



## **FAQ and Troubleshooting Guide for Cisco Security Manager 3.x**

### **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

Text Part Number: OL-8213-04

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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

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.x*  
© 2007 Cisco Systems, Inc. All rights reserved.



# CONTENTS

<b>Preface</b>	vii
Audience	vii
Conventions	vii
Product Documentation	viii
Obtaining Documentation, Obtaining Support, and Security Guidelines	viii

---

## CHAPTER 1

<b>Security Manager Server</b>	1
Collecting Server Troubleshooting Information	1
Security Manager Database	2
Restoring the Database Using Backed-Up Files	3
Unable to Launch the Security Manager Server	3
Restricting Access to the Security Manager Server	3
Installation, Uninstallation, or Reinstallation	4

---

## CHAPTER 2

<b>Security Manager Client</b>	1
FAQs About the Security Manager Client	1
Resetting the Client Password	2
Using HTTP to Communicate with Server	3
Display Problems in Dual-Screen Setup	3
Unable to Reinstall Client	4
Removing Another User's Locks in Non-Workflow Mode	4
Loading the Online Help	4
Preserving Search Results in Online Help	5
Unable to Display Activity Report	5
Installation, Uninstallation, or Reinstallation	5

---

## CHAPTER 3

<b>Security Manager and Cisco Secure ACS</b>	1
Using Multiple Versions of Security Manager with Same ACS	1
Authentication Fails When in ACS Mode	1
System Administrator Granted Read-Only Access	2
DCR Error When Adding Devices	2
ACS Changes Not Appearing in Security Manager	3

Devices Configured in ACS Not Appearing in Security Manager 3  
 Working in Security Manager after Cisco Secure ACS Becomes Unreachable 3  
 Restoring Access to Cisco Secure ACS 4  
 Authentication Problems with Multihomed Devices 4  
 Updating Device Credentials via Cisco Secure ACS 4

**CHAPTER 4**

**Cisco Security Agent 1**

FAQs About the Cisco Security Agent 1  
 Installation, Uninstallation, or Reinstallation 2

**CHAPTER 5**

**Device Management 1**

FAQs About Device Communication 1  
 FAQs About Device Management 2  
 Changing the Image Version on a Device 3  
     Case 1: Image Version Changes That Do Not Change the Feature Set in Security Manager 3  
     Case 2: Image Version Changes That Change the Feature Set in Security Manager 4  
     Case 3: Security Context and Mode Changes That Change the Feature Set in Security Manager 6  
     Case 4: Device Type or Hardware Model Changes 7  
 Security Certificate Rejected When Discovering Device 9  
 Invalid Certificate Error During Device Discovery 9  
 Adding Routers Running 12.1 or 12.2 from the DCR 9  
 Deleting Config File When Deleting Security Context 10  
 Simultaneous Operations on Same Device 10  
 Troubleshooting the Setup of CNS-Managed Devices 11

**CHAPTER 6**

**Policy Discovery 1**

FAQs About Policy Discovery 1  
 Performing Discovery in Multi-User Environment 5  
 Undiscovered VPN Features 5  
 ACL Names Preserved by Security Manager 6  
     ACL Naming Conventions 6  
     Resolving Conflicts Between Policies 7  
 Resource Names Changed by Security Manager 8  
     Name Changes in PIX/ASA Object Groups 8  
     Name Changes in AAA Rules Policies 9  
     Name Changes in Access Rules Policies 9  
     Name Changes in Inspection Rules Policies 10

Name Changes in Transparent Rules Policies	10
Name Changes in Dynamic NAT Policies	11
Name Changes in Service Policy Rules Policies	12
Name Changes in Dialer Policies	13
Name Changes in PPP Policies	13
Name Changes in AAA Policies	14
Name Changes in HTTP Policies	14
Name Changes in Line Access Policies	15
Name Changes in NAC Policies	16
Name Changes in Quality of Service Policies	17

**CHAPTER 7****Firewall Services 1**

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

**CHAPTER 8****IPS 1**

Adding and Managing IPS Sensors in Security Manager 3.0.1	1
Importing IPS 5.0 Sensors	2
Retrieving Signature Updates	2
Performing IPS Updates	2
Updating IOS IPS Crypto Configurations	4
Creating ACLs During IOS IPS Configuration	4
Performing IOS IPS Deployment	4
Provisioning Trusted Hosts	4
Managing Signature Updates	4

**CHAPTER 9****VPNs 1**

Updating VPNs That Include Routing Processes	1
Loss of Communication with Spoke	2
Configuring PKI with AAA on IOS Devices	2
Defining Multiple CA Servers for Site-to-Site VPNs	2
Unneeded Policy in Easy VPN Topology	3
Discovering a VPN Already Configured in Security Manager	4
Enabling and Disabling VRF on Catalyst 6500/7600 Devices	4
Commands That Cannot be Configured When Easy VPN is Enabled	5
Defining VPNs with Multiple Spoke Definitions	5
SSL VPN Limitations	6
SSL VPN Limitations Due to Device OS Defects	7

Removing Group Policy Attributes from SSL VPNs Defined on ASA 7.x Devices 8

**CHAPTER 10**

**Router Platform Policies 1**

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

**CHAPTER 11**

**Catalyst 6500/7600 Devices 1**

- FAQs about Catalyst 6500/7600 Devices 1
- Migrating from Security Manager 3.0.x to 3.1.x 2
- Discovering Failover Pairs 2
- Deployment Fails for Interface Settings 2

Deployment Fails for Internal VLANs	3
Performing Rollback on Catalyst 6500/7600 Devices	3

---

**CHAPTER 12****Deployment** 1

FAQs About Deployment	1
Performing Rollback When Deploying to a File	14
Mixing Deployment Methods	14
SSL Handshake Failure When Deploying to PIX/ASA Devices	15
Deployment Failures to Devices Managed by AUS	15

---

**INDEX**





## Preface

---

**Revised: October 3rd, 2007, OL-8213-05**

This document contains FAQs and troubleshooting information for Cisco Security Manager 3.x.

## Audience

This document is 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	<b>boldface</b> font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	<code>screen</code> font
Information you enter	<b>boldface screen</b> font
Variables you enter	<i>italic screen</i> font
Menu items and button names	<b>boldface</b> font
Selecting a menu item	<b>Option &gt; Network Preferences</b>

# Product Documentation

Table 1 describes the product documentation that is available. For information on ordering printed documents, see [Obtaining Documentation, Obtaining Support, and Security Guidelines](#), page viii.

**Table 1** Product Documentation

Document Title	Available Formats
<i>Release Notes for Security Manager 3.1</i>	<ul style="list-style-type: none"> <li>On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html">http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html</a></li> </ul>
<i>Installation Guide for Cisco Security Manager 3.1</i>	<ul style="list-style-type: none"> <li>PDF on the product DVD.</li> <li>On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html</a></li> </ul>
<i>User Guide for Cisco Security Manager 3.1</i>	<ul style="list-style-type: none"> <li>PDF on the product DVD.</li> <li>On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html">http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html</a></li> </ul>
<i>Supported Devices and Software Versions for Cisco Security Manager 3.1</i>	<ul style="list-style-type: none"> <li>On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html</a></li> </ul>
<i>User Guide for Auto Update Server 3.0</i>	<ul style="list-style-type: none"> <li>On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html">http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html</a></li> </ul>
User Guide for Cisco IPS Manager 3.0	<ul style="list-style-type: none"> <li>On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html">http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html</a></li> </ul>
Context-sensitive online help	Click the Help button in a window or dialog box.

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>



# 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 1-3](#)
- [Installation, Uninstallation, or Reinstallation, page 1-4](#)

## 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 to 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 > Deployment**, then select the **Enabled Advanced Debugging** 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.

---



### 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"> <li>1. On a client system from which you have established a Security Manager Client session to your server, click <b>Tools &gt; Security Manager Diagnostics</b>.</li> <li>2. Click <b>OK</b> 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).</li> <li>3. Click <b>Close</b> to close the Security Manager Diagnostics dialog box.</li> </ol> <p><b>Note</b> 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"> <li>1. Select <b>Start &gt; Run</b>, then enter <b>command</b>. Alternatively, if your server keyboard includes a Windows key, press <b>Windows-R</b>, then enter <b>command</b>.</li> <li>2. Enter <b>C:\Program Files\CSCOpX\MDC\bin\CSMDiagnostics</b>. Alternatively, to save the ZIP file in a different location than <i>NMSROOT\MDC\etc\</i>, enter <b>CSMDiagnostics drive:\path</b>. For example, CSMDiagnostics D:\temp.</li> </ol>

## Security Manager Database

This procedure describes the steps to take if you are having problems with the Security Manager database or if the database is corrupted.

### 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 information about backing up and restoring databases, see the “Backing Up Data” and “Restoring Data” sections of the *User Guide for CiscoWorks Common Services 3.0*, beginning at:  
  
[http://www.cisco.com/en/US/docs/net\\_mgmt/cisoworks\\_common\\_services\\_software/3.0/user/guide/admin.html#wp257472](http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0/user/guide/admin.html#wp257472)
- 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.

## 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.
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"> <li>1. Open a command line.</li> <li>2. Type <code>C:\Program Files\CSC0px\setup\support\resetCasuser.exe</code>, then press <b>Enter</b>.</li> <li>3. Choose option 1 (Randomly generate casuser password).</li> </ol>

## 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 “[Troubleshooting](#)” in *Installation Guide for Cisco Security Manager 3.0.1* on Cisco.com 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](#)
- [Unable to Reinstall Client, page 2-4](#)
- [Removing Another User's Locks in Non-Workflow Mode, page 2-4](#)
- [Loading the Online Help, page 2-4](#)
- [Preserving Search Results in Online Help, page 2-5](#)
- [Installation, Uninstallation, or Reinstallation, page 2-5](#)
- [Unable to Display Activity Report, page 2-5](#)

## 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.

**Q.** How can I clean up the server list from the Server Name field in the Login window?

**A.** Delete `cmsserver.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. Do not edit the version fields in the client.info file manually.
- 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.

## Resetting the Client Password

**Problem** You cannot remember the password to the Security Manager client that was entered during installation.

**Solution** Reset the password by having an administrator do the following:

- 
- Step 1** On the Security Manager server, shut down the Cisco Security Manager Daemon Manager service.
- Step 2** Navigate to \CSCOp\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.
- 



**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.

---

# 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.

---

## Unable to Reinstall Client

**Problem** When you attempt to install the the Security Manager client (or perform a reinstall, for example, after upgrading the operating system), you receive an error message indicating that the client is already installed and needs to be removed, even though the application does not appear in the list of installed programs.

**Solution** 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\{f427e212-99b0-dd25-4754-c0d2778f-ec4-837992615}
- 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.

---

## 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—Select **Tools > Internet Options > Advanced > Security > Allow active content to run in files on My Computer**.
- Windows XP—Select **Tools > Internet Options > Advanced > Security > Allow active content to run in files on My Computer**.
- Windows 2000—Enable Javascript and disable your popup blockers.

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

- Add the following line to default/prefs/browser-prefs.js:  

```
pref("dom.allow_scripts_to_close_windows", true);
```
- Enable Javascript.

