



CHAPTER 6

Policy Discovery

This chapter contains the following topics:

- [FAQs About Policy Discovery, page 6-1](#)
- [Performing Discovery in a Multi-User Environment, page 6-5](#)
- [SSL VPN Policies Negated When Discovered From Configuration File, page 6-5](#)
- [Undiscovered VPN Features, page 6-6](#)
- [ACL Names Preserved by Security Manager, page 6-6](#)
- [Resource Names Changed by Security Manager, page 6-8](#)



Note

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

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 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.Why does the AAA policy not show the AAA configuration that I discovered on the router?
 - Q.Why are parts of the AAA method list definitions configured on my router not discovered?
 - Q.Can I discover AAA servers on devices running IOS software that were configured using the server-private command?
 - Q.What do I need to know about discovery and device hostnames?
- Q.** How does policy discovery work?
- A.** After you select the device whose policies, settings, and interfaces (inventory) you want to discover, Security Manager obtains the running configuration (from live devices) or the supplied configuration (when discovering from configuration files) and translates the CLI into Security Manager policies and objects. The imported configuration is added to the Configuration Archive as the initial configuration for the device. After discovery, you can review the resulting policies and objects and decide whether to commit them to the database or discard them. Please note that when discovering policies on multiple devices, commit and discard affect all the devices as a group and cannot be implemented on a per-device basis.
- Q.** When should I discover policies?
- A.** Typically, you should discover policies when you add devices to Security Manager. However, if you are creating devices in Security Manager (instead of importing live devices or configuration files), you must perform policy discovery after adding the device. You should also perform policy discovery to synchronize Security Manager with any out-of-band changes that have been made to the device, for example through the CLI.
- Q.** How can I determine the results of the discovery?
- A.** When you initiate a discovery task, a window opens that shows you the discovery status and results. You can also view a history of discovery task results on the Policy Discovery Status page (select **Tools > Policy Discovery Status**).
- Q.** Does Security Manager show which commands are not discovered and what can I do about them?
- A.** In the discovery status window, go to the Message Summary section, then select **Commands Not Discovered**. Any undiscovered commands are listed in the Description field.
- Q.** How are discovered policies reflected in the user interface?
- A.** Security Manager converts device commands into policies. There is no difference between a policy discovered from a device configuration and one defined in Security Manager.

- Q.** I am using Auto Update Server for my PIX or ASA devices. How do I discover policies?
- A.** If a device has a static IP address, you can discover policies from the device. If it has a dynamic IP address, you must discover policies from the device's configuration file.
- Q.** I am using a Cisco Secure Access Control Server (ACS) to manage authentication and authorization to Security Manager. How does this affect policy discovery?
- A.** You must add all managed devices to the ACS, including security contexts on PIX, ASA, and FWSM devices, before you can perform policy discovery and manage these devices in Security Manager.
- Q.** What should I do after discovering VPN or router platform policies?
- A.** Due to the way these features are discovered, Security Manager does not assume management of discovered VPN and router platform policies until after it deploys them. This means that if you discover a router, unassign one of its policies and deploy, no commands are removed from the router's configuration. We recommend, therefore, that you perform deployment to a file immediately after discovering VPN or router platform policies, *before* you make any changes to those policies. After this initial deployment, you can reconfigure these policies and deploy your changes as required.
- Q.** If I discover policies on a device and then deploy the policies from Security Manager without changing them, what is the difference between the original configuration on the device and the one that exists after deployment?
- A.** Typically, there are no differences between the new configuration and your original one, assuming you set up FlexConfigs for any unsupported CLI commands (because they are not displayed in Security Manager). However, in certain cases minor changes might occur in your ACL or object-group naming schemes. For more information, see "How Policy Objects are Provisioned as PIX Object Groups" in the Security Manager online help. In addition, any discovered objects that are not being used by a policy are removed from the configuration. There can also be instances where the new configuration is functionally equivalent to the old one but does not use the same commands.
- Q.** How does Security Manager handle my current CLI naming schemes for ACLs and object groups?
- A.** When you discover policies from a device, Security Manager tries to use the same names you have used. However, depending on your naming scheme, some minor differences might occur between what you defined on your device and the policies created through discovery. For more information, see [ACL Names Preserved by Security Manager, page 6-6](#) and [Name Changes in PIX/ASA Object Groups, page 6-8](#). 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 local to that device; none of them are shared with other devices. If you want to use shared policies with the device, you must redo the assignments after policy discovery.

