

CSM 3.x: Set Up User Permission and Roles

Document ID: 91762

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Set Up User Permissions

Security Manager Permissions

- View Permissions

- Modify Permissions

- Assign Permissions

- Approve Permissions

Understanding CiscoWorks Roles

- CiscoWorks Common Services Default Roles

- Assigning Roles to Users in CiscoWorks Common Services

Understanding Cisco Secure ACS Roles

- Cisco Secure ACS Default Roles

- Customizing Cisco Secure ACS Roles

Default Associations Between Permissions and Roles in Security Manager

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to set up the permissions and roles to the users in the Cisco Security Manager (CSM).

Prerequisites

Requirements

This document assumes that the CSM is installed and works properly.

Components Used

The information in this document is based on the CSM 3.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Set Up User Permissions

Cisco Security Manager authenticates your username and password before you can log in. After they are authenticated, Security Manager establishes your role within the application. This role defines your permissions (also called privileges), which are the set of tasks or operations that you are authorized to perform. If you are not authorized for certain tasks or devices, the related menu items, TOC items, and buttons are hidden or disabled. In addition, a message tells you that you do not have permission to view the selected information or perform the selected operation.

Authentication and authorization for Security Manager is managed either by the CiscoWorks server or the Cisco Secure Access Control Server (ACS). By default, CiscoWorks manages authentication and authorization, but you can change to Cisco Secure ACS by using the AAA Mode Setup page in CiscoWorks Common Services.

The major advantages of using Cisco Secure ACS are the ability to create highly granular user roles with specialized permissions sets (for example, allowing the user to configure certain policy types but not others) and the ability to restrict users to certain devices by configuring network device groups (NDGs).

The following topics describe user permissions:

- Security Manager Permissions
- Understanding CiscoWorks Roles
- Understanding Cisco Secure ACS Roles
- Default Associations Between Permissions and Roles in Security Manager

Security Manager Permissions

Security Manager classifies permissions into the categories as shown:

1. **View** Allows you to view the current settings. For more information, see View Permissions.
 2. **Modify** Allows you to change the current settings. For more information, see Modify Permissions.
 3. **Assign** Allows you to assign policies to devices and VPN topologies. For more information, see Assign Permissions
 4. **Approve** Allows you to approve policy changes and deployment jobs. For more information, see Approve Permissions.
 5. **Import** Allows you to import the configurations that are already deployed on devices into Security Manager.
 6. **Deploy** Allows you to deploy configuration changes to the devices in your network and perform rollback to return to a previously deployed configuration.
 7. **Control** Allows you to issue commands to devices, such as ping.
 8. **Submit** Allows you to submit your configuration changes for approval.
- When you select modify, assign, approve, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager will not function properly.
 - When you select modify policy permissions, you must also select the corresponding assign and view policy permissions.
 - When you permit a policy that uses policy objects as part of its definition, you must also grant view permissions to these object types. For example, if you select the permission for modifying routing policies, you must also select the permissions for viewing network objects and interface roles, which are the object types required by routing policies.
 - The same holds true when permitting an object that uses other objects as part of its definition. For

example, if you select the permission for modifying user groups, you must also select the permissions for viewing network objects, ACL objects, and AAA server groups.

View Permissions

View (read-only) permissions in Security Manager are divided into the categories as shown:

- View Policies Permissions
- View Objects Permissions
- Additional View Permissions

View Policies Permissions

Security Manager includes the following view permissions for policies:

1. **View > Policies > Firewall.** Allows you to view firewall service policies (located in the Policy selector under Firewall) on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of firewall service policies include access rules, AAA rules, and inspection rules.
2. **View > Policies > Intrusion Prevention System.** Allows you to view IPS policies (located in the Policy selector under IPS), including policies for IPS running on IOS routers.
3. **View > Policies > Image.** Allows you to select a signature update package in the Apply IPS Updates wizard (located under Tools > Apply IPS Update), but does not allow you to assign the package to specific devices, unless you also have the Modify > Policies > Image permission.
4. **View > Policies > NAT.** Allows you to view network address translation policies on PIX/ASA/FWSM devices and IOS routers. Examples of NAT policies include static rules and dynamic rules.
5. **View > Policies > Site-to-Site VPN.** Allows you to view site-to-site VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of site-to-site VPN policies include IKE proposals, IPsec proposals, and preshared keys.
6. **View > Policies > Remote Access VPN.** Allows you to view remote access VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of remote access VPN policies include IKE proposals, IPsec proposals, and PKI policies.
7. **View > Policies > SSL VPN.** Allows you to view SSL VPN policies on PIX/ASA/FWSM devices and IOS routers, such as the SSL VPN wizard.
8. **View > Policies > Interfaces.** Allows you to view interface policies (located in the Policy selector under Interfaces) on PIX/ASA/FWSM devices, IOS routers, IPS sensors, and Catalyst 6500/7600 devices.
 - a. On PIX/ASA/FWSM devices, this permission covers hardware ports and interface settings.
 - b. On IOS routers, this permission covers basic and advanced interface settings, as well as other interface-related policies, such as DSL, PVC, PPP, and dialer policies.
 - c. On IPS sensors, this permission covers physical interfaces and summary maps.
 - d. On Catalyst 6500/7600 devices, this permission covers interfaces and VLAN settings.
9. **View > Policies > Bridging.** Allows you to view ARP table policies (located in the Policy selector under Platform > Bridging) on PIX/ASA/FWSM devices.
10. **View > Policies > Device Administration.** Allows you to view device administration policies (located in the Policy selector under Platform > Device Admin) on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices:
 - a. On PIX/ASA/FWSM devices, examples include device access policies, server access policies, and failover policies.