If you use Google Toolbar or any other popup-blocking utility that enables you to allow popups from particular servers, you must configure that utility to allow popups from the \Local Settings\Temp\ subdirectory that Windows associates with your Windows username on the client system. The path to that subdirectory might be, for example, D:\Documents and Settings\*USERNAME*\Local Settings\Temp.

If your popup blocker is not configured in this way, you must temporarily enable all popups. Otherwise, no window opens.

## 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 “[Troubleshooting](#)” in *Installation Guide for Cisco Security Manager 3.0* on Cisco.com 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 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 3-1](#)
- [System Administrator Granted Read-Only Access, page 3-2](#)
- [DCR Error When Adding Devices, 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](#)
- [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 3.0.1 with a Cisco Secure ACS and another part of your organization plans to use Security Manager 3.1 *without* upgrading the existing installation, you must integrate Security Manager 3.1 with a different ACS than the one used for Security Manager 3.0.1.

If you upgrade from Security Manager 3.0.1 to 3.1, you can continue to use the same Cisco Secure ACS. The permission settings will be updated as required.

## Authentication Fails When in ACS Mode

**Problem** 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.

**Solution** 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 Service 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 are using ACS 4.x and 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.

## DCR Error When Adding Devices

**Problem** You get an error message about the DCR when you try to add a device to Security Manager.

**Solution** Do the following:

- Make sure that the System Identity user defined in CiscoWorks Common Services is also defined in Cisco Secure ACS and is granted all privileges. We recommend that you assign this user to the group containing other system administrators.
- (When using network device groups (NDGs)) Click **Group Setup** on the Cisco Secure ACS navigation bar, then verify that the appropriate user role is associated with the correct NDG for *both* CiscoWorks and Cisco Security Manager.

## ACS Changes Not Appearing in Security Manager

**Problem** Changes that you made in the Network Configuration and Group Setup sections of Cisco Secure ACS 3.3.(x) are not appearing in Security Manager.

**Solution** Open Windows Services and restart the Cisco Security Manager Daemon Manager service.



### Note

You do not need to restart the Daemon Manager if you are using ACS 4.0(1) or later. Any changes that you submit in ACS are immediately reflected in Security Manager. For example, if you add a device as a AAA client in ACS, you can immediately go to Security Manager and add that same device without having to close your browsers or clear the cache.

## 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

**Problem** The Cisco Secure ACS becomes unreachable after you have begun working in Security Manager.

**Solution** 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

**Problem** You cannot access Security Manager because the Cisco Secure ACS is down.

**Solution** 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 *User Guide for Cisco Security Manager*. In addition, you must modify the `gatekeeper.cfg` file on the Security Manager server after completing the installation process. For more information, see the [Installation Guide for Cisco Security Manager 3.0](#).

## 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 information, see *Troubleshooting the Standalone Security Agent* and *Cisco Security Agent: Standalone Agent Overview* in the *Installation Guide for Cisco Security Manager 3.1*.

---

## 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 3.1*.

---

- 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 “[Troubleshooting](#)” in *Installation Guide for Cisco Security Manager 3.0.1* on Cisco.com 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 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:

- [FAQs About Device Communication, page 5-1](#)
- [FAQs About Device Management, page 5-2](#)
- [Changing the Image Version on a Device, page 5-3](#)
- [Security Certificate Rejected When Discovering Device, page 5-9](#)
- [Invalid Certificate Error During Device Discovery, page 5-9](#)
- [Adding Routers Running 12.1 or 12.2 from the DCR, page 5-9](#)
- [Deleting Config File When Deleting Security Context, page 5-10](#)
- [Simultaneous Operations on Same Device, page 5-10](#)
- [Troubleshooting the Setup of CNS-Managed Devices, page 5-11](#)

## 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 can't 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 via 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 can't Security Manager connect to a Cisco IOS router after configuration rollback?
- A.** This could occur because of one of the following reasons:

- At rollback, the necessary 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. To resolve this, we recommend that you wait for the device to be reloaded completely, then try to connect to it again.
- The configuration contains nonexistent or unauthorized username and password.

## FAQs About Device Management

This section answers the following questions about device management:

- [Q.How do I configure Security Manager to ignore an error message that is generated by the device?](#)
- [Q.How do I make a device response not tagged with an “Error” prefix appear as an error message?](#)

**Q.** How do I configure Security Manager to ignore an error message that is generated by the device?

**A.** When you try to deploy certain configurations to a device, the message status is “error” even though it is a warning or an informational message. You can choose to ignore such error messages. To ignore error messages, do the following:

1. Select the job with the error message from the Deployment Manager window.
2. Click the **Transcript** button in the Deployment Details tab to open the transcript.
3. Identify the error text that you want to ignore.
4. Go to `...\CSCOPx\MDC\athena\config`.
5. Select **DCS.properties file** to open the DCS properties file.
6. Locate the appropriate warning expressions property.  
For PIX devices, this property is called **dev.pix.warningExpressions**.  
For IOS devices, this property is called **dev.ios.warningExpressions**.
7. Add the error text you identified in step 3 to the warning expressions list.



---

**Note** The warning message should be a generic regular expression string. Except for the last expression, you must limit all expressions with “\$”.

---

8. Restart the CiscoWorks Daemon Manager.

**Q.** How do I make a device response not tagged with an “Error” prefix appear as an error message?

**A.** Do the following:

1. Make a generic regular expression string for the device response that you want to treat as an error message.
2. Go to `...\CSCOPx\MDC\athena\config\DCS.properties file` to open the DCS properties file.
3. Locate the appropriate error expressions property.  
For PIX devices, this property is called, **dev.pix.ErrorExpressions**.  
For IOS devices, this property is called, **dev.pix.ErrorExpression**.
4. Add the error text you identified in step 1 to the error expressions list.



**Note** The error message should be a generic regular expression string. Except for the last expression, you must limit all expressions with “\$”.

5. Restart the CiscoWorks Daemon Manager.

## Changing the Image Version on a Device

You must use caution when changing the image version of a device managed by Security Manager or when modifying the security context or operational mode of FWSM and ASA devices. In certain cases, these changes enable a different set of features for the device. As a result, some of the policies that you configured for the device in Security Manager might no longer apply.

The key device changes, their effect on the policies available in Security Manager, and the procedure you should follow to implement these device changes, are described in the following sections:

- [Case 1: Image Version Changes That Do Not Change the Feature Set in Security Manager, page 5-3](#)
- [Case 2: Image Version Changes That Change the Feature Set in Security Manager, page 5-4](#)
- [Case 3: Security Context and Mode Changes That Change the Feature Set in Security Manager, page 5-6](#)
- [Case 4: Device Type or Hardware Model Changes, page 5-7](#)

### Case 1: Image Version Changes That Do Not Change the Feature Set in Security Manager

The following image version changes *do not* affect the types of policies available for that device in Security Manager:

- Upgrading from any Cisco IOS version supported by Security Manager to any other Cisco IOS version supported by Security Manager.
- Upgrading from any PIX 6.x image to another PIX 6.x image.
- Upgrading from any PIX 7.x image to another PIX 7.x image, retaining the same security context and mode configuration.
- Upgrading from any ASA 7.x image to another ASA 7.x image, retaining the same security context and mode configuration.
- Upgrading from any FWSM 2.x image to another 2.x FWSM image, retaining the same security context and mode configuration.
- Upgrading a Catalyst 6500/7600 chassis from any IOS 12.x image to another IOS 12.x image.
- Upgrading from IPS 4.x to IPS 5.x or downgrading from IPS 5.x to IPS 4.x.



**Note**

This list applies only to images that are supported by Security Manager. For a list of supported images, see [Supported Devices and Software Versions for Cisco Security Manager 3.0.1](#).

In all of these cases, change the image version as follows:

#### Procedure

- 
- Step 1** Upgrade the image version on the device.
- Step 2** Select **Tools > Device Properties** in Security Manager, then update the target OS version.
- Step 3** Click **Save**.
- 

#### Related Topics

- [Changing the Image Version on a Device, page 5-3](#)

## Case 2: Image Version Changes That Change the Feature Set in Security Manager

The following image version changes *do* affect the types of policies available for that device in Security Manager:

- Upgrading from a PIX 6.x to a PIX 7.x image.
- Downgrading from a PIX 7.x image to a PIX 6.x image.
- Upgrading from a FWSM 2.x image to a FWSM 3.x image.
- Downgrading from a FWSM 3.x image to a FWSM 2.x image.
- Upgrading from an IOS 12.1 or 12.2 image to an IOS 12.3 or 12.4 image.
- Downgrading from an IOS 12.3 or 12.4 image to an IOS 12.1 or 12.2 image.



#### Note

FWSM 3.x is supported in Security Manager 3.0.1 only. It is not supported in Security Manager 3.0.

Security Manager prevents you from changing the target OS version of a managed device to a version that changes the types of policies that are available for that device. Therefore, you must first delete the device from Security Manager, perform the image change, then add the device back.

Certain types of policies, such as access rules, are not affected by changes in image version or changes in platform type. We recommend, therefore, that you share the policies configured on your device before you remove it from Security Manager. This provides a useful method for reassigning the policies to the device (with any inheritance and policy object references intact) after you add it back to Security Manager.

#### Procedure

- 
- Step 1** Submit and deploy all the changes you configured for the device in Security Manager. This ensures that the desired configuration is on the device before the image upgrade.
- Step 2** Share the local policies defined on the device:
- Right-click the device in the Device selector, then select **Share Device Policies**. By default, all policies configured on the device (local and shared) are selected for sharing in the Share Policies wizard.



## Case 3: Security Context and Mode Changes That Change the Feature Set in Security Manager

Changes that you make to the security context and operational mode settings on a FWSM or ASA device enable a different set of features on that device. These changes occur if you change the device from:

- Single context to multi-context (or vice-versa).
- Routed mode to transparent mode (or vice-versa).

Security Manager prevents you from changing the security context or operational mode settings of a managed device. Therefore, you must first delete the device from Security Manager, change the context or mode, then add the device back.

Certain policy types (for example, Banner, Clock, Console Timeout, and HTTP) are not affected by changes in operational mode. Other policy types (for example, ICMP, SSH, and TFTP, in addition to Banner and Clock) are not affected by changes in security context settings. We recommend, therefore, that you share the policies configured on your device before you remove it from Security Manager. This provides a useful method for reassigning the policies to the device (with any inheritance and policy object references intact) after you add it back to Security Manager.

### Procedure

- 
- Step 1** Submit and deploy all the changes you configured for the device in Security Manager. This ensures that the desired configuration is on the device before the image upgrade.
- Step 2** Share the local policies defined on the device:
- a. Right-click the device in the Device selector, then select **Share Device Policies**. By default, all policies configured on the device (local and shared) are selected for sharing in the Share Policies wizard.
  - b. Deselect the check box next to each existing shared policy, as indicated by the hand in the policy icon. You should do this because there is no need to create a copy of the shared policies that already exist; you will reassign the existing shared policies after the image version upgrade.
  - c. Enter a name for the shared policies. We recommend using the device name as a convenient means of identification. For example, if the device name is MyRouter, each shared policy is given the name MyRouter.
  - d. Click **Finish**. The selected local policies become shared policies.
- Step 3** Delete the device from Security Manager. We recommend that you delete the device from the DCR also, unless you plan to manage the device in another CiscoWorks application, such as RME.
- Step 4** Change the operational mode or the context settings on the device.
- Step 5** Add the device back to Security Manager and perform policy discovery. If you did *not* delete the device from the DCR in step 3, use the Add Device from DCR option to bring it back into Security Manager.
- Step 6** Reassign the policies to the device:
- a. Right-click the first policy type displayed in the Device Policies selector, then select **Assign Shared Policy**.
  - b. In the Assign Shared Policy dialog box, do one of the following:
    - If a local policy was previously defined on the device, select the shared policy defined in step 2, then click **OK**. Proceed with step c.

