CSM 3.x ：设置用户权限和角色

目录

简介

本文描述如何设置权限和角色对用户在Cisco Security Manager (CSM)。

先决条件

要求

本文假设， CSM安装并且适当地运作。

使用的组件

本文档中的信息根据CSM 3.1。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

设置用户权限

在您能登陆前， Cisco Security Manager验证您的用户名和密码。在他们验证后，安全经理设立您的在应用程序内的角色。此角色定义了您的权限(也呼叫权限)，是套任务或操作您授权执行。如果没有为某些任务或设备授权，相关菜单项、TOC项目和按钮隐藏或禁用。另外，消息告诉您您没有权限查看选定信息或执行选定操作。

安全经理的认证和授权由CiscoWorks服务器或思科安全访问控制服务器(ACS)管理。默认情况下，CiscoWorks管理认证和授权，通过使用在CiscoWorks Common Services的AAA模式设置页，但是您能变成Cisco Secure ACS。

使用Cisco Secure ACS主要优点是能力创建与专门化权限集的高颗粒的用户角色(例如，允许用户配置某一策略键入，但是不是其他)和能力限制用户到某些设备通过配置网络设备组(NDGs)。

以下主题描述用户权限：

- 安全经理权限
- 了解CiscoWorks角色
- 了解Cisco Secure ACS角色
- 在权限和角色之间的默认关联在安全经理

安全经理权限

安全经理分类权限到类别如显示：

1. **查看**—允许您查看当前设置。欲知更多信息，请参阅视图权限。
2. **修改**—允许您更改当前设置。欲知更多信息，请参阅修改权限。
3. **分配**—给您分配策略到设备和VPN拓扑。欲知更多信息，请参阅分配权限
4. **审批**—允许您批准策略变更和部署工作。欲知更多信息，请参阅审批权限。
5. **导入**—允许您导入在设备已经部署到安全经理的配置。
6. **部署**—允许您部署对设备的配置更改在您的网络和执行回退返回到一以前部署的配置。
7. **控制**—允许您发出命令到设备，例如ping。
8. **提交**—允许您提交您的配置更改为获得批准。

- 当您选择修改，分配，审批，导入，控制或者部署权限时，您必须也选择对应的视图权限;否则，安全经理不会正常运行。
- 当您选择修改策略权限时，您必须也选择对应分配并且查看策略权限。
- 当您允许作为其定义一部分，使用策略对象的策略时，您必须也同意视图权限到这些对象类型。例如，如果选择正在修改的路由策略的权限，您必须也选择查看的网络对象和接口角色的权限，是路由策略要求的对象类型。
- 同样适用，当允许作为其定义一部分，使用其他对象的对象。例如，如果选择正在修改的用户组的权限，您必须也选择查看的网络对象、ACL对象和AAA服务器组的权限。

查看权限

查看(在安全经理的只读)权限分开成类别如显示：

查看策略权限

安全经理包括策略的以下视图权限：

1. **查看>策略>防火墙。**允许您查看防火墙服务服务策略(查找在策略选择器在防火墙下)在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备。防火墙服务服务策略示例包括访问规则、AAA规则和检查规则。
2. **查看>策略>入侵防御系统。**允许您查看IPS策略(查找在策略选择器在IPS下)，包括运行在IOS路由器的IPS的策略。
3. **查看>策略>镜像。**允许您选择在应用IPS更新向导的一个签名更新包(查找在Tools>下请运用IPS更新)，但是不给您分配包到特定设备，除非也有修改>策略>镜像权限。
4. **查看>策略> NAT。**允许您查看在PIX/ASA/FWSM设备和IOS路由器的网络地址转换策略。NAT策略示例包括静态规则和动态规则。
5. **查看>策略>站点到站点VPN。**允许您查看在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备的站点到站点VPN策略。站点到站点VPN策略示例包括IKE建议， IPsec建议和预共享密匙。
6. **查看>策略>远程访问VPN。**允许您查看在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备的远程访问VPN策略。远程访问VPN策略示例包括IKE建议， IPsec建议和PKI策略。
7. **查看>策略> SSL VPN。**允许您查看在PIX/ASA/FWSM设备和IOS路由器的SSL VPN策略，例如SSL VPN向导。
8. **查看>策略>接口。**允许您查看接口策略(查找在策略选择器在接口下)在PIX/ASA/FWSM设备、IOS路由器、IPS传感器和Catalyst 6500/7600设备。在PIX/ASA/FWSM设备上，此权限包括硬件端口和接口设置。在IOS路由器上，此权限包括基本和先进的接口设置，以及其他接口相关的策略，例如DSL、PVC、PPP和拨号程序策略。在IPS传感器上，此权限包括物理接口和概略的地图。在Catalyst 6500/7600设备上，此权限包括接口和VLAN设置。
9. **查看>策略>桥接。**允许您查看ARP表策略(查找在策略选择器在平台下>桥接)在PIX/ASA/FWSM设备。
10. **查看>策略>设备管理。**允许您查看设备管理策略(查找在策略选择器在平台>设备Admin)下在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备：在PIX/ASA/FWSM设备上，示例包括设备访问修正，服务器访问策略和故障切换策略。在IOS路由器上，示例包括设备访问(包括线路访问)修正，服务器访问策略， AAA，并且获取设备设置。在IPS传感器上，此权限包括设备访问策略和服务器访问策略。在Catalyst 6500/7600设备上，此权限包括IDSM设置和VLAN访问列表。
11. **查看>策略>标识。**允许您查看标识策略(查找在策略选择器在平台>标识下)在Cisco IOS路由器，包括802.1x和网络准入控制(NAC)策略。
12. **查看>策略>记录日志。**允许您查看记录日志策略(查找在策略选择器在平台>记录日志下)在PIX/ASA/FWSM设备、IOS路由器和IPS传感器。记录日志策略示例包括记录日志设置、服务器设置和系统日志服务器策略。
13. **查看>策略>组播。**允许您查看组播策略(查找在策略选择器在平台>组播下)在PIX/ASA/FWSM设备。组播策略示例包括组播路由和IGMP策略。
14. **查看>策略> QoS。**允许您查看QoS策略(查找在策略选择器在平台>服务质量下)在Cisco IOS路由器。
15. **查看>策略>路由。**允许您查看路由策略(查找在策略选择器在平台>路由下)在

