sysopt connection permit-vpn`
- `tunnel-group`
- `webvpn enable`

**Note**

The `clear configure interface` command disables Easy VPN Remote.

Defining VPNs with Multiple Spoke Definitions

Problem If you discover a VPN whose spokes contain different definitions (for example, different client modes for Easy VPN spokes), Security Manager changes the definitions during discovery to create a uniform definition for all spokes. This behavior occurs because VPN topologies in Security Manager can contain only one set of spoke definitions.

Solution You can choose one of two approaches:

- Define multiple VPN topologies in Security Manager, where each topology includes spokes containing matching spoke definitions.
- Define a FlexConfig policy that contains the specialized definition, then assign the policy to the spokes that require this definition, as described in the procedure below.

Procedure

-
- Step 1** Create a shared FlexConfig policy in Policy view:
- a. Select **View > Policy View**.
 - b. Right-click **FlexConfigs** in the Policy Type selector, then select **New FlexConfigs Policy**.
 - c. Enter a name for the policy, then click **OK**. The new shared policy is displayed in the Shared Policy selector in the lower-left pane of Policy view.
- Step 2** Define the FlexConfig policy by creating and selecting a FlexConfig object:
- a. In the work area of Policy view, click the **Add** button on the Details tab.
 - b. In the FlexConfigs Selector, click the **Create** button in the lower-left corner of the window. The FlexConfig dialog box is displayed.
 - c. Define an appended FlexConfig object that contains the required client definition. For example, to define the client mode on an Easy VPN spoke, enter the following commands:

```
crypto ipsec client ezvpn CSM_EASY_VPN_CLIENT_1
mode client
exit
```
 - d. After you create the FlexConfig object, add it to the FlexConfig policy using the selector.
- Step 3** In the work area of Policy view, use the Assignments tab to select the spokes to which this policy should be assigned, then click **Save**.
- Step 4** Deploy the policy.
-



Note

For more information about the steps described in this procedure, see the following topics in [User Guide for Cisco Security Manager](#) for your release:

- [Creating a New Shared Policy](#)
 - [Creating FlexConfig Policy Objects](#)
 - [Modifying Policy Assignments in Policy View](#)
-

SSL VPN Limitations

The current implementation of SSL VPN in Security Manager is subject to the following limitations:

- SSL VPN license information cannot be imported into Security Manager. As a result, certain command parameters, such as **vpn sessiondb** and **max-webvpn-session-limit**, cannot be validated.
- You must configure DNS on each device in the topology in order to use clientless SSL VPN. Without DNS, the device cannot retrieve named URLs, but only URLs with IP addresses.
- If you share your Connection Profiles policy among multiple ASA devices, bear in mind that all devices share the same address pool unless you use device-level object overrides to replace the global definition with a unique address pool for each device. Unique address pools are required to avoid overlapping addresses in cases where the devices are not using NAT.
- You must use interface roles, not physical interfaces, when defining SSL VPN gateways on IOS devices. On ASA devices, however, you can select physical interfaces when defining an Access policy. For more information about interface roles, see “Working with Interface Role Objects” in the *User Guide for Cisco Security Manager*.
- Security Manager (and ASA devices in general) do not check whether proxy-bypass interfaces are also configured as SSL VPN-enabled. If proxy-bypass is enabled on an interface that is not SSL VPN-enabled, certain 7.2 releases prevent you from reusing the proxy-bypass port after the rule is removed. The only solution to this problem is to reboot the device.
- If the device configuration contains an address pool for SSL VPN with a name that begins CSM_ (the naming convention used by Security Manager), Security Manager cannot detect whether the addresses in that pool overlap with the pool configured in your SSL VPN policy. (This can occur, for example, when the pool was configured by a user on a different installation of Security Manager.) This can lead to errors during deployment. Therefore, we recommend that you configure the same IP address pool as a network/host object in Security Manager and define it as part of the SSL VPN policy. This enables the proper validation to take place.
- The same IP address and port number cannot be shared by multiple SSL VPN gateways on the same IOS device. As a result, deployment errors can occur if a duplicate gateway exists in the device configuration but was not redefined using the Security Manager interface. If such an error occurs, you must choose a different IP address and port number and redeploy.
- If you define AAA authentication or accounting as part of an SSL VPN policy, the **aaa new-model** command is deployed to enable AAA services. Bear in mind that this command is not removed if you later delete the SSL VPN policy, as there might be other parts of the device configuration that require the **aaa new-model** command for AAA services.

**Note**

In addition, we recommend that you define at least one local user on the device with a privilege level of 15. This ensures that you will not be locked out of the device if the **aaa new-model** command is configured without an associated AAA server.

SSL VPN Limitations Due to Device OS Defects

The current implementation of SSL VPN in Security Manager is subject to the following limitations caused by existing IOS and ASA defects:

- Deployment fails if you remove a port forwarding list used by an SSL VPN user group. This problem occurs in IOS 12.4(9)T and was corrected in IOS 12.4(12.15)T. The workaround is to delete all the attributes of the port forwarding list (other than the name, which is mandatory) instead of removing it from the user group. For more information, see [CSCsh50799](#).



Note If the port forwarding list is used by other user groups, you can ignore the deployment error.

- Deployment fails if you modify the attributes of a WINS master server (for example, the timeout) used by an SSL VPN user group. This problem occurs in IOS 12.4(9)T and was corrected in 12.4(13.11)T. The workaround is to remove the WINS server from the user group and deploy. After deployment, you can make the necessary changes to the WINS server and add it back to the user group. For more information, see [CSCsg16935](#).
- Deployment fails if the addresses in the address pool used by an SSL VPN user group do not belong to the same subnet as one of the interfaces on the device. This problem occurs in IOS 12.4(11)T. The workaround is to create a loopback interface that is on the same subnet as the addresses in the pool.
- If you define a AAA accounting server in the SSL VPN policy, you must have a default accounting server defined on the device. Otherwise, accounting functions (such as keeping track of how many times an SSL VPN connection is used, by whom, and for how long) are not performed. This problem occurs in IOS 12.4(9)T and was corrected in 12.4(10.04)T. For more information, see [CSCse90029](#). To assign an accounting server to SSL VPN, enter the following CLI command:

```
aaa accounting network default start-stop group radius
```



Note If you use a FlexConfig to enter this command, be sure to remove the FlexConfig after deployment. Otherwise, the command will be reissued each time that you redeploy.

- When CNS is configured, the port forwarding list and the URL list defined in Security Manager are assigned to the wrong SSL VPN context. For example, if these lists are defined to context 1, they are deployed to context 2. This problem occurs in IOS 12.4(11)T and was corrected in 12.4(19.14)T. The workaround is to remove the CNS configuration before defining these lists and restoring the configuration afterwards. For more information, see [CSCsh72072](#).

Removing Group Policy Attributes from SSL VPNs Defined on ASA 7.x Devices

Problem After you deploy changes to a Tunnel Group policy for a remote access VPN on a PIX/ASA 7.x+ device, you find that the **group-policy** commands defined on the device for SSL VPN have been removed.

Solution Security Manager does not discover SSL VPN device configurations. As a result, it does not make changes to these configurations unless you define and deploy SSL VPN policies using the Security Manager interface. However, **group-policy** (which is modeled in Security Manager as ASA user group objects) is an exception, because it is used by both SSL VPNs and IPsec remote access VPNs, as follows:

- SSL VPNs—User Groups policy, Connection Profiles policy
- Remote access VPNs—Tunnel Group policy (General tab)

A device configuration can use the same group-policy definition (that is, the same ASA user group object) in both policies. When you discover that configuration, only the remote access VPN attributes are imported into Security Manager. As a result, on the next deployment, the remote access VPN attributes are deployed to the device and any SSL VPN attributes are removed.

Therefore, if the device configuration uses the same group-policy definition for remote access VPN as well as for SSL VPN, you must configure an SSL user groups policy to compensate for the fact that it was not defined as part of the discovery process.

VPN Policy Discovery Fails When Backup Servers Use Hostname

Problem VPN Policy Discovery fails with the following error:

Policy Discovery Failed: com.cisco.nm.vms.discovery.DiscoveryException: Internal Error

Solution A User Group policy is configured with backup servers using hostnames instead of an IP addresses. For discovery to be successful, you need to reconfigure the user group policy on the device with backup servers using IP address, not hostnames.

Provisioning GET VPN Using Security Manager Is Not Working

Problem After provisioning and deploying GET VPN using Security Manager, the GET VPN is not working.

Solution Check the following:

- Because Security Manager does not support automatic key synchronization between cooperative key servers, make sure to export the RSA key from the primary key server and import it on other key servers manually.
- Make sure the security ACL has the permit ACE for the desired traffic. For asymmetric ACEs (different source and destination), check whether the mirrored ACE is also present.
- If multicast rekey is selected, check whether there is a deny ACE in the key server security ACL for the multicast group address to prevent encryption of multicast rekey messages.
- For multicast rekey, make sure that the network is multicast enabled.
- Check that the local security ACL on the group member has only deny ACEs.
- For group member authorization using certificates, check that the ISAKMP authentication uses certificates and that a PKI policy is configured. ISAKMP identity on the group member and key server should be set to use the distinguished name (dn).

Preshared Key Policies Not Getting Discovered

Problem Security Manager is not discovering preshared key policies.

Solution Security Manager discovers preshared key policies only when the preshared key has the same value on all devices.

Edit Wizard of GETVPN Does Not Allow Editing of Key Servers or Group Members

Problem The Edit VPN wizard only allows editing of the VPN name and description.

Solution This behavior is by design. To edit other GET VPN attributes and policies, use the Site-to-Site VPN Manager tool.



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.
- Access Control Settings.
- Interfaces.
- FlexConfigs.

All other policies require Cisco IOS Software Release 12.3 or higher.

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](#)
- [Security Manager Indicates Deployment Failed on an 83x Router, 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.

Security Manager Indicates Deployment Failed on an 83x Router

Problem Security Manager indicates that the deployment of NAT interface commands (**ip nat inside** and **ip nat outside**) fails.

Solution This problem occurs occasionally on Cisco 83x Series routers. When deploying NAT interface commands, the router returns the following reply:

```
% Failed to allocate regular expression state table : 62976
% PDL Error : Failed to compile regexp
  File : rtsp.pdl
  Line : 113
      : (regexp store insensitive
```

Deployment fails as a result of this error. Nevertheless, these NAT commands appear in the running configuration of the device. The error has no known affect on the NAT configuration of 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. This problem is corrected in Cisco IOS Software Releases 12.4(09.10)T and 12.4(09)T01 and subsequent releases. 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](#)

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.

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 10-6](#)
- [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](#)

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



CHAPTER 11

Catalyst Switches and 7600 Devices

This chapter contains the following topics:

- [FAQs about Catalyst Switches and 7600 Devices, page 11-1](#)
- [Discovering Failover Pairs, page 11-2](#)
- [Deployment Fails for Interface Settings, page 11-2](#)
- [Deployment Fails for Internal VLANs, page 11-2](#)
- [Deployment Fails When Changing the Running Mode of an ISDM Data Port VLAN, page 11-3](#)

FAQs about Catalyst Switches and 7600 Devices

This section answers the following questions about Catalyst Switches and 7600 devices:

- [Q.Which VTP modes are supported by Security Manager?](#)
- [Q.How do I add a Catalyst 6503-E switch to Security Manager? The device does not appear in the list of supported devices in the New Device wizard.](#)
- [Q.What kinds of matching ACLs are supported by VLAN ACLs \(VACLs\) configured on Catalyst Switches and 7600 devices?](#)
- [Q.What are the limitations in support for ISDM settings in Security Manager?](#)
- [Q.Can I reference an undefined VLAN in Security Manager?](#)

Q. Which VTP modes are supported by Security Manager?

A. Before 3.2, Security Manager supported only VTP transparent mode for Catalyst switches and 7600 devices. Security Manager 3.2 and higher can now also manage switches configured in the VTP client/server mode. Security Manager manages switches configured in client/server mode by bypassing VLAN database management on the device (including VLAN creation, deletion, and monitoring VLANs in the VLAN database on switches).

Q. How do I add a Catalyst 6503-E switch to Security Manager? The device does not appear in the list of supported devices in the New Device wizard.

A. The Catalyst 6503-E switch shares the same System Object ID as the Catalyst 6503; therefore, only the 6503 appears in the list of devices. Both devices, however, are supported. The same holds true for the Catalyst 6506-E and the Catalyst 6509-E.

- Q.** What kinds of matching ACLs are supported by VLAN ACLs (VACLs) configured on Catalyst Switches and 7600 devices?
- A.** Security Manager supports the use of standard and extended ACLs as matching criteria for VACLs on Catalyst switches and 7600 devices. MAC-layer ACLs are not supported.
- Q.** What are the limitations in support for IDSM settings in Security Manager?
- A.** Security Manager supports a subset of IDSM settings on chassis running IOS 12.2(18)SXF4 or later. Trunk (IPS) and Capture (IDS) modes are supported; inline mode is not supported. Security Manager cannot manage IDSM data ports that are part of a spanning tree or access VLAN.
- Q.** Can I reference an undefined VLAN in Security Manager?
- A.** Yes, you can reference an undefined VLAN in VLAN group, VACL, and IDSM definitions. However, when you submit your changes, a warning message is displayed that recommends you either define the VLAN or delete it, as the configuration might interfere with device operation. Bear in mind that deleting a VLAN does not delete its references. Therefore, if you have defined a VACL that references an undefined VLAN, deleting the VLAN does not remove the reference in the VACL.

Discovering Failover Pairs

Only one device of a failover pair should be managed by Security Manager. During discovery, use the wizard to set the discovery mode of the second device to Do Not Discover Module. Security Manager always manages the active admin context, regardless of whether you added the primary or secondary failover service module.

Deployment Fails for Interface Settings

Problem Deployment fails for interface settings on a Catalyst 6550/7600 device.

Solution Certain interface settings (such as speed, duplex, and MTU settings) are specific to particular card types and are not validated prior to deployment. Make sure to enter the correct values for your specific card type to ensure successful deployment.

Deployment Fails for Internal VLANs

Problem Deployment fails when Security Manager tries to create a VLAN with an ID that is within the range of the device's internal VLAN list.

Solution Security Manager cannot detect internal VLANs. Therefore, you must define a VLAN ID that falls outside of the device's internal VLAN list. Use the **show vlan internal usage** command to view the list of internal VLANs.

Deployment Fails When Changing the Running Mode of an ISDM Data Port VLAN

Problem Deployment fails when you attempt to change the running mode of the data port VLAN from Trunk (IPS) to Capture (IDS) from the ISDM Data Port VLANs dialog box and the following error message is displayed:

Command Rejected: Remove trunk allowed vlan configuration from data port 2 before configuring capture allowed-vlans

Solution On some software releases such as 12.2(18)SFX4, there is a bug that prevents the change from occurring correctly. Reload the device to overcome the problem.