- If a shared policy of this type was previously assigned to the device, select it, then click **OK**. Proceed with step **d**.
  - c.** (Local policies only) Right-click the policy type again in the Device Policies selector, then select **Unshare Policy**.
  - d.** Repeat steps **a** through **c** for each policy type that is relevant to the device's configuration. If a shared policy is not available, this indicates that this is a policy type that was not available for the previous image version.
- Step 7** (Optional) Delete the policies created in step **2** from Policy view:
- a.** Select **View > Policy View** or click the **Policy View** icon on the toolbar.
  - b.** Starting from the top of the Policy Type selector, select a policy type, then examine the list of policies of that type displayed in the Shared Policy selector. If you see a policy with the name you assigned in step **2**, click the **Assignments** tab in the work area to verify that the policy is not assigned to any devices.
  - c.** Click the **Delete Policy** button beneath the Shared Policy selector to delete the policy.
  - d.** Repeat steps **a** through **c** for each policy type that is relevant to the device's configuration.
- 

#### Related Topics

- [Changing the Image Version on a Device, page 5-3](#)

## Case 4: Device Type or Hardware Model Changes

In some cases, you might replace a particular device but retain the original contact information, for example:

- Replacing a PIX firewall with a Cisco IOS router.
- Replacing a PIX 7.x device with an ASA device.
- Replacing a Cisco IOS router with a firewall device.

In all of these cases, the new device changes the types of policies available for that device in Security Manager. Security Manager prevents you from modifying the hardware model of an existing device. In addition, we do not recommend that you change the device type in the DCR. Therefore, you must first delete the device from Security Manager, change the physical device, then add the device back.

Certain policy types (for example, access rules) are not affected by changes in device type. We recommend, therefore, that you share the policies configured on your device before you remove it from Security Manager. This provides a useful method for reassigning the policies to the device (with any inheritance and policy object references intact) after you add it back to Security Manager.

#### Procedure

---

- Step 1** Submit and deploy all the changes you configured for the device in Security Manager. This ensures that the desired configuration is on the device before the image upgrade.
- Step 2** Share the local policies defined on the device:
- a.** Right-click the device in the Device selector, then select **Share Device Policies**. By default, all policies configured on the device (local and shared) are selected for sharing in the Share Policies wizard.

- b. Deselect the check box next to each existing shared policy, as indicated by the hand in the policy icon. You should do this because there is no need to create a copy of the shared policies that already exist; you will reassign the existing shared policies after the image version upgrade.
  - c. Enter a name for the shared policies. We recommend using the device name as a convenient means of identification. For example, if the device name is MyRouter, each shared policy is given the name MyRouter.
  - d. Click **Finish**. The selected local policies become shared policies.
- Step 3** Delete the device from Security Manager. We recommend that you delete the device from the DCR also, unless you plan to manage the device in another CiscoWorks application, such as RME.
- Step 4** Replace the device.
- Step 5** Add the device back to Security Manager and perform policy discovery. If you did *not* delete the device from the DCR in step 3, use the Add Device from DCR option to bring it back into Security Manager.
- Step 6** Reassign the policies to the device:
- a. Right-click the first policy type displayed in the Device Policies selector, then select **Assign Shared Policy**.
  - b. In the Assign Shared Policy dialog box, do one of the following:
    - If a local policy was previously defined on the device, select the shared policy defined in step 2, then click **OK**. Proceed with step c.
    - If a shared policy of this type was previously assigned to the device, select it, then click **OK**. Proceed with step d.
  - c. (Local policies only) Right-click the policy type again in the Device Policies selector, then select **Unshare Policy**.
  - d. Repeat steps a through c for each policy type that is relevant to the device's configuration. If a shared policy is not available, this indicates that this is a policy type that was not available for the previous image version.
- Step 7** (Optional) Delete the policies created in step 2 from Policy view:
- a. Select **View > Policy View** or click the **Policy View** icon on the toolbar.
  - b. Starting from the top of the Policy Type selector, select a policy type, then examine the list of policies of that type displayed in the Shared Policy selector. If you see a policy with the name you assigned in step 2, click the **Assignments** tab in the work area to verify that the policy is not assigned to any devices.
  - c. Click the **Delete Policy** button beneath the Shared Policy selector to delete the policy.
  - d. Repeat steps a through c for each policy type that is relevant to the device's configuration.

---

#### Related Topics

- [Changing the Image Version on a Device, page 5-3](#)

## Security Certificate Rejected When Discovering Device

**Problem** An error occurs when you attempt to discover a device. The error message states that the security certificate received from the device was rejected.

**Solution** Manually enter the thumbprint required by the certificate by doing *one* of the following:

- Go to **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, then 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 DCR options.

## 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 is unable to validate the device certificate as the start time of the validity period is ahead of the Security Manager time setting. Even if the timezones 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 timezone 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 timezone on the device and Security Manager, and modify the timezone after you discover the certificates at a later time, if necessary.

## Adding Routers Running 12.1 or 12.2 from the DCR

**Problem** You cannot add a router running IOS Software Release 12.1 or 12.2 from the DCR.

**Solution** Security Manager uses Telnet as the transport protocol for communicating with routers running IOS 12.1 or 12.2. Security Manager uses SSL and SSH as the transport protocol for routers running IOS 12.3 and later. When you add a live device using the Add Device From Network option, you can specify that the device is running IOS 12.1 or 12.2, which enables Security Manager to select the appropriate transport protocol (Telnet). However, when you add a device from the DCR, Security Manager automatically selects the default transport protocol for routers running IOS 12.3 or later. As a result, Security Manager cannot communicate with the device and the operation fails. This behavior is described in bug [CSCsg74138](#).

The workaround requires you to temporarily change the default transport protocol for routers running IOS 12.3 or later, as described in the following procedure.

**Procedure**

- 
- Step 1** Change the default transport protocol:
- Select **Tools > Security Manager Administration > Device Communication**.
  - In the Transport Protocol (IOS Routers 12.3 and above) field, change the protocol from HTTPS to Telnet, then click **Save**.
  - Click **Close** to return to the main Security Manager window.
- Step 2** Add the router that is running IOS 12.1 or 12.2:
- Click the **New Device** button above the Device selector. The New Device wizard is displayed.
  - Select **Add Device from DCR**, then complete the steps outlined in the wizard.
- Step 3** Restore the default transport protocol to its original setting:
- Select **Tools > Security Manager Administration > Device Communication**.
  - In the Transport Protocol (IOS Routers 12.3 and above) field, change the protocol back from Telnet to HTTPS, then click **Save**.
  - Click **Close** to return to the main Security Manager window.

**Note**

For more information about the policies supported on routers running IOS 12.1 or 12.2, see [Configuring Routers Running IOS Software Releases 12.1 and 12.2, page 10-1](#).

---

## Deleting Config File When Deleting Security Context

**Problem** Deleting a security context from a 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 (as described in CSCsg20999) and is not connected to the behavior of Security Manager. The current workaround is to use the CLI to delete the configuration file from the device.

## Simultaneous Operations on 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 since 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 CNS-Managed Devices

The following topics describe issues that might arise when you set up a device managed by a Cisco Networking Services (CNS) server and how to solve them:

- [Q. Why do I receive an InvalidParameterException when I click on an IOS device on the CNS 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 CNS-managed PIX device not working?](#)
  - [Q. Why was I able to deploy successfully to a CNS-managed PIX device the first time, but subsequent deployments were unsuccessful?](#)
  - [Q. How do I debug CNS on a PIX device?](#)
  - [Q. How do I debug CNS on an IOS device?](#)
  - [Q. Why did I fail to discover an IOS device and acquire its configuration via CNS?](#)
  - [Q. Why doesn't the event mode router appear on the CNS Discover Device page or appear in green on the CNS web page?](#)
- Q.** Why do I receive an InvalidParameterException when I click on an IOS device on the CNS web page?
- A.** This is the expected behavior. For IOS devices, Security Manager uses deployment jobs to deploy configurations to CNS 1.5 and 2.0, instead of associating a configuration to the IOS device in CNS. Therefore, you do not see an associated configuration when you click the device name on the CNS web page. For PIX devices, Security Manager associates the configuration to the device in CNS. 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 CNS. 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 CNS.
- 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 CNS device id defined in the Device Properties window in Security Manager matches the CNS device id configured on the router (using the **cns id string** command).
- Call home mode setup—The device is not connected to CNS in this mode; therefore, all Security Manager operations that require the retrieval of the device configuration via CNS are not supported. This includes discovery, preview configuration, display running config, and connectivity tests (and rollback, for IOS devices).

**Q.** Why is deployment to my CNS-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 CNS 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 CNS server for the same PIX device and did not delete the PIX from the CNS server before you started the current task, it is possible that the PIX device received the previous configuration from the CNS server before you deployed the new configuration to it.
- If none of the suggestions above solves the problem, turn on CNS debug mode (see [Q.How do I debug CNS 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 CNS-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 CNS 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 3.1 does not support this command directly. As a result, even though the command was discovered, it does not appear in the full configuration.




---

**Note** For more information, see TAC case [CSCsa73337](#).

---

**Q.** How do I debug CNS 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 CNS server.

---

**Q.** How do I debug CNS 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 CNS server. When working in call home mode, check the config server log on the CNS server.

**Q.** Why did I fail to discover an IOS device and acquire its configuration via CNS?

**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 rror-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 host name> <cns ip>**”.

**Q.** Why doesn't the event mode router appear on the CNS Discover Device page or appear in green on the CNS web page?

**A.** Check the following:

- Make sure that the router and the CNS server can ping each other.
- Clear the **cns event** command, then re-enter it without specifying a port number.





## CHAPTER 6

# Policy Discovery

---

This chapter contains the following topic:

- [FAQs About Policy Discovery, page 6-1](#)
- [Performing Discovery in Multi-User Environment, page 6-5](#)
- [Undiscovered VPN Features, page 6-5](#)
- [ACL Names Preserved by Security Manager, page 6-6](#)
- [Resource Names Changed by Security Manager, page 6-8](#)

## 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?](#)
- [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 6500 switches and 7600 routers 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.Can I import policies from my existing VPN/Security Management Suite (VMS) 2.x products into Security Manager?
  - 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 via 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?
- A.** In the task status window, go to the Message Summary section, then select **Commands Not Discovered**. Any undiscovered commands are listed in the Description field.
- 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 (offline).

- 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/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. (For quick results, access the online help and use the search function to find this topic.) 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 6-8](#). 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.
- 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 specific 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 6500 switches and 7600 routers 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.
- 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.** Can I import policies from my existing VPN/Security Management Suite (VMS) 2.x products into Security Manager?
- A.** No, you cannot. Instead, add the devices that you were managing with VMS into Security Manager and run policy discovery on them to add their policies to Security Manager.
- 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 (if-needed, local-case, if-authenticated, krb5-telnet). 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 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.