- Q.** Does Security Manager use existing policies and objects during policy discovery?
- A.** During policy discovery, Security Manager uses existing policy objects (ones that you already defined in Security Manager) when creating policies for the device. However, Security Manager does not reuse existing policies; all policies created during discovery are local to the device being discovered. Thus, you might find it beneficial to define your policy objects (such as network objects) before adding devices to Security Manager.
- Q.** What do I need to know about security contexts on PIX 7.0 and ASA devices in terms of policy discovery?
- A.** On devices running PIX 7.0 or ASA software, you can create security contexts, which act like independent firewalls. When you add a device that has security contexts, you should discover all contexts and policies at the same time; otherwise, you will have to discover policies for each context separately. When you add the device, select **MULTI** for Context and do not select Security Context of Unmanaged Device. (If you select this option, only the admin context is imported, and it has no relationship to other security contexts on the device; select this option only if you want to manage the security context independently from the parent device.) Depending on how you add the device, you might need to select the option to discover security contexts. During discovery, Security Manager identifies each security context and adds it as a separate device to the device list, appending the security context name to the end of the parent's name; for example, if the parent is pix_141, the admin context would be pix_141_admin. When managing PIX 7.0 and ASA devices in Security Manager, you can create security contexts or delete contexts, as well as create and delete policies for those contexts.
- Q.** What do I need to know about security contexts for Firewall Services Modules (FWSMs) on Catalyst switches 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.** 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 a Multi-User Environment

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

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

SSL VPN Policies Negated When Discovered From Configuration File

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

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

Undiscovered VPN Features

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

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

If you define and deploy policies of these types using the Security Manager interface, your policies overwrite the device configurations that were not discovered. Therefore, if you want Security Manager to manage existing configurations, you should define policies that match the existing configurations as closely as possible. (Use the Preview Configuration feature to examine the results before deploying.) The VPN provisioning mechanism leverages the content of the existing configuration as much as possible (assuming the content matches the policies configured in Security Manager), but does not retain the naming conventions used in the CLI commands. For more information, see [Resource Names Changed by Security Manager, page 6-8](#).



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 9-9](#).

ACL Names Preserved by Security Manager

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

- Access lists (PIX, ASA, 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"> Inbound: CSM_FW_ACL_InterfaceName Outbound: CSM_FW_ACL_OUT_InterfaceName
NAT0 ACLs	<ul style="list-style-type: none"> Inbound: CSM_nat0_InterfaceName_in Outbound: CSM_nat0_InterfaceName
NAT ACLs	<ul style="list-style-type: none"> Inbound: CSM_nat_InterfaceName_poolID_in Outbound: CSM_nat_InterfaceName_poolID <p>Note For PIX 6.3(x) devices, the following is added to the ACL name: add <code>_dns</code> for dns, <code>_nrseq</code> for norandomseq, <code>_emb##</code> for embryonic limit and <code>_tcp##</code> and <code>_udp##</code> for tcp and udp max connection limits.</p>
Policy Static ACLs	<ul style="list-style-type: none"> For PIX 6.3(x) devices: <ul style="list-style-type: none"> For IP: CSM_static_globalIP_LocalInterfaceName_globalInterfaceName For other protocols: CSM_static_globalIP_LocalInterfaceName_globalInterfaceName_protocol_globalPort For devices running other OS versions, the localIP is added: <ul style="list-style-type: none"> For IP: CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName For other protocols: CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName_protocol_globalPort
AAA ACLs	CSM_AAA_{AUTHO ATHEN ACCT}_InterfaceName_ServerTag

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.

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 6-11](#)
- [Name Changes in Dialer Policies, page 6-12](#)
- [Name Changes in PPP Policies, page 6-13](#)
- [Name Changes in AAA Policies, page 6-13](#)
- [Name Changes in HTTP Policies, page 6-14](#)
- [Name Changes in Line Access Policies, page 6-14](#)
- [Name Changes in NAC Policies, page 6-15](#)
- [Name Changes in Quality of Service Policies, page 6-16](#)

Name Changes in PIX/ASA Object Groups

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

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

For example, if the device contains the following:

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

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

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



Tip

To have Security Manager delete unused object groups from a device during deployment, select **Tools Security Manager Administration > Deployment**, then select 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].