- b. On IOS routers, examples include device access (including line access) polices, server access policies, AAA, and Secure Device Provisioning.
 - c. On IPS sensors, this permission covers device access policies and server access policies.
 - d. On Catalyst 6500/7600 devices, this permission covers IDSM settings and VLAN access lists.
11. **View > Policies > Identity.** Allows you to view identity policies (located in the Policy selector under Platform > Identity) on Cisco IOS routers, including 802.1x and Network Admission Control (NAC) policies.
 12. **View > Policies > Logging.** Allows you to view logging policies (located in the Policy selector under Platform > Logging) on PIX/ASA/FWSM devices, IOS routers, and IPS sensors. Examples of logging policies include logging setup, server setup, and syslog server policies.
 13. **View > Policies > Multicast.** Allows you to view multicast policies (located in the Policy selector under Platform > Multicast) on PIX/ASA/FWSM devices. Examples of multicast policies include multicast routing and IGMP policies.
 14. **View > Policies > QoS.** Allows you to view QoS policies (located in the Policy selector under Platform > Quality of Service) on Cisco IOS routers.
 15. **View > Policies > Routing.** Allows you to view routing policies (located in the Policy selector under Platform > Routing) on PIX/ASA/FWSM devices and IOS routers. Examples of routing policies include OSPF, RIP, and static routing policies.
 16. **View > Policies > Security.** Allows you to view security policies (located in the Policy selector under Platform > Security) on PIX/ASA/FWSM devices and IPS sensors:
 - a. On PIX/ASA/FWSM devices, security policies include anti-spoofing, fragment, and timeout settings.
 - b. On IPS sensors, security policies include blocking settings.
 17. **View > Policies > Service Policy Rules.** Allows you to view service policy rule policies (located in the Policy selector under Platform > Service Policy Rules) on PIX 7.x/ASA devices. Examples include priority queues and IPS, QoS, and connection rules.
 18. **View > Policies > User Preferences.** Allows you to view the Deployment policy (located in the Policy selector under Platform > User Preferences) on PIX/ASA/FWSM devices. This policy contains an option for clearing all NAT translations on deployment.
 19. **View > Policies > Virtual Device.** Allows you to view virtual sensor policies on IPS devices. This policy is used to create virtual sensors.
 20. **View > Policies > FlexConfig.** Allows you to view FlexConfigs, which are additional CLI commands and instructions that can be deployed to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices.

View Objects Permissions

Security Manager includes the following view permissions for objects:

1. **View > Objects > AAA Server Groups.** Allows you to view AAA server group objects. These objects are used in policies that require AAA services (authentication, authorization, and accounting).
2. **View > Objects > AAA Servers.** Allows you to view AAA server objects. These objects represent individual AAA servers that are defined as part of a AAA server group.
3. **View > Objects > Access Control Lists – Standard/Extended.** Allows you to view standard and extended ACL objects. Extended ACL objects are used for a variety of policies, such as NAT and NAC, and for establishing VPN access. Standard ACL objects are used for such policies as OSPF and SNMP, as well as for establishing VPN access.
4. **View > Objects > Access Control Lists – Web.** Allows you to view web ACL objects. Web ACL objects are used to perform content filtering in SSL VPN policies.
5. **View > Objects > ASA User Groups.** Allows you to view ASA user group objects. These objects are configured on ASA security appliances in Easy VPN, remote access VPN, and SSL VPN

configurations.

6. **View > Objects > Categories.** Allows you to view category objects. These objects help you easily identify rules and objects in rules tables through the use of color.
7. **View > Objects > Credentials.** Allows you to view credential objects. These objects are used in Easy VPN configuration during IKE Extended Authentication (Xauth).
8. **View > Objects > FlexConfigs.** Allows you to view FlexConfig objects. These objects, which contain configuration commands with additional scripting language instructions, can be used to configure commands that are not supported by the Security Manager user interface.
9. **View > Objects > IKE Proposals.** Allows you to view IKE proposal objects. These objects contain the parameters required for IKE proposals in remote access VPN policies.
10. **View > Objects > Inspect – Class Maps – DNS.** Allows you to view DNS class map objects. These objects match DNS traffic with specific criteria so that actions can be performed on that traffic.
11. **View > Objects > Inspect – Class Maps – FTP.** Allows you to view FTP class map objects. These objects match FTP traffic with specific criteria so that actions can be performed on that traffic.
12. **View > Objects > Inspect – Class Maps – HTTP.** Allows you to view HTTP class map objects. These objects match HTTP traffic with specific criteria so that actions can be performed on that traffic.
13. **View > Objects > Inspect – Class Maps – IM.** Allows you to view IM class map objects. These objects match IM traffic with specific criteria so that actions can be performed on that traffic.
14. **View > Objects > Inspect – Class Maps – SIP.** Allows you to view SIP class map objects. These objects match SIP traffic with specific criteria so that actions can be performed on that traffic.
15. **View > Objects > Inspect – Policy Maps – DNS.** Allows you to view DNS policy map objects. These objects are used to create inspection maps for DNS traffic.
16. **View > Objects > Inspect – Policy Maps – FTP.** Allows you to view FTP policy map objects. These objects are used to create inspection maps for FTP traffic.
17. **View > Objects > Inspect – Policy Maps – GTP.** Allows you to view GTP policy map objects. These objects are used to create inspection maps for GTP traffic.
18. **View > Objects > Inspect – Policy Maps – HTTP (ASA7.1.x/PIX7.1.x/IOS).** Allows you to view HTTP policy map objects created for ASA/PIX 7.1.x devices and IOS routers. These objects are used to create inspection maps for HTTP traffic.
19. **View > Objects > Inspect – Policy Maps – HTTP (ASA7.2/PIX7.2).** Allows you to view HTTP policy map objects created for ASA 7.2/PIX 7.2 devices. These objects are used to create inspection maps for HTTP traffic.
20. **View > Objects > Inspect – Policy Maps – IM (ASA7.2/PIX7.2).** Allows you to view IM policy map objects created for ASA 7.2/PIX 7.2 devices. These objects are used to create inspection maps for IM traffic.
21. **View > Objects > Inspect – Policy Maps – IM (IOS).** Allows you to view IM policy map objects created for IOS devices. These objects are used to create inspection maps for IM traffic.
22. **View > Objects > Inspect – Policy Maps – SIP.** Allows you to view SIP policy map objects. These objects are used to create inspection maps for SIP traffic.
23. **View > Objects > Inspect – Regular Expressions.** Allows you to view regular expression objects. These objects represent individual regular expressions that are defined as part of a regular expression group.
24. **View > Objects > Inspect – Regular Expressions Groups.** Allows you to view regular expression group objects. These objects are used by certain class maps and inspect maps to match text inside a packet.
25. **View > Objects > Inspect – TCP Maps.** Allows you to view TCP map objects. These objects customize inspection on TCP flow in both directions.
26. **View > Objects > Interface Roles.** Allows you to view interface role objects. These objects define naming patterns that can represent multiple interfaces on different types of devices. Interface roles enable you to apply policies to specific interfaces on multiple devices without having to manually define the name of each interface.