## Undiscovered VPN Features

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

- SSL VPN
- 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 6-8](#).

**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 9-8](#).

## ACL Names Preserved by Security Manager

Security Manager provides the option to preserve the following types of ACL names:

- Access lists (PIX/ASA and IOS)
- Translation ACLs (PIX/ASA)
- AAA ACLs (PIX/ASA)

Security Manager can preserve the ACL names configured on a device in the following circumstances:

- If the ACL name is specified in Security Manager.
- 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.

**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. Beginning with Security Manager 3.1, 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.

## ACL Naming Conventions

All newly created ACLs are given a name by Security Manager based on the naming conventions shown in [Table 6-1](#).

**Table 6-1** *ACL Naming Conventions*

Policy Type	Naming Convention
Access ACLs	<ul style="list-style-type: none"> <li>• Inbound: CSM_FW_ACL_InterfaceName</li> <li>• Outbound: CSM_FW_ACL_OUT_InterfaceName</li> </ul>
NAT0 ACLs	<ul style="list-style-type: none"> <li>• Inbound: CSM_nat0_InterfaceName_in</li> <li>• Outbound: CSM_nat0_InterfaceName</li> </ul>

**Table 6-1** ACL Naming Conventions (continued)

Policy Type	Naming Convention
NAT ACLs	<ul style="list-style-type: none"> <li>Inbound: CSM_nat_InterfaceName_poolID_in</li> <li>Outbound: CSM_nat_InterfaceName_poolID</li> </ul> <p><b>Note</b> 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>
Policy Static ACLs	<ul style="list-style-type: none"> <li>For PIX 6.3(x) devices: <ul style="list-style-type: none"> <li>For IP: CSM_static_globalIP_LocalInterfaceName_globalInterfaceName</li> <li>For other protocols: CSM_static_globalIP_LocalInterfaceName_globalInterfaceName_protocol_globalPort</li> </ul> </li> <li>For devices running other OS versions, the localIP is added: <ul style="list-style-type: none"> <li>For IP: CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName</li> <li>For other protocols: CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName_protocol_globalPort</li> </ul> </li> </ul>
AAA ACLs	CSM_AAA_{AUTHO   ATHEN   ACCT}_InterfaceName_ServerTag

**Related Topics**

- [ACL Names Preserved by Security Manager, page 6-6](#)

## Resolving Conflicts Between Policies

If the 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 policy 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.

**Related Topics**

- [ACL Names Preserved by Security Manager, page 6-6](#)

# 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 6-8](#)
- [Name Changes in AAA Rules Policies, page 6-9](#)
- [Name Changes in Access Rules Policies, page 6-9](#)
- [Name Changes in Inspection Rules Policies, page 6-10](#)
- [Name Changes in Transparent Rules Policies, page 6-10](#)
- [Name Changes in Dynamic NAT Policies, page 6-11](#)
- [Name Changes in Service Policy Rules Policies, page 6-12](#)
- [Name Changes in Dialer Policies, page 6-13](#)
- [Name Changes in PPP Policies, page 6-13](#)
- [Name Changes in AAA Policies, page 6-14](#)
- [Name Changes in HTTP Policies, page 6-14](#)
- [Name Changes in Line Access Policies, page 6-15](#)
- [Name Changes in NAC Policies, page 6-16](#)
- [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 3.1*.



Tip

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

## 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].

### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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
```



Note

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.

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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 a new 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 a new 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
```

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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.

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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	svcmap	(Globally applied rules) CSM_POLICY_MAP_GLOBAL_0  (Rules applied to specific interface) CSM_POLICY_MAP_[INTERFACE_N AME]

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 a new 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.

### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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 new policy in Security Manager. The following keywords are unsupported:

- Authentication: if-needed, local-case
- Network authorization: if-authenticated

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
<b>Global configuration commands</b>	
aaa authentication ppp <i>list-name</i>	CSM_PPP_AUTHENTICATION_#
aaa authorization network <i>list-name</i>	CSM_PPP_AUTHORIZATION_#
<b>Interface configuration commands</b>	
ppp authentication <i>protocols list-name</i>	CSM_PPP_AUTHENTICATION_#
ppp authorization <i>list-name</i>	CSM_PPP_AUTHORIZATION_#

For example, if the device contains:

```
aaa authentication ppp My_Auth_List group tacacs+ local-case
```

Security Manager cannot discover the command because of the unsupported keyword (local-case). If you create a PPP policy with an equivalent AAA authentication definition, the following CLI command is deployed:

```
aaa authentication ppp CSM_PPP_AUTHENTICATION_1 group tacacs+
interface Serial0/1
    ppp authentication chap callIn callout callback optional CSM_PPP_AUTHENTICATION_1
```

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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.

However, there are certain keywords that are unsupported in Security Manager:

- krb5-telnet
- local-case
- if-authenticated

If you try to discover a method list containing any of these unsupported keywords, 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.

For example, if the device contains:

```
aaa authorization exec default group tacacs+ local if-authenticated
```

Security Manager will not discover this command. If you then configure an authorization method list in the AAA policy that uses the same methods, the following command is deployed to replace the original command:

```
aaa authorization exec default group tacacs+ local
```

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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 (krb5-telnet, local-case, if-authenticated), the method list is not discovered. Instead, Security Manager creates a new method list using the naming format: CSM\_HTTP\_AAA\_1.

For example, if the device contains:

```
aaa authorization exec my_list group tacacs+ local if-authenticated
```

And the HTTP policy in Security Manager uses the default AAA method list for EXEC authorization, the following CLI commands are deployed:

```
aaa authorization exec CSM_HTTP_AAA_1 group tacacs+ local
ip http authentication aaa exec-authorization CSM_HTTP_AAA_1
```

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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.

However, if the AAA configuration on the device contains an unsupported keyword (krb5-telnet, local-case, if-authenticated), the method list is not discovered. Instead, you must create a new 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
<b>Global configuration commands</b>		
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_#
<b>Line configuration commands</b>		
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_#

**Table 6-8** Line Access Resource Naming Conventions (continued)

Resource	Naming Convention for VTY	Naming Convention for Console
accounting connection <i>list-name</i>	CSM_VTY_CONN_ACCOUNTING_ G_#	CSM_CON_CONN_ACCOUNTING_ NG_#
accounting commands <i>level</i> <i>list-name</i>	CSM_VTY_COMM_ACCOUNTING_ NG_#	CSM_CON_COMM_ACCOUNTING_ NG_#

For example, if the device contains:

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

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
```

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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.

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)

## 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

#### 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.