CHAPTER 12

Deployment

This chapter contains the following topics:

- [FAQs About Deployment](#), page 12-1
- [Changing How Security Manager Responds to Device Messages](#), page 12-8
- [Performing Rollback When Deploying to a File](#), page 12-9
- [Mixing Deployment Methods](#), page 12-9
- [SSL Handshake Failure When Deploying to PIX/ASA Devices](#), page 12-10
- [Deployment Failures to Devices Managed by AUS](#), page 12-10
- [Deployment Failures to FWSM Virtual Contexts After Changing Interface Policies](#), page 12-11

FAQs About Deployment

This section answers the following questions about deployment:

- [Q.How does Security Manager perform deployment?](#)
- [Q.Which deployment method should I use?](#)
- [Q.How can I control the location used when I deploy to configuration files?](#)
- [Q.If I deploy to files, how does Security Manager know that I applied the configuration to the device?](#)
- [Q.What happens during configuration rollback?](#)
- [Q.After configurations are deployed, which are completely owned by Security Manager, and which are only partially owned, and what does this mean?](#)
- [Q.What happens if I make changes to a device configuration outside of Security Manager \(an out-of-band change\)?](#)
- [Q.How can I get out-of-band changes into Security Manager?](#)
- [Q.What happens during deployment if the version of the OS running on the device is not the same version listed for the device in Security Manager?](#)
- [Q.How do I fix a version mismatch problem?](#)
- [Q.Does Security Manager deploy full configurations or only the changes made since the last deployment \(delta configurations\)?](#)
- [Q.How many devices can Security Manager deploy to simultaneously or in a single job?](#)

- Q. Deployment to a Cisco IOS router fails and an “Error Writing to Server” or “Http Response Code 500” error message occurs. Why?
 - Q. Why does deployment to FWSM fail when the configuration contains a large number of ACLs?
 - Q. Why does deployment fail even though the warning expression in the properties files is set to ignore the error?
 - Q. Why do some platforms require a reload after performing configuration rollback but not others?
 - Q. Why were no changes deployed to a device in a job created from a schedule even though preview configuration shows some changes?
- Q.** How does Security Manager perform deployment?
- A.** Security Manager performs a three-step process when deploying your configurations to devices, as described in [Table 12-1](#).

Table 12-1 **Deployment Process**

Deployment Steps	
Step 1	<p>Security Manager obtains the current configuration for the device and compares it to the most recent saved policies for the device in Security Manager. What Security Manager considers the “current configuration” depends on the type of device, the deployment method, and the settings for deployment preferences. These are the possible sources of configurations and the conditions under which they are used:</p> <ul style="list-style-type: none"> • Obtain the running configuration from the device. <ul style="list-style-type: none"> – Used when deploying to the device <i>unless</i> the deployment method is AUS, TMS, or CNS. You can force Security Manager to use Configuration Archive by selecting Deploy to Device Reference Configuration: Config Archive as the deployment preference (select Tools > Security Manager Administration, then select Deployment). • Obtain the last full configuration from the Security Manager Configuration Archive. <ul style="list-style-type: none"> – Used when deploying to file, unless you select Deploy to File Reference Configuration: Device as the deployment preference. – Used when the deployment method is TMS or CNS. – Used when the device is not managed by Security Manager. – Used when you preview configurations. • Obtain the factory default configuration. <ul style="list-style-type: none"> – Used with PIX or ASA devices if you use the AUS deployment method. – Used when previewing PIX or ASA configurations if you use the AUS deployment method.

Table 12-1 *Deployment Process (continued)***Deployment Steps**

Step 2	Security Manager builds a delta configuration that contains the commands needed to update the device configuration to make it consistent with the assigned policies. It also builds a full device configuration.
Step 3	<p>If you are deploying to the device, Security Manager deploys either the delta configuration or the full configuration, depending on which deployment method you use. If you are deploying to a file, Security Manager creates two files: <i>device_name_delta.cfg</i> for the delta configuration, and <i>device_name_full.cfg</i> for the full configuration. In both cases, the configurations are also added to Configuration Archive. These are the actions based on deployment method:</p> <ul style="list-style-type: none"> • SSL or SSH—Security Manager contacts the device directly and sends the delta configuration to it. • Auto Update Server for PIX and ASA devices—Security Manager sends the full configuration to Auto Update Server, where the device retrieves it. The delta configuration is not sent. • Configuration Engine for IOS devices—Security Manager sends the delta configuration to Configuration Engine, where the device retrieves it. • TMS—Security Manager sends the delta configuration to the TMS server, from which it can be downloaded to an eToken to be loaded onto the device.

Q. Which deployment method should I use?

A. If you are using Configuration Engine (CNS) or Auto Update Server (AUS), use those deployment methods. You must use one of these for devices that use dynamic IP addresses. Otherwise, for devices with static IP addresses, use SSL for IOS, PIX, ASA, and standalone FWSM devices, and SSH for FWSM with Catalyst 6000 and 7600 router devices. If you are using the Token Management Server (TMS) for some devices, you can also use that method with Security Manager.

Q. How can I control the location used when I deploy to configuration files?

A. To set a default directory for file deployments, select **Tools > Security Manager Administration**, then select **Deployment**. If you select File for the default deployment method, you also select the default directory. When you create a deployment job, you can change this directory for that job. Note that the file location is in the Security Manager server not the Security Manager client PC.

Q. If I deploy to files, how does Security Manager know that I applied the configuration to the device?

A. Security Manager assumes that the previously deployed configuration was applied to the device no matter which deployment method you use. Later deployments include only the changes you made since the last deployment (the delta). If for some reason the last change was not applied to the device, the new delta configuration does not bring the device configuration up to the one reflected in Security Manager.

Q. What happens during configuration rollback?

A. When you roll back the configuration on a device, Security Manager redeploys either the last good configuration or the configuration that you selected from the Configuration Archive. In either case, after rollback, the configuration on the device is no longer consistent with the configuration in Security Manager. After rollback, you should rediscover policies on the device to make the device configuration and its configuration in Security Manager consistent. Rollback can be triggered from

either the deployment manager or the configuration archive. If it occurs from the deployment manager, it rolls back all devices in the job to their last good configuration. If it occurs from the configuration archive, it rolls back to the configuration you select.

- Q.** After configurations are deployed, which are completely owned by Security Manager, and which are only partially owned, and what does this mean?
- A.** When you manage devices that run the IPS, ASA, PIX, or FWSM operating systems, Security Manager controls their configurations; you should make all changes within Security Manager. For devices running IOS software, you have more control. If you do not create policies for a feature in Security Manager, such as routing policies, Security Manager does not control those features on the device. If you do create policies for these features, Security Manager overwrites the settings on the device with the settings you defined in Security Manager. Through administration settings, you can control the types of policies that are available for IOS devices, thereby preventing Security Manager from displaying or changing policies for these features. To see the available features for IOS routers and control whether they are available for management in Security Manager, select **Tools > Security Manager Administration**, then select **Policy Management**. For IOS devices, Security Manager does manage VPN-related policies.
- Q.** What happens if I make changes to a device configuration outside of Security Manager (an out-of-band change)?
- A.** During deployment, if Security Manager determines that the configuration on the device differs from the last deployed configuration, Security Manager overwrites the changes by default. You can control this behavior using the deployment preferences; select **Tools > Security Manager Administration**, then select **Deployment**, and look for the **When Out of Bound Changes Detected** setting. You can also control this for a specific deployment job by selecting **Edit Deployment Method** for the job.
- Q.** How can I get out-of-band changes into Security Manager?
- A.** If you make changes to the device configuration outside of Security Manager, you have two choices for bringing those changes into Security Manager:
- You can rediscover policies on the device, in which case all policies for the device become local policies, and any assignments of shared policies to the device are removed.
 - You can make the required changes in Security Manager and deploy them to the device.
- Q.** What happens during deployment if the version of the OS running on the device is not the same version listed for the device in Security Manager?
- A.** In some cases, Security Manager deploys the configuration and issues a warning, but in other cases, Security Manager cannot deploy the configuration. Security Manager deploys the configuration when:
- The device has a newer minor version, for example, PIX 6.3(4) instead of the 6.3(1), indicated in Security Manager.
 - Security Manager does not support the version running on the device. In this case, Security Manager builds the configuration using the CLI for the closest supported version.
 - The device has a down-level minor version, for example, 6.3(1) instead of 6.3(4).
- Security Manager does not deploy the configuration when the device is running a new major version of the OS (for example, PIX 7.0 instead of the 6.3 indicated in Security Manager) or if the device is running a down-level major version (6.3 instead of 7.0).

Table 12-2 lists the possible actions Security Manager takes depending on the whether the OS versions match or differ from each other.



Note The PIX Firewall is used as an example; however, the actions apply to all supported device types.

Table 12-2 Deployment Action Based on OS Version Match or Mismatch

Scenario	OS Version in Security Manager Database	OS Version On Device	OS Version Used In Deployment	Action
Versions match	pix 6.3 (1)	pix 6.3 (1)	pix 6.3 (1)	Deployment proceeds with no warnings.
Device has newer minor OS version.	pix 6.3 (1)	pix 6.3 (4)	pix 6.3 (4)	Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database. Security Manager generates CLI based on the OS version running on the device.
Device has newer minor OS version, which is not supported by Security Manager.	pix 6.3 (1)	pix 6.3 (6)	pix 6.3 (4)	Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database. Security Manager generates CLI based on the highest OS version that it supports.
Device has new major OS version.	pix 6.3 (1)	pix 7.0	pix 7.0	Security Manager reports an error indicating that it has detected a different OS version on the device than the one in the Security Manager database. Security Manager cannot proceed until you correct this mismatch. Remove the device from inventory and create a new device with the correct OS version.
Device has older OS version.	pix 6.3 (4)	pix 6.3 (1)	pix 6.3 (1)	If the older version is a different major version (6.0 vs. 7.0), Security Manager reports an error and aborts the deployment. If the older version is within the same major version (6.0 vs. 6.3), Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database, and it continues with the deployment.

- Q.** How do I fix a version mismatch problem?
- A.** You must delete the device, add it again, and discover policies again.

- Q.** Does Security Manager deploy full configurations or only the changes made since the last deployment (delta configurations)?
- A.** In most cases, Security Manager sends only delta configurations to the device. The only exception is if you are using Auto Update Server for PIX and ASA devices, in which case the full configuration is sent to the Auto Update Server.
- Q.** How many devices can Security Manager deploy to simultaneously or in a single job?
- A.** Security Manager can deploy to up to 20 devices simultaneously per job, up to 40 devices total. These restrictions enable Security Manager to use system memory efficiently, which ensures that jobs with many devices do not prevent jobs with fewer devices from deployment. There is no restriction to the number of jobs that Security Manager processes simultaneously. Although you can add as many devices to a deployment job as you desire (there is no limitation), as a practical matter, you should limit the number of devices per job. The deployment job might fail if you select a large number of devices or several devices that have large configuration files. If you encounter deployment failures, resubmit the job with fewer devices selected.
- Q.** Deployment to a Cisco IOS router fails and an “Error Writing to Server” or “Http Response Code 500” error message occurs. Why?
- A.** When you use SSL as the transport protocol for deploying configurations to a Cisco IOS router, the configuration is split into multiple configuration bulks. The size of this configuration bulk varies from platform to platform. If Security Manager tries to deploy a configuration bulk that exceeds the size of the SSL chunk configured on that device, the deployment fails and you get an “Error Writing to Server” or “Http Response Code 500” error message.

To resolve this, do the following:

1. On the Security Manager server, open the DCS.properties file in the \CSCOpx\MDC\athena\config folder in the installation directory (usually C:\Program Files).
 2. Locate **DCS.IOS.ssl.maxChunkSize=<value of the configuration bulk>**.
 3. Reduce the value of the configuration bulk.
 4. Restart the CiscoWorks Daemon Manager.
- Q.** Why does deployment to FWSM fail when the configuration contains a large number of ACLs?
- A.** This could occur because the CPU utilization is high during ACL compilation. To resolve this, reconfigure the CPU utilization threshold limit by doing the following:
1. On the Security Manager server, open the DCS.properties file in the \CSCOpx\MDC\athena\config folder in the installation directory (usually C:\Program Files).
 2. Locate the **DCS.FWSM.checkThreshold=False** property.
 3. Change the value to true: **DCS.FWSM.checkThreshold=True**.
 4. Restart the CiscoWorks Daemon Manager.
 5. Deploy the configuration to the device again.

After you set the value to true, discovery and deployment checks the CPU utilization and generates error messages if the CPU utilization is not within the configured value set in the DCS.FWSM.minThresholdLimit property. The default value is 85.

- Q.** Why does deployment fail even though the warning expression in the properties files is set to ignore the error?
- A.** Setting the properties file to ignore the error is not sufficient. Deployment fails because the Allow Download on Error check box (located on the **Tools > Security Manager Administration > Deployment** page) is deselected by default. To resolve this, select the Allow Download on Error check box and deploy again.

The following tables provide further details about how Security Manager behaves when an error occurs during deployment and the Allow Download on Error checkbox is either selected or deselected:

- [Table 12-3](#) describes the behavior when SSL transport protocol is used on PIX Firewall, ASA, and Cisco IOS routers.
- [Table 12-4](#) describes the behavior when SSH transport protocol is used on Cisco IOS routers.



Note On Cisco IOS routers with SSL protocol, deployment on devices stops on command syntax errors. It does not stop when configuration-related errors occur. There is no workaround for this.

Table 12-3 Security Manager Behavior When SSL is Used on PIX Firewall, ASA, and Cisco IOS Routers

Allow Download on Error	Error Occurred	Error Ignored Using Warning Expression	Deployment Status	Write Memory Done
Selected	Yes	No	Failed	Based on Write Memory flag setting.
Selected	Yes	Yes	Success	Based on Write Memory flag setting.
Selected	No	Not Applicable	Success	Based on Write Memory flag setting.
Deselected	Yes	No	Failed ¹	No
Deselected	Yes	Yes	Failed	No
Deselected	No	Not Applicable	Success	Based on Write Memory flag setting.

1. You get a “Deploy Not Completed” error message.

Table 12-4 Security Manager Behavior When SSH is Used on Cisco IOS Routers

Allow Download on Error	Error Occurred	Error Ignored Using Warning Expression	Deployment Status	Write Memory Done
Selected	Yes	No	Failed	Based on Write Memory flag setting.
Selected	Yes	Yes	Success	Based on Write Memory flag setting.
Selected	No	Not Applicable	Success	Based on Write Memory flag setting.
Deselected	Yes	No	Failed	No
Deselected	Yes	Yes	Success	Based on Write Memory flag setting.
Deselected	No	Not Applicable	Success	Based on Write Memory flag setting.

- Q.** Why do some platforms require a reload after performing configuration rollback but not others?
- A.** On PIX/ASA/FWSM devices, Security Manager uses the `replace config` option on the device's SSL interface to perform the equivalent of a reload (xlates are cleared, IPsec tunnels are torn down, and so on).

