CSM 3.x ：设置用户权限和角色

目录

简介

本文档介绍如何在思科安全管理器(CSM)中为用户设置权限和角色。

先决条件

要求

本文档假设CSM已安装且工作正常。

使用的组件

本文档中的信息基于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

思科安全管理器在您登录之前对用户名和密码进行身份验证。通过身份验证后，安全管理器将在应用中建立您的角色。此角色定义您的权限（也称为权限），这些权限是您有权执行的一组任务或操作。如果您没有授权执行某些任务或设备，则相关菜单项、目录项和按钮将被隐藏或禁用。此外，一条消息会告诉您您没有查看所选信息或执行所选操作的权限。

安全管理器的身份验证和授权由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管理身份验证和授权，但您可以使用CiscoWorks公共服务中的AAA模式设置页面更改为Cisco Secure ACS。

使用Cisco Secure ACS的主要优势是能够创建具有专用权限集的高度精细的用户角色（例如，允许用户配置某些策略类型，但不配置其他策略类型），以及通过配置网络设备组(NDG)将用户限制到某些设备。

以下主题介绍用户权限：

- 安全管理器权限
- 了解CiscoWorks角色
- 了解Cisco Secure ACS角色
- 安全管理器中权限和角色之间的默认关联

安全管理器权限

安全管理器将权限分类为以下类别：

1. **View** — 用于查看当前设置。有关详细信息，请参阅查看权限。
2. **修改** — 允许您更改当前设置。有关详细信息，请参阅修改权限。
3. **Assign** — 允许您将策略分配给设备和VPN拓扑。有关详细信息，请参阅分配权限
4. **批准** — 允许您批准策略更改和部署作业。有关详细信息，请参阅批准权限。
5. **导入** — 允许您将已在设备上部署的配置导入安全管理器。
6. **Deploy** — 允许您将配置更改部署到网络中的设备并执行回滚以返回以前部署的配置。
7. **Control** — 允许您向设备发出命令，例如ping。
8. **Submit** — 允许您提交配置更改供审批。

- 在选择修改、分配、批准、导入、控制或部署权限时，还必须选择相应的查看权限；否则，安全管理器将无法正常运行。
- 选择修改策略权限时，还必须选择相应的分配和查看策略权限。
- 当允许将策略对象用作其定义一部分的策略时，还必须向这些对象类型授予查看权限。例如，如果选择修改路由策略的权限，则还必须选择查看网络对象和接口角色的权限，这些是路由策略所需的对象类型。
- 当允许将其他对象用作其定义一部分的对象时，这一点也成立。例如，如果选择修改用户组的权限，则还必须选择查看网络对象、ACL对象和AAA服务器组的权限。