27. **View > Objects > IPsec Transform Sets.** Allows you to view IPsec transform set objects. These objects comprise a combination of security protocols, algorithms and other settings that specify exactly how the data in the IPsec tunnel will be encrypted and authenticated.
28. **View > Objects > LDAP Attribute Maps.** Allows you to view LDAP attribute map objects. These objects are used to map custom (user-defined) attribute names to Cisco LDAP attribute names.
29. **View > Objects > Networks/Hosts.** Allows you to view network/host objects. These objects are logical collections of IP addresses that represent networks, hosts, or both. Network/host objects enable you to define policies without specifying each network or host individually.
30. **View > Objects > PKI Enrollments.** Allows you to view PKI enrollment objects. These objects define the Certification Authority (CA) servers that operate within a public key infrastructure.
31. **View > Objects > Port Forwarding Lists.** Allows you to view port forwarding list objects. These objects define the mappings of port numbers on a remote client to the application's IP address and port behind an SSL VPN gateway.
32. **View > Objects > Secure Desktop Configurations.** Allows you to view secure desktop configuration objects. These objects are reusable, named components that can be referenced by SSL VPN policies to provide a reliable means of eliminating all traces of sensitive data that is shared for the duration of an SSL VPN session.
33. **View > Objects > Services – Port Lists.** Allows you to view port list objects. These objects, which contain one or more ranges of port numbers, are used to streamline the process of creating service objects.
34. **View > Objects > Services/Service Groups** Allows you to view service and service group objects. These objects are defined mappings of protocol and port definitions that describe network services used by policies, such as Kerberos, SSH, and POP3.
35. **View > Objects > Single Sign On Servers.** Allows you to view single sign on server objects. Single Sign-On (SSO) lets SSL VPN users enter a username and password once and be able to access multiple protected services and web servers.
36. **View > Objects > SLA Monitors.** Allows you to view SLA monitor objects. These objects are used by PIX/ASA security appliances running version 7.2 or later to perform route tracking. This feature provides a method to track the availability of a primary route and install a backup route if the primary route fails.
37. **View > Objects > SSL VPN Customizations.** Allows you to view SSL VPN customization objects. These objects define how to change the appearance of SSL VPN pages that are displayed to users, such as Login/Logout and Home pages.
38. **View > Objects > SSL VPN Gateways.** Allows you to view SSL VPN gateway objects. These objects define parameters that enable the gateway to be used as a proxy for connections to the protected resources in your SSL VPN.
39. **View > Objects > Style Objects.** Allows you to view style objects. These objects let you configure style elements, such as font characteristics and colors, to customize the appearance of the SSL VPN page that appears to SSL VPN users when they connect to the security appliance.
40. **View > Objects > Text Objects.** Allows you to view free-form text objects. These objects comprise a name and value pair, where the value can be a single string, a list of strings, or a table of strings.
41. **View > Objects > Time Ranges.** Allows you to view time range objects. These objects are used when creating time-based ACLs and inspection rules. They are also used when defining ASA user groups to restrict VPN access to specific times during the week.
42. **View > Objects > Traffic Flows.** Allows you to view traffic flow objects. These objects define specific traffic flows for use by PIX 7.x/ASA 7.x devices.
43. **View > Objects > URL Lists.** Allows you to view URL list objects. These objects define the URLs that are displayed on the portal page after a successful login. This enables users to access the resources available on SSL VPN websites when operating in Clientless access mode.
44. **View > Objects > User Groups.** Allows you to view user group objects. These objects define groups of remote clients that are used in Easy VPN topologies, remote access VPNs, and SSL VPNs.
45. **View > Objects > WINS Server Lists.** Allows you to view WINS server list objects. These objects

- represent WINS servers, which are used by SSL VPN to access or share files on remote systems.
46. **View > Objects > Internal – DN Rules.** Allows you to view the DN rules used by DN policies. This is an internal object used by Security Manager that does not appear in the Policy Object Manager.
 47. **View > Objects > Internal – Client Updates.** This is an internal object required by user group objects that does not appear in the Policy Object Manager.
 48. **View > Objects > Internal – Standard ACEs.** This is an internal object for standard access control entries, which are used by ACL objects.
 49. **View > Objects > Internal – Extended ACEs.** This is an internal object for extended access control entries, which are used by ACL objects.