Routers running IOS 12.3(7)T or later use the **configure replace** command to replace the running config with the contents of a configuration file. Support for this command is dependent on the IOS version installed on the router:

- On routers running IOS 12.3(7)T or later, Security Manager copies the configuration file to the startup configuration before executing the **configure replace** command. If the `configure replace` operation fails, Security Manager issues the **reload** command to reload the operating system using the contents of the startup configuration. Please note that the **reload** command restarts the system, which might result in a temporary network outage.
 - On routers running a version prior to 12.3(7)T, Security Manager copies the configuration file to the startup configuration and issues the **reload** command.
- Q.** Why were no changes deployed to a device in a job created from a schedule even though preview configuration shows some changes?
 - A.** Schedules generate jobs automatically and deploy whatever changes, if any, were submitted for the devices selected in the schedule. If you made changes to a device, but did not submit the changes before the start of the scheduled job, those changes are not deployed. Ensure that you make timely submissions of your changes to ensure they are deployed when desired.

Changing How Security Manager Responds to Device Messages

Security Manager has built-in responses to many of the response messages that can be encountered when configuring a device. You might find that messages Security Manager treats as errors are messages that you want to ignore or treat as informational. Although you can configure your deployment jobs to ignore errors, you might instead want to update Security Manager to treat specific messages differently.

To change how Security Manager treats a message, you need to update the `DCS.properties` file in `\CSCOPx\MDC\athena\config` folder in the installation directory (usually `c:\Program Files`). Use a text editor such as NotePad to update the file.

It is easiest to determine the message you want to ignore by looking at the transcript of a deployment job that encountered the error using these steps:

-
- Step 1** Select the job with the error message from the Deployment Manager window.
 - Step 2** Click the **Transcript** button in the Deployment Details tab to open the transcript.
 - Step 3** Identify the error text that you want to ignore.
 - Step 4** Locate the appropriate warning expressions property in the `DCS.properties` file. For example, for PIX devices the property is called **dev.pix.warningExpressions**, whereas for IOS devices the property is called **dev.ios.warningExpressions**.

**Tip**

Conversely, you can make device responses that are not tagged with the Error prefix to appear as error messages. To do this, add the message to the Error Expressions list (for example, `dev.pix.ErrorExpressions`).

Step 5 Add the error text to the warning expressions list. The warning message should be a generic regular expression string. Except for the last expression, you must delimit all expressions with “\$”. For example, if the message you want to ignore is “Enter a public key as a hexadecimal number,” enter the following string:

```
.*Enter a public key as a hexadecimal number .*$
```

Step 6 Restart the CiscoWorks Daemon Manager.

Performing Rollback When Deploying to a File

You cannot perform rollback when deploying to a file instead of a device. To revert to a previously stored configuration, do the following:

Step 1 Select **Tools > Configuration Archive**.

Step 2 In the Configuration Archive window, select a device, then select the configuration to which you want to revert.

Step 3 Click **View**.

Step 4 In the Configuration Version Viewer window, make sure the Config Type is set to Full.

Step 5 Click in the left-hand pane, then press **Ctrl-A** followed by **Ctrl-C** to copy the selected configuration to the Windows clipboard.

Step 6 Open a text editor, then press **Ctrl-V** to paste the contents of the clipboard.

Step 7 Save the file. You can then use this file to perform manual rollback.

Mixing Deployment Methods

Problem You receive unpredictable results when you deploy router platform and VPN policies to a live device after previously deploying to a configuration file.

Solution This problem can occur when you use a mix of deployment methods (deploy to device and deploy to file) with router platform policies and VPN policies. Because Security Manager does not manage all the available CLI commands for these policy types, it maintains a snapshot of the commands it has configured and leaves all other commands (which includes unsupported commands as well as supported commands in policies that have not been configured in Security Manager) intact on the device.

After each deployment, Security Manager creates a snapshot of the policies that were deployed to each device. This snapshot is used during the next deployment to generate the list of configuration changes that will be deployed to the device. Only one snapshot is maintained at a time per device.

Mixing deployment methods with router platform policies and VPN policies can lead to unpredictable results, as shown in this example:

1. Configure router platform policy A to a live device. When deployment completes, Security Manager creates a snapshot for that device with policy A.
2. Next, configure policy B to replace policy A, but instead of deploying policy B to the device, deploy it to a file instead. When this deployment completes, Security Manager creates a snapshot with policy B that replaces the previous snapshot with policy A. However, because you did not deploy policy B to the device, the CLI commands that are required to negate policy A have not been deployed. Policy A is still deployed on the device.
3. Deploy again to the device without first copying the changes in the configuration file to the device. Security Manager cannot generate the commands that are required to negate policy A from the device because the snapshot with policy A no longer exists.

Because policy A is a router platform policy, any of the following results might occur:

- The policy in the latest deployment overrides policy A.
- Both policies end up defined on the device.
- Deployment fails because the two policies cannot coexist.

Therefore, if you deploy to a file when working on a live device, we strongly recommend that you copy your configuration changes from the file to the device before performing additional deployments to the device.

SSL Handshake Failure When Deploying to PIX/ASA Devices

Problem You receive SSL handshake failures when deploying to PIX or ASA devices.

Solution Examine the device's running configuration to verify that the device is using 3DES/AES encryption, not DES. VPN-DES encryption is not supported on Common Services 3.0 and later. If the device is using DES encryption, install a VPN-3DES-AED license and retry deployment.

Deployment Failures to Devices Managed by AUS

Problem Deployment fails when deploying to multiple AUS-managed devices after starting the AUS.

Solution This problem can occur if you perform deployment before the Auto Update Server (AUS) is fully operational. The AUS requires time to start up after the following operations:

- New installation or upgrade.
- Manual restart (including after a power outage).
- Manual restart of the Cisco Security Manager Daemon Manager service.

You can verify whether the AUS is fully operational by verifying the status of its Windows services. To do this, select **Start > Control Panel > Administrative Services > Services**, then check the status of the CiscoWorks AUS Database Engine service. If this service has started, try again to deploy.

Deployment Failures to FWSM Virtual Contexts After Changing Interface Policies

Problem You add an FWSM with virtual contexts and discover its policies. The configuration includes interface aliases (the **allocate interface** command). After changing the interfaces policy for a context, deployment fails.

Solution Connect directly to the FWSM and remove all mapped interface names from the system execution space configuration and in all other contexts, replace interface references to mapped names with the VLAN ID of the interface. You can then delete the FWSM from the Security Manager inventory and rediscover it.



CHAPTER 13

Interoperation of CS-MARS and Security Manager

This chapter contains the following topics:

- [FAQs about Policy Lookup from a CS-MARS Event](#), page 13-1
- [Policy Lookup for Events Generated by Devices with Multiple Contexts](#), page 13-12
- [FAQs about CS-MARS Events Lookup from a Security Manager Policy](#), page 13-13
- [Changing the Association of the CS-MARS Appliance with a Device](#), page 13-19
- [Configuring Required Browser Settings for Policy and Events Lookup](#), page 13-19



Note

For more detailed information on the interoperation of CS-MARS and Security Manager, see the “MARS Events Lookup from a Security Manager Policy” section in the [installation guide for Cisco Security Manager](#) for your release.

FAQs about Policy Lookup from a CS-MARS Event

This section answers the following questions about Security Manager policy lookup from CS-MARS events:

- [Q. Why do I get an error message when I click the Security Manager icon for a connection-teardown event in CS-MARS?](#)
- [Q. Why am I asked to select a different event, when I click the Security Manager icon for an event?](#)
- [Q. Why is an error message displayed stating that the syslog is invalid even when I click the Security Manager icon for one of the syslogs supported for policy lookup?](#)
- [Q. During policy lookup, I receive an “An internal error has occurred” message. Why?](#)
- [Q. What are the possible causes for not finding a matching access rule during policy lookup from an event?](#)
- [Q. I get an error stating that the access rule on the device is not synchronized with the one in Security Manager during policy lookup. Why?](#)
- [Q. Why does an error message appear stating that an implicit permit statement in the access rule generated the selected event when I perform lookup?](#)
- [Q. Why am I seeing a discrepancy in the access rule that is shown as matched in the read-only policy query page of CS-MARS and the Access Rules page in Security Manager?](#)

- Q. Can I look up the signature matching an event generated by a virtual sensor?
- Q. Why am I not seeing the Security Manager icon for Packet Data and Context Data events, although they are events reported by Cisco IDS 4.x and Cisco IPS 5.x devices?
- Q. What are the various ways in which I can navigate to a page in CS-MARS in which the Security Manager icon is displayed?
- Q. When and why is the multiple events window displayed during access rule lookup?
- Q. Why is the multiple devices window displayed during policy lookup?
- Q. Why is the Save Credentials check box in the read-only policy query window disabled?
- Q. Can I start Security Manager from the read-only policy query window without having the client installed on my system?
- Q. If I did not have a Security Manager client instance open at the time of policy lookup, is it terminated when I log out of the CS-MARS session?
- Q. What are the different authentication mechanisms for policy lookup?
- Q. Why do I get an error stating that the device is not found in Security Manager?
- Q. Why is the access rule table displayed after lookup in the read-only policy query window different from the one configured in Security Manager?
- Q. Can I test the connectivity between CS-MARS and Security Manager before running a policy lookup query?
- Q. Can I add a Security Manager running 3.0.1, 3.0.2, or 3.1.x to a CS-MARS appliance running 4.3.4 or 5.3.4?
- Q. Under what circumstances are the Security Manager credentials in the User Management page enabled or disabled?
- Q. Is it always necessary to configure the CS-MARS user account in the Security Manager database to perform policy lookup?
- Q. Why is a new Security Manager client instance opened even though a session is currently active?
- Q. Why is the password automatically populated in the login section of the read-only policy query window after I enter the user name?
- Q. What are the device types and their operating-system versions that are supported for policy lookup?
- Q. What is the scope of the search on the Access Rules page or Signatures page of Security Manager when a policy lookup query is run?
- Q. How is policy lookup performed if Workflow mode is enabled in Security Manager?
- Q. How is policy lookup performed if non-Workflow mode is enabled in Security Manager?
- Q. Can I perform any other task from the read-only policy query page for a signature-fired event, besides tuning of signatures?
- Q. Can I check whether Workflow mode is enabled or not and details of the activity from which the read-only policy table is retrieved?
- Q. What are the supported CS-MARS user roles to modify the Security Manager credentials in the User Management page of CS-MARS?
- Q. Do I need to possess administrative privileges to add a Security Manager to CS-MARS?
- Q. Is the Security Manager icon displayed only for events that have 5-tuple data?

- Q. Why do I receive an error stating that I do not have necessary privileges to start the Security Manager client from the read-only policy query window?
 - Q. What are the ACS, Common Services, and CS-MARS roles that are supported to start the Security Manager client from the read-only policy query window?
 - Q. What are the types of CS-MARS events for which the Security Manager icon is displayed?
 - Q. Why does policy lookup take a long time for certain events?
 - Q. Can I view the contents of objects contained in the matching access rules from the read-only policy query popup window?
 - Q. I see the Security Manager icon for “Unknown Device Event Type” events. What do these events represent?
 - Q. Are the Security Manager login credentials that I enter in the read-only policy query popup window cached until the current session is active?
 - Q. When I perform policy lookup for an event for the second time, it is faster than the previous occasion. What could be the reason for this behavior?
 - Q. During policy lookup, I get an error stating that a temporary connection problem occurred. How can I correct this problem?
 - Q. Why am I prompted for credentials to log in to Security Manager, even though I selected the option to use CS-MARS credentials for policy lookup?
 - Q. Why is an error message displayed when I try to Start Security Manager from the read-only policy window for the matching rule or signature?
 - Q. What are the system message log IDs supported for policy lookup for events generated by security appliances and routers?
 - Q. How many Security Manager servers can I add to a CS-MARS Local Controller to perform policy lookup?
 - Q. My CS-MARS Local Controller is administered by a Global Controller. Can I perform policy lookup for events generated on the Local Controller from the Global Controller interface?
 - Q. There are two places in which I need to enter the Security Manager user name and password. What is the difference between the credentials in the Reporting Applications tab and the one in the User Management page of CS-MARS?
- Q.** Why do I get an error message when I click the Security Manager icon for a connection-teardown event in CS-MARS?
- A.** If an event is generated by a connection teardown syslog and the setup and teardown of the connection occur in two different sessions (with a gap of 2 minutes in-between), the corresponding connection establishment syslog is not sent by CS-MARS to Security Manager when you perform policy lookup for such events. As a result, an error message is displayed stating that the connection setup syslog is not available to display the matching rules for that event. An identical error message is also displayed if you attempt to query access rules for a connection teardown event from the realtime event viewer of CS-MARS.
- Q.** Why am I asked to select a different event, when I click the Security Manager icon for an event?
- A.** When you click the Security Manager icon for an event that contains a syslog ID that is not supported for policy lookup, you are prompted to select another supported event. Although the Security Manager icon is displayed in CS-MARS, only for those events that support policy lookup, you might see this error message while looking up policies for events generated by management traffic or connection teardown syslogs without a corresponding setup syslog.



Note For more information on the list of syslogs supported for policy lookup, see “Security Appliance and Router System Log Messages Supported for Policy Lookup” in the *User Guide for Cisco Security Manager*.

- Q.** Why is an error message displayed stating that the syslog is invalid even when I click the Security Manager icon for one of the syslogs supported for policy lookup?
- A.** This problem occurs if the syslog is not parsed by Security Manager and the syslog format received from CS-MARS is incorrect. In such cases, you need to select a different syslog and perform policy lookup.
- Q.** During policy lookup, I receive an “An internal error has occurred” message. Why?
- A.** When you run a query for realtime or historical events and try to perform policy lookup from an incident in the query results, occasionally, an error message is displayed in the Policy Query popup window stating that an internal error has occurred. This error is temporary and disappears if you retry this operation after a while. You are prompted to log in again to Security Manager, and policy lookup should be successful from then on. An error of this type also occurs when RPC connection fails or when policy changes to the device are not submitted to the Security Manager server.
- Q.** What are the possible causes for not finding a matching access rule during policy lookup from an event?
- A.** An access rule matching the selected event might not be found in any of the following cases:
- If no access rule is configured on the lower security interface in the “in” direction of the device for inbound traffic for the selected event.
 - If the access rule specified in the syslog is not available on the device. Make sure that the device is added to Security Manager and access rules are configured on it.
 - If the event is generated by outbound traffic setup/teardown syslog with an access rule configured on the higher security interface in the “in” direction.
 - The interface name logged in the syslog event might not match the interface name in that policy in Security Manager. (Interface names are not case-sensitive in Security Manager, but they are in CS-MARS. Further, syslog messages use lowercase for all interface names. To avoid this problem, use lower case for all interface names, and in the definition of interface roles, in CS-MARS.)
 - If a firewall device is added to Security Manager and the changes are not submitted to the database at the time of performing policy lookup from CS-MARS.
- Q.** I get an error stating that the access rule on the device is not synchronized with the one in Security Manager during policy lookup. Why?
- A.** This error can occur under any of the following circumstances:
- When an event is generated by an access rule present on the lower security interface in the “in” direction for inbound traffic and no matching rule is found in Security Manager.
 - When an event is generated by an access rule present on the higher security interface in the “in” direction for outbound traffic and no matching rule is found in Security Manager.
 - When an event is generated by an access rule present on the lower security interface in the “out” direction for outbound traffic and no matching rule is found in Security Manager.