PIX/ASA/FWSM设备和IOS路由器。路由策略示例包括OSPF、RIP和静态路由策略。

16. **查看>策略> Security**。允许您查看安全策略(查找在策略选择器在平台> Security下)在PIX/ASA/FWSM设备和IPS传感器：在PIX/ASA/FWSM设备上，安全策略包括反电子欺骗、片段和超时设置。在IPS传感器上，安全策略包括阻塞设置。
17. **查看>策略>服务策略规则**。允许您查看服务策略规则策略(查找在策略选择器根据平台>服务策略规则)在PIX 7.x/ASA设备。示例包括优先级队列和IPS、QoS和连接规则。
18. **查看>策略>用户首选项**。允许您查看部署策略(查找在策略选择器在平台>用户首选项下)在PIX/ASA/FWSM设备。此策略包含清除的所有NAT转换一个选项在部署。
19. **查看>策略>虚拟设备**。允许您查看在IPS设备的虚拟传感器策略。此策略用于创建虚拟传感器。
20. **查看>策略> FlexConfig**。允许您查看FlexConfigs，是另外的CLI命令和说明可以在PIX/ASA/FWSM设备 ， IOS路由器和Catalyst 6500/7600设备被部署。

视图对象权限

安全经理包括对象的以下视图权限：

1. **查看>对象>AAA服务器组**。允许您查看AAA服务器组对象。这些对象用于要求AAA服务的策略(认证、授权和记帐)。
2. **查看>对象>AAA服务器**。允许您查看AAA服务器对象。这些对象代表作为AAA服务器组一部分，定义的各自的AAA服务器。
3. **查看>对象>访问控制列表-标准/延伸**。允许您查看标准和扩展ACL对象。扩展ACL对象使用各种各样的策略，例如NAT和美洲台和设立VPN访问。标准ACL对象使用这样策略象OSPF和SNMP，以及设立VPN访问。
4. **查看>对象>访问控制列表**- Web。允许您查看Web ACL对象。Web ACL对象在SSL VPN策略用于执行内容过滤。
5. **查看>对象> ASA用户组**。允许您查看ASA用户组对象。这些对象在ASA安全工具在Easy VPN、远程访问VPN和SSL VPN配置方面配置。
6. **查看>对象>类别**。允许您查看类别对象。这些对象容易地帮助您通过使用颜色识别规则和对象在规则表里。
7. **查看>对象>凭证**。允许您查看证件对象。在IKE扩展身份验证(Xauth)期间，这些对象用于Easy VPN配置。
8. **查看>对象> FlexConfigs**。允许您查看FlexConfig对象。这些对象，包含与另外的脚本语言说明的配置命令，可以用于配置安全经理用户界面不支持的命令。
9. **查看>对象> IKE Proposals**。允许您查看IKE建议对象。这些对象包含为在远程访问VPN策略的IKE建议要求的参数。
10. **查看>对象> Inspect -类映射**- DNS.允许您查看DNS类映射对象。这些对象匹配与特定标准的DNS流量，以便操作在该流量可以进行。
11. **查看>对象> Inspect -类映射- FTP**。允许您查看FTP类映射对象。这些对象匹配与特定标准的FTP流量，以便操作在该流量可以进行。
12. **查看>对象> Inspect -类映射- HTTP**.允许您查看HTTP类别映射对象。这些对象匹配与特定标准的HTTP数据流，以便操作在该流量可以进行。
13. **查看>对象> Inspect -类映射- IM**.允许您查看IM类映射对象。这些对象匹配与特定标准的IM流量，以便操作在该流量可以进行。
14. **查看>对象> Inspect -类映射- SIP**.允许您查看SIP类映射对象。这些对象匹配与特定标准的SIP流量，以便操作在该流量可以进行。
15. **查看>对象> Inspect -策略映射- DNS.**允许您查看DNS策略映射对象。这些对象用于创建DNS流量的检查地图。