```
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
```

As can be seen in this 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.

#### Related Topics

- [Resource Names Changed by Security Manager, page 6-8](#)





# CHAPTER 7

## Firewall Services

---

This chapter contains the following topics:

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

### FAQs About Firewall Services

This section answers the following questions about firewall services:

- [Q. Why doesn't the Hit Count report show all ACEs that are discovered for my FWSM devices?](#)
- [Q. Why do I lose my connection after I deploy my firewall rules to an IOS device?](#)
- [Q. Why doesn't the Hit Count report 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't I deploy my policies with the BGP routing protocol to IOS devices?](#)
- [Q. Why is an ACE removed from the ACL even though it is bound to the interface?, page 7-2](#)
- [Q. Why am I getting a validation error during the discovery of my transparent firewall rules?, page 7-2](#)
- [Q. Why are my commands supporting GTP Map policies dropped during discovery?, page 7-2](#)
- [Q. How do I create an ACL 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 without going to the device to configure it?](#)
- [Q. Why is the OK button missing on the Combined Rules Results Summary page?](#)
- [Q. Why do I get an error when I try to create a service group from the cell contents of an access rule or AAA rule?](#)

**Q.** Why doesn't the Hit Count report show all ACEs that are discovered for my FWSM devices?

**A.** When you run a **show access-list** command in PIX 6.3 and 7.0 devices, all object groups in the ACE are expanded; however, FWSM does not expand object groups when listing access rules if the Object Group Search feature is enabled. If you discover the device, then request a Hit Count report, the report results are not accurate.

**Q.** Why do I lose my connection after I deploy my firewall rules to an IOS 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 IOS 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 ACLs contain a global rule that permits Security Manager to access the device.
- Q.** Why doesn't the Hit Count report show standard ACLs for my IOS device?
- A.** IOS devices use standard ACLs for filtering, which are not recognized when Hit Count reports are generated. After you deploy to the device, standard ACLs are replaced by extended ACLs and the results are displayed in the Hit Count report.
- 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 authentication proxy from the device in Security Manager. If you do not plan to run the web server on the IOS device, you can manually remove the CLI or create a FlexConfig object to remove the CLI from the devices.
- Q.** Why can't I deploy my policies with the BGP routing protocol to IOS devices?
- 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 ACL with ACEs having 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.** Why am I getting a validation error during the discovery of my transparent firewall rules?
- A.** When you configure transparent firewall on IOS devices, only one bridge group is supported. Bridge Group 1 is dedicated to transparent firewall. If you use Bridge Group 1 for something else, and only one interface exists for that group, a validation error results upon discovery.
- Q.** Why are my commands supporting GTP Map policies dropped during discovery?
- A.** GTP Map in Security Manager 3.0.x does not support the permit response subcommand that was introduced in later versions of the PIX OS software. The permit response subcommand from GTP Map CLI in PIX 7.0(4) and later is dropped during the discovery process and is not deployed when you deploy the GTP Map to the device. You can create a FlexConfig that will insert the needed permit response CLI for the desired GTP Map in the deployed configuration.



---

**Note** The permit response subcommand is supported in Security Manager 3.1.x.

---

- Q.** How do I create an ACL 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 ACLs. The first ACL should define those addresses that you want to deny. You can create a network/host object for that purpose. The second ACL, 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 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 via the system context. The management IP is now configured on the device.
- Step 4** In the Device selector, right-click the security context, then 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.
- 

**Q.** Why is the OK button missing on the Combined Rules Results Summary page?

- A.** The OK button is not displayed under the following circumstances:
- If you have read-only permissions.
  - If you selected an inherited policy in Device view.

In both cases, the Combined Rules Results Summary displays a preview of what the rules would look like after they are combined, but without the OK button you cannot implement the changes.

To save the changes displayed on the Combine Rules page, you must use an account that has the necessary permissions for modifying policies. For more information, see "Setting Up User Permissions" in the *User Guide for Cisco Security Manager*. When you are working with an inherited policy, run the Combine Rules option from Policy view instead of from Device view.

- Q.** Why do I get an error when I try to create a service group from the cell contents of an access rule or AAA rule?
- A.** You cannot create a service group from a cell that contains a nameless service (that is, a service that you defined directly in the cell, such as tcp/10 or udp/20/30, rather than selecting a service object). First, you must create a service object from each nameless service. Then you can create a service group from the individual services.





# CHAPTER 8

## IPS

---

This chapter contains the following topics:

- [Adding and Managing IPS Sensors in Security Manager 3.0.1, page 8-1](#)
- [Importing IPS 5.0 Sensors, page 8-2](#)
- [Retrieving Signature Updates, page 8-2](#)
- [Performing IPS Updates, page 8-2](#)
- [Updating IOS IPS Crypto Configurations, page 8-4](#)
- [Creating ACLs During IOS IPS Configuration, page 8-4](#)
- [Performing IOS IPS Deployment, page 8-4](#)
- [Provisioning Trusted Hosts, page 8-4](#)
- [Managing Signature Updates, page 8-4](#)



**Note**

---

Unless marked otherwise, all the troubleshooting information contained in this chapter is relevant to Cisco Security Manager 3.1.

---

## Adding and Managing IPS Sensors in Security Manager 3.0.1

**Problem** You cannot add IPS sensors to Security Manager 3.0.1.

**Solution** Although sensors are managed with the CiscoWorks Management Center for IPS Sensors (IPS Management Center) when using Security Manager 3.0.1, you cannot add devices directly to the IPS Management Center. Instead, you must first add the device to Security Manager, then perform a re-import from the IPS Management Center. Perform the procedure described below.

### Procedure

- 
- Step 1** In Security Manager, select **File > New Device**, then select one of the following options in the New Device wizard:
- Add New Device (Select **Device Type > Security and VPN > Cisco IPS 4200 Series Sensors** to select the appropriate sensor.)
  - Add Device from DCR (if the device is already configured in the DCR)

You cannot use the Add Device from Network or Add from Configuration File options.

- Step 2** Select **Tools > IPS Manager** to launch the IPS Management Center. When using Security Manager 3.0.1, you must use the IPS Management Center to manage IPS sensors.
- Step 3** Select **Devices > Sensor**.
- Step 4** Select the IPS sensor that you added in Step 1, then click **Re-Import**. You can now manage the sensor.

**Note**

- Primary credentials are mandatory when adding IPS devices. SDEE credentials are optional when adding IOS IPS devices.
- Devices are added automatically to the Global sensor group in the IPS Management Center. You can assign the devices to other groups, if required. The sensor groups in the IPS Management Center are not related to the device groups defined in Security Manager.
- In Security Manager 3.1, you can add an IPS sensor using any of the methods available in the New Device wizard. In addition, you can use Security Manager to manage the sensor.

## Importing IPS 5.0 Sensors

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

**Solution** Security Manager 3.1 supports IPS 5.1, IPS 6.0, 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.

## 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 that you are managing with IPS Manager.

The following procedures describes how to identify an NTP server.

**Caution**

If your sensors already have an NTP server configuration (including a configuration performed outside of IPS Manager), 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.

---

### Procedure When Using Security Manager 3.0.1

---

- Step 1** In IPS Manager, select **Configuration > Settings**.
- Step 2** In the TOC, click the **Object Selector** handle.
- Step 3** In the Object Selector, select the sensor or group for which you want to identify an NTP server. We recommend selecting the Global group.  
The Object Selector closes.
- Step 4** In the TOC, select **NTP Server**.  
The NTP Server page appears, and the Object bar displays the sensor or group that you selected.
- Step 5** In the Server IP field, enter the IP address of the NTP server.
- Step 6** In the Key field, enter the key value of the NTP server.
- Step 7** In the Key ID field, enter the key ID value of the NTP server. Valid values are 1 through 4294967295.  
The Mandatory check box is present if you selected a group in Step 3. Select the **Mandatory** check box to apply these settings to all objects in the group and in all subgroups. Otherwise, objects in this group and in all subgroups will override the settings of this group.

### Procedure When Using Security Manager 3.1

---

- 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.
- Step 6** Click **Save** to save your definitions to the Security Manager server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---



---

**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 IPS 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 IPS 6.0.







## CHAPTER 9

# VPNs

---

This chapter contains the following topics:

- [Updating VPNs That Include Routing Processes, page 9-1](#)
- [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 9-3](#)
- [Discovering a VPN Already Configured in Security Manager, page 9-4](#)
- [Enabling and Disabling VRF on Catalyst 6500/7600 Devices, page 9-4](#)
- [Commands That Cannot be Configured When Easy VPN is Enabled, page 9-5](#)
- [Defining VPNs with Multiple Spoke Definitions, page 9-5](#)
- [SSL VPN Limitations, page 9-6](#)
- [SSL VPN Limitations Due to Device OS Defects, page 9-7](#)
- [Removing Group Policy Attributes from SSL VPNs Defined on ASA 7.x Devices, page 9-8](#)



**Note**

For information about VPN features that are not discovered by Security Manager, see [Undiscovered VPN Features, page 6-5](#).

---

## 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 of the 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:
- Via the Public Key Infrastructure policy—Click the **Add** button beneath the Selected field. See *Configuring Public Key Infrastructure Policies*.
  - Via 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:
- Via 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*.
  - Via 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 6500/7600 Devices

**Problem** Deployment fails when you change the virtual routing and forwarding (VRF) mode on the Catalyst 6500/7600 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:
- Select **View > Policy View**.
  - Right-click **FlexConfigs** in the Policy Type selector, then select **New FlexConfigs Policy**.
  - 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:
- In the work area of Policy view, click the **Add** button on the Details tab.
  - In the FlexConfigs Selector, click the **Create** button in the lower-left corner of the window. The FlexConfig dialog box is displayed.
  - 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
```
  - 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 3.1*:

- *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.
- Bear in mind that 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:

- ASA deployment with AUS fails with images that support SSL VPN (including 7.1, 7.2.2, and 7.3) when you configure the **auto-signon** command. This command causes the security appliance to pass SSL VPN user login credentials on to internal servers. For more information, see [CSCsh91913](#).
- 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. 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. 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. The workaround is 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 and until 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) 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 the 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 define an SSL user groups policy to compensate for the fact that it was not defined as a result of the discovery process.



# CHAPTER 10

## Router Platform Policies

---

This chapter describes how to troubleshoot common problems that may 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](#)

## Configuring Routers Running IOS Software Releases 12.1 and 12.2

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

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

All other policies require Cisco IOS Software Release 12.3 or higher. For more information, see [Supported Devices and Software Versions for Cisco Security Manager 3.1](#).

# 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 may 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 may occur when you configure NAT policies on Cisco IOS routers in Security Manager:

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

## VPN Traffic Sent Unencrypted

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

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



### Note

This option can be used only on site-to-site VPNs. For remote access VPNs, you need to create an ACL object that explicitly denies the flow containing VPN traffic and define this ACL as part of a dynamic rule in the NAT policy. For more information, see *Defining Dynamic NAT Rules* in the *User Guide for Cisco Security Manager 3.1*.

## Loss of Communication Between Security Manager and Device

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

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

## Discovering Dynamic NAT Rules Containing Route Maps

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

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

## Troubleshooting DSL Policies

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

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

## Unable to Deploy PVC Policy

**Problem** Deployment fails for your PVC policy.

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

## Unable to Deploy IP Protocol Mappings

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

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

## Troubleshooting Device Access Policies

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

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

## Selected Traps Not Being Sent by Device

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

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

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

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, go to:

[http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc\\_monitor\\_maint\\_ps6350\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_monitor_maint_ps6350_TSD_Products_Configuration_Guide_Chapter.html)

You can also use FlexConfigs to fully configure these traps.

## Removing SNMP Traps Unintentionally from Device

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

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

# Troubleshooting NAC Policies

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

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

## NAC Not Implemented on Router

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

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

## Deployment of NAC Policy Fails

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

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

## Troubleshooting Static Routing Policies

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

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

## Floating Route Not Inserted When Static Route Used as Backup

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

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

[http://www.cisco.com/en/US/tech/tk365/technologies\\_tech\\_note09186a00800ef7b2.shtml](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800ef7b2.shtml)

## Deployment Fails After Database Upgrade

**Problem** Deployment and preview configuration fail for static routing policies after you upgrade to Security Manager 3.1.

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



### Note

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





# CHAPTER 11

## Catalyst 6500/7600 Devices

---

This chapter contains the following topics:

- [FAQs about Catalyst 6500/7600 Devices, page 11-1](#)
- [Migrating from Security Manager 3.0.x to 3.1.x, page 11-2](#)
- [Discovering Failover Pairs, page 11-2](#)
- [Deployment Fails for Interface Settings, page 11-2](#)
- [Deployment Fails for Internal VLANs, page 11-3](#)
- [Performing Rollback on Catalyst 6500/7600 Devices, page 11-3](#)

## FAQs about Catalyst 6500/7600 Devices

This section answers the following questions about Catalyst 6500/7600 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 6500/7600 devices?](#)
- [Q.What are the limitations in support for IDSM settings in Security Manager?](#)
- [Q.Can I reference an undefined VLAN in Security Manager?](#)

**Q.** Which VTP modes are supported by Security Manager?

**A.** Security Manager 3.1 supports transparent mode. Other VTP modes, such as client mode and server mode, might be supported in future releases.

**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 6500/7600 devices?

- A.** Security Manager supports the use of standard and extended ACLs as matching criteria for VACLs on Catalyst 6500/7600 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.

## Migrating from Security Manager 3.0.x to 3.1.x

Security Manager 3.1.x differs significantly from 3.0.x in its features for managing Catalyst 6500 Series switches and Cisco 7600 Series routers, as well as their associated firewall services modules (FWSMs) and security contexts:

- Security Manager 3.0.x used features from an embedded variant of CiscoView Device Manager, which is not included in Security Manager 3.1.x.
- Security Manager 3.1.x offers a fully integrated management tool that is consistent with other Security Manager features.

This change to an integrated management tool affects the installation process when upgrading from Security Manager 3.0.x to Security Manager 3.1.x. For more information about how to migrate Catalyst 6500/7600 devices after the upgrade, please see “Migrating Inventory from an Earlier Security Manager Release” in the *User Guide for Cisco Security Manager*.

## 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.

## Performing Rollback on Catalyst 6500/7600 Devices

The proper order for performing rollback on Catalyst 6500/7600 devices is as follows:

- Security contexts.
- Service modules.
- Chassis.

We recommend performing rediscovery after the rollback operation is complete.

If you are rolling back an FWSM deployment and the system is configured to retrieve security certificates when adding devices, you might need to retrieve the certificate after the rollback operation is complete. This can be done using either of the following methods:

- Retrieving the certificate on a per-device basis from Device Properties.
- Configuring Security Manager to automatically retrieve certificates after rollback. To do this, select **Tools > Security Manager Administration > Device Communication**, then select the **Retrieve while adding devices** option under SSL Certificate Parameters.





## CHAPTER 12

# Deployment

---

This chapter contains the following topics:

- [FAQs About Deployment](#), page 12-1
- [Performing Rollback When Deploying to a File](#), page 12-14
- [Mixing Deployment Methods](#), page 12-14
- [SSL Handshake Failure When Deploying to PIX/ASA Devices](#), page 12-15
- [Deployment Failures to Devices Managed by AUS](#), page 12-15

## 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.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.Can I use Security Manager and ACL Manager together to manage ACLs?](#)
- [Q.Does Security Manager deploy full configurations or only the changes made since the last deployment \(delta configurations\)?](#)
- [Q.What are the default deployment methods for each type of device, and how do I change one for a device or for a deployment job?](#)
- [Q.How many devices can Security Manager deploy to simultaneously?](#)
- [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. How can I deploy configurations to devices using a Token Management Server (TMS)?
- Q. How can I deploy configurations to devices using an Auto Update Server (AUS)?
- Q. How can I deploy configurations to devices using a Cisco Networking Services (CNS) server?
- Q. Why do some platforms require a reload after performing configuration rollback but not others?