- If the device for which you perform access rule lookup has been added to Security Manager without submitting the configuration to the database or if the access rule that generated the syslog is not available on the device.
- Q.** Why does an error message appear stating that an implicit permit statement in the access rule generated the selected event when I perform lookup?
- A.** This error occurs because you performed lookup for an event generated by outbound traffic setup/teardown syslog with an access rule configured on the higher security interface in the “in” direction. Also, this error message occurs if a firewall device is added to Security Manager and the changes are not submitted to the database at the time of performing policy lookup from CS-MARS.
- Q.** Why am I seeing a discrepancy in the access rule that is shown as matched in the read-only policy query page of CS-MARS and the Access Rules page in Security Manager?
- A.** If you modify the access rule in Security Manager after the read-only policy query window is displayed with highlighted rules that generated the event and start the Security Manager client, the rule table in the read-only policy page is used as the basis for displaying the matched rule in Security Manager and the modified rule table in Security Manager is not considered. For example, if the first row in the read-only policy query window is shown as highlighted and is TCP-based, and you change the order of the rules in the Access Rules page of Security Manager to move an ICMP-based rule to the top of the table, the ICMP-based rule (not the TCP-based rule) is highlighted when you start the Security Manager client from CS-MARS.
- Q.** Can I look up the signature matching an event generated by a virtual sensor?
- A.** No. Signature policy lookup is not supported for virtual sensors because the sensor ID is not contained in the raw syslog message that is logged in CS-MARS to enable Security Manager to perform a lookup.
- Q.** Why am I not seeing the Security Manager icon for Packet Data and Context Data events, although they are events reported by Cisco IDS 4.x and Cisco IPS 5.x devices?
- A.** Packet Data events that identify the data that was being transmitted on the network the instant an alarm was detected on IPS and IDS sensors can cause the size of the raw message associated with this event to become very huge. Also, these events are not triggered by signature rules on sensors. As a result, the Security Manager icon is not displayed for Packet Data and Context Data events in CS-MARS for policy lookup.
- Q.** What are the various ways in which I can navigate to a page in CS-MARS in which the Security Manager icon is displayed?
- A.** You can perform policy lookup in any one of the following ways in CS-MARS:
- From the Query Reports page, run a query with one of the following result formats: All Matching Events, All Matching Event Raw Messages, All Matching Sessions, or All Matching Sessions, Custom Columns (when Reporting Device Set is selected as one of the custom columns).
 - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
 - From the Recent Incidents section of the Dashboard, click the link in the Incident ID column.
 - Click the Incidents tab to navigate to the Incidents page, which displays recent incidents, and click the link in the Incident ID column.
 - Search for the Incident ID by entering the ID in the appropriate field and clicking Show.

- Q.** When and why is the multiple events window displayed during access rule lookup?
- A.** This window appears when you run a query for events with All Matching Sessions, or All Matching Sessions, Custom Columns as the result format and if there are two or more events in a session. From the multiple events window, click the Security Manager icon for the event that you want to examine to display the read-only policy query popup window.
- Q.** Why is the multiple devices window displayed during policy lookup?
- A.** Although CS-MARS tries to identify a unique device by matching the host name, domain name, and reporting IP address of the device that generated the event against the corresponding details in Security Manager, the multiple devices window is displayed when there are two or more devices that match the device lookup process between CS-MARS and Security Manager. From the multiple devices window, you can select the device for which you want to view and modify the configured access rules.
- Q.** Why is the Save Credentials check box in the read-only policy query window disabled?
- A.** This check box is available only if the Allow Users to Save Credentials check box is selected in the Device Discovery-Cisco Security Manager ANY page. Selecting the Save Credentials check box causes the Security Manager credentials to be saved in the CS-MARS database and you are not prompted for access details during subsequent lookups. Otherwise, you are prompted to enter the login details each time you start the Security Manager policy table from CS-MARS in a new session or after the timeout period.
- Q.** Can I start Security Manager from the read-only policy query window without having the client installed on my system?
- A.** Yes. If the Security Manager client is not installed on the system from which you are accessing the CS-MARS Web interface, you are prompted to install the Security Manager client during policy lookup and the page to download the client software is opened.
- Q.** If I did not have a Security Manager client instance open at the time of policy lookup, is it terminated when I log out of the CS-MARS session?
- A.** If a Security Manager client session is not open at the time you perform policy lookup, you are not logged out from the Security Manager instance (opened for the purpose of policy lookup) when the idle timeout period is exceeded or when you log out of the CS-MARS session. The Security Manager session closes only when you log out from it or when the idle timeout configured for it is exceeded.
- Q.** What are the different authentication mechanisms for policy lookup?
- A.** You can enable CS-MARS to either contact Security Manager using the credentials that you entered while logging in to CS-MARS or use Security Manager credentials for CS-MARS to authenticate with Security Manager during policy lookup. You can configure these settings under the Cross-Launch Authentication Settings section in the Reporting Applications tab of CS-MARS. See “Adding a Security Manager Server to CS-MARS” in the *User Guide for Cisco Security Manager* for details.
- Q.** Why do I get an error stating that the device is not found in Security Manager?
- A.** If you perform the policy table lookup for a device added to CS-MARS only and not to Security Manager, an error message is displayed in the read-only policy table window. Make sure that you add the device to Security Manager and discover the policies so that the configuration on the device is synchronized with Security Manager.

- Q.** Why is the access rule table displayed after lookup in the read-only policy query window different from the one configured in Security Manager?
- A.** This problem occurs because CS-MARS displays the Security Manager security policy committed views, not the deployed views. If you change the access rule in Security Manager and do not deploy the changes to the device, the syslog is generated by the older access rule on the device because the changes are not synchronized and policy lookup is performed on the access rule saved on the device and not on the most recently saved changes in Security Manager.
- Q.** Can I test the connectivity between CS-MARS and Security Manager before running a policy lookup query?
- A.** Yes, you can test the connectivity between CS-MARS and Security Manager any time before policy lookup, either during the process of adding Security Manager to CS-MARS or after addition. To do this task, navigate to the Device Discovery-Cisco Security Manager ANY page, then click **Test Connectivity** to verify that the settings are correct and that the CS-MARS Appliance can communicate with this Security Manager server.
- Q.** Can I add a Security Manager running 3.0.1, 3.0.2, or 3.1.x to a CS-MARS appliance running 4.3.4 or 5.3.4?
- A.** Although you can add a Security Manager server running 3.0.1, 3.0.2, or 3.1.x to a CS-MARS appliance running 4.3.2 through 4.3.4 or 5.3.2 through 5.3.4, you can query for policies in view mode only; you must open a Security Manager client instance separately to modify the policies.
- Adding a Security Manager server running 3.0.1, 3.0.2, or 3.1.x to a CS-MARS appliance provides the same behavior that existed in versions of CS-MARS earlier than 4.3.4 and 5.3.4 to perform policy lookup. Make sure that the Security Manager server is running the version 3.2 or later if you want to lookup the policy table and also modify matching rules or signatures.
- Q.** Under what circumstances are the Security Manager credentials in the User Management page enabled or disabled?
- A.** If you selected the option to use the Security Manager login credentials for CS-MARS to authenticate with Security Manager and chose to allow the login credentials to be saved in the login dialog box, the user name and password fields under the Cisco Security Manager section of the User Configuration Page are activated and can be edited by CS-MARS users with Admin or Security Analyst roles.
- If you selected the option to be prompted for Security Manager login credentials to authenticate CS-MARS during policy table lookup and deleted the Security Manager server from the CS-MARS database, the user name and password fields under the Cisco Security Manager section of the User Configuration Page (Management > User Management tab > Add) in CS-MARS are unavailable. These fields are also unavailable if you chose not to allow saving of Security Manager login credentials when CS-MARS authenticates with Security Manager.
- Q.** Is it always necessary to configure the CS-MARS user account in the Security Manager database to perform policy lookup?
- A.** When you add a Security Manager server to CS-MARS, if you choose to use the option to prompt users for Security Manager credentials for the policy table lookup, you do not need to create a separate CS-MARS user account in Common Services for authentication purposes.
- Q.** Why is a new Security Manager client instance opened even though a session is currently active?
- A.** This behavior occurs if you logged in to Security Manager using a user account that is different from the one that is being used to start Security Manager from CS-MARS for the policy table lookup and you selected the option to use Security Manager credentials.

- Q.** Why is the password automatically populated in the login section of the read-only policy query window after I enter the user name?
- A.** If you access CS-MARS using Internet Explorer, it is possible that the password is automatically entered in the login dialog box after you enter the user name. This behavior occurs if you configured your browser to remember passwords. See [Working with Cached Passwords in Internet Explorer, page 13-20](#) for information on how cached passwords can be cleared or the caching feature can be disabled.
- Q.** What are the device types and their operating-system versions that are supported for policy lookup?
- A.** You must ensure that devices that need to be monitored by CS-MARS and managed by Security Manager are running a software versions supported by both CS-MARS and Security Manager to perform the policy table lookup from CS-MARS syslogs and events lookup from Security Manager policies. See “Devices and OS Versions Supported by Both Security Manager and CS-MARS” in the *User Guide for Cisco Security Manager*.
- Q.** What is the scope of the search on the Access Rules page or Signatures page of Security Manager when a policy lookup query is run?
- A.** The policy table lookup query is done in one of the following three ways, depending on whether Workflow or non-Workflow mode is enabled and Security Manager client is running or not.
- If an instance of the Security Manager client is not running and either Workflow or non-Workflow mode is enabled in Security Manager, the lookup query is performed on the policies committed to the Security Manager database.
 - If Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies within the context of the current activity (in an editable state, namely, Edit, Edit Open, Submit, or Submit Open) as well as references found in data committed to the Security Manager database.
 - If non-Workflow mode is enabled and a Security Manager client session is open, the lookup operation is performed on all policies in the current login session (within the context of the automatically created activity in non-Workflow mode).
- Q.** How is policy lookup performed if Workflow mode is enabled in Security Manager?
- A.** If Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies within the context of the current activity (in an editable state, namely, Edit, Edit Open, Submit, or Submit Open) as well as references found in the data committed to the Security Manager database.
- Q.** How is policy lookup performed if non-Workflow mode is enabled in Security Manager?
- A.** If non-Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies in the current login session.
- Q.** Can I perform any other task from the read-only policy query page for a signature-fired event, besides tuning of signatures?
- A.** Yes, you can also configure an event action filter to remove one or more actions from the read-only policy query window for a signature event.

- Q.** Can I check whether Workflow mode is enabled or not and details of the activity from which the read-only policy table is retrieved?
- A.** Yes, click the **CS Manager Details** link at the bottom of the Policy Query window to open a dialog box displaying the server name, user name used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved.
- Q.** What are the supported CS-MARS user roles to modify the Security Manager credentials in the User Management page of CS-MARS?
- A.** All users associated with any of the CS-MARS roles, with the exception of the Operator and Notifications Only roles, can modify the Security Manager authentication credentials while editing an existing user account in CS-MARS.
- Q.** Do I need to possess administrative privileges to add a Security Manager to CS-MARS?
- A.** Yes. While adding a Security Manager to CS-MARS, only users with Admin role can be configured to enable CS-MARS contact and discover Security Manager server configuration. Otherwise, an error message is displayed when you submit your changes.
- Q.** Is the Security Manager icon displayed only for events that have 5-tuple data?
- A.** No. The Security Manager policy table lookup icon in CS-MARS is displayed for access rules from a PIX firewall, ASA device, IOS router, or an FWSM blade, regardless of whether the 5-tuple information is available or not. If the 5-tuple data cannot be derived from the syslog, the most accurate match is displayed after policy table lookup.
- Q.** Why do I receive an error stating that I do not have necessary privileges to start the Security Manager client from the read-only policy query window?
- A.** If you used CS-MARS user credentials to perform policy lookup, you might be associated with the Operator or Notifications Only role, which enable to only view matching policies. If you used Security Manager credentials to perform policy lookup, you might be associated with the Help Desk role in CiscoWorks Common Services role or Cisco Secure ACS, which do not enable you to start Security Manager to modify a policy from the read-only popup window in CS-MARS.
- Q.** What are the ACS, Common Services, and CS-MARS roles that are supported to start the Security Manager client from the read-only policy query window?
- A.** The following are the user roles supported to perform policy lookup and modify the matching policy, depending on the authentication server that you are using:
- ACS user roles—Any predefined Cisco Secure ACS roles with the exception of the Help Desk role.
 - Common Services user roles—Approver, Network Operator, Network Administrator, or System Administrator.
 - CS-MARS user roles—Administrator or Security Analyst.
- Q.** What are the types of CS-MARS events for which the Security Manager icon is displayed?
- A.** The Security Manager policy table lookup icon in CS-MARS is displayed only for traffic logs triggered by the following event types:
- Access rules from a PIX Firewall, ASA device, IOS router, or an FWSM blade, regardless of whether the 5-tuple information is available or not. If the 5-tuple data cannot be derived from the syslog, the most accurate match is displayed after policy table lookup.

- Connection establishment and tear-down using TCP, UDP, and ICMP on PIX, ASA, and FWSM devices.
 - Signatures from IPS and IOS IPS devices.
- Q.** Why does policy lookup take a long time for certain events?
- A.** The time taken to display the policy table lookup query results is proportional to the number of rules in the policy table of Security Manager. Increased number of rules might impact the performance of CS-MARS and Security Manager. Also, if a new instance of the Security Manager client is started during policy table lookup, the time taken to display the matching rules might be slightly greater than the time consumed when a Security Manager client session is active.
- Q.** Can I view the contents of objects contained in the matching access rules from the read-only policy query popup window?
- A.** Yes. If an access rule contains network/host, interface, or service objects, you can click the object in the read-only policy lookup table to view the definitions of these objects in a popup window. The contents of the objects that match with the values in the syslog that generated the rule are highlighted. However, expanded object entries are highlighted only for TCP and UDP protocol in service objects, destination object names, and source object names. The Source, Destination, Service, and Interface cells are not clickable if they do not contain objects.
- Q.** I see the Security Manager icon for “Unknown Device Event Type” events. What do these events represent?
- A.** Events triggered by custom signature configured on a sensor are categorized as “Unknown Device Event Type” in CS-MARS and the Security Manager icon is displayed for these events to enable policy lookup.
- Q.** Are the Security Manager login credentials that I enter in the read-only policy query popup window cached until the current session is active?
- A.** Yes. Login credentials are cached by CS-MARS when you successfully log in to Security Manager. These credentials are discarded when you exit CS-MARS or the idle session timeout period is exceeded.
- Q.** When I perform policy lookup for an event for the second time, it is faster than the previous occasion. What could be the reason for this behavior?
- A.** The policy rules retrieved from the Security Manager policy table and displayed in the read-only policy query window in CS-MARS are cached to enhance performance. Caching reduces the time taken to display query results on subsequent lookups as the query results are reused when a request is made to query policies for the same event.
- Q.** During policy lookup, I get an error stating that a temporary connection problem occurred. How can I correct this problem?
- A.** This error can occur if the connection between CS-MARS and Security Manager is aborted temporarily and necessary details are not supplied by CS-MARS and Security Manager. In such cases, retry the operation after some time.