查看权限

安全管理器中的查看（只读）权限分为以下类别：

- 查看策略权限
- 查看对象权限
- 其他查看权限

查看策略权限

安全管理器包括以下策略的查看权限：

1. **查看>策略>防火墙。**允许您查看PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的防火墙服务策略（位于防火墙下的策略选择器中）。防火墙服务策略的示例包括访问规则、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（位于IPS下的Policy选择器中），包括在IOS路由器上运行的IPS的策略。
3. **查看>策略>映像。**允许您在Apply IPS Updates向导（位于Tools > Apply IPS Update下）中选择签名更新包，但不允许您将包分配给特定设备，除非您还具有Modify > Policies > Image权限。
4. **查看>策略> NAT。**允许您查看PIX/ASA/FWSM设备和IOS路由器上的网络地址转换策略。NAT策略的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PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的站点到站点VPN策略。站点到站点VPN策略的示例包括IKE提议、IPsec提议和预共享密钥。
6. **查看>策略>远程访问VPN。**允许您查看PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的远程访问VPN策略。远程访问VPN策略的示例包括IKE提议、IPsec提议和PKI策略。
7. **查看>策略> SSL VPN。**允许您查看PIX/ASA/FWSM设备和IOS路由器上的SSL VPN策略，如SSL VPN向导。
8. **查看>策略>接口。**允许您查看PIX/ASA/FWSM设备、IOS路由器、IPS传感器和Catalyst 6500/7600设备上的接口策略（位于Interfaces下的Policy选择器中）。在PIX/ASA/FWSM设备上，此权限涵盖硬件端口和接口设置。在IOS路由器上，此权限涵盖基本和高级接口设置，以及其他接口相关策略，如DSL、PVC、PPP和拨号器策略。在IPS传感器上，此权限涵盖物理接口和摘要映射。在Catalyst 6500/7600设备上，此权限涵盖接口和VLAN设置。
9. **查看>策略>桥接。**允许您查看PIX/ASA/FWSM设备上的ARP表策略（位于Platform > Bridging下的Policy选择器中）。
10. **查看>策略>设备管理。**允许您查看PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的设备管理策略（位于Platform > Device Admin下的策略选择器中）：在PIX/ASA/FWSM设备上，示例包括设备访问策略、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）策略、服务器访问策略、AAA和安全设备调配。在IPS传感器上，此权限涵盖设备访问策略和服务器访问策略。在Catalyst 6500/7600设备上，此权限涵盖IDSM设置和VLAN访问列表。
11. **查看>策略>身份。**允许您查看Cisco IOS路由器上的身份策略（位于Platform > Identity下的Policy选择器中），包括802.1x和网络准入控制(NAC)策略。
12. **查看>策略>日志记录。**允许您查看PIX/ASA/FWSM设备、IOS路由器和IPS传感器上的日志记录策略（位于Platform > Logging下的Policy选择器中）。日志记录策略的示例包括日志记录设置、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PIX/ASA/FWSM设备上的组播策略（位于Platform > Multicast下的Policy选择器中）。组播策略的示例包括组播路由和IGMP策略。

14. **查看>策略> QoS**。允许您查看Cisco IOS路由器上的QoS策略（位于Platform > Quality of Service下的Policy选择器中）。
15. **查看>策略>路由**。允许您查看PIX/ASA/FWSM设备和IOS路由器上的路由策略（位于Platform > Routing下的Policy选择器中）。路由策略的示例包括OSPF、RIP和静态路由策略。
16. **查看>策略>安全**。允许您查看PIX/ASA/FWSM设备和IPS传感器上的安全策略（位于Platform > Security下的Policy选择器中）：在PIX/ASA/FWSM设备上，安全策略包括反欺骗、分段和超时设置。在IPS传感器上，安全策略包括阻止设置。
17. **查看>策略>服务策略规则**。允许您查看PIX 7.x/ASA设备上的服务策略规则策略（位于Platform > Service Policy Rules下的Policy选择器中）。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PIX/ASA/FWSM设备上的部署策略（位于Platform > User Preferences下的Policy选择器中）。此策略包含用于清除部署上所有NAT转换的选项。
19. **查看>策略>虚拟设备**。允许您查看IPS设备上的虚拟传感器策略。此策略用于创建虚拟传感器。
20. **查看>策略> FlexConfig**。允许您查看FlexConfigs，这些是可部署到PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备的附加CLI命令和说明。