16. **查看>对象> Inspect -策略映射- FTP。**允许您查看FTP策略映射对象。这些对象用于创建FTP流量的检查地图。
17. **查看>对象> Inspect -策略映射- GTP。**允许您查看GTP策略映射对象。这些对象用于创建GTP流量的检查地图。
18. **查看>对象> Inspect -策略映射- HTTP (ASA7.1.x/PIX7.1.x/IOS)。**允许您查看HTTP为ASA/PIX 7.1.x设备和IOS路由器创建的策略映射对象。这些对象用于创建HTTP数据流的检查地图。
19. **查看>对象> Inspect -策略映射- HTTP (ASA7.2/PIX7.2)。**允许您查看HTTP为ASA7.2/PIX7.2设备创建的策略映射对象。这些对象用于创建HTTP数据流的检查地图。
20. **查看>对象> Inspect -策略映射- IM (ASA7.2/PIX7.2)。**允许您查看IM为ASA7.2/PIX7.2设备创建的策略映射对象。这些对象用于创建IM流量的检查地图。
21. **查看>对象> Inspect -策略映射- IM (IOS)。**允许您查看IM为IOS设备创建的策略映射对象。这些对象用于创建IM流量的检查地图。
22. **查看>对象> Inspect -策略映射- SIP**.允许您查看SIP策略映射对象。这些对象用于创建SIP流量的检查地图。
23. **查看>对象> Inspect -常规表达。**允许您查看常规表示对象。作为一常规表示组一部分，定义的这些对象代表单个常规表达。
24. **查看>对象> Inspect -常规表达组。**允许您查看常规表示组对象。部分组地图和Inspect地图用于这些对象匹配文本在数据包里面。
25. **查看>对象> Inspect - TCP映射。**允许您查看TCP地图对象。在TCP流的这些对象自定义检查在两个方向。
26. **查看>对象>接口角色。**允许您查看接口角色对象。这些对象定义了能代表在不同种类的多个接口的设备的名字模式。接口角色enable (event)运用策略的您对在多个设备的特定接口，而不必手工定义每个接口名称。
27. **查看>对象> IPsec转换集。**允许您查看IPsec转换集合对象。这些对象包括正确地指定的组合安全协议、算法和其他设置在IPSec隧道的数据如何将加密并且验证。
28. **查看>对象> LDAP属性地图。**允许您查看LDAP属性地图对象。这些对象用于映射自定义(用户定义的)属性名称到思科LDAP属性名称。
29. **查看>对象>网络/主机。**允许您查看网络/host对象。这些对象是代表网络，主机或者两个的逻辑集合IP地址。网络/host对象使您定义策略，无需指定每网络或单个主机。
30. **查看>对象> PKI登记。**允许您查看PKI登记对象。这些对象定义了在公共钥匙结构内运行的认证机构(CA)服务器。
31. **查看>对象>波尔特转发列表。**允许您查看端口转发列表对象。这些对象定义了端口号映射在远程客户端的到应用程序的IP地址和端口在SSL VPN网关背后。
32. **查看>对象>安全桌面配置。**允许您查看安全桌面配置对象。这些对象是可以由SSL VPN策略参考提供排除敏感数据所有跟踪可靠的手段共享处于SSL VPN会话的可再用，已命名组件。
33. **查看>对象> Services -端口列表。**允许您查看端口列表对象。这些对象，包含一个或更多端口范围编号，用于简化创建服务对象进程。
34. **查看>对象> Services/服务组**允许您查看服务和服务组对象。这些对象是描述网络服务使用由策略，例如Kerberos、SSH和POP3协议和端口定义的定义的映射。
35. **查看>对象>在服务器的单个符号。**允许您查看在服务器对象的单个符号。单一登录(SSO)让SSL VPN用户一次输入用户名和密码和能访问多个保护的服务和Web服务器。
36. **查看>对象> SLA监视器。**允许您查看SLA监视器对象。PIX/ASA运行版本7.2或以上的安全工具使用这些对象执行路由追踪。如果主路由出故障，此功能提供一个方法跟踪主路由的可用性和安装备份路由。
37. **查看>对象> SSL VPN自定义。**允许您查看SSL VPN自定义对象。这些对象定义了如何更改的SSL VPN页外观显示给用户，例如洛金/logout和主页。
38. **查看>对象> SSL VPN网关。**允许您查看SSL VPN网关对象。这些对象定义了启用使用的网

关作为代理对已保护资源的连接在您的SSL VPN的参数。

39. **查看>对象>斯太尔对象。**允许您查看样式对象。这些对象让您配置样式元素，例如字体特性和颜色，定制出版给SSL VPN用户SSL VPN页的外观，当他们连接到安全工具时。
40. **查看>对象>文本对象。**允许您查看自由形态的文本对象。这些对象包括一个名称和值对，值可以是单个字符串、字符串列表或者字符串表。
41. **查看>对象>时间范围。**允许您查看时间范围对象。这些对象，当创建基于时间的ACL和检查规则时，使用。在周期间时，当定义ASA用户组限制对特定时间的VPN访问他们也用于。
42. **查看>对象>通信流。**允许您查看通信流对象。这些对象定义了供PIX 7.x/ASA 7.x设备使用的特定的流量流。
43. **查看>对象> URL列表。**允许您查看URL列表对象。这些对象定义了在入口页面显示在成功登录以后的URL。当操作在无客户端接入模式时，这使用户访问资源可以找到在SSL VPN网站。
44. **查看>对象>用户组。**允许您查看用户组对象。这些对象定义了在Easy VPN拓扑、远程访问VPN和SSL VPN使用远程客户端的组。
45. **查看>对象> WINS服务器列表。**允许您查看WINS服务器列表对象。这些对象代表WINS服务器， SSL用于VPN访问或共享在远程系统的文件。
46. **查看>对象>内部- DN规定。**允许您查看DN策略使用的DN规则。这是在策略对象管理器没出现的安全经理使用的一个内部对象。
47. **查看>对象>内部客户端更新。**这是在策略对象管理器没出现用户组对象要求的一个内部对象。
48. **查看>对象>内部-英文虎报ACE。**这是标准的访问控制条目的一个内部对象， ACL对象使用。
49. **查看>对象>内部-延长的ACE。**这是延长的访问控制条目的一个内部对象， ACL对象使用。