Additional View Permissions

Security Manager includes the following additional view permissions:

1. **View > Admin.** Allows you to view Security Manager administrative settings.
2. **View > CLI.** Allows you to view the CLI commands configured on a device and preview the commands that are about to be deployed.
3. **View > Config Archive.** Allows you to view the list of configurations contained in the configuration archive. You cannot view the device configuration or any CLI commands.
4. **View > Devices.** Allows you to view devices in Device view and all related information, including their device settings, properties, assignments, and so on.
5. **View > Device Managers.** Allows you to launch read-only versions of the device managers for individual devices, such as the Cisco Router and Security Device Manager (SDM) for Cisco IOS routers.
6. **View > Topology.** Allows you to view maps configured in Map view.

Modify Permissions

Modify (read-write) permissions in Security Manager are divided into the categories as shown:

- Modify Policies Permissions
- Modify Objects Permissions
- Additional Modify Permissions

Modify Policies Permissions

Note: When you specify modify policy permissions, make sure that you have selected the corresponding assign and view policy permissions as well.

Security Manager includes the following modify permissions for policies:

1. **Modify > Policies > Firewall.** Allows you to modify firewall service policies (located in the Policy selector under Firewall) on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of firewall service policies include access rules, AAA rules, and inspection rules.
2. **Modify > Policies > Intrusion Prevention System.** Allows you to modify IPS policies (located in the Policy selector under IPS), including policies for IPS running on IOS routers. This permission also allows you to tune signatures in the Signature Update wizard (located under Tools > Apply IPS Update).
3. **Modify > Policies > Image.** Allows you to assign a signature update package to devices in the Apply IPS Updates wizard (located under Tools > Apply IPS Update). This permission also allows you to assign auto update settings to specific devices (located under Tools > Security Manager Administration > IPS Updates).

4. **Modify > Policies > NAT.** Allows you to modify network address translation policies on PIX/ASA/FWSM devices and IOS routers. Examples of NAT policies include static rules and dynamic rules.
5. **Modify > Policies > Site-to-Site VPN.** Allows you to modify site-to-site VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of site-to-site VPN policies include IKE proposals, IPsec proposals, and preshared keys.
6. **Modify > Policies > Remote Access VPN.** Allows you to modify remote access VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of remote access VPN policies include IKE proposals, IPsec proposals, and PKI policies.
7. **Modify > Policies > SSL VPN.** Allows you to modify SSL VPN policies on PIX/ASA/FWSM devices and IOS routers, such as the SSL VPN wizard.
8. **Modify > Policies > Interfaces.** Allows you to modify interface policies (located in the Policy selector under Interfaces) on PIX/ASA/FWSM devices, IOS routers, IPS sensors, and Catalyst 6500/7600 devices:
 - a. On PIX/ASA/FWSM devices, this permission covers hardware ports and interface settings.
 - b. On IOS routers, this permission covers basic and advanced interface settings, as well as other interface-related policies, such as DSL, PVC, PPP, and dialer policies.
 - c. On IPS sensors, this permission covers physical interfaces and summary maps.
 - d. On Catalyst 6500/7600 devices, this permission covers interfaces and VLAN settings.
9. **Modify > Policies > Bridging.** Allows you to modify ARP table policies (located in the Policy selector under Platform > Bridging) on PIX/ASA/FWSM devices.
10. **Modify > Policies > Device Administration.** Allows you to modify device administration policies (located in the Policy selector under Platform > Device Admin) on PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices:
 - a. On PIX/ASA/FWSM devices, examples include device access polices, server access policies, and failover policies.
 - b. On IOS routers, examples include device access (including line access) polices, server access policies, AAA, and Secure Device Provisioning.
 - c. On IPS sensors, this permission covers device access policies and server access policies.
 - d. On Catalyst 6500/7600 devices, this permission covers IDSM settings and VLAN access list.
11. **Modify > Policies > Identity.** Allows you to modify identity policies (located in the Policy selector under Platform > Identity) on Cisco IOS routers, including 802.1x and Network Admission Control (NAC) policies.
12. **Modify > Policies > Logging.** Allows you to modify logging policies (located in the Policy selector under Platform > Logging) on PIX/ASA/FWSM devices, IOS routers, and IPS sensors. Examples of logging policies include logging setup, server setup, and syslog server policies.
13. **Modify > Policies > Multicast.** Allows you to modify multicast policies (located in the Policy selector under Platform > Multicast) on PIX/ASA/FWSM devices. Examples of multicast policies include multicast routing and IGMP policies.
14. **Modify > Policies > QoS.** Allows you to modify QoS policies (located in the Policy selector under Platform > Quality of Service) on Cisco IOS routers.
15. **Modify > Policies > Routing.** Allows you to modify routing policies (located in the Policy selector under Platform > Routing) on PIX/ASA/FWSM devices and IOS routers. Examples of routing policies include OSPF, RIP, and static routing policies.
16. **Modify > Policies > Security.** Allows you to modify security policies (located in the Policy selector under Platform > Security) on PIX/ASA/FWSM devices and IPS sensors:
 - a. On PIX/ASA/FWSM devices, security policies include anti-spoofing, fragment, and timeout settings.
 - b. On IPS sensors, security policies include blocking settings.