You can also navigate to the Device Discovery-Cisco Security Manager ANY page, then click **Test Connectivity** to verify that the settings are correct and that the CS-MARS Appliance can communicate with this Security Manager server. If the user name and password are correct and the CS-MARS Appliance is configured as an administrative host for the device, a popup window

appears with a “Connectivity successful.” message when the discovery operation is successfully completed. Otherwise, an error message appears asking you to click the View Error link for more information about the probable cause and its possible solution.

- Q.** Why am I prompted for credentials to log in to Security Manager, even though I selected the option to use CS-MARS credentials for policy lookup?
- A.** This occurs because you logged in to CS-MARS using an account that is not defined in the Common Services database of Security Manager. You must define the CS-MARS user account on the Security Manager server (the Local User Setup page in the Common Services) with a role other than Help Desk to navigate successfully to the Security Manager policy table without being prompted for credentials.
- Q.** Why is an error message displayed when I try to Start Security Manager from the read-only policy window for the matching rule or signature?
- A.** This problem can occur in any one of the following scenarios:
- You did not configure the Security Manager server to use HTTPS for communication with CS-MARS. Before CS-MARS can query the policies defined on the Security Manager server, you must enable HTTPS on the Security Manager server. Because Security Manager runs on Common Services, you must enable browser-security from Common Services to establish secure communication between Security Manager and CS-MARS. For more information on enabling HTTPS using Common Services, see *User Guide for CiscoWorks Common Services*.
 - If the Daemon Manager on the Security Manager server is not running, an error message is displayed prompting you to restart the service when you try to start the client.
 - If a modal window or dialog box is open in Security Manager or the modal window is overlaid with any other application window, an error message is displayed when the policy lookup query is performed. Close the modal dialog box in Security Manager and retry the task.
- Q.** What are the system message log IDs supported for policy lookup for events generated by security appliances and routers?
- A.** The following syslog message IDs are supported for looking up policies in Security Manager from incidents generated in CS-MARS. If you change the logging level of the firewall, ensure that the following messages IDs are generated at the new level so the CS-MARS Appliance receives them.
106100, 106023, 302013, 302014, 302015, 302016, 302020, 302021
- For IOS routers, system log messages with the following identifiers support policy lookup and the Security Manager icon is displayed beside them in CS-MARS:
- `%SEC-6-IPACCESSLOGDP, %SEC-6-IPACCESSLOGNP, %SEC-6-IPACCESSLOGS,
%SEC-6-IPACCESSLOGP`
- Q.** How many Security Manager servers can I add to a CS-MARS Local Controller to perform policy lookup?
- A.** A Local Controller can be configured to retrieve the policy tables from only one Security Manager server at a time. An error message is displayed when you attempt to add more than Security Manager server to a Local Controller.

- Q.** My CS-MARS Local Controller is administered by a Global Controller. Can I perform policy lookup for events generated on the Local Controller from the Global Controller interface?
- A.** No. If you add a Local Controller, to which Security Manager server has been added, to a Global Controller, you can view the Security Manager server in the Security and Monitoring Information list of the Local Controller from the Global Controller interface. However, the Security Manager policy query icon is not displayed beside events or incidents displayed on a Global Controller.
- Q.** There are two places in which I need to enter the Security Manager user name and password. What is the difference between the credentials in the Reporting Applications tab and the one in the User Management page of CS-MARS?
- A.** The Security Manager user name and password values that you enter or modify in the Reporting Applications tab is used by CS-MARS to communicate with Security Manager server and discover meta information, such as version of software running on the server and configuration details. These credentials are different from the user name and password in the Cisco Security Manager section of the User Configuration page.

The user name and password pair in the User Configuration page comprise the credentials that CS-MARS uses to authenticate with Security Manager to look up the policy table, when you select the option to use Security Manager credentials for policy lookup. The Security Manager user name and password fields in the User Configuration page are populated with the values you enter in the policy query login dialog box if you chose to allow saving of Security Manager login credentials during policy lookup.

Policy Lookup for Events Generated by Devices with Multiple Contexts

Problem Policy lookup fails when you click the Security Manager icon for an event generated by access rules or connection establishment/teardown on devices with multiple contexts.

Solution When you add FWSM and ASA devices with multiple security contexts to Security Manager, the context name is set as the host name in the Device Properties page and policy lookup from CS-MARS events for these contexts works properly. If the host name is not the same as the context name, policy lookup from events fails. In such cases, make sure that the host name defined for that context in the Device Name field in CS-MARS matches with the host name configured in the Device Properties page of Security Manager for policy lookup to work correctly.

Problem Security Manager icon is not displayed in the Reporting Device column for events generated by devices in multiple context mode.

Solution For PIX and ASA devices or FWSM blades with multiple security contexts, you must enter the reporting IP address for each context while configuring the device in CS-MARS. Otherwise, the Security Manager icon is not displayed beside events received from the contexts for which the reporting IP address is not defined in CS-MARS. You can query events from such contexts only by running a query for “Unknown Reporting Devices” from CS-MARS.

FAQs about CS-MARS Events Lookup from a Security Manager Policy

This section answers the following questions about looking up CS-MARS events from Security Manager policies:

- Q. What are the versions of CS-MARS and Security Manager that are supported for events lookup from policies?
- Q. Can I add multiple CS-MARS appliances to a Security Manager server?
- Q. What are the benefits of querying for CS-MARS events from policies?
- Q. Is there any limit to the number of keywords that are populated in the Query page of CS-MARS when I perform events lookup from an access rule that supports hashcodes?
- Q. Am I returned to the Query Criteria page or the Query Results page on successful lookup of events from a policy?
- Q. Why does event lookup fail from policies generated by FWSM, PIX, and ASA devices in which multiple security contexts exist?
- Q. Why do I get a “Policy not found” error message when I query for CS-MARS events from the default signature policy?
- Q. If my CS-MARS session is active, the events query criteria or results are displayed in the existing CS-MARS browser window, making me lose the data I was viewing in CS-MARS. Is this behavior changeable?
- Q. Why do I get the Security Alert dialog box when I perform events lookup?
- Q. Can I perform events lookup from a signature that is disabled for a sensor?
- Q. Why do I receive a warning message when I try to look up events matching an access rule?
- Q. Is it possible to view events for access rules for which logging is not enabled?
- Q. Is there any difference in the types of syslogs that are displayed for events matching a flow and events matching a rule?
- Q. What is the difference between the CS-MARS user credentials entered in the New/Edit CS-MARS dialog box and in the login dialog box during events lookup?
- Q. Is it possible to query for events generated by a signature configured on a virtual sensor?
- Q. What are the different authentication mechanisms for events lookup?
- Q. Why is the check box to save credentials for subsequent event lookups disabled in the Login to CS-MARS dialog box?
- Q. Is it always necessary to configure the Security Manager user account in the CS-MARS database to perform events lookup?
- Q. Are the CS-MARS login credentials that I enter in the Login to CS-MARS dialog box cached until the current Security Manager session is active?
- Q. Can I test the connectivity between CS-MARS and Security Manager before querying for events?
- Q. How does the absence of hashcodes in ACEs on devices that do not support them affect the accuracy of event matches for a policy?
- Q. Can I query events for more than one access rule or signature at the same time?
- Q. Why do I see no events when I perform a lookup from an access rule for which object grouping or rule optimization is enabled?

- **Q.** If a device is monitored by multiple CS-MARS appliances, how can I choose the CS-MARS appliance for which I want to view the events after lookup?
 - **Q.** Do I need to associate the CS-MARS appliance with the device that it monitors before lookup, even if only one CS-MARS monitors the device?
 - **Q.** Can I select the CS-MARS appliance to associate it the device during lookup or does it need to be done before lookup?
 - **Q.** If I delete a CS-MARS device from Security Manager, is the association between the device and CS-MARS automatically removed?
- Q.** What are the versions of CS-MARS and Security Manager that are supported for events lookup from policies?
- A.** You need to use Security Manager and CS-MARS 4.3.4 or 5.3.4 to navigate to the events in CS-MARS from the Security Manager policy table. You cannot add a CS-MARS appliance running a version lower than 4.3.4 or 5.3.4 to Security Manager.
- Q.** Can I add multiple CS-MARS appliances to a Security Manager server?
- A.** You can add multiple CS-MARS Local Controllers to a Security Manager server, although you cannot add a CS-MARS Global Controller to a Security Manager server.
- Q.** What are the benefits of querying for CS-MARS events from policies?
- A.** Navigation from a Security Manager policy to a CS-MARS event eliminates the need to run a detailed query in CS-MARS by retrieving and populating the query criteria from the policy settings. If objects are referenced in policies, the complexity of the query criteria is increased because the components of the objects might need to be entered in the strings to be queried. However, when you select a Security Manager policy to navigate to the event generated in CS-MARS by that policy, the contents of the objects are also expanded and prepopulated in the query fields.
- Q.** Is there any limit to the number of keywords that are populated in the Query page of CS-MARS when I perform events lookup from an access rule that supports hashcodes?
- A.** Because Security Manager uses the hashcodes of the ACEs on devices that support them to uniquely query for syslogs generated by the ACE in CS-MARS, large access rules might contain thousands of such hashcodes contained in them. These hashcodes are displayed as keywords in the query criteria. If the number of keywords or the sum of the number of sources, destinations, and protocols for an ACE or a signature exceeds the permissible limit of 150, an error message is displayed in CS-MARS. The error message displays the possible cause and recommended action.
- Q.** Am I returned to the Query Criteria page or the Query Results page on successful lookup of events from a policy?
- A.** For real-time events, the query is automatically run when you lookup access rules or signatures and the results of the query are displayed in the realtime event viewer of CS-MARS. However, for historical events, only the query criteria fields are populated from the data derived from Security Manager and the query must be submitted to view matching events. The time to be used to filter logged historical events is set to the last 10 minutes from the present time.
- Q.** Why does event lookup fail from policies generated by FWSM, PIX, and ASA devices in which multiple security contexts exist?
- A.** This problem occurs if you did not define a unique management IP address in Security Manager for each security context or if you did not configure the host name and reporting IP address for each virtual context while adding it to CS-MARS.

- Q.** Why do I get a “Policy not found” error message when I query for CS-MARS events from the default signature policy?
- A.** If you add an IPS device to Security Manager and deselect the IPS check box in the Create Discovery dialog box to exclude IPS policies on the device from being discovered, the icon next to the IPS policy reverts to an empty icon to show that the policy was unassigned from the device’s configuration. For all IPS device and service policies, a default signature policy is assigned to the device when you remove the configured policies from the device. If you try to perform events lookup from the default signature, a “Policy not found” error message is displayed. However, if you edit the default signature and save it, the policy icon changes to show that a local policy is configured on the device and you can navigate to events in CS-MARS.
- Q.** If my CS-MARS session is active, the events query criteria or results are displayed in the existing CS-MARS browser window, making me lose the data I was viewing in CS-MARS. Is this behavior changeable?
- A.** If an instance of CS-MARS is already running, the existing browser window is reused to display the Query page of CS-MARS because of the way in which you have set your browser to reuse windows. Set your browser to not reuse windows (such as deselecting the Reuse Windows for Launching Shortcuts check box from Tools > Internet Options > Advanced in your Internet Explorer) if you do not want the content in your current window to be replaced with whatever content is generated after events lookup.
- Events lookup determines whether to reuse an existing window or open a new window based on your browser setting and does not use a predefined method. The actual setting you configure to allow reuse of browser instances varies depending on which browser you use. See your browser documentation or help system for more information on this configuration.
- Q.** Why do I get the Security Alert dialog box when I perform events lookup?
- A.** The first time you navigate to events in CS-MARS, a Security Alert dialog box is displayed if the SSL certificate of CS-MARS is not saved in the trusted folder of the browser. Click **Yes** to choose to trust the certificate for the current session.
- Q.** Can I perform events lookup from a signature that is disabled for a sensor?
- A.** Yes. If you right-click a signature that is disabled in the signature summary page and try to navigate to realtime or historical events in CS-MARS, a warning message is displayed asking you to confirm whether you want to proceed with the events lookup. Click **Yes** to continue.
- Q.** Why do I receive a warning message when I try to look up events matching an access rule?
- A.** If the selected device does not support hashcodes in ACEs, a warning dialog box is displayed that query results might be inaccurate if the selected ACE conflicts or overlaps with other ACEs. Click **OK** to run the query.
- Q.** Is it possible to view events for access rules for which logging is not enabled?
- A.** If logging is not enabled for a permit ACE on ASA, PIX, and FWSM devices, or if logging is not enabled on IOS routers for ACEs, a warning message is displayed when you view events. To view syslogs associated with access rules for which logging is not enabled, you can perform a lookup for events matching a traffic flow.

- Q.** Is there any difference in the types of syslogs that are displayed for events matching a flow and events matching a rule?
- A.** When you perform a query for events matching a traffic flow, events triggered by access rules and connection setup/teardown are displayed. However, when you perform a query for events matching a rule, only events triggered by access rules and not connection setup/teardown are displayed.
- Q.** What is the difference between the CS-MARS user credentials entered in the New/Edit CS-MARS dialog box and in the login dialog box during events lookup?
- A.** The CS-MARS user name and password values that you enter or modify in the New/Edit CS-MARS Device dialog box is used by Security Manager server to communicate with CS-MARS and discover meta information, such as version of software running on the server and certificate details. These credentials are different from the user name and password that you enter in the Login to CS-MARS *ip_address* dialog box.

The user name and password pair in the Login to CS-MARS *ip_address* dialog box comprise the credentials that Security Manager uses to authenticate with CS-MARS to look up events matching a policy rule, when you select the option to use CS-MARS credentials during the addition of CS-MARS to Security Manager. The CS-MARS user name and password values you enter in the events lookup login dialog box are saved in the Security Manager database until the client session times out, if you chose to allow saving of CS-MARS login credentials during events lookup.

- Q.** Is it possible to query for events generated by a signature configured on a virtual sensor?
- A.** Yes. If a signature configured on your virtual sensor generates an event, the Keyword field displays the virtual sensor name in addition to the signature and subsignature IDs.
- Q.** What are the different authentication mechanisms for events lookup?
- A.** You can enable Security Manager to either contact CS-MARS using the credentials that you entered while logging in to Security Manager or use CS-MARS credentials for Security Manager to authenticate with CS-MARS. If you select the option to be prompted for CS-MARS credentials when the event query lookup is performed, you can also choose to save the CS-MARS credentials in the login dialog box to avoid being prompted every time you look up CS-MARS events in a new Security Manager client session or if the client session times out.
- Q.** Why is the check box to save credentials for subsequent event lookups disabled in the Login to CS-MARS dialog box?
- A.** This check box is available only if the Allow users to save passwords check box is selected in the CS-MARS page. When it is selected, CS-MARS credentials are saved in the Security Manager database and reused during events lookup. The Login to CS-MARS *ip_address* dialog box is not displayed during subsequent events lookup operations if you select this check box.
- Q.** Is it always necessary to configure the Security Manager user account in the CS-MARS database to perform events lookup?
- A.** You need to create the Security Manager user account in the CS-MARS database only if you select the option to use Security Manager credentials for events lookup.