另外的视图权限

安全经理包括下列各项视图权限：

1. **查看> Admin。**允许您查看安全经理管理设置。
2. **查看> CLI。**允许您查看在设备配置的CLI命令和预览将部署的命令。
3. **查看>config存档。**允许您查看在配置存档包含的配置列表。您不能查看设备配置或任何CLI命令。
4. **查看>设备。**允许您查看设备视线内设备视图和所有相关信息，包括他们的设备设置，属性，分配，等等。
5. **查看>设备管理器。**允许您发行设备管理器的只读版本各台设备的，例如思科路由器和安全设备管理器(SDM) Cisco IOS路由器的。
6. **查看>拓扑。**允许您查看在地图视图配置的地图。

修改权限

在安全经理的修改(读写)权限分开成类别如显示：

- 修改策略权限
- 修改对象权限
- 另外的修改权限

修改策略权限

注意： 当您指定修改策略权限时，请确保您选择对应分配并且查看策略权限。

安全经理包括策略的以下修改权限：

1. **修改>策略>防火墙**。允许您修改防火墙服务服务策略(查找在策略选择器在防火墙下)在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备。防火墙服务服务策略示例包括访问规则、AAA规则和检查规则。
2. **修改>策略>入侵防御系统**。允许您修改IPS策略(查找在策略选择器在IPS下)，包括运行在IOS路由器的IPS的策略。此权限也允许您调整在签名更新向导的签名(查找在Tools>下请运用IPS更新)。
3. **修改>策略>镜像**。给您分配每签名更新包到在应用IPS更新向导的设备(查找在Tools>下请运用IPS更新)。此权限也给您分配自动更新设置到特定设备(查找在Tools > Security管理器管理> IPS更新下)。
4. **修改>策略> NAT**。允许您修改在PIX/ASA/FWSM设备和IOS路由器的网络地址转换策略。NAT策略示例包括静态规则和动态规则。
5. **修改>策略>站点到站点VPN**。允许您修改在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备的站点到站点VPN策略。站点到站点VPN策略示例包括IKE建议， IPsec建议和预共享密匙。
6. **修改>策略>远程访问VPN**。允许您修改在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备的远程访问VPN策略。远程访问VPN策略示例包括IKE建议， IPsec建议和PKI策略。
7. **修改>策略> SSL VPN**。允许您修改在PIX/ASA/FWSM设备和IOS路由器的SSL VPN策略，例如SSL VPN向导。
8. **修改>策略>接口**。允许您修改接口策略(查找在策略选择器在接口下)在PIX/ASA/FWSM设备、IOS路由器、IPS传感器和Catalyst 6500/7600设备：在PIX/ASA/FWSM设备上，此权限包括硬件端口和接口设置。在IOS路由器上，此权限包括基本和先进的接口设置，以及其他接口相关的策略，例如DSL、PVC、PPP和拨号程序策略。在IPS传感器上，此权限包括物理接口和概略的地图。在Catalyst 6500/7600设备上，此权限包括接口和VLAN设置。
9. **修改>策略>桥接**。允许您修改ARP表策略(查找在策略选择器在平台下>桥接)在PIX/ASA/FWSM设备。
10. **修改>策略>设备管理**。允许您修改设备管理策略(查找在策略选择器在平台>设备Admin)下在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备：在PIX/ASA/FWSM设备上，示例包括设备访问修正，服务器访问策略和故障切换策略。在IOS路由器上，示例包括设备访问(包括线路访问)修正，服务器访问策略， AAA，并且获取设备设置。在IPS传感器上，此权限包括设备访问策略和服务器访问策略。在Catalyst 6500/7600设备上，此权限包括IDSM设置和VLAN访问列表。
11. **修改>策略>标识**。允许您修改标识策略(查找在策略选择器在平台>标识下)在Cisco IOS路由器，包括802.1x和网络准入控制(NAC)策略。
12. **修改>策略>记录日志**。允许您修改记录日志策略(查找在策略选择器在平台>记录日志下)在PIX/ASA/FWSM设备、IOS路由器和IPS传感器。记录日志策略示例包括记录日志设置、服务器设置和系统日志服务器策略。
13. **修改>策略>组播**。允许您修改组播策略(查找在策略选择器在平台>组播下)在PIX/ASA/FWSM设备。组播策略示例包括组播路由和IGMP策略。
14. **修改>策略> QoS**。允许您修改QoS策略(查找在策略选择器在平台>服务质量下)在Cisco IOS路由器。
15. **修改>策略>路由**。允许您修改路由策略(查找在策略选择器在平台>路由下)在PIX/ASA/FWSM设备和IOS路由器。路由策略示例包括OSPF、RIP和静态路由策略。
16. **修改>策略> Security**。允许您修改安全策略(查找在策略选择器在平台> Security下)在