17. **Modify > Policies > Service Policy Rules.** Allows you to modify service policy rule policies (located in the Policy selector under Platform > Service Policy Rules) on PIX 7.x/ASA devices. Examples include priority queues and IPS, QoS, and connection rules.
18. **Modify > Policies > User Preferences.** Allows you to modify the Deployment policy (located in the Policy selector under Platform > User Preferences) on PIX/ASA/FWSM devices. This policy contains an option for clearing all NAT translations on deployment.
19. **Modify > Policies > Virtual Device.** Allows you to modify virtual sensor policies on IPS devices. Use this policy to create virtual sensors.
20. **Modify > Policies > FlexConfig.** Allows you to modify FlexConfigs, which are additional CLI commands and instructions that can be deployed to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices.

Modify Objects Permissions

Security Manager includes the following view permissions for objects:

1. **Modify > Objects > AAA Server Groups.** Allows you to view AAA server group objects. These objects are used in policies that require AAA services (authentication, authorization, and accounting).
2. **Modify > Objects > AAA Servers.** Allows you to view AAA server objects. These objects represent individual AAA servers that are defined as part of a AAA server group.
3. **Modify > Objects > Access Control Lists – Standard/Extended.** Allows you to view standard and extended ACL objects. Extended ACL objects are used for a variety of policies, such as NAT and NAC, and for establishing VPN access. Standard ACL objects are used for such policies as OSPF and SNMP, as well as for establishing VPN access.
4. **Modify > Objects > Access Control Lists – Web.** Allows you to view web ACL objects. Web ACL objects are used to perform content filtering in SSL VPN policies.
5. **Modify > Objects > ASA User Groups.** Allows you to view ASA user group objects. These objects are configured on ASA security appliances in Easy VPN, remote access VPN, and SSL VPN configurations.
6. **Modify > Objects > Categories.** Allows you to view category objects. These objects help you easily identify rules and objects in rules tables through the use of color.
7. **Modify > Objects > Credentials.** Allows you to view credential objects. These objects are used in Easy VPN configuration during IKE Extended Authentication (Xauth).
8. **Modify > Objects > FlexConfigs.** Allows you to view FlexConfig objects. These objects, which contain configuration commands with additional scripting language instructions, can be used to configure commands that are not supported by the Security Manager user interface.
9. **Modify > Objects > IKE Proposals.** Allows you to view IKE proposal objects. These objects contain the parameters required for IKE proposals in remote access VPN policies.
10. **Modify > Objects > Inspect – Class Maps – DNS.** Allows you to view DNS class map objects. These objects match DNS traffic with specific criteria so that actions can be performed on that traffic.
11. **Modify > Objects > Inspect – Class Maps – FTP.** Allows you to view FTP class map objects. These objects match FTP traffic with specific criteria so that actions can be performed on that traffic.
12. **Modify > Objects > Inspect – Class Maps – HTTP.** Allows you to view HTTP class map objects. These objects match HTTP traffic with specific criteria so that actions can be performed on that traffic.
13. **Modify > Objects > Inspect – Class Maps – IM.** Allows you to view IM class map objects. These objects match IM traffic with specific criteria so that actions can be performed on that traffic.
14. **Modify > Objects > Inspect – Class Maps – SIP.** Allows you to view SIP class map objects. These objects match SIP traffic with specific criteria so that actions can be performed on that traffic.
15. **Modify > Objects > Inspect – Policy Maps – DNS.** Allows you to view DNS policy map objects. These objects are used to create inspection maps for DNS traffic.
16. **Modify > Objects > Inspect – Policy Maps – FTP.** Allows you to view FTP policy map objects.

These objects are used to create inspection maps for FTP traffic.

17. **Modify > Objects > Inspect – Policy Maps – HTTP (ASA7.1.x/PIX7.1.x/IOS).** Allows you to view HTTP policy map objects created for ASA/PIX 7.x devices and IOS routers. These objects are used to create inspection maps for HTTP traffic.
18. **Modify > Objects > Inspect – Policy Maps – HTTP (ASA7.2/PIX7.2).** Allows you to view HTTP policy map objects created for ASA 7.2/PIX 7.2 devices. These objects are used to create inspection maps for HTTP traffic.
19. **Modify > Objects > Inspect – Policy Maps – IM (ASA7.2/PIX7.2).** Allows you to view IM policy map objects created for ASA 7.2/PIX 7.2 devices. These objects are used to create inspection maps for IM traffic.
20. **Modify > Objects > Inspect – Policy Maps – IM (IOS).** Allows you to view IM policy map objects created for IOS devices. These objects are used to create inspection maps for IM traffic.
21. **Modify > Objects > Inspect – Policy Maps – SIP.** Allows you to view SIP policy map objects. These objects are used to create inspection maps for SIP traffic.
22. **Modify > Objects > Inspect – Regular Expressions.** Allows you to view regular expression objects. These objects represent individual regular expressions that are defined as part of a regular expression group.
23. **Modify > Objects > Inspect – Regular Expressions Groups.** Allows you to view regular expression group objects. These objects are used by certain class maps and inspect maps to match text inside a packet.
24. **Modify > Objects > Inspect – TCP Maps.** Allows you to view TCP map objects. These objects customize inspection on TCP flow in both directions.
25. **Modify > Objects > Interface Roles.** Allows you to view interface role objects. These objects define naming patterns that can represent multiple interfaces on different types of devices. Interface roles enable you to apply policies to specific interfaces on multiple devices without having to manually define the name of each interface.
26. **Modify > Objects > IPsec Transform Sets.** Allows you to view IPsec transform set objects. These objects comprise a combination of security protocols, algorithms and other settings that specify exactly how the data in the IPsec tunnel will be encrypted and authenticated.
27. **Modify > Objects > LDAP Attribute Maps.** Allows you to view LDAP attribute map objects. These objects are used to map custom (user-defined) attribute names to Cisco LDAP attribute names.
28. **Modify > Objects > Networks/Hosts.** Allows you to view network/host objects. These objects are logical collections of IP addresses that represent networks, hosts, or both. Network/host objects enable you to define policies without specifying each network or host individually.
29. **Modify > Objects > PKI Enrollments.** Allows you to view PKI enrollment objects. These objects define the Certification Authority (CA) servers that operate within a public key infrastructure.
30. **Modify > Objects > Port Forwarding Lists.** Allows you to view port forwarding list objects. These objects define the mappings of port numbers on a remote client to the application's IP address and port behind an SSL VPN gateway.
31. **Modify > Objects > Secure Desktop Configurations.** Allows you to view secure desktop configuration objects. These objects are reusable, named components that can be referenced by SSL VPN policies to provide a reliable means of eliminating all traces of sensitive data that is shared for the duration of an SSL VPN session.
32. **Modify > Objects > Services – Port Lists.** Allows you to view port list objects. These objects, which contain one or more ranges of port numbers, are used to streamline the process of creating service objects.
33. **Modify > Objects > Services/Service Groups.** Allows you to view service and service group objects. These objects are defined mappings of protocol and port definitions that describe network services used by policies, such as Kerberos, SSH, and POP3.
34. **Modify > Objects > Single Sign On Servers.** Allows you to view single sign on server objects. Single Sign-On (SSO) lets SSL VPN users enter a username and password once and be able to access multiple protected services and web servers.