**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** 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:
- Obtain the running configuration from the device.
    - Used when deploying to the device *unless* the deployment method is AUS, TMS, or CNS. You can force Security Manager to use Configuration Archive by selecting **When Deploying to Device Get Reference Config from: 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.
    - Used when deploying to file, unless you select **When Deploying to File Get Reference Config from: 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 deploying to a device if uploading the configuration from the device failed. (Configuration Archive is used as a backup to obtaining the configuration from the live device.)
    - Used when you preview configurations.
  - Obtain the factory default configuration.
    - 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**Deployment Steps**

<b>Step 2</b>	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.
<b>Step 3</b>	<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"> <li>• SSL or SSH—Security Manager contacts the device directly and sends the delta configuration to it.</li> <li>• Auto Update Server (standalone or running on Configuration Engine) 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.</li> <li>• CNS gateway running on an Auto Update Server (for IOS devices with dynamic IP addresses)—Security Manager contacts the CNS gateway to get the device IP address, then uses SSL to contact the device directly and send it the delta configuration.</li> <li>• Configuration Engine for IOS devices—Security Manager sends the delta configuration to Configuration Engine, where the device retrieves it.</li> <li>• 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.</li> </ul>

**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.

**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. If you roll back configurations on Catalyst or IOS devices, you also need to restart the device.

- 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 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 editing the 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 redeploy them to the device. During deployment, do not select the option to force an error if out-of-band changes are found on 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 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 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 rediscover policies.
- Q.** Can I use Security Manager and ACL Manager together to manage ACLs?
- A.** Do not use Security Manager and ACL Manager (or any other software) to manage the same ACLs. Use Security Manager to manage all firewall- and VPN-related ACLs. You can use ACL Manager to manage ACLs for other features, such as quality of service (QoS).

- 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.** What are the default deployment methods for each type of device, and how do I change one for a device or for a deployment job?
- A.** When you add devices to Security Manager, you select the deployment method to be used by that device. This determines the method used for deploying to the device (instead of a file). When you create a deployment job, an additional deployment method default applies to the job as a whole, which determines whether deployment creates configuration files or whether it sends the configuration to the device using the method selected for the device. You control this default in the administration settings (select **Tools > Security Manager Administration**, then select **Deployment**). When you create a deployment job, you can also change whether the deployment is to a file or to the device for each device by clicking **Edit Deploy Method** in the Create Job window
- Q.** How many devices can Security Manager deploy to simultaneously?
- 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.
- 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. Go to `...\CSCOPx\MDC\athena\config`.
  2. Select **DCS.properties file** to open the DCS properties file.
  3. Locate **DCS.IOS.ssl.maxChunkSize=<value of the configuration bulk>**.
  4. Reduce the value of the configuration bulk.
  5. 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. Go to `...\CSCOPx\MDC\athena\config`.
  2. Select **DCS.properties file** to open the DCS properties file.
  3. Locate the **DCS.FWSM.checkThreshold=False** property.
  4. Change the value to true: **DCS.FWSM.checkThreshold=True**.
  5. Restart the CiscoWorks Daemon Manager.
  6. 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 <sup>1</sup>	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

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

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

- Q.** How can I deploy configurations to devices using a Token Management Server (TMS)?
- A.** To perform this type of deployment, you need to set up the device, TMS, and Security Manager. The following checklist shows the tasks that you need to perform.






**Tip** For more information, click **Help** from any Security Manager dialog box or page.

Table 12-5 TMS Setup Checklist

✓	Task
<input type="checkbox"/>	<p><b>1. Set up the TMS as an FTP server.</b></p> <p>You must set up the TMS as an FTP server because files are transferred from Security Manager to the TMS server using FTP.</p>
<input type="checkbox"/>	<p><b>2. Add devices to Security Manager inventory.</b></p> <p>Select <b>File &gt; Add Devices</b>.</p>
<input type="checkbox"/>	<p><b>3. Specify TMS as the transport protocol to be used for Cisco IOS devices.</b></p> <p>You can set this parameter globally for all Cisco IOS devices or for a specific device, as follows:</p> <ul style="list-style-type: none"> <li>• Globally—Select <b>Tools &gt; Security Manager Administration &gt; Device Communication</b>.</li> <li>• Device—Select <b>Device properties &gt; DCS settings &gt; Transport protocols</b>.</li> </ul>
<input type="checkbox"/>	<p><b>4. Configure TMS parameters on Security Manager.</b></p> <p>Specify the TMS name or IP address, username and password, directory where configuration files are to be copied, and public key file information in Security Manager. Select <b>Tools &gt; Security Manager Administration &gt; Token Management</b>.</p>
<input type="checkbox"/>	<p><b>5. Set the deployment method to Device either globally or for a specific device.</b></p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Globally—Select <b>Tools &gt; Security Manager Administration &gt; Deployment</b>.</li> <li>• Device—Depends on workflow mode: <ul style="list-style-type: none"> <li>– Non-Workflow mode—Select <b>Submit and Deploy Changes &gt; Edit Deploy Method</b>.</li> <li>– Workflow mode—Select <b>Tools &gt; Deployment Management &gt; Create &gt; Edit Deploy Method</b>.</li> </ul> </li> </ul>

Table 12-5 TMS Setup Checklist (continued)

✓	Task
	<p><b>6. Deploy the configuration to the device.</b></p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Non-Workflow mode—Select <b>Submit and Deploy Changes</b>.</li> <li>• Workflow mode (if no deployment job exists)—Select <b>Tools &gt; Deployment Management &gt; Create</b>.</li> <li>• Workflow mode (if a deployment already job exists)—Select <b>Tools &gt; Deployment Management</b> and select the desired deployment job; then click <b>Deploy</b>.</li> </ul>
	<p><b>7. Using TMS, download the configuration to the eToken.</b></p> <p>See TMS product documentation.</p>
	<p><b>8. Download the configuration from the eToken to the router and save the configuration to the device.</b></p> <p>Plug the eToken into the router, then enter the following commands to download the configuration to the router:</p> <pre>router# <b>crypto pki token &lt;usb_token_id&gt; login &lt;PIN&gt;</b> router# <b>config terminal</b> router(config)# <b>crypto pki token default secondary config CCD</b> router(config)# <b>exit</b> router# <b>write memory</b></pre>

**Q.** How can I deploy configurations to devices using an Auto Update Server (AUS)?

**A.** To perform this type of deployment, you need to set up AUS, the device, and Security Manager. The following checklist shows the tasks that you need to perform.



**Tip** For more information, click **Help** from any Security Manager dialog box or page.



**Note** If deployment to an AUS fails, see [Deployment Failures to Devices Managed by AUS, page 12-15](#).

Table 12-6 AUS Setup Checklist

✓	Task
☐	<p><b>1. Set up the AUS.</b></p> <p>See the AUS product documentation.</p>
☐	<p><b>2. Bootstrap firewall devices for AUS.</b></p> <p>Enter the following commands to bootstrap devices:</p> <pre>hostname(config)# auto-update server https://username:password@AUSserver_IP_address:port/autoupdate/AutoUpdateServlet hostname(config)# auto-update poll-period poll_period [retry_count] [retry_period] hostname(config)# auto-update device-id hardware-serial   hostname   ipaddress [&lt;if_name&gt;]   mac-address [&lt;if_name&gt;]   string&lt;text&gt; hostname(config)# write memory</pre>
☐	<p><b>3. Add devices to Security Manager inventory and assign AUS to devices.</b></p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• If you are adding a new device, from the Device view, select <b>File &gt; New Device &gt; Add New Device</b>. Configure the following fields on the Device Information page: <ul style="list-style-type: none"> <li>– Device selector—Select a PIX Firewall or ASA device type.</li> <li>– IP Type—Select <b>Static</b> or <b>Dynamic</b>.</li> <li>– Auto Update Server—Click the arrow to display a list of servers. Select the server that is managing the device. If the server does not appear in the list, click the arrow, then select <b>+ Add Server...</b> to add the server.</li> <li>– Device Identity—Enter the string value that uniquely identifies the device in AUS.</li> </ul> </li> <li>• If you are adding a device by importing it from DCR, from the Device view, select <b>File &gt; New Device &gt; Add Device From DCR</b>. The device must have been created as an AUS device in DCR for it to be successfully imported into Security Manager as an AUS device.</li> </ul> <p>For more information, see "Adding Devices from DCR" in the Security Manager online help. For quick results, access the online help and use the search function to find this topic.</p>
☐	<p><b>4. Configure AUS settings in Security Manager.</b></p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• (Device view) Select <b>Platform &gt; Device Admin &gt; Server Access &gt; AUS</b> from the Device Policy selector.</li> <li>• (Policy view) Select <b>PIX/ASA/FWSM Platform &gt; Device Admin &gt; Server Access &gt; AUS</b> from the Policy Types selector. Right-click <b>AUS</b> and select <b>New AUS Policy</b> to create a policy, or select an existing policy from the Policies selector.</li> </ul>

Table 12-6 AUS Setup Checklist (continued)

✓	Task
☐	<p><b>5. Set the deployment method to Device.</b></p> <p>You can set this parameter either globally or for a specific device, as follows:</p> <ul style="list-style-type: none"> <li>• Globally—Select <b>Tools &gt; Security Manager Administration &gt; Deployment</b>.</li> <li>• Device—Depends on workflow mode: <ul style="list-style-type: none"> <li>– Non-Workflow mode—Select <b>Submit and Deploy Changes &gt; Edit Deploy Method</b></li> <li>– Workflow mode—Select <b>Tools &gt; Deployment Management &gt; Create &gt; Edit Deploy Method</b>.</li> </ul> </li> </ul>
☐	<p><b>6. Deploy the configuration to the device.</b></p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Non-Workflow mode—Select <b>Submit and Deploy Changes</b>.</li> <li>• Workflow mode (if no deployment job exists)—Select <b>Tools &gt; Deployment Management &gt; Create</b>.</li> <li>• Workflow mode (if a deployment already job exists)—Select <b>Tools &gt; Deployment Management</b> and select the desired deployment job; then click <b>Deploy</b>.</li> </ul>

**Q.** How can I deploy configurations to devices using a Cisco Networking Services (CNS) server?

**A.** To perform this type of deployment, you need to set up the configuration engine (CE), the device, and Security Manager. The following checklist shows the tasks that you need to perform.

**Note**

If PIX Firewall and ASA devices are configured for CNS, they use the AUS protocol. The required steps are identical to the steps that you follow when you configure PIX Firewall and ASA for AUS. See [Q.How can I deploy configurations to devices using an Auto Update Server \(AUS\)?, page 12-9](#)

**Note**

For CNS troubleshooting information, see [Troubleshooting the Setup of CNS-Managed Devices, page 5-11](#).