PIX/ASA/FWSM设备和IPS传感器：在PIX/ASA/FWSM设备上，安全策略包括反电子欺骗、片段和超时设置。在IPS传感器上，安全策略包括阻塞设置。

17. **修改>策略>服务策略规则**。允许您修改服务策略规则策略(查找在策略选择器根据平台>服务策略规则)在PIX 7.x/ASA设备。示例包括优先级队列和IPS、QoS和连接规则。
18. **修改>策略>用户首选项**。允许您修改部署策略(查找在策略选择器在平台>用户首选项下)在PIX/ASA/FWSM设备。此策略包含清除的所有NAT转换一个选项在部署。
19. **修改>策略>虚拟设备**。允许您修改在IPS设备的虚拟传感器策略。请使用此策略创建虚拟传感器。
20. **修改>策略> FlexConfig**。允许您修改FlexConfigs，是另外的CLI命令和说明可以在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备被部署。

修改对象权限

安全经理包括对象的以下视图权限：

1. **修改>对象>AAA服务器组**。允许您查看AAA服务器组对象。这些对象用于要求AAA服务的策略(认证、授权和记帐)。
2. **修改>对象>AAA服务器**。允许您查看AAA服务器对象。这些对象代表作为AAA服务器组一部分，定义的各自的AAA服务器。
3. **修改>对象>访问控制列表-标准/延伸**。允许您查看标准和扩展ACL对象。扩展ACL对象使用各种各样的策略，例如NAT和美洲台和设立VPN访问。标准ACL对象使用这样策略象OSPF和SNMP，以及设立VPN访问。
4. **修改>对象>访问控制列表- Web**。允许您查看Web ACL对象。Web ACL对象在SSL VPN策略用于执行内容过滤。
5. **修改>对象> ASA用户组**。允许您查看ASA用户组对象。这些对象在ASA安全工具在Easy VPN、远程访问VPN和SSL VPN配置方面配置。
6. **修改>对象>类别**。允许您查看类别对象。这些对象容易地帮助您通过使用颜色识别规则和对象在规则表里。
7. **修改>对象>凭证**。允许您查看证件对象。在IKE扩展身份验证(Xauth)期间，这些对象用于Easy VPN配置。
8. **修改>对象> FlexConfigs**。允许您查看FlexConfig对象。这些对象，包含与另外的脚本语言说明的配置命令，可以用于配置安全经理用户界面不支持的命令。
9. **修改>对象> IKE Proposals**。允许您查看IKE建议对象。这些对象包含为在远程访问VPN策略的IKE建议要求的参数。
10. **修改>对象> Inspect -类映射- DNS**.允许您查看DNS类映射对象。这些对象匹配与特定标准的DNS流量，以便操作在该流量可以进行。
11. **修改>对象> Inspect -类映射- FTP**。允许您查看FTP类映射对象。这些对象匹配与特定标准的FTP流量，以便操作在该流量可以进行。
12. **修改>对象> Inspect -类映射- HTTP**.允许您查看HTTP类别映射对象。这些对象匹配与特定标准的HTTP数据流，以便操作在该流量可以进行。
13. **修改>对象> Inspect -类映射- IM**.允许您查看IM类映射对象。这些对象匹配与特定标准的IM流量，以便操作在该流量可以进行。
14. **修改>对象> Inspect -类映射- SIP**.允许您查看SIP类映射对象。这些对象匹配与特定标准的SIP流量，以便操作在该流量可以进行。
15. **修改>对象> Inspect -策略映射- DNS**.允许您查看DNS策略映射对象。这些对象用于创建DNS流量的检查地图。
16. **修改>对象> Inspect -策略映射- FTP**。允许您查看FTP策略映射对象。这些对象用于创建FTP流量的检查地图。