35. **Modify > Objects > SLA Monitors.** Allows you to view SLA monitor objects. These objects are used by PIX/ASA security appliances running version 7.2 or later to perform route tracking. This feature provides a method to track the availability of a primary route and install a backup route if the primary route fails.
36. **Modify > Objects > SSL VPN Customizations.** Allows you to view SSL VPN customization objects. These objects define how to change the appearance of SSL VPN pages that are displayed to users, such as Login/Logout and Home pages.
37. **Modify > Objects > SSL VPN Gateways.** Allows you to view SSL VPN gateway objects. These objects define parameters that enable the gateway to be used as a proxy for connections to the protected resources in your SSL VPN.
38. **Modify > Objects > Style Objects.** Allows you to view style objects. These objects let you configure style elements, such as font characteristics and colors, to customize the appearance of the SSL VPN page that appears to SSL VPN users when they connect to the security appliance.
39. **Modify > Objects > Text Objects.** Allows you to view free-form text objects. These objects comprise a name and value pair, where the value can be a single string, a list of strings, or a table of strings.
40. **Modify > Objects > Time Ranges.** Allows you to view time range objects. These objects are used when creating time-based ACLs and inspection rules. They are also used when defining ASA user groups to restrict VPN access to specific times during the week.
41. **Modify > Objects > Traffic Flows.** Allows you to view traffic flow objects. These objects define specific traffic flows for use by PIX 7.x/ASA 7.x devices.
42. **Modify > Objects > URL Lists.** Allows you to view URL list objects. These objects define the URLs that are displayed on the portal page after a successful login. This enables users to access the resources available on SSL VPN websites when operating in Clientless access mode.
43. **Modify > Objects > User Groups.** Allows you to view user group objects. These objects define groups of remote clients that are used in Easy VPN topologies, remote access VPNs, and SSL VPN
44. **Modify > Objects > WINS Server Lists.** Allows you to view WINS server list objects. These objects represent WINS servers, which are used by SSL VPN to access or share files on remote systems.
45. **Modify > Objects > Internal – DN Rules.** Allows you to view the DN rules used by DN policies. This is an internal object used by Security Manager that does not appear in the Policy Object Manager.
46. **Modify > Objects > Internal – Client Updates.** This is an internal object required by user group objects that does not appear in the Policy Object Manager.
47. **Modify > Objects > Internal – Standard ACE.** This is an internal object for standard access control entries, which are used by ACL objects.
48. **Modify > Objects > Internal – Extended ACE.** This is an internal object for extended access control entries, which are used by ACL objects.

Additional Modify Permissions

Security Manager includes the additional modify permissions as shown:

1. **Modify > Admin.** Allows you to modify Security Manager administrative settings.
2. **Modify > Config Archive.** Allows you to modify the device configuration in the Configuration Archive. In addition, it allows you to add configurations to the archive and customize the Configuration Archive tool.
3. **Modify > Devices.** Allows you to add and delete devices, as well as modify device properties and attributes. To discover the policies on the device being added, you must also enable the Import permission. In addition, if you enable the Modify > Devices permission, make sure that you also enable the Assign > Policies > Interfaces permission.
4. **Modify > Hierarchy.** Allows you to modify device groups.
5. **Modify > Topology.** Allows you to modify maps in Map view.