**Table 12-7 CNS Setup Checklist**


✓	Task
☐	<p><b>1. Set up the Configuration Engine.</b></p> <p>If you are setting up the Configuration Server on AUS, see the AUS product documentation for more information. If you are setting up the Configuration Server on another server, see the Configuration Server documentation.</p>
☐	<p><b>2. Bootstrap devices for CNS.</b></p> <p>If PIX Firewall and ASA devices are configured for CNS, they use the AUS protocol. The required steps are identical to the steps that you follow when you configure PIX Firewall and ASA for AUS. See <a href="#">Table 12-6</a>.</p> <p>For Cisco IOS routers, you can configure CNS in the event-bus mode or the call-home mode.</p> <p>To configure CNS in event-bus mode, enter the following commands:</p> <pre>hostname(config)# hostname&lt;name&gt; hostname(config)# ip domain-name &lt;your_domain&gt; hostname(config)# cns trusted-server all-agents &lt;ip_address&gt; hostname(config)# cns event &lt;ip_address&gt; [port] hostname(config)# cns config partial &lt;ip_address&gt; hostname(config)# cns password &lt;password&gt; hostname(config)# cns exec hostname(config)# exit hostname# copy running startup</pre> <p>To configure CNS in call-home mode, enter the following commands:</p> <pre>hostname# config terminal hostname(config)# ip domain-name &lt;your_domain&gt; hostname(config)# cns trusted-server all-agents &lt;ip_address&gt; hostname(config)# kron occurrence occurrence-name [user username] {in [[numdays:]numhours:]nummin   at hours:min [[month] day-of-month] [day-of-week]} {oneshot   recurring} hostname(config-kron-occurrence)# policy-list &lt;list-name&gt; hostname(config-kron-occurrence)# exit hostname(config)# kron policy-list &lt;list-name&gt; hostname(config-kron-policy)# cli cns config retrieve &lt;ip_address&gt; page /cns/JobbedDynaConfig status http://&lt;ip_address&gt;/cns/PostStatus hostname(config-kron-policy)# exit hostname(config)# cns exec hostname(config)# exit hostname# copy running startup</pre> <p> <b>Note</b> For more information about these commands, see "Setting Up CNS" in the Security Manager online help. For quick results, access the online help and use the search function to find the desired topic.</p>

Table 12-7 CNS Setup Checklist (continued)

✓	Task
☐	<p><b>3. Add devices to Security Manager inventory.</b></p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• If you are adding a new device, from the Device view, select <b>File &gt; New Device &gt; Add New Device</b>. Configure the following fields on the Device Information page: <ul style="list-style-type: none"> <li>– IP Type—Select <b>Static</b> or <b>Dynamic</b>, as appropriate.</li> <li>– Device selector—Select a Cisco IOS router (excludes Cisco 7600 series routers).</li> <li>– CNS-Configuration Engine Server—If the device is using static addressing, select a Configuration Engine from the CNS-Configuration Engine Server field. If the desired Configuration Engine does not appear in the list, you can add it now. Click the arrow, then select <b>+ Add Configuration Engine....</b> The Configuration Engine Properties dialog box appears.</li> </ul> <p>If the device is using dynamic addressing, select the server that is managing the device (Auto Update Server or Configuration Engine). If the desired server does not appear in the list, click the arrow, then select <b>+ Add Server....</b> The Server Properties dialog box appears.</p> </li> <li>• If you are adding a device that already exists in the network, from the Device view, select <b>File &gt; New Device &gt; Add Device From Network</b>. If the device is using dynamic addressing, you must select the Configuration Engine (CNS Gateway) that is managing the device. If the desired Configuration Engine does not appear in the list, click the arrow, then select <b>+ Add Auto Update Server....</b> The Auto Update Server Properties dialog box appears.</li> </ul>
☐	<p><b>4. Set the deployment method to Device.</b></p> <p>You can set this parameter either globally or for a specific device, as follows:</p> <ul style="list-style-type: none"> <li>• Globally—Select <b>Tools &gt; Security Manager Administration &gt; Deployment</b>.</li> <li>• Device—Depends on workflow mode: <ul style="list-style-type: none"> <li>– Non-Workflow mode—Select <b>Submit and Deploy Changes &gt; Edit Deploy Method</b>.</li> <li>– Workflow mode—Select <b>Tools &gt; Deployment Management &gt; Create &gt; Edit Deploy Method</b>.</li> </ul> </li> </ul>
☐	<p><b>5. Deploy the configuration to the device.</b></p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Non-Workflow mode—Select <b>Submit and Deploy Changes</b>.</li> <li>• Workflow mode (if no deployment job exists)—Select <b>Tools &gt; Deployment Management &gt; Create</b>.</li> <li>• Workflow mode (if a deployment already job exists)—Select <b>Tools &gt; Deployment Management</b> and select the desired deployment job; then click <b>Deploy</b>.</li> </ul>

- 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.

## Performing Rollback When Deploying to a File

**Problem** You cannot perform rollback when deploying to a file instead of a device.

**Solution** 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/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.

**Note**

---

For more information about deploying to an AUS, see the FAQ entry, [Q.How can I deploy configurations to devices using an Auto Update Server \(AUS\)?](#), page 12-9.

---



## INDEX

---

### A

#### AAA

- accounting not implemented on SSL VPN [1-8](#)
- 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 [6-14](#)
- name changes when discovering rules [6-9](#)
- removing aaa new-model command [1-7](#)

#### access control lists (ACLs)

- creating during IOS IPS configuration [10-4](#)
- deployment errors on FWSMs [9-6](#)
- handling names during discovery [6-3](#)
- name changes during discovery [6-9](#)
- names preserved during discovery [6-6](#)
- naming conventions [6-6](#)
- resolving naming conflicts [6-7](#)
- using ACL manager [9-5](#)

#### access rules

- cannot save combined rules [8-3](#)

#### address pools

- deployment failure [1-7](#)
- on same subnet as interface [1-8](#)
- overriding in connection profiles [1-7](#)

#### ADSL policies

- unable to deploy [7-4](#)

#### ASA 7.1

- deployment failure with auto-signon command [1-7](#)

#### AUS

- ASA deployment failure [1-7](#)

#### auto-signon

- ASA deployment failure with AUS [1-7](#)

#### Auto Update Server (AUS)

- deploying to devices [9-9](#)
- discovering policies [6-2](#)
- failure during deployment [9-15](#)

---

### C

#### Catalyst 6500/7600 devices

- adding 6503-E devices [11-1](#)
- discovering failover pairs [11-2](#)
- discovering policies on security contexts [6-4](#)
- IDS support [11-2](#)
- interface deployment failure [11-2](#)
- internal VLAN deployment failure [11-3](#)
- migrating to 3.1.x [11-2](#)
- performing rollback [11-3](#)
- supported modes [11-1](#)
- supported VACLs [11-1](#)
- troubleshooting [11-1](#)
- undefined VLANs [11-2](#)

#### changes, out-of-band [9-4](#)

#### Cisco Marketplace [1-viii](#)

#### Cisco Networking Services (CNS)

- debugging IOS device [5-12](#)
- debugging PIX device [5-12](#)
- deploying to devices [9-11](#)
- deployment failures to PIX device [5-12](#)
- device id not connected error [5-11](#)
- device name does not exist error [5-11](#)
- discovery failure for IOS device [5-13](#)
- event mode router does not appear [5-13](#)
- first deployment to PIX fails [5-12](#)
- InvalidParameterException error [5-11](#)

- troubleshooting device setup [5-11](#)
- Cisco Press [1-viii](#)
- Cisco Product Quick Reference Guide, obtaining [1-viii](#)
- Cisco product security
  - PSIRT [1-viii](#)
  - vulnerability policy portal [1-viii](#)
- Cisco Secure ACS (ACS)
  - adding multihomed devices [3-4](#)
  - authentication fails [3-1](#)
  - changes not appearing in Security Manager [3-3](#)
  - DCR error when adding devices [3-2](#)
  - 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 Security Agent
  - already installed on server [4-1, 11-2](#)
  - 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 [2-5](#)
- client log files
  - locating [2-2](#)
- CNS
  - lists applied to wrong SSL VPN context [1-8](#)
- combining rules
  - cannot save changes [8-3](#)
- configuration ownership [9-4](#)
- configuration rollback
  - cannot connect to a Cisco IOS router after [5-1](#)
  - performing reload [9-14](#)
- configure replace command [9-14](#)
- connection profiles
  - sharing among multiple ASAs [1-7](#)

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

---

## D

- daylight saving time
  - and certificate error
    - during discovery [5-9](#)
- DCR
  - adding 12.1 and 12.2 routers [5-9](#)
- deleting
  - referenced interfaces [7-2](#)
- deployment
  - ADSL deployment failures [7-4](#)
  - Catalyst interface settings [11-2](#)
  - Catalyst internal VLANs [11-3](#)
  - changing default deployment methods [9-6](#)
  - determining method to use [9-3](#)
  - devices with same IP [5-10](#)
  - duplicate SSL VPN gateway failure [1-7](#)
  - errors with ACLs [9-6](#)
  - failure due to overlapping pools [1-7](#)
  - failure due to pools not on interface subnet [1-8](#)
  - failures with AUS-managed devices [9-15](#)
  - failure when modifying WINS master server [1-8](#)
  - failure when port forwarding list removed [1-7](#)
  - fixing an OS version mismatch [9-4](#)
  - ignoring errors [9-7](#)
  - IOS errors [9-6](#)
  - IOS IPS [10-4](#)
  - layer 2 interfaces [7-2](#)
  - maximum number of devices [9-6](#)
  - mixing methods [9-14](#)
  - performing immediately after discovery [6-3](#)
  - PVC deployment failures [7-4](#)
  - PVC IP protocol mappings [7-4](#)
  - rolling back configurations [9-3](#)
  - setting default directory [9-3](#)
  - SSL handshake failure [9-15](#)

- understanding
  - effects of deploying to files [9-3](#)
  - full vs. delta configurations [9-6](#)
  - process [9-2](#)
- using a Cisco Networking Services (CNS) server [9-11](#)
- using an Auto Update Server (AUS) [9-9](#)
- using a Token Management Server (TMS) [9-8](#)
- device communication
  - loss of contact due to NAT [7-3](#)
  - routers without K8/K9 crypto image [5-1](#)
- device configuration
  - discovering commands [6-3](#)
  - unable to configure [7-5](#)
- device management [9-4](#)
  - changing image version [5-3](#)
  - content and mode changes [5-6](#)
  - hardware model changes [5-7](#)
  - image version changes affecting feature set [5-4](#)
  - image version changes not affecting feature set [5-3](#)
  - simultaneous operations on device [5-10](#)
- device response
  - to appear as an error message [5-2](#)
- devices
  - DCR error when adding [3-2](#)
  - updating credentials from ACS [3-4](#)
- DHCP
  - traffic blocked [7-5](#)
- diagnostic information
  - generating [1-1](#)
- dialers
  - name changes during discovery [6-13](#)
- discovery
  - Catalyst failover pairs [11-2](#)
  - devices with same IP [5-10](#)
  - invalid certificate error [5-9](#)
  - security certificate error [5-9](#)
- discovery task
  - frequently asked questions [6-2](#)

- DNS
  - configuring for SSL VPN [1-6](#)
- documentation
  - on Cisco.com [1-viii](#)
  - ordering [1-viii](#)
- documentation feedback, sending to Cisco [1-viii](#)

---

## E

- errors
  - deployment [9-6](#)
- event log
  - CSA error message [4-2](#)