- Q.** Are the CS-MARS login credentials that I enter in the Login to CS-MARS dialog box cached until the current Security Manager session is active?
- A.** Yes. If you selected the option to use the CS-MARS login credentials for Security Manager to authenticate with CS-MARS and did not choose to allow the login credentials to be saved in the login dialog box, these credentials are cached until you exit Security Manager or the idle session timeout period is exceeded; you are not prompted for login details until the Security Manager session is active.
- Q.** Can I test the connectivity between CS-MARS and Security Manager before querying for events?
- A.** Yes. You can test the connectivity from Security Manager to CS-MARS in one of the following ways:
- From the New/Edit CS-MARS dialog box, click **Retrieve from Device** next to the field to have Security Manager retrieve the certificate from CS-MARS. When you click this button, the Retrieving certificate from *ip_address* dialog box appears for a short period to indicate the process of Security Manager contacting CS-MARS.
 - From the General page in Device Properties, click **Discover CS-MARS** next to the Monitored By field. The Finding CS-MARS Device for *device_IP_address* dialog box appears for a brief period when Security Manager attempts to establish communication with CS-MARS.

If the initial configuration to enable the CS-MARS Appliance communicate with other devices on the network and prepare it to monitor data from reporting devices is not completed, an error message is displayed during connectivity test.

If the CS-MARS appliance has been shut down or cannot be reached from the Security Manager server when you try to view events, an error message is displayed asking you to restore the connection between CS-MARS and Security Manager.

- Q.** How does the absence of hashcodes in ACEs on devices that do not support them affect the accuracy of event matches for a policy?
- A.** When you select the option to display events matching a rule, the support of ACE hashcodes by the version of software running on a device determines the accuracy of syslog matches. Although Security Manager is able to gather the device information, the appropriate event types in CS-MARS, 5-tuple data from the ACEs, and the ACL, these details can result in inaccurate or excessive syslog matches. To produce most accurate syslog matches for an ACE, PIX and ASA 7.0 and later support ACE hashcodes. Each ACE contains an MD5 hashcode, which is included in the syslogs generated by that ACE. For PIX and ASA devices running 7.0 or later, Security Manager includes the hashcodes of the ACEs generated by the selected rule in the query sent to CS-MARS. ACE hashcodes are not supported on security appliances running a version of PIX or ASA software earlier than 7.0.
- Q.** Can I query events for more than one access rule or signature at the same time?
- A.** You can select only one row at a time from the Access Rules page to look up events that are generated by them. However, you can select one or more signature IDs at a time from the Signatures page and navigate to the Query page of CS-MARS for running a query on historical and real-time events.
- Q.** Why do I see no events when I perform a lookup from an access rule for which object grouping or rule optimization is enabled?
- A.** If object grouping or rule optimization is enabled for an access rule defined in Security Manager and the associated access-list commands on the device do not match with the optimized rules, no events are displayed in CS-MARS because of the mismatch in access rule relationship between Security Manager and the device.

- Q.** If a device is monitored by multiple CS-MARS appliances, how can I choose the CS-MARS appliance for which I want to view the events after lookup?
- A.** If more than one CS-MARS monitors a device added to Security Manager, the Select CS-MARS dialog box appears, prompting you to select the CS-MARS device that you want to associate with the device or use to view events for the selected policy rule. This dialog box appears when you try to discover the CS-MARS device for a device from the Device Properties page or when you lookup events for a device monitored by multiple CS-MARS devices, whichever operation is performed first. Once a CS-MARS device is resolved to a device, you are not prompted to select from a list of available choices.
- Q.** Do I need to associate the CS-MARS appliance with the device that it monitors before lookup, even if only one CS-MARS monitors the device?
- A.** If only one CS-MARS appliance monitors a device and you do not associate the CS-MARS appliance with the device that it monitors from the Device Properties page by discovering the CS-MARS appliance, the CS-MARS appliance is automatically resolved to the device when you perform the events lookup for the first time.
- Q.** Can I select the CS-MARS appliance to associate it the device during lookup or does it need to be done before lookup?
- A.** You can associate the CS-MARS device with the device in inventory either before you perform events lookup or at the time of the lookup query. If you try to navigate to CS-MARS events from the policy table of a device before associating the CS-MARS device with it, Security Manager automatically resolves the device to the correct CS-MARS device if only one CS-MARS device monitors it or presents you with a list of CS-MARS devices monitoring the device if multiple CS-MARS devices monitor the same device. You can establish the association and continue with the lookup of events. Once you associate the CS-MARS device with the device, the CS-MARS host name or IP address is populated in the Monitored By field of the Device Properties page.
- Alternatively, you can discover a CS-MARS device monitoring a device already added to Security Manager from the General pane of the Device Properties page to reduce a task in the process of looking up events.
- Q.** If I delete a CS-MARS device from Security Manager, is the association between the device and CS-MARS automatically removed?
- A.** If you delete a CS-MARS appliance monitoring a device from the Security Manager database, it is also removed from the Monitored By field in the Device Properties page of that device. If a device is monitored by two CS-MARS appliances and you later delete one of them from the Security Manager database, the device is automatically associated with the remaining CS-MARS device. You do not have to manually discover the CS-MARS appliance for that device.

Changing the Association of the CS-MARS Appliance with a Device

Problem A device is monitored by multiple CS-MARS appliances that are added to Security Manager. You associated the device with a CS-MARS appliance during events lookup. You want to select a different CS-MARS appliance for the device and perform events lookup.

Solution Once you associate a CS-MARS appliance with a device during events lookup, the same CS-MARS device is used to query for events even if multiple CS-MARS devices monitor a device. To change the CS-MARS device to be used to look up events, you must rediscover the CS-MARS device from the General pane of the Device Properties page.

This procedure describes how to discover a CS-MARS device monitoring a device added to the inventory.

Before You Begin

Make sure that you added the necessary CS-MARS appliances to Security Manager.

Procedure

-
- Step 1** Click the Device View button on the toolbar. The Devices page appears.
 - Step 2** Double-click a device in the Device selector. The Device Properties page appears.
 - Step 3** Click **General** from the left pane. The General page appears.
 - Step 4** Under CS-MARS Monitoring, click **Discover CS-MARS** next to the Monitored By field.
The Finding CS-MARS Device for *device_IP_address* dialog box appears for a brief period when Security Manager attempts to establish communication with CS-MARS. If connectivity and discovery are successful, the Select CS-MARS dialog box is displayed.
 - Step 5** Click the radio button next to the CS-MARS appliance to be used to query events for the policy rule on the selected device.
 - Step 6** Click **OK**. The selected CS-MARS host name or IP address is populated in the Monitored By field of the Device Properties page.
-

Configuring Required Browser Settings for Policy and Events Lookup

You might have to change browser settings on the system from which you access CS-MARS for policy and events lookup. Default browser settings might cause a number of popup warning or error messages to be displayed when you perform policy or events lookup. In some cases, navigation to the Security Manager client for policy lookup or to CS-MARS for events lookup might be blocked due to browser settings. The topics in this section are our recommendations for managing browser settings that can affect policy and events lookup. Refer to your browser manual or online help for detailed instructions about accessing and setting the options in these procedures.

- [Working with Cached Passwords in Internet Explorer, page 13-20](#)
- [Setting Internet Explorer Security Options, page 13-20](#)
- [Setting Internet Explorer to Allow Display of Nonsecure Content, page 13-21](#)

Working with Cached Passwords in Internet Explorer

If you selected the option to be prompted for Security Manager credentials during policy lookup, it is possible that the Password field in the login section of the policy query popup window is automatically filled after you enter the use rname. You might notice this behavior due to a configuration in Internet Explorer, whereby passwords are cached or are remembered by the browser.

Internet Explorer can store user passwords, thereby saving you a few steps when logging in to Web applications. If you enabled the AutoComplete feature, when you visit a web page for the first time, Internet Explorer prompts you with a message whether you want to remember the password you entered. If you click Yes, the password is automatically filled on subsequent visits to this page. If you click No when asked whether you want passwords to be remembered and if the AutoComplete feature is enabled, a list of possible matches appears as you type if you have entered a similar entry before. If a suggestion in the list matches what you want to enter in that field, the browser automatically fills the entry. However, for security reasons, we recommend that you prevent the browser from remembering passwords when you log in, especially if you share your computer with others. You can either disable the feature of the browser to cache passwords or clear the cache at intervals to be not prompted with suggestions during entry.

To disable the AutoComplete feature altogether, follow these steps:

-
- Step 1** Select **Tools > Internet Options**.
The Internet Options dialog box appears.
 - Step 2** Click the **Advanced** tab.
 - Step 3** In the Browsing pane, deselect the **Use inline auto complete** check box.
 - Step 4** Click **OK** in the Internet Options dialog box.
-

To clear cached passwords from your browser, follow these steps:

-
- Step 1** Select **Tools > Internet Options**.
The Internet Options dialog box appears.
 - Step 2** Click the **Content** tab.
 - Step 3** Under Personal Information, click the **AutoComplete** button.
The AutoComplete Settings dialog box appears.
 - Step 4** Click **Clear Passwords**. When you are prompted to confirm your action, click **OK**.
 - Step 5** Click **OK** as many times as necessary to close the opened dialog boxes.
-

Setting Internet Explorer Security Options

When you try to start the Security Manager client from the read-only policy query window in CS-MARS, the File Download dialog box might appear prompting you to confirm whether you want to save the CsmContentProvider file to your system. The option to open the file without downloading it to your local disk is not available because of security settings in Internet Explorer. To enable the Open button to be displayed in this dialog box when it appears during policy lookup, do the following:

-
- Step 1** Select **Tools > Internet Options**.
 - Step 2** Click the **Advanced** tab.
 - Step 3** Scroll to the Security area, then deselect the **Do not save encrypted Pages to Disk** check box.
 - Step 4** Click **OK**.
-

Setting Internet Explorer to Allow Display of Nonsecure Content

When you try to open the Security Manager client from the read-only signature or access rule policy query page in CS-MARS, the Security Information Error dialog box might be displayed if you configured your browser to prompt for confirmation whenever a web page that contains both secure and nonsecure content must be opened. You may receive the following Security Information message when you open the Security Manager client:

This page contains both secure and nonsecure items.
Do you want to display the nonsecure items?

You can configure your browser to seamlessly display nonsecure content without being prompted each time the Security Manager client is opened. To configure Internet Explorer to allow display of nonsecure content, follow these steps:

-
- Step 1** Select **Tools > Internet Options**.
 - Step 2** Click the **Security** tab.
 - Step 3** Click **Custom Level** on the Security tab of the Internet Options dialog box.
 - Step 4** Under the Miscellaneous heading, select the **Enable** radio button for the “Display mixed content” setting. This option specifies whether Web pages can display content from both secure and non-secure servers.

By default, the “Display mixed content” setting is set to Prompt for all security levels. If the “Display mixed content” setting is set to Enable, the message box is not displayed and nonsecure content can be displayed. If the “Display mixed content” setting is set to Disable, the message box is not displayed and nonsecure content is not downloaded for display.

- Step 5** Click **OK**.
-



INDEX

A

AAA

- accounting not implemented on SSL VPN [9-9](#)
- discovered configuration not displayed [6-5](#)
- discovering servers with server-private command [6-5](#)
- method lists partially discovered [6-5](#)
- name changes when discovering policies [6-15](#)
- name changes when discovering rules [6-11](#)
- removing aaa new-model command [9-8](#)

access control lists (ACLs)

- creating during IOS IPS configuration [8-3](#)
- deployment errors on FWSMs [12-6](#)
- handling names during discovery [6-3](#)
- name changes during discovery [6-11](#)
- names preserved during discovery [6-6](#)
- naming conventions [6-7](#)
- resolving naming conflicts [6-9](#)

access rule lookup

- deployed changes
 - synchronization with [13-7](#)
- device software versions
 - supported for [13-8](#)
- devices with multiple contexts
 - prerequisites for [13-12](#)
- error message [13-4](#)
- from MARS
 - without Security Manager client running [13-8](#)
- syslogs supported for
 - by firewall devices [13-11](#)
- with Security Manager client active
 - in non-Workflow mode [13-8](#)
 - in Workflow mode [13-8](#)

access rules

- events lookup
 - large number of hashcodes [13-14](#)
 - warning message [13-15](#)
 - hashcodes
 - accuracy of syslog matches [13-17](#)
 - modified
 - after read-only policy display [13-5](#)
 - not synchronized with device [13-5](#)
 - object grouping
 - events lookup and [13-17](#)
 - on higher security interface, inbound
 - policy lookup [13-4](#)
 - on lower security interface, inbound
 - policy lookup [13-4](#)
 - policy query icon [13-4](#)
 - on lower security interface, outbound
 - policy lookup [13-4](#)
 - optimization
 - events lookup and [13-17](#)
 - unavailable on the device
 - for MARS syslogs [13-5](#)
- #### activities
- in an editable state
 - and policy table lookup from MARS [13-8](#)
 - policy table lookup
 - with Security Manager client active [13-8](#)
- #### address pools
- deployment failure [9-8](#)
 - on same subnet as interface [9-9](#)
 - overriding in connection profiles [9-8](#)
- #### ADSL policies
- unable to deploy [10-4](#)

approvers

- associating with user account
 - for policy lookup from MARS [13-9](#)

ASA devices

- with multiple contexts
 - and policy lookup from MARS [13-12](#)
 - MARS events lookup [13-14](#)
 - prerequisite for policy table lookup [13-12](#)

authentication

- of MARS for policy lookup
 - Security Manager deleted from MARS [13-7](#)

authentication settings

- for events lookup
 - Security Manager credentials [13-16](#)

authorization

- changes in ACS for devices [3-3](#)

Auto Update Server (AUS)

- discovering policies [6-3](#)
- failure during deployment [12-10](#)

B

browser settings

- reusing windows
 - for events lookup [13-15](#)

C

Catalyst switches and 7600 devices

- adding 6503-E devices [11-1](#)
- deployment failure when changing IDSM data port running mode [11-3](#)
- discovering failover pairs [11-2](#)
- discovering policies on security contexts [6-4](#)
- IDSM support [11-2](#)
- interface deployment failure [11-2](#)
- internal VLAN deployment failure [11-2](#)
- supported modes [11-1](#)
- supported VACLs [11-2](#)

troubleshooting [11-1](#)

undefined VLANs [11-2](#)

changes, out-of-band [12-4](#)

Cisco Configuration Engine

troubleshooting device setup [5-4](#)

Cisco Marketplace [1-x](#)

Cisco Press [1-x](#)

Cisco Product Quick Reference Guide, obtaining [1-x](#)

Cisco product security

PSIRT [1-x](#)

vulnerability policy portal [1-x](#)

Cisco Secure ACS (ACS)

adding multihomed devices [3-4](#)

authentication fails [3-2](#)

changes not appearing in Security Manager [3-3](#)

devices not appearing in Security Manager [3-3](#)

effect on policy discovery [6-3](#)

read-only access for system administrators [3-2](#)

restoring access [3-4](#)

updating device credentials in Security Manager [3-4](#)

using multiple versions of Security Manager [3-1](#)

working after ACS becomes unreachable [3-3](#)