Assign Permissions

Security Manager includes the policy assignment permissions as shown:

1. **Assign > Policies > Firewall.** Allows you to assign firewall service policies (located in the Policy selector under Firewall) to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of firewall service policies include access rules, AAA rules, and inspection rules.
2. **Assign > Policies > Intrusion Prevention System.** Allows you to assign IPS policies (located in the Policy selector under IPS), including policies for IPS running on IOS routers.
3. **Assign > Policies > Image.** This permission is currently not used by Security Manager.
4. **Assign > Policies > NAT.** Allows you to assign network address translation policies to PIX/ASA/FWSM devices and IOS routers. Examples of NAT policies include static rules and dynamic rules.
5. **Assign > Policies > Site-to-Site VPN.** Allows you to assign site-to-site VPN policies to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of site-to-site VPN policies include IKE proposals, IPsec proposals, and preshared keys.
6. **Assign > Policies > Remote Access VPN.** Allows you to assign remote access VPN policies to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of remote access VPN policies include IKE proposals, IPsec proposals, and PKI policies.
7. **Assign > Policies > SSL VPN.** Allows you to assign SSL VPN policies to PIX/ASA/FWSM devices and IOS routers, such as the SSL VPN wizard.
8. **Assign > Policies > Interfaces.** Allows you to assign interface policies (located in the Policy selector under Interfaces) to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices:
 - a. On PIX/ASA/FWSM devices, this permission covers hardware ports and interface settings.
 - b. On IOS routers, this permission covers basic and advanced interface settings, as well as other interface-related policies, such as DSL, PVC, PPP, and dialer policies.
 - c. On Catalyst 6500/7600 devices, this permission covers interfaces and VLAN settings.
9. **Assign > Policies > Bridging.** Allows you to assign ARP table policies (located in the Policy selector under Platform > Bridging) to PIX/ASA/FWSM devices.
10. **Assign > Policies > Device Administration.** Allows you to assign device administration policies (located in the Policy selector under Platform > Device Admin) to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices:
 - a. On PIX/ASA/FWSM devices, examples include device access policies, server access policies, and failover policies.
 - b. On IOS routers, examples include device access (including line access) policies, server access policies, AAA, and Secure Device Provisioning.
 - c. On IPS sensors, this permission covers device access policies and server access policies.
 - d. On Catalyst 6500/7600 devices, this permission covers IDSM settings and VLAN access lists.
11. **Assign > Policies > Identity.** Allows you to assign identity policies (located in the Policy selector under Platform > Identity) to Cisco IOS routers, including 802.1x and Network Admission Control (NAC) policies.
12. **Assign > Policies > Logging.** Allows you to assign logging policies (located in the Policy selector under Platform > Logging) to PIX/ASA/FWSM devices and IOS routers. Examples of logging policies include logging setup, server setup, and syslog server policies.
13. **Assign > Policies > Multicast.** Allows you to assign multicast policies (located in the Policy selector under Platform > Multicast) to PIX/ASA/FWSM devices. Examples of multicast policies include multicast routing and IGMP policies.
14. **Assign > Policies > QoS.** Allows you to assign QoS policies (located in the Policy selector under Platform > Quality of Service) to Cisco IOS routers.

15. **Assign > Policies > Routing.** Allows you to assign routing policies (located in the Policy selector under Platform > Routing) to PIX/ASA/FWSM devices and IOS routers. Examples of routing policies include OSPF, RIP, and static routing policies.
16. **Assign > Policies > Security.** Allows you to assign security policies (located in the Policy selector under Platform > Security) to PIX/ASA/FWSM devices. Security policies include anti-spoofing, fragment, and timeout settings.
17. **Assign > Policies > Service Policy Rules.** Allows you to assign service policy rule policies (located in the Policy selector under Platform > Service Policy Rules) to PIX 7.x/ASA devices. Examples include priority queues and IPS, QoS, and connection rules.
18. **Assign > Policies > User Preferences.** Allows you to assign the Deployment policy (located in the Policy selector under Platform > User Preferences) to PIX/ASA/FWSM devices. This policy contains an option for clearing all NAT translations on deployment.
19. **Assign > Policies > Virtual Device.** Allows you to assign virtual sensor policies to IPS devices. Use this policy to create virtual sensors.
20. **Assign > Policies > FlexConfig.** Allows you to assign FlexConfigs, which are additional CLI commands and instructions that can be deployed to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices.

Note: When you specify assign permissions, make sure that you have selected the corresponding view permissions as well.

Approve Permissions

Security Manager provides the approve permissions as shown:

1. **Approve > CLI.** Allows you to approve the CLI command changes contained in a deployment job.
2. **Approve > Policy.** Allows you to approve the configuration changes contained in the policies that were configured in a workflow activity.

Understanding CiscoWorks Roles

When users are created in CiscoWorks Common Services, they are assigned one or more roles. The permissions associated with each role determine the operations that each user is authorized to perform in Security Manager.

The following topics describe CiscoWorks roles:

- CiscoWorks Common Services Default Roles
- Assigning Roles to Users in CiscoWorks Common Services

CiscoWorks Common Services Default Roles

CiscoWorks Common Services contains the following default roles:

1. **Help Desk** Help desk users can view (but not modify) devices, policies, objects, and topology maps.
2. **Network Operator** In addition to view permissions, network operators can view CLI commands and Security Manager administrative settings. Network operators can also modify the configuration archive and issue commands (such as ping) to devices.
3. **Approver** In addition to view permissions, approvers can approve or reject deployment jobs. They cannot perform deployment.
4. **Network Administrator** Network administrators have complete view and modify permissions,

except for modifying administrative settings. They can discover devices and the policies configured on these devices, assign policies to devices, and issue commands to devices. Network administrators cannot approve activities or deployment jobs; however, they can deploy jobs that were approved by others.

5. **System Administrator** System administrators have complete access to all Security Manager permissions, including modification, policy assignment, activity and job approval, discovery, deployment, and issuing commands to devices.

Note: Additional roles, such as export data, might be displayed in Common Services if additional applications are installed on the server. The export data role is for third-party developers and is not used by Security Manager.

Tip: Although you cannot change the definition of CiscoWorks roles, you can define which roles are assigned to each user. For more information, see Assigning Roles to Users in CiscoWorks Common Services.