17. **修改>对象> Inspect -策略映射- HTTP (ASA7.1.x/PIX7.1.x/IOS)**。允许您查看HTTP为ASA/PIX 7.x设备和IOS路由器创建的策略映射对象。这些对象用于创建HTTP数据流的检查地图。
18. **修改>对象> Inspect -策略映射- HTTP (ASA7.2/PIX7.2)**。允许您查看HTTP为ASA7.2/PIX7.2设备创建的策略映射对象。这些对象用于创建HTTP数据流的检查地图。
19. **修改>对象> Inspect -策略映射- IM (ASA7.2/PIX7.2)**。允许您查看IM为ASA7.2/PIX7.2设备创建的策略映射对象。这些对象用于创建IM流量的检查地图。
20. **修改>对象> Inspect -策略映射- IM (IOS)**。允许您查看IM为IOS设备创建的策略映射对象。这些对象用于创建IM流量的检查地图。
21. **修改>对象> Inspect -策略映射- SIP**.允许您查看SIP策略映射对象。这些对象用于创建SIP流量的检查地图。
22. **修改>对象> Inspect -常规表达**。允许您查看常规表示对象。作为一常规表示组一部分，定义的这些对象代表单个常规表达。
23. **修改>对象> Inspect -常规表达组**。允许您查看常规表示组对象。部分组地图和Inspect地图用于这些对象匹配文本在数据包里面。
24. **修改>对象> Inspect - TCP地图**。允许您查看TCP地图对象。在TCP流的这些对象自定义检查在两个方向。
25. **修改>对象>接口角色**。允许您查看接口角色对象。这些对象定义了能代表在不同种类的多个接口的设备的名字模式。接口角色enable (event)运用策略的您对在多个设备的特定接口，而不必手工定义每个接口名称。
26. **修改>对象> IPsec转换集**。允许您查看IPsec转换集合对象。这些对象包括正确地指定的组合安全协议、算法和其他设置在IPSec隧道的数据如何将加密并且验证。
27. **修改>对象> LDAP属性地图**。允许您查看LDAP属性地图对象。这些对象用于映射自定义(用户定义的)属性名称到思科LDAP属性名称。
28. **修改>对象>网络/主机**。允许您查看网络/host对象。这些对象是代表网络，主机或者两个的逻辑集合IP地址。网络/host对象使您定义策略，无需指定每网络或单个主机。
29. **修改>对象> PKI登记**。允许您查看PKI登记对象。这些对象定义了在公共钥匙结构内运行的认证机构(CA)服务器。
30. **修改>对象>波尔特转发列表**。允许您查看端口转发列表对象。这些对象定义了端口号映射在远程客户端的到应用程序的IP地址和端口在SSL VPN网关背后。
31. **修改>对象>安全桌面配置**。允许您查看安全桌面配置对象。这些对象是可以由SSL VPN策略参考提供排除敏感数据所有跟踪可靠的手段共享处于SSL VPN会话的可再用，已命名组件。
32. **修改>对象> Services -端口列表**。允许您查看端口列表对象。这些对象，包含一个或更多端口范围编号，用于简化创建服务对象进程。
33. **修改>对象> Services/服务组。**允许您查看服务和服务组对象。这些对象是描述网络服务使用由策略，例如Kerberos、SSH和POP3协议和端口定义的定义的映射。
34. **修改>对象>在服务器的单个符号。**允许您查看在服务器对象的单个符号。单一登录(SSO)让SSL VPN用户一次输入用户名和密码和能访问多个保护的服务和Web服务器。
35. **修改>对象> SLA监视器**。允许您查看SLA监视器对象。PIX/ASA运行版本7.2或以上的安全工具使用这些对象执行路由追踪。如果主路由出故障，此功能提供一个方法跟踪主路由的可用性和安装备份路由。
36. **修改>对象> SSL VPN自定义**。允许您查看SSL VPN自定义对象。这些对象定义了如何更改的SSL VPN页外观显示给用户，例如洛金/logout和主页。
37. **修改>对象> SSL VPN网关**。允许您查看SSL VPN网关对象。这些对象定义了启用使用的网关作为代理对已保护资源的连接在您的SSL VPN的参数。
38. **修改>对象>斯太尔对象**。允许您查看样式对象。这些对象让您配置样式元素，例如字体特性和颜色，定制出版给SSL VPN用户SSL VPN页的外观，当他们连接到安全工具时。
39. **修改>对象>文本对象**。允许您查看自由形态的文本对象。这些对象包括一个名称和值对，值

可以是单个字符串、字符串列表或者字符串表。

40. **修改>对象>时间范围。**允许您查看时间范围对象。这些对象，当创建基于时间的ACL和检查规则时，使用。在周期间时，当定义ASA用户组限制对特定时间的VPN访问他们也用于。
41. **修改>对象>通信流。**允许您查看通信流对象。这些对象定义了供PIX 7.x/ASA 7.x设备使用的特定的流量流。
42. **修改>对象> URL列表。**允许您查看URL列表对象。这些对象定义了在入口页面显示在成功登录以后的URL。当操作在无客户端接入模式时，这使用户访问资源可以找到在SSL VPN网站。
43. **修改>对象>用户组。**允许您查看用户组对象。这些对象定义了在Easy VPN拓扑、远程访问VPN和SSL VPN使用远程客户端的组
44. **修改>对象> WINS服务器列表。**允许您查看WINS服务器列表对象。这些对象代表WINS服务器， SSL用于VPN访问或共享在远程系统的文件。
45. **修改>对象>内部- DN规则。**允许您查看DN策略使用的DN规则。这是在策略对象管理器没出现的安全经理使用的一个内部对象。
46. **修改>对象>内部客户端更新。**这是在策略对象管理器没出现用户组对象要求的一个内部对象。
47. **修改>对象>内部-英文虎报ACE。**这是标准的访问控制条目的一个内部对象， ACL对象使用。
48. **修改>对象>内部-延长的ACE。**这是延长的访问控制条目的一个内部对象， ACL对象使用。

另外的修改权限

安全经理包括另外的修改权限如显示：

1. **修改> Admin。**允许您修改安全经理管理设置。
2. **修改>config存档。**在配置存档允许您修改设备配置。另外，它给您添加配置到存档并且定制配置存档工具。
3. **修改>设备。**给您添加和删除设备，以及修改设备属性和属性。要发现在已添加设备的策略，您必须也启用导入权限。另外，如果启用修改>设备权限，请确保您也启用分配>策略>接口权限。
4. **修改>层级。**允许您修改设备组。
5. **修改>拓扑。**允许您修改在地图视图的地图。

分配权限

安全经理包括分配权限如显示：

1. **分配>策略>防火墙。**给您分配防火墙服务服务策略(查找在策略选择器在防火墙下)到PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备。防火墙服务服务策略示例包括访问规则、AAA规则和检查规则。
2. **分配>策略>入侵防御系统。**允许您分配IPS策略(查找在策略选择器在IPS下)，包括策略运行在IOS路由器的IPS。
3. **分配>策略>镜像。**安全经理当前没有使用此权限。
4. **分配>策略> NAT。**给您分配网络地址转换策略到PIX/ASA/FWSM设备和IOS路由器。NAT策略示例包括静态规则和动态规则。
5. **分配>策略>站点到站点VPN。**给您分配站点到站点VPN策略到PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备。站点到站点VPN策略示例包括IKE建议， IPsec建议和预共享密匙。