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.

Name Changes in Inspection Rules Policies

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

Table 6-3 Inspection Rules Resource Name Changes

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

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

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

Name Changes in Transparent Rules Policies

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

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

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

It changes the name of the ACL, as follows:

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

Name Changes in Dynamic NAT Policies

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

Table 6-4 NAT Resource Name Changes

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

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

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

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



Note

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

Name Changes in Service Policy Rules Policies

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

Table 6-5 Service Policy Rules Resource Name Changes

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

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

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

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

Name Changes in Dialer Policies

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

Table 6-6 Dialer Resource Name Changes

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

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

Name Changes in PPP Policies

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

However, if the AAA configuration on the device contains an unsupported keyword, the method list is not discovered. Instead, you must create a policy in Security Manager. 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
Global configuration commands	
aaa authentication ppp <i>list-name</i>	CSM_PPP_AUTHENTICATION_#
aaa authorization network <i>list-name</i>	CSM_PPP_AUTHORIZATION_#
Interface configuration commands	
ppp authentication <i>protocols list-name</i>	CSM_PPP_AUTHENTICATION_#
ppp authorization <i>list-name</i>	CSM_PPP_AUTHORIZATION_#

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
```

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
```

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
```

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 policy in Security Manager.

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

Table 6-8 Line Access Resource Naming Conventions

Resource	Naming Convention for VTY	Naming Convention for Console
Global configuration commands		
aaa authentication login <i>list-name</i>	CSM_VTY_AUTHENTICATION _#	CSM_CON_AUTHENTICATION _#

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

Resource	Naming Convention for VTY	Naming Convention for Console
aaa authorization exec <i>list-name</i>	CSM_VTY_EXEC_AUTHORIZA TION_#	CSM_CON_EXEC_AUTHORIZA TION_#
aaa authorization commands <i>level list-name</i>	CSM_VTY_COMM_AUTHORIZ ATION_#	CSM_CON_COMM_AUTHORIZ ATION_#
aaa accounting exec <i>list-name</i>	CSM_VTY_EXEC_ACCOUNTIN G_#	CSM_CON_EXEC_ACCOUNTIN G_#
aaa accounting connection <i>list-name</i>	CSM_VTY_CONN_ACCOUNTIN G_#	CSM_CON_CONN_ACCOUNTI NG_#
aaa accounting commands <i>list-name</i>	CSM_VTY_COMM_ACCOUNTI NG_#	CSM_CON_COMM_ACCOUNTI NG_#
Line configuration commands		
login authentication <i>list-name</i>	CSM_VTY_AUTHENTICATION _#	CSM_CON_AUTHENTICATION _#
authorization exec <i>list-name</i>	CSM_VTY_EXEC_AUTHORIZA TION_#	CSM_CON_EXEC_AUTHORIZA TION_#
authorization commands <i>level list-name</i>	CSM_VTY_COMM_AUTHORIZ ATION_#	CSM_CON_COMM_AUTHORIZ ATION_#
accounting exec <i>list-name</i>	CSM_VTY_EXEC_ACCOUNTIN G_#	CSM_CON_EXEC_ACCOUNTIN G_#
accounting connection <i>list-name</i>	CSM_VTY_CONN_ACCOUNTIN G_#	CSM_CON_CONN_ACCOUNTI NG_#
accounting commands <i>level list-name</i>	CSM_VTY_COMM_ACCOUNTI NG_#	CSM_CON_COMM_ACCOUNTI 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
```

Name Changes in NAC Policies

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

Table 6-9 NAC Resource Name Changes

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

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

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

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

Name Changes in Quality of Service Policies

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

Table 6-10 QoS Resource Name Changes

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

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

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

```
class-map match-any myClassMap
  match access-group name myAcl
  match protocol arp
class-map match-any CSM_CLASS_MAP_0
  match access-group name myAcl
  match protocol arp
!
policy-map myPolicyMap
```

```
class myClassMap
policy-map CSM_POLICY_MAP_0
  class CSM_CLASS_MAP_0
  !
interface GigabitEthernet0/0
  ip address 10.56.12.22 255.255.255.128
  duplex auto
  speed auto
  service-policy output CSM_POLICY_MAP_0
```