Cisco Secure ACS roles

policy table lookup from MARS [13-9](#)

Cisco Security Agent

already installed on server [4-1](#)

co-existing with IPS systems [4-2](#)

error message in event log [4-2](#)

frequently asked questions [4-1](#)

reinstalling bundled version [4-1](#)

client installation

troubleshooting [2-7](#)

client log files

locating [2-2](#)

CNS

lists applied to wrong SSL VPN context [9-9](#)

Common Services

MARS user account, creating [13-7](#)

MARS user not defined in

- policy lookup [13-11](#)
 - user account not defined in
 - logging in to MARS [13-11](#)
- Common Services roles
 - policy table lookup from MARS [13-9](#)
- communication, device
 - troubleshooting [5-1](#)
- Configuration Engine
 - debugging IOS device [5-6](#)
 - debugging PIX device [5-6](#)
 - deployment failure [5-4](#)
 - deployment failures to PIX device [5-5](#)
 - device id not connected error [5-5](#)
 - device name does not exist error [5-5](#)
 - discovery failure for IOS device [5-6](#)
 - event mode router does not appear [5-6](#)
 - first deployment to PIX fails [5-5](#)
 - InvalidParameterException error [5-4](#)
- configuration ownership [12-4](#)
- configuration rollback
 - cannot connect to a Cisco IOS router after [5-2](#)
 - performing reload [12-8](#)
- configure replace command [12-8](#)
- connection profiles
 - sharing among multiple ASAs [9-8](#)
- connection-related messages
 - generated by
 - outbound traffic, policy lookup [13-4, 13-5](#)
- connection teardown messages
 - 2-minute gap with
 - connection setup [13-3](#)
 - in a different session from setup [13-3](#)
 - realtime event viewer [13-3](#)
- connectivity test
 - between MARS and Security Manager
 - configuring administrative host [13-10](#)
 - correct credentials [13-10](#)
 - error message [13-7, 13-10](#)
 - success [13-7, 13-10](#)

- console port
 - name changes during discovery [6-15](#)
- Context Data events
 - on IPS and IDS sensors
 - policy query icon and [13-5](#)
- cross-launch authentication settings
 - for events lookup
 - disabling saving of credentials [13-16](#)
 - using MARS login credentials [13-16](#)
 - using Security Manager credentials [13-16](#)
- custom signatures
 - policy lookup for [13-10](#)

D

- Daemon Manager
 - not running on Security Manager
 - policy table lookup [13-11](#)
- deleting
 - referenced interfaces [10-2](#)
- deployment
 - ADSL deployment failures [10-4](#)
 - Catalyst interface settings [11-2](#)
 - Catalyst internal VLANs [11-2](#)
 - changes not deployed [12-8](#)
 - determining method to use [12-3](#)
 - devices with same IP address [5-3](#)
 - duplicate SSL VPN gateway failure [9-8](#)
 - errors with ACLs [12-6](#)
 - failure due to overlapping pools [9-8](#)
 - failure due to pools not on interface subnet [9-9](#)
 - failures with AUS-managed devices [12-10](#)
 - failure when modifying WINS master server [9-9](#)
 - failure when port forwarding list removed [9-9](#)
 - fixing an OS version mismatch [12-4](#)
 - IDSM data port VLAN running mode [11-3](#)
 - ignoring errors [12-7](#)
 - IOS errors [12-6](#)
 - IOS IPS [8-3](#)

- layer 2 interfaces [10-2](#)
- maximum number of devices [12-6](#)
- mixing methods [12-9](#)
- of access rule changes
 - synchronization with device [13-7](#)
- performing immediately after discovery [6-3](#)
- PVC deployment failures [10-4](#)
- PVC IP protocol mappings [10-4](#)
- rolling back configurations [12-3](#)
- setting default directory [12-3](#)
- SSL handshake failure [12-10](#)
- understanding
 - effects of deploying to files [12-3](#)
 - full vs. delta configurations [12-6](#)
 - process [12-2](#)
- device communication
 - FAQs [5-2](#)
 - loss of contact due to NAT [10-3](#)
 - routers without K8/K9 crypto image [5-2](#)
 - troubleshooting [5-1](#)
- device configuration
 - discovering commands [6-3](#)
 - unable to configure [10-5](#)
- device management [12-4](#)
 - simultaneous operations on device [5-3](#)
- Device Properties page
 - deleting a MARS appliance [13-18](#)
 - discovering
 - MARS [13-18](#)
- device response
 - to appear as an error message [12-8](#)
- devices
 - added to MARS only
 - policy lookup [13-6](#)
 - changes to ACS authorization not appearing in Security Manager [3-3](#)
 - losing connection after deploying access rules [7-1](#)
 - signature policies
 - not discovered [13-15](#)
 - software versions
 - supported by MARS and Security Manager [13-8](#)
 - synchronization with
 - changed policies [13-7](#)
 - updating credentials from ACS [3-4](#)
 - with multiple contexts
 - Device Properties page [13-12](#)
 - differing host and context names [13-12](#)
 - policy query icon [13-12](#)
 - reporting IP address in MARS [13-12](#)
 - setting hostname for policy lookup from MARS [13-12](#)
- DHCP
 - traffic blocked [10-5](#)
- diagnostic information
 - generating [1-1](#)
- dialers
 - name changes during discovery [6-14](#)
- discovering
 - MARS
 - after deleting [13-18](#)
- discovery
 - Catalyst failover pairs [11-2](#)
 - devices with same IP address [5-3](#)
 - invalid certificate error [5-3](#)
 - of MARS
 - into Security Manager [13-18](#)
 - security certificate error [5-2](#)
- discovery task
 - frequently asked questions [6-2](#)
- DNS
 - configuring for SSL VPN [9-8](#)
- documentation
 - on Cisco.com [1-x](#)
 - ordering [1-x](#)
- documentation feedback, sending to Cisco [1-x](#)

E

error message

- events lookup from policies
 - MARS appliance not configured [13-17](#)
- testing connectivity
 - between MARS and Security Manager [13-11](#)

error messages

- events lookup from policies
 - MARS appliance is shut down [13-17](#)
- policy table lookup from MARS
 - access rules not on device [13-4](#)
 - addition of multiple Security Managers to Local Controller [13-11](#)
 - connection setup syslog unavailable [13-3](#)
 - connection teardown events in realtime viewer [13-3](#)
 - Daemon Manager not running on Security Manager [13-11](#)
 - device added to MARS only [13-6](#)
 - implicit permit statement in access rules [13-4](#), [13-5](#)
 - modal dialog box open [13-11](#)
 - RPC connection failure [13-4](#)
 - unsynchronized changes [13-4](#)

errors

- deployment [12-6](#)

event action filter

- configuring
 - during policy table lookup from MARS [13-8](#)

event log

- CSA error message [4-2](#)

events lookup

- advantages [13-14](#)
- browser settings [13-15](#)
- device software versions
 - supported for [13-8](#)
- from access rules
 - ACE hashcodes [13-17](#)
 - hashcodes [13-17](#)

- object grouping [13-17](#)
- optimization enabled [13-17](#)
- from default signatures [13-15](#)
- from policies
 - error message [13-17](#)
 - for multiple contexts [13-14](#)
- from signatures
 - for virtual sensors [13-16](#)

F

FAQ

- Catalyst switches and 7600 devices [11-1](#)
- policy discovery
 - AAA configuration not displayed [6-5](#)
 - AAA method lists partially discovered [6-5](#)
 - AAA servers and server-private command [6-5](#)
 - deploying after discovering VPN and router policies [6-3](#)
 - determining results [6-2](#)
 - device hostnames [6-5](#)
 - discovering configuration commands [6-3](#)
 - discovering with AUS [6-3](#)
 - discovery and ACS [6-3](#)
 - FWSM and Catalyst security contexts [6-4](#)
 - how it works [6-2](#)
 - naming ACLs and object groups [6-3](#)
 - PIX/ASA security contexts [6-4](#)
 - redeploying after discovery [6-3](#)
 - rediscovering existing policies [6-4](#)
 - unable to submit changes [6-5](#)
 - using existing policies and objects [6-4](#)
 - viewing discovered policies [6-3](#)
 - viewing undiscovered policies [6-2](#)
 - when to perform [6-2](#)

FAQs

- device communication [5-2](#)
- firewall services
 - cli for authentication proxy [7-2](#)

- configuring management IP of security contexts [7-2](#)
- hit count
 - standard ACLs [7-2](#)
- losing connection to a device [7-1](#)
- negating addresses within a range [7-2](#)
- removal of bound ACEs [7-2](#)
- unable to deploy BGP [7-2](#)
- Firewall Services Module (FWSM)
 - deployment error [12-6](#)
 - discovering policies on security contexts [6-4](#)
- FWSM
 - multiple contexts
 - MARS events lookup [13-14](#)
 - with multiple contexts
 - and policy lookup from MARS [13-12](#)
 - prerequisite for policy table lookup [13-12](#)

G

- gateways
 - sharing address and port [9-8](#)
- Global Controller
 - adding to
 - Security Manager [13-14](#)
 - policy query icon for events [13-12](#)
 - policy table lookup and [13-12](#)
 - viewing Security Manager server from [13-12](#)
- group-policy
 - removing SSL VPN definitions [9-9](#)

H

- hashcodes
 - ACE
 - accuracy of syslog matches [13-17](#)
 - supported device OS versions [13-17](#)
 - in large access rules
 - looking up events [13-14](#)

- Help Desk role
 - policy table lookup and [13-9](#)
- historical events
 - filtering time [13-14](#)
 - lookup from policies
 - running query manually [13-14](#)
 - policy lookup
 - error message [13-4](#)
- historical events lookup
 - device versions
 - supported for [13-8](#)
- hostnames
 - effect on policy discovery [6-5](#)
- HTTP
 - name changes during discovery [6-15](#)
- HTTPS mode
 - determining [2-2](#)

I

- idle timeout
 - exceeded for MARS session
 - without Security Manager client open before lookup [13-6](#)
 - with Security Manager login credentials for lookup [13-6](#)
- IDS
 - support limitations [11-2](#)
- IDS sensors
 - Context Data events
 - and signature policy lookup [13-5](#)
 - Packet Data events
 - and signature policy lookup [13-5](#)
- ignore error message
 - configure Security Manager to [12-8](#)
- implicit permit
 - configured in access rules
 - lookup from MARS events [13-4](#), [13-5](#)
- inspection rules

- name changes during discovery [6-12](#)
 - installation
 - troubleshooting [2-7](#)
 - Internet Explorer
 - accessing MARS GUI using
 - for access rule lookup [13-8](#)
 - cached passwords
 - policy table lookup [13-8](#)
 - remembered passwords
 - policy table lookup [13-8](#)
 - IOS 12.1 and 12.2
 - configuring in Security Manager [10-1](#)
 - IOS 12.4(11)T
 - address pool deployment failure [9-9](#)
 - CNS problem with SSL VPN contexts [9-9](#)
 - IOS 12.4(9)T
 - AAA accounting failure [9-9](#)
 - port forwarding list deployment failure [9-9](#)
 - WINS master server deployment failure [9-9](#)
 - IP mappings
 - unable to deploy [10-4](#)
 - IPS
 - co-existing with CSA [4-2](#)
 - creating ACLs [8-3](#)
 - deploying [8-3](#)
 - importing 5.0 sensors [8-1](#)
 - performing updates [8-2](#)
 - provisioning trusted hosts [8-3](#)
 - retrieving signature updates [8-1](#)
 - signature updates [8-3](#)
 - updating IOS IPS crypto configurations [8-2](#)
 - IPS sensors
 - Context Data events
 - and signature policy lookup [13-5](#)
 - Packet Data events
 - and signature policy lookup [13-5](#)
 - IPS signature policy lookup
 - device software versions
 - supported for [13-8](#)
 - event action filter, configuring [13-8](#)
 - for MARS events of type
 - Context Data [13-5](#)
 - Packet Data [13-5](#)
 - from MARS
 - without Security Manager client running [13-8](#)
 - with Security Manager client active
 - in non-Workflow mode [13-8](#)
 - in Workflow mode [13-8](#)
 - IPS virtual sensors
 - signature policy lookup
 - from MARS events [13-5](#)
-
- ## L
- license
 - SSL VPN import [9-8](#)
 - line access
 - name changes during discovery [6-15](#)
 - Local Controller
 - adding
 - multiple Security Manager servers to [13-11](#)
 - one Security Manager server to [13-11](#)
 - adding multiple
 - to Security Manager [13-14](#)
 - logging
 - disabled for permit ACEs
 - events lookup [13-15](#)
 - logging in to
 - MARS
 - using an account not defined in Common Services [13-11](#)
 - Security Manager
 - after error during policy lookup [13-4](#)
 - using a different account from the one in MARS [13-7](#)
 - logging level
 - changing for firewalls
 - and syslogs in MARS [13-11](#)

login credentials
 of Security Manager
 saved in MARS during policy lookup [13-12](#)

login credentials, Security Manager
 authenticating MARS
 Security Manager deleted from MARS [13-7](#)

editing
 from User Configuration page in MARS [13-7](#)

using a different account from the one in MARS
 for policy lookup [13-7](#)

looking up
 events from signatures
 for virtual sensors [13-16](#)

MARS events
 advantages [13-14](#)
 from default signature [13-15](#)
 from large access rules [13-14](#)

M

management IP address
 defining for multiple contexts
 events lookup [13-14](#)

MARS
 adding Security Manager to
 users with admin privileges [13-9](#)

committed view
 of Security Manager policy [13-7](#)

deployed view
 of Security Manager policy [13-7](#)

downloading Security Manager [13-6](#)

policy table lookup
 time taken for [13-10](#)
 with Security Manager client not running [13-8](#)
 with Security Manager in non-Workflow mode [13-8](#)
 with Security Manager in Workflow mode [13-8](#)

starting a new instance of Security Manager
 with client session active [13-7](#)

starting Security Manager for policy lookup
 using Security Manager credentials [13-7](#)

User Configuration page
 Security Manager credentials [13-7](#)

MARS appliance
 automatic mapping
 with Security manager [13-18](#)

deleting
 from Security Manager [13-18](#)

not associated with monitored device
 in Security Manager [13-18](#)

shutting down
 events lookup [13-17](#)

testing connectivity
 with Security Manager [13-7, 13-10](#)

version 4.3.4, 5.3.4
 adding to Security Manager [13-14](#)

MARS authentication
 with Security Manager for policy lookup
 deleting Security Manager from MARS [13-7](#)
 editing Security Manager credentials in MARS [13-7](#)

MARS database
 deleting
 Security Manager server from [13-7](#)

saving Security Manager credentials
 during policy lookup [13-6](#)

MARS events
 for connection teardown
 in realtime event viewer [13-3](#)

generated by custom signatures
 and policy lookup [13-10](#)

of type
 Context Data [13-5](#)
 Packet Data [13-5](#)