6. **分配>策略>远程访问VPN**。给您分配远程访问VPN策略到PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备。远程访问VPN策略示例包括IKE建议， IPsec建议和PKI策略。
7. **分配>策略> SSL VPN**。给您分配SSL VPN策略到PIX/ASA/FWSM设备和IOS路由器，例如SSL VPN向导。
8. **分配>策略>接口**。给您分配接口策略(查找在策略选择器在接口下)到PIX/ASA/FWSM设备，IOS路由器和Catalyst 6500/7600设备：在PIX/ASA/FWSM设备上，此权限包括硬件端口和接口设置。在IOS路由器上，此权限包括基本和先进的接口设置，以及其他接口相关的策略，例如DSL、PVC、PPP和拨号程序策略。在Catalyst 6500/7600设备上，此权限包括接口和VLAN设置。
9. **分配>策略>桥接**。给您分配ARP表策略(查找在策略选择器在平台下>桥接)到PIX/ASA/FWSM设备。
10. **分配>策略>设备管理**。给您分配设备管理策略(查找在策略选择器在平台>设备Admin)下到PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备：在PIX/ASA/FWSM设备上，示例包括设备访问修正，服务器访问策略和故障切换策略。在IOS路由器上，示例包括设备访问(包括线路访问)修正，服务器访问策略， AAA，并且获取设备设置。在IPS传感器上，此权限包括设备访问策略和服务器访问策略。在Catalyst 6500/7600设备上，此权限包括IDSM设置和VLAN访问列表。
11. **分配>策略>标识**。给您分配标识策略(查找在策略选择器在平台>标识下)到Cisco IOS路由器，包括802.1x和网络准入控制(NAC)策略。
12. **分配>策略>记录日志**。给您记录策略的分配(查找在策略选择器在平台>记录日志下)对PIX/ASA/FWSM设备和IOS路由器。记录日志策略示例包括记录日志设置、服务器设置和系统日志服务器策略。
13. **分配>策略>组播**。给您分配组播策略(查找在策略选择器在平台>组播下)到PIX/ASA/FWSM设备。组播策略示例包括组播路由和IGMP策略。
14. **分配>策略> QoS**。给您分配QoS策略(查找在策略选择器在平台>服务质量下)到Cisco IOS路由器。
15. **分配>策略>路由**。给您分配路由策略(查找在策略选择器在平台>路由下)到PIX/ASA/FWSM设备和IOS路由器。路由策略示例包括OSPF、RIP和静态路由策略。
16. **分配>策略> Security**。给您分配安全策略(查找在策略选择器在平台> Security下)到PIX/ASA/FWSM设备。安全策略包括反电子欺骗、片段和超时设置。
17. **分配>策略>服务策略规则**。给您分配服务策略规则策略(查找在策略选择器根据平台>服务策略规则)到PIX 7.x/ASA设备。示例包括优先级队列和IPS、QoS和连接规则。
18. **分配>策略>用户首选项**。给您分配部署策略(查找在策略选择器在平台>用户首选项下)到PIX/ASA/FWSM设备。此策略包含清除的所有NAT转换一个选项在部署。
19. **分配>策略>虚拟设备**。给您分配虚拟传感器策略到IPS设备。请使用此策略创建虚拟传感器。
20. **分配>策略> FlexConfig**。给您分配FlexConfigs，是另外的CLI命令和说明可以在PIX/ASA/FWSM设备， IOS路由器和Catalyst 6500/7600设备被部署。

注意： 当您指定时请分配权限，确保，您选择对应的视图权限。

审批权限

安全经理提供审批权限如显示：

1. **审批> CLI**。允许您审批包含的CLI命令变化在部署工作上。
2. **审批>Policy**。允许您审批包含的配置更改在工作流活动配置的策略。

了解CiscoWorks角色

当用户在CiscoWorks Common Services时创建，他们分配一个或更多角色。权限关联与每个角色确定每个用户在安全经理授权执行的操作。

以下主题描述CiscoWorks角色：

CiscoWorks Common Services默认角色

CiscoWorks Common Services包含以下默认角色：

1. **支持中心**—支持中心用户能查看(但是不是修改)设备、策略、对象和拓扑图。
2. **网络操作员**—除视图权限之外，网络操作员能查看CLI命令和安全经理管理设置。网络操作员能也修改配置存档和发出命令(例如ping)到设备。
3. **审批人**—除视图权限之外，审批人能批准或拒绝部署工作。他们不可进行部署。
4. **网络管理员**—网络管理员有完整视图并且修改权限，除了正在修改的管理设置。他们能发现设备和在这些设备配置的策略，分配策略到设备和发出命令到设备。网络管理员不能批准活动或部署工作;然而，他们能部署由其他审批的工作。
5. **系统管理员**—系统管理员得以进入对所有安全经理权限的完整，包括修改、分配、活动和工作批准、发现，部署和发出命令对设备。

注意： 如果另外的应用程序在服务器，安装另外的作用，例如出口数据，也许显示在普通的服务中。是为第三方开发商和安全经理没有使用出口数据角色。

提示： 虽然您不能更改CiscoWorks角色的定义，您能定义哪些角色分配到每个用户。欲知更多信息，请参阅分配角色到用户在CiscoWorks Common Services。

分配角色到用户在CiscoWorks Common Services

CiscoWorks Common Services使您定义哪些角色分配到每个用户。通过更改角色用户的定义，您更改此用户在安全经理授权实行操作的种类。例如，如果分配支持中心角色，用户被限制查看操作，并且不能修改任何数据。然而，如果分配网络操作员角色，用户也能修改配置存档。您能分配多个角色到每个用户。