Assigning Roles to Users in CiscoWorks Common Services

CiscoWorks Common Services enables you to define which roles are assigned to each user. By changing the role definition for a user, you change the types of operations this user is authorized perform in Security Manager. For example, if you assign the Help Desk role, the user is limited to view operations and cannot modify any data. However, if you assign the Network Operator role, the user is also able to modify the configuration archive. You can assign multiple roles to each user.

Note: You must restart Security Manager after making changes to user permissions.

Procedure:

1. In Common Services, select **Server > Security**, then select **Single-Server Trust Management > Local User Setup** from the TOC.

Tip: To reach the Local User Setup page from within Security Manager, select Tools > Security Manager Administration > Server Security, then click Local User Setup.

2. Select the check box next to an existing user, then click **Edit**.
3. On the User Information page, select the roles to assign to this user by clicking the check boxes.

For more information about each role, see CiscoWorks Common Services Default Roles.

4. Click **OK** to save your changes.
5. Restart Security Manager.

Understanding Cisco Secure ACS Roles

Cisco Secure ACS provides greater flexibility for managing Security Manager permissions than does CiscoWorks because it supports application-specific roles that you can configure. Each role is made up of a set of permissions that determine the level of authorization to Security Manager tasks. In Cisco Secure ACS, you assign a role to each user group (and optionally, to individual users as well), which enables each user in that group to perform the operations authorized by the permissions defined for that role.

In addition, you can assign these roles to Cisco Secure ACS device groups, allowing permissions to be differentiated on different sets of devices.

Note: Cisco Secure ACS device groups are independent of Security Manager device groups.

The following topics describe Cisco Secure ACS roles:

- Cisco Secure ACS Default Roles
- Customizing Cisco Secure ACS Roles

Cisco Secure ACS Default Roles

Cisco Secure ACS includes the same roles as CiscoWorks (see Understanding CiscoWorks Roles), plus these additional roles:

1. **Security Approver** Security approvers can view (but not modify) devices, policies, objects, maps, CLI commands, and administrative settings. In addition, security approvers can approve or reject the configuration changes contained in an activity. They cannot approve or reject the deployment job, nor can they perform deployment.
2. **Security Administrator** In addition to having view permissions, security administrators can modify devices, device groups, policies, objects, and topology maps. They can also assign policies to devices and VPN topologies, and perform discovery to import new devices into the system.
3. **Network Administrator** In addition to view permissions, network administrators can modify the configuration archive, perform deployment, and issue commands to devices.

Note: The permissions contained in the Cisco Secure ACS network administrator role are different from those contained in the CiscoWorks network administrator role. For more information, see Understanding CiscoWorks Roles.

Unlike CiscoWorks, Cisco Secure ACS enables you to customize the permissions associated with each Security Manager role. For more information about modifying the default roles, see Customizing Cisco Secure ACS Roles.

Note: Cisco Secure ACS 3.3 or later must be installed for Security Manager authorization.

Customizing Cisco Secure ACS Roles

Cisco Secure ACS enables you to modify the permissions associated with each Security Manager role. You can also customize Cisco Secure ACS by creating specialized user roles with permissions that are targeted to particular Security Manager tasks.

Note: You must restart Security Manager after making changes to user permissions.

Procedure:

1. In Cisco Secure ACS, click **Shared Profile Components** on the navigation bar.
2. Click **Cisco Security Manager** on the Shared Components page. The roles that are configured for Security Manager are displayed.
3. Do one of the following:
 - ◆ To create a role, click **Add**. Go to Step 4.
 - ◆ To modify an existing role, click the role. Go to Step 5.
4. Enter a name for the role and, optionally, a description.
5. Select and deselect the check boxes in the permissions tree to define the permissions for this role

Selecting the check box for a branch of the tree selects all permissions in that branch. For example, selecting **Assign** selects all the assign permissions.

For a complete list of Security Manager permissions, see Security Manager Permissions.

Note: When you select modify, approve, assign, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager will not function properly.

6. Click **Submit** to save your changes.
7. Restart Security Manager.

Default Associations Between Permissions and Roles in Security Manager

This table shows how Security Manager permissions are associated with CiscoWorks Common Services roles and the default roles in Cisco Secure ACS.

Permissions	Roles							
	System Admin	Security Admin (ACS)	Security Approver (ACS)	Network Admin (CW)	Network Admin (ACS)	Approver	Network Operator	Help Desk
View Permissions								
View Device	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Topology	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View CLI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
View Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
View Config Archive	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Device Managers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Modify Permissions								
Modify Device	Yes	Yes	No	Yes	No	No	No	No
Modify Hierarchy	Yes	Yes	No	Yes	No	No	No	No
Modify Policy	Yes	Yes	No	Yes	No	No	No	No
Modify Image	Yes	Yes	No	Yes	No	No	No	No

Modify Objects	Yes	Yes	No	Yes	No	No	No	No
Modify Topology	Yes	Yes	No	Yes	No	No	No	No
Modify Admin	Yes	No	No	No	No	No	No	No
Modify Config Archive	Yes	Yes	No	Yes	Yes	No	Yes	No
Additional Permissions								
Assign Policy	Yes	Yes	No	Yes	No	No	No	No
Approve Policy	Yes	No	Yes	No	No	No	No	No
Approve CLI	Yes	No	No	No	No	Yes	No	No
Discover (Import)	Yes	Yes	No	Yes	No	No	No	No
Deploy	Yes	No	No	Yes	Yes	No	No	No
Control	Yes	No	No	Yes	Yes	No	Yes	No
Submit	Yes	Yes	No	Yes	No	No	No	No

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco Security Manager Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 30, 2007

Document ID: 91762