---

## F

- FAQ
  - Catalyst 6500/7600 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 [6-2](#)
    - discovery and ACS [6-3](#)
    - FWSM and Catalyst security contexts [6-4](#)
    - how it works [6-2](#)
    - importing from VMS 2.x [6-5](#)
    - naming ACLs and object groups [6-3](#)
    - PIX/ASA security contexts [6-4](#)
    - redeploying after discovery [6-3](#)
    - rediscovering existing policies [6-3](#)
    - unable to submit changes [6-4](#)
    - using existing policies and objects [6-4](#)
    - viewing discovered policies [6-2](#)

- viewing undiscovered policies [6-2](#)
    - when to perform [6-2](#)
  - firewall services
    - cli for authentication proxy [8-2](#)
    - configuring management IP of security contexts [8-3](#)
    - dropped GTP map commands [8-2](#)
    - hit count [8-1](#)
      - standard ACLs [8-2](#)
    - losing connection to a device [8-1](#)
    - negating addresses within a range [8-3](#)
    - removal of bound ACEs [8-2](#)
    - unable to deploy using BGP [8-2](#)
    - validation error on transparent rules [8-2](#)
  - Firewall Services Module (FWSM)
    - deployment error [9-6](#)
    - discovering policies on security contexts [6-4](#)
- 
- G**
- gateways
    - sharing address and port [1-7](#)
  - group-policy
    - removing SSL VPN definitions [1-8](#)
- 
- H**
- hostnames
    - effect on policy discovery [6-5](#)
  - HTTP
    - name changes during discovery [6-14](#)
  - HTTPS mode
    - determining [2-2](#)
- 
- I**
- IDSM
    - support limitations [11-2](#)
  - ignore error message
    - configure Security Manager to [5-2](#)
  - inspection rules
    - name changes during discovery [6-10](#)
  - installation
    - troubleshooting [2-5](#)
  - IOS 12.1 and 12.2
    - configuring in Security Manager [7-1](#)
  - IOS 12.4(11)T
    - address pool deployment failure [1-8](#)
    - CNS problem with SSL VPN contexts [1-8](#)
  - IOS 12.4(9)T
    - AAA accounting failure [1-8](#)
    - port forwarding list deployment failure [1-7](#)
    - WINS master server deployment failure [1-8](#)
  - IP mappings
    - unable to deploy [7-4](#)
  - IPS
    - adding and managing sensors [10-1](#)
    - co-existing with CSA [4-2](#)
    - creating ACLs [10-4](#)
    - deploying [10-4](#)
    - importing 5.0 sensors [10-2](#)
    - performing updates [10-2](#)
    - provisioning trusted hosts [10-4](#)
    - retrieving signature updates [10-2](#)
    - signature updates [10-4](#)
    - updating IOS IPS crypto configurations [10-4](#)
- 
- L**
- line access
    - name changes during discovery [6-15](#)
- 
- M**
- max-webvpn-session-limit
    - cannot be imported [1-6](#)

---

**N**

## NAC

- deployment fails [7-7](#)
- name changes during discovery [6-16](#)
- posture validation not occurring [7-7](#)

## NAT

- discovering rules with route maps [7-3](#)
- name changes during discovery [6-11](#)
- VPN traffic sent unencrypted [7-3](#)

Networking Professionals Connection [1-viii](#)


---

**O**

## object-groups

- name changes during discovery [6-8](#)

## objects

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

## online help

- loading [2-4](#)
- preserving search results [2-5](#)

## OS version mismatch

- fixing [9-4](#)

## out-of-band changes

- resolving [9-4](#)

---

**P**

## passwords

- encrypted passwords on routers [7-2](#)

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

## PIX/ASA devices

- discovering policies on security contexts [6-4](#)
- discovering policies when using AUS [6-2](#)

## PIX object groups

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

## policies

- policy discovery FAQ [6-2](#)
- rediscovery and current assignments [6-3](#)

- 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](#)
- adding routers running 12.1 or 12.2 [5-9](#)
- 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 [6-2](#)
- discovery and ACS [6-3](#)
- frequently asked questions [6-2](#)
- FWSM and Catalyst security contexts [6-4](#)
- how it works [6-2](#)
- importing from VMS 2.x [6-5](#)
- naming ACLs and object groups [6-3](#)
- NAT rules with route maps [7-3](#)
- PIX/ASA security contexts [6-4](#)
- preserving ACL names [6-6](#)
- redeploying after discovery [6-3](#)
- rediscovering existing policies [6-3](#)
- resource names changed during discovery [6-8](#)
- unable to submit changes [6-4](#)
- undiscovered VPN features [6-5](#)
- using existing policies and objects [6-4](#)
- viewing discovered policies [6-2](#)
- viewing undiscovered policies [6-2](#)
- when to perform [6-2](#)
- while deploying to device [6-5](#)

## port forwarding list

- applied to wrong SSL VPN context [1-8](#)
- deployment failure when removed [1-7](#)

## PPP

- name changes during discovery [6-13](#)

## proxy-bypass interfaces

- configured for SSL VPN [1-7](#)

PSIRT [1-viii](#)

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

PVC policies

unable to deploy [7-4](#)

## Q

quality of service (QoS)

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

## R

reload

after configuration rollback [9-14](#)

resources

AAA name changes [6-9](#)

AAA policy name changes [6-14](#)

ACL name changes [6-9](#)

dialer name changes [6-13](#)

dynamic NAT name changes [6-11](#)

HTTP name changes [6-14](#)

inspection rule name changes [6-10](#)

line access name changes [6-15](#)

NAC name changes [6-16](#)

names changed during discovery [6-8](#)

object-group name changes [6-8](#)

PPP name changes [6-13](#)

QoS name changes [6-17](#)

service policy rule name changes [6-12](#)

transparent rule name changes [6-10](#)

rollback [9-3](#)

Catalyst 6500/7600 devices [11-3](#)

performing when deploying to file [9-14](#)

router platform

policy troubleshooting [7-1](#)

device access policies [7-4](#)

device interface policies [7-2](#)

DHCP policies [7-5](#)

DSL policies [7-3](#)

NAC policies [7-6](#)

NAT policies [7-2](#)

PVC policies [7-4](#)

SDP policies [7-5](#)

SNMP policies [7-6](#)

static routing policies [7-7](#)

routers

configuring routers with 12.1 or 12.2 [7-1](#)

managing encrypted passwords [7-2](#)

## S

security

advisories [1-viii](#)

incidents, obtaining assistance [1-viii](#)

news from Cisco

registering to receive [1-viii](#)

RSS feed URL [1-viii](#)

notices [1-viii](#)

PSIRT [1-viii](#)

vulnerabilities, reporting [1-viii](#)

Security Agent installation

troubleshooting [2-5](#)

security certificate

invalid during discovery [5-9](#)

validity period

and time setting on Security Manager [5-9](#)

security context

configuring management IP [8-3](#)

security contexts

deleting config file [5-10](#)

discovering policies on FWSM and Catalyst devices [6-4](#)

discovering policies on PIX/ASA devices [6-4](#)

Security Manager 3.0.1

adding and managing IPS sensors [10-1](#)

Security Manager client

cleaning server list in Login window [2-1](#)

determining HTTPS mode [2-2](#)

- entering server names after installation [2-2](#)
  - frequently asked questions [2-1](#)
  - installing on same machine as server [2-1](#)
  - loading online help [2-4](#)
  - locating client logs [2-2](#)
  - reinstalling [2-4](#)
  - removing locks of another user [2-4](#)
  - resetting password [2-2](#)
  - resolving version mismatch [2-2](#)
  - running in dual-screen mode [2-3](#)
  - using HTTP [2-3](#)
  - Security Manager database
    - corrupted [1-2](#)
    - troubleshooting [1-2](#)
  - Security Manager Diagnostics utility
    - accessing [1-1](#)
  - Security Manager server
    - collecting troubleshooting information [1-1](#)
    - database issues [1-2](#)
    - installation [1-4](#)
    - restoring database from files [1-3](#)
    - restricting access [1-3](#)
    - unable to launch [1-3](#)
  - service policy rules
    - name changes during discovery [6-12](#)
  - service requests
    - submitting [1-viii](#)
  - services
    - creating groups from nameless services [8-3](#)
  - signatures
    - managing updates [10-4](#)
    - retrieving updates [10-2](#)
  - SNMP
    - removing traps unintentionally [7-6](#)
    - traps not being sent [7-6](#)
  - SSL
    - handshake failure during deployment [9-15](#)
  - SSL VPN
    - AAA accounting not implemented [1-8](#)
    - address pools on interface subnet [1-8](#)
    - ASA deployment failure with AUS failure [1-7](#)
    - cannot import license information [1-6](#)
    - detecting overlapping pools [1-7](#)
    - limitations [1-6](#)
    - limitations due to OS defects [1-7](#)
    - lists applied to wrong context [1-8](#)
    - modifying WINS master server [1-8](#)
    - need for DNS [1-6](#)
    - removing aaa new-model command [1-7](#)
    - removing group policies from PIX/ASAs [1-8](#)
    - removing port forwarding list [1-7](#)
    - sharing connection profiles on ASAs [1-7](#)
    - sharing gateway addresses [1-7](#)
    - use of proxy-bypass interfaces [1-7](#)
    - using interface roles [1-7](#)
  - static routing
    - deployment fails after upgrade [7-7](#)
    - floating route not inserted [7-7](#)
  - summertime
    - and certificate error
      - during discovery [5-9](#)
  - support
    - Networking Professionals Connection [1-viii](#)
    - obtaining from Cisco [1-viii](#)
- 
- ## T
- technical support (TAC)
    - obtaining [1-viii](#)
    - URL for service requests [1-viii](#)
  - time setting
    - on Security Manager
      - certificate error [5-9](#)
      - certificate validity period [5-9](#)
      - lagging behind device [5-9](#)
  - timezone settings
    - and certificate error [5-9](#)
    - on device [5-9](#)

- on Security Manager [5-9](#)
- Token Management Server (TMS) [9-8](#)
  - deploying to [9-8](#)
- training, obtaining [1-viii](#)
- transparent rules
  - name changes during discovery [6-10](#)
- troubleshooting information
  - generating [1-1](#)
- trusted hosts
  - provisioning [10-4](#)

---

## U

- URL list
  - applied to wrong SSL VPN context [1-8](#)

---

## V

- version mismatch, resolving [2-2](#)
- VLAN ACLs (VACLs)
  - supported types [11-1](#)
- VLANs
  - referencing undefined [11-2](#)
- VPN
  - defining multiple CA servers [1-2](#)
  - defining multiple spoke definitions [1-5](#)
  - discovering after configuring [1-4](#)
  - enabling/disabling VRF on Catalyst 6500/7600 [1-4](#)
  - loss of communication with spoke [1-2](#)
  - PKI with AAA [1-2](#)
  - SSL VPN limitations [1-6](#)
  - SSL VPN limitations due to OS defects [1-7](#)
  - traffic sent unencrypted [7-3](#)
  - unconfigurable commands when Easy VPN enabled [1-5](#)
  - undiscovered features [6-5](#)
  - unnneeded Easy VPN policies [1-3](#)
  - updating routing processes [1-1](#)
- VPN/Security Management Suite (VMS)

- importing policies from [6-5](#)
- vpn sessiondb
  - cannot be imported [1-6](#)
- VTY
  - name changes during discovery [6-15](#)

---

## W

- WINS
  - modifying master server [1-8](#)