注意： 您必须重新启动安全经理，在对用户权限后的进行的更改。

步骤：

1. 在普通的服务中，请选择**Server>安全**，然后选择**单服务器托拉斯**从TOC**设置的Management>本地用户**。**提示：** 要到达本地用户设置页从安全经理的内部，请选择Tools > Security管理器管理>Server安全，然后点击本地用户设置。
2. 在一个现有用户旁边选择复选框，然后单击**编辑**。
3. 在User Information页，请选择角色分配给此用户通过单击复选框。关于每个角色的更多信息，请参阅CiscoWorks Common Services默认角色。
4. 点击OK键保存您的更改。
5. 重新启动安全经理。

了解Cisco Secure ACS角色

Cisco Secure ACS为管理安全经理权限比CiscoWorks提供较大适应性，因为支持您能配置的专用角色。每个角色组成确定级别授权对安全经理任务的一套权限。在Cisco Secure ACS，您分配角色到每个用户组(和或者，对个人用户)，在该组中使每个用户执行操作由为该角色定义的权限授权。

另外，您在不同的一套设备能分配这些角色到Cisco Secure ACS设备组，允许权限被区分。

注意： Cisco Secure ACS设备组对立于安全经理设备组。

以下主题描述Cisco Secure ACS角色：

Cisco Secure ACS默认角色

Cisco Secure ACS包括角色和CiscoWorks一样(请参阅了解CiscoWorks角色)，加上这些另外的角色：

1. **安全审批人**—安全审批人能查看(但是不是修改)设备、策略、对象、地图、CLI命令和管理设置。另外，安全审批人能审批或拒绝包含的配置更改在活动。他们不能批准或拒绝部署工作，亦不可他们进行部署。
2. **安全管理员**—除有之外视图权限，安全管理员能修改设备、设备组、策略、对象和拓扑图。他们能也分配策略到设备和VPN拓扑，并且进行发现插入新建的设备到系统。
3. **网络管理员**—除视图权限之外，网络管理员能修改配置存档，进行部署和发出命令到设备。

注意： 在Cisco Secure ACS网络管理员角色包含的权限是与在CiscoWorks网络管理员角色包含的那些不同。欲知更多信息，请参阅了解CiscoWorks角色。

不同于CiscoWorks， Cisco Secure ACS使您定制权限关联与每个安全经理角色。关于的更多信息正在修改默认角色，参见定制Cisco Secure ACS角色。

注意： 必须为安全经理授权安装Cisco Secure ACS 3.3或以后。

定制Cisco Secure ACS角色

Cisco Secure ACS使您修改权限关联与每个安全经理角色。您能通过创建与被瞄准对特定的安全经理任务的权限的专门化用户角色也定制Cisco Secure ACS。

注意： 您必须重新启动安全经理，在对用户权限后的进行的更改。

步骤：

1. 在Cisco Secure ACS，请点击在导航条的**共享配置文件组件**。
2. 点击共享组件页的**Cisco Security Manager**。为安全经理配置的角色显示。
3. 执行以下操作之一：要创建角色，请单击**添加**。转到第 4 步。要修改一个现有角色，请点击角色。进入步骤5。
4. 输入一名称对于角色，并且，或者，说明。
5. 选择并且取消选定在权限树的复选框定义此角色的权限选择树的分组的复选框选择在该分组的

所有权限。例如，选择**分配**选择所有分配权限。关于安全经理权限完整列表，请参阅安全经理权限。**注意：** 当您选择修改，审批，分配，导入，控制或者部署权限时，您必须也选择对应的视图权限;否则，安全经理不会正常运行。

6. 单击 **Submit** 以保存更改。
7. 重新启动安全经理。

默认在权限和角色之间的关联在安全经理

此表显示安全经理权限如何关联与CiscoWorks Common Services作用和默认作用在Cisco Secure ACS。

权限	角色							
	系统管理员	安全Admin (ACS)	安全审批人 (ACS)	网络Admin (CW)	网络Admin (ACS)	审批人	网络操作员	帮助台
查看权限								
查看设备	是	是	是	是	是	是	是	是
查看策略	是	是	是	是	是	是	是	是
视图对象	是	是	是	是	是	是	是	是
查看拓扑	是	是	是	是	是	是	是	是
查看CLI	是	是	是	是	是	是	是	否
查看Admin	是	是	是	是	是	是	是	否
查看配置存档	是	是	是	是	是	是	是	是
查看设备管理器	是	是	是	是	是	是	是	否
修改权限								
修改设备	是	是	否	是	否	否	否	否
修改层级	是	是	否	是	否	否	否	否
修改策略	是	是	否	是	否	否	否	否
修改镜像	是	是	否	是	否	否	否	否
修改对象	是	是	否	是	否	否	否	否
修改拓扑	是	是	否	是	否	否	否	否
修改Admin	是	否	否	否	否	否	否	否
修改配置存档	是	是	否	是	是	否	是	否
另外的权限								
分配策略	是	是	否	是	否	否	否	否
审批策略	是	否	是	否	否	否	否	否
审批CLI	是	否	否	否	否	是	否	否

发现(导入)	是	是	否	是	否	否	否	否
部署	是	否	否	是	是	否	否	否
控制	是	否	否	是	是	否	是	否
提交	是	是	否	是	否	否	否	否

相关信息

- Cisco Security Manager支持页面
- 技术支持和文档 - Cisco Systems