MARS Global Controller
 See Global Controller

MARS GUI
 accessing using

- Internet Explorer, note [13-8](#)
 - MARS Local Controller
 - See Local Controller
 - MARS session
 - idle timeout, exceeding
 - using Security Manager credentials for policy lookup [13-6](#)
 - MARS user account
 - defining in Common Services
 - for policy lookup [13-7](#)
 - not defined in Common Services
 - prompting for credentials [13-11](#)
 - MARS user roles
 - Admin
 - editing Security Manager credentials [13-7](#)
 - for modifying Security Manager credentials [13-9](#)
 - Notifications Only [13-9](#)
 - Operator [13-9](#)
 - Security Analyst
 - editing Security Manager credentials [13-7](#)
 - MARS web interface
 - policy table lookup
 - with Security Manager not installed [13-6](#)
 - max-webvpn-session-limit
 - cannot be imported [9-8](#)
 - MD5 hashcodes
 - See hashcodes
 - modal dialog box
 - looking up policy table
 - from MARS [13-11](#)
-
- N**
- NAC
 - deployment fails [10-7](#)
 - name changes during discovery [6-17](#)
 - posture validation not occurring [10-6](#)
 - NAT
 - deployment failure on 83x routers [10-3](#)
 - name changes during discovery [6-13](#)
 - VPN traffic sent unencrypted [10-3](#)
 - navigating
 - from multiple signature IDs
 - to historical events in MARS [13-17](#)
 - to realtime events in MARS [13-17](#)
 - from policies
 - to MARS events, advantages [13-14](#)
 - network administrators
 - associating with user account
 - for policy lookup from MARS [13-9](#)
 - Networking Professionals Connection [1-x](#)
 - network operators
 - associating with user account
 - for policy lookup from MARS [13-9](#)
 - non-Workflow mode
 - policy table lookup
 - from MARS events [13-8](#)
 - with Security Manager client active [13-8](#)
 - number of rules [13-10](#)
-
- O**
- object groups
 - enabled for access rules
 - MARS events lookup [13-17](#)
 - object-groups
 - name changes during discovery [6-10](#)
 - objects
 - expanding contents
 - in MARS event query [13-14](#)
 - query criteria in MARS [13-14](#)
 - using existing objects during discovery [6-4](#)
 - online help
 - loading [2-6](#)
 - preserving search results [2-7](#)
 - OS version mismatch
 - fixing [12-4](#)
 - out-of-band changes

resolving [12-4](#)

P

Packet Data events

huge syslog messages [13-5](#)

on IPS and IDS sensors

policy query icon and [13-5](#)

parsing

invalid syslog messages

[13-4](#)

passwords

encrypted passwords on routers [10-2](#)

peer support, Networking Professionals Connection [1-x](#)

performance

of MARS

number of rules [13-10](#)

of Security Manager [13-10](#)

PIX/ASA devices

discovering policies on security contexts [6-4](#)

discovering policies when using AUS [6-3](#)

PIX firewalls

multiple contexts

MARS events lookup [13-14](#)

PIX object groups

handling names during discovery [6-3](#)

policies

policy discovery FAQ [6-2](#)

rediscovery and current assignments [6-4](#)

using existing policies during discovery [6-4](#)

policy discovery

AAA commands not displayed in AAA policy [6-5](#)

AAA method lists partially discovered [6-5](#)

AAA servers and server-private command [6-5](#)

deploying after discovering VPN and router policies [6-3](#)

determining results [6-2](#)

device hostnames [6-5](#)

discovering configuration commands [6-3](#)

discovering with AUS [6-3](#)

discovery and ACS [6-3](#)

frequently asked questions [6-2](#)

FWSM and Catalyst security contexts [6-4](#)

how it works [6-2](#)

naming ACLs and object groups [6-3](#)

negated SSL VPN policies [6-6](#)

PIX/ASA security contexts [6-4](#)

preserving ACL names [6-6](#)

redeploying after discovery [6-3](#)

rediscovering existing policies [6-4](#)

resource names changed during discovery [6-9](#)

unable to submit changes [6-5](#)

undiscovered VPN features [6-6](#)

using existing policies and objects [6-4](#)

viewing discovered policies [6-3](#)

viewing undiscovered policies [6-2](#)

when to perform [6-2](#)

while deploying to device [6-5](#)

policy lookup [13-3](#)

policy lookup from MARS [13-7](#)

policy query icon

for access rules

not found on the device [13-4](#)

for Context Data events [13-5](#)

for devices with multiple contexts

without reporting IP address [13-12](#)

for events in Global Controller [13-12](#)

for Packet Data events [13-5](#)

for Unknown Device Event Type

triggered by custom signatures [13-10](#)

for unsupported syslog IDs [13-3](#)

policy query login dialog box

saving Security Manager credentials [13-12](#)

Policy Query popup window

See read-only policy table

policy table lookup

devices with multiple contexts

prerequisites for [13-12](#)

- error message [13-11](#)
- event action filter, configuring [13-8](#)
- MARS user roles [13-9](#)
- modal dialog box [13-11](#)
- prompting for credentials
 - MARS user not in Common Services [13-11](#)
- time taken for [13-10](#)
- with Security Manager client active
 - in non-Workflow mode [13-8](#)
 - in Workflow mode [13-8](#)
- with Security Manager client not running [13-8](#)

port forwarding list

- applied to wrong SSL VPN context [9-9](#)
- deployment failure when removed [9-9](#)

PPP

- name changes during discovery [6-15](#)

proxy-bypass interfaces

- configured for SSL VPN [9-8](#)

PSIRT [1-x](#)

publications, obtaining additional [1-x](#)

PVC policies

- unable to deploy [10-4](#)

Q

quality of service (QoS)

- name changes during discovery [6-17](#)

queries

- criteria
 - complexity [13-14](#)
 - objects in policies [13-14](#)
 - populated from policies [13-14](#)
- expanding objects in MARS [13-14](#)
- for historical events
 - run manually [13-14](#)
- for realtime events
 - run automatically [13-14](#)

Query/Reports tab

- identifying incident

- for signature policy lookup [13-5](#)

querying

- for MARS events from devices
 - without reporting IP address [13-12](#)
- for Unknown Reporting Devices in MARS [13-12](#)

Query page

- reusing browser window
 - during events lookup [13-15](#)

R

read-only policy table

- after display of
 - access rules, modifying [13-5](#)
- error message
 - corrective action [13-6](#)
 - device added to MARS only [13-6](#)

read-only signature policy page

- viewing
 - Security Manager details [13-9](#)

realtime events

- policy lookup
 - error message [13-4](#)
- running query automatically [13-14](#)

realtime events lookup

- device versions
 - supported for [13-8](#)

realtime event viewer

- access rule lookup
 - for connection teardown events [13-3](#)
- in MARS
 - navigating from policies [13-14](#)

reload

- after configuration rollback [12-8](#)

Reporting Applications tab

- Security Manager user credentials
 - for initial communication [13-12](#)
- using MARS credentials
 - not defined in Common Services [13-11](#)

reporting IP address
 for devices with multiple contexts
 policy table lookup [13-12](#)

resources

- AAA name changes [6-11](#)
- AAA policy name changes [6-15](#)
- ACL name changes [6-11](#)
- dialer name changes [6-14](#)
- dynamic NAT name changes [6-13](#)
- HTTP name changes [6-15](#)
- inspection rule name changes [6-12](#)
- line access name changes [6-15](#)
- NAC name changes [6-17](#)
- names changed during discovery [6-9](#)
- object-group name changes [6-10](#)
- PPP name changes [6-15](#)
- QoS name changes [6-17](#)
- service policy rule name changes [6-13](#)
- transparent rule name changes [6-12](#)

rollback [12-3](#)
 performing when deploying to file [12-9](#)

router platform

- policy troubleshooting [10-1](#)
 - device access policies [10-4](#)
 - device interface policies [10-2](#)
 - DHCP policies [10-5](#)
 - DSL policies [10-3](#)
 - NAC policies [10-6](#)
 - NAT policies [10-2](#)
 - PVC policies [10-4](#)
 - SDP policies [10-5](#)
 - SNMP policies [10-6](#)
 - static routing policies [10-7](#)

routers

- configuring routers with 12.1 or 12.2 [10-1](#)
- managing encrypted passwords [10-2](#)
- NAT deployment fails [10-3](#)

S

security

- advisories [1-x](#)
- incidents, obtaining assistance [1-x](#)
- news from Cisco
 - registering to receive [1-x](#)
 - RSS feed URL [1-x](#)
- notices [1-x](#)
- PSIRT [1-x](#)
- vulnerabilities, reporting [1-x](#)

Security Agent installation

- troubleshooting [2-7](#)

security certificate

- invalid during discovery [5-3](#)

security context

- configuring management IP [7-2](#)

security contexts

- deleting configuration file [5-3](#)
- discovering policies on FWSM and Catalyst devices [6-4](#)
- discovering policies on PIX/ASA devices [6-4](#)

Security Manager client

- cleaning server list in Login window [2-2](#)
- determining HTTPS mode [2-2](#)
- entering server names after installation [2-2](#)
- frequently asked questions [2-1](#)
- installing on same machine as server [2-2](#)
- loading online help [2-6](#)
- locating client logs [2-2](#)
- reinstalling [2-5](#)
- removing locks of another user [2-6](#)
- resetting password [2-2](#)
- resolving version mismatch [2-2](#)
- running in dual-screen mode [2-3](#)
- upgrading
 - from a previous version [2-5](#)
 - using HTTP [2-3](#)

Security Manager database

- corrupted [1-2](#)
- troubleshooting [1-2](#)
- Security Manager Diagnostics utility
 - accessing [1-1](#)
- Security Manager policy query icon
 - See policy query icon
- Security Manager server
 - collecting troubleshooting information [1-1](#)
 - database issues [1-2](#)
 - installation [1-4](#)
 - restoring database from files [1-3](#)
 - restricting access [1-4](#)
 - unable to launch [1-3](#)
- sensor ID
 - in IPS syslog messages in MARS
 - for virtual sensors [13-5](#)
- service policy rules
 - name changes during discovery [6-13](#)
- service requests
 - submitting [1-x](#)
- signature policy
 - default
 - assigned to devices [13-15](#)
 - excluded from discovery
 - empty icon [13-15](#)
 - not discovered on device
 - and events lookup [13-15](#)
- signatures
 - default
 - editing, policy icon [13-15](#)
 - events lookup [13-15](#)
 - managing updates [8-3](#)
 - retrieving updates [8-1](#)
- signature summary table
 - navigating to
 - historical events in MARS [13-15](#)
 - realtime events in MARS [13-15](#)
- SNMP
 - traps not being sent [10-6](#)
- SSL
 - handshake failure during deployment [12-10](#)
- SSL VPN
 - AAA accounting not implemented [9-9](#)
 - address pools on interface subnet [9-9](#)
 - cannot import license information [9-8](#)
 - detecting overlapping pools [9-8](#)
 - limitations [9-8](#)
 - limitations due to OS defects [9-9](#)
 - lists applied to wrong context [9-9](#)
 - modifying WINS master server [9-9](#)
 - need for DNS [9-8](#)
 - removing aaa new-model command [9-8](#)
 - removing group policies from PIX/ASAs [9-9](#)
 - removing port forwarding list [9-9](#)
 - sharing connection profiles on ASAs [9-8](#)
 - sharing gateway addresses [9-8](#)
 - use of proxy-bypass interfaces [9-8](#)
 - using interface roles [9-8](#)
- static routing
 - floating route not inserted [10-7](#)
- support
 - Networking Professionals Connection [1-x](#)
 - obtaining from Cisco [1-x](#)
- syslog message IDs
 - for IOS routers
 - supported for policy lookup from MARS [13-11](#)
 - supported for policy lookup from MARS
 - by firewall devices [13-11](#)
 - unsupported
 - for policy lookup [13-3](#)
 - policy query icon [13-3](#)
- syslog messages
 - accuracy of matches
 - hashcodes [13-17](#)
 - for IPS events
 - absence of sensor ID [13-5](#)
 - for Packet Data events [13-5](#)
- system administrators

- associating with user account
 - for policy lookup from MARS [13-9](#)
- system log messages
 - connection teardown
 - policy lookup, error [13-3](#)
 - deployed rules
 - synchronization with device [13-7](#)
 - generated by access rules
 - unavailable on device [13-5](#)
 - invalid format
 - policy lookup [13-4](#)

T

- technical support (TAC)
 - obtaining [1-x](#)
 - URL for service requests [1-x](#)
- testing
 - connectivity
 - between MARS and Security Manager [13-7, 13-10](#)
- time consumption
 - for policy table lookup
 - number of rules [13-10](#)
 - with Security Manager client open [13-10](#)
- timezone settings
 - certificate errors [5-3](#)
- training, obtaining [1-x](#)
- transparent rules
 - name changes during discovery [6-12](#)
- troubleshooting information
 - generating [1-1](#)
- trusted hosts
 - provisioning [8-3](#)

U

- Unknown Device Event Type
 - custom signatures and [13-10](#)

- Unknown Reporting Devices
 - querying for
 - in MARS [13-12](#)
- URL list
 - applied to wrong SSL VPN context [9-9](#)
- user account
 - creating a separate one
 - for policy lookup [13-7](#)
 - with admin privileges
 - for adding Security Manager to MARS [13-9](#)
- User Configuration page
 - in MARS
 - editing Security Manager credentials [13-7](#)
 - Security Manager credentials disabled [13-7](#)
- user credentials
 - of Security Manager added to MARS
 - in Reporting Applications tab [13-12](#)
 - in the User Configuration page [13-12](#)
 - Reporting Applications tab of MARS
 - different from those in User Configuration page [13-12](#)
 - User Configuration page of MARS
 - authenticating Security Manager [13-12](#)
 - populated from policy query login dialog box [13-12](#)
- user roles
 - in MARS
 - editing Security Manager credentials [13-7](#)
 - modifying Security Manager credentials [13-9](#)

V

- version mismatch, resolving [2-2](#)
- views
 - committed [13-7](#)
 - deployed
 - policy lookup from MARS [13-7](#)
- virtual sensors
 - signature policy lookup

- from MARS events [13-5](#)
- VLAN ACLs (VACLs)
 - supported types [11-2](#)
- VLANs
 - referencing undefined [11-2](#)
- VPN
 - defining multiple CA servers [9-2](#)
 - defining multiple spoke definitions [9-7](#)
 - discovering after configuring [9-5](#)
 - enabling/disabling VRF on Catalyst 6500/7600 [9-5](#)
 - loss of communication with spoke [9-2](#)
 - negated SSL VPN policies [6-6](#)
 - PKI with AAA [9-2](#)
 - SSL VPN limitations [9-8](#)
 - SSL VPN limitations due to OS defects [9-9](#)
 - traffic sent unencrypted [10-3](#)
 - unconfigurable commands when Easy VPN enabled [9-6](#)
 - undiscovered features [6-6](#)
 - unnneeded Easy VPN policies [9-5](#)
 - updating routing processes [9-2](#)
- vpn sessiondb
 - cannot be imported [9-8](#)
- VTY
 - name changes during discovery [6-15](#)

W

- WINS
 - modifying master server [9-9](#)
- Workflow mode
 - policy table lookup
 - editable activities [13-8](#)
 - from MARS events [13-8](#)
 - with Security Manager client active [13-8](#)