查看对象权限

安全管理器包括对象的以下视图权限：

1. **View > Objects > AAA Server Groups**。允许您查看AAA服务器组对象。这些对象用于需要AAA服务（身份验证、授权和记帐）的策略。
2. **查看>对象> AAA服务器**。允许您查看AAA服务器对象。这些对象代表定义为AAA服务器组一部分的单个AAA服务器。
3. **视图>对象>访问控制列表 — 标准/扩展**。允许您查看标准ACL对象和扩展ACL对象。扩展ACL对象用于各种策略（如NAT和NAC）和建立VPN访问。标准ACL对象用于OSPF和SNMP等策略，以及建立VPN访问。
4. **“视图”(View)>“对象”(Objects)>“访问控制列表”(Access Control Lists)**- “网络”(Web)。允许您查看Web ACL对象。Web ACL对象用于在SSL VPN策略中执行内容过滤。
5. **视图>对象> ASA用户组**。允许您查看ASA用户组对象。这些对象在ASA安全设备上以Easy VPN、远程访问VPN和SSL VPN配置进行配置。
6. **查看>对象>类别**。允许您查看类别对象。这些对象通过使用颜色帮助您轻松识别规则表中的规则和对象。
7. **查看>对象>凭据**。允许您查看凭证对象。在IKE扩展身份验证(Xauth)期间，这些对象在Easy VPN配置中使用。
8. **视图>对象> FlexConfigs**。允许您查看FlexConfig对象。这些对象包含配置命令和其他脚本语言说明，可用于配置安全管理器用户界面不支持的命令。
9. **View > Objects > IKE Proposals**。允许您查看IKE建议对象。这些对象包含远程访问VPN策略中IKE提议所需的参数。
10. **View > Objects > Inspect - Class Maps** - DNS。允许您查看DNS类映射对象。这些对象与具有特定条件的DNS流量匹配，以便对该流量执行操作。
11. **View > Objects > Inspect - Class Maps - FTP**。允许您查看FTP类映射对象。这些对象与具有特定条件的FTP流量匹配，以便对该流量执行操作。
12. **View > Objects > Inspect - Class Maps - HTTP**。允许您查看HTTP类映射对象。这些对象与具有特定条件的HTTP流量匹配，以便对该流量执行操作。
13. **View > Objects > Inspect - Class Maps - IM**。允许您查看IM类映射对象。这些对象与具有特

定条件的即时消息流量匹配，以便对该流量执行操作。

14. **View > Objects > Inspect - Class Maps - SIP**。允许您查看SIP类映射对象。这些对象与具有特定条件的SIP流量匹配，以便对该流量执行操作。
15. **View > Objects > Inspect - Policy Maps - DNS。**允许您查看DNS策略映射对象。这些对象用于为DNS流量创建检测映射。
16. **View > Objects > Inspect - Policy Maps - FTP。**允许您查看FTP策略映射对象。这些对象用于为FTP流量创建检测映射。
17. **View > Objects > Inspect - Policy Maps - GTP**。允许您查看GTP策略映射对象。这些对象用于为GTP流量创建检测映射。
18. **View > Objects > Inspect - Policy Maps - HTTP(ASA7.1.x/PIX7.1.x/IOS)**。 允许您查看为ASA/PIX 7.1.x设备和IOS路由器创建的HTTP策略映射对象。这些对象用于为HTTP流量创建检测映射。
19. **View > Objects > Inspect - Policy Maps - HTTP(ASA7.2/PIX7.2)**。 允许您查看为ASA 7.2/PIX 7.2设备创建的HTTP策略映射对象。这些对象用于为HTTP流量创建检测映射。
20. **View > Objects > Inspect - Policy Maps - IM(ASA7.2/PIX7.2)**。 允许您查看为ASA 7.2/PIX 7.2设备创建的IM策略映射对象。这些对象用于为IM流量创建检测映射。
21. **View > Objects > Inspect - Policy Maps - IM(IOS)**。 允许您查看为IOS设备创建的IM策略映射对象。这些对象用于为IM流量创建检测映射。
22. **View > Objects > Inspect - Policy Maps - SIP**。允许您查看SIP策略映射对象。这些对象用于为SIP流量创建检测映射。
23. **查看>对象>检查 — 正则表达式**。允许您查看正则表达式对象。这些对象表示作为正则表达式组一部分定义的各个正则表达式。
24. **查看>对象>检查 — 正则表达式组**。允许您查看正则表达式组对象。某些类映射使用这些对象并检查映射以匹配数据包中的文本。
25. **View > Objects > Inspect - TCP Maps**。允许您查看TCP映射对象。这些对象自定义对TCP流双向的检查。
26. **视图>对象>接口角色**。允许您查看接口角色对象。这些对象定义可代表不同类型设备上多个接口的命名模式。接口角色使您能够将策略应用到多台设备上的特定接口，而无需手动定义每个接口的名称。
27. **视图>对象> IPsec转换集**。允许您查看IPsec转换集对象。这些对象包括安全协议、算法和其他设置的组合，这些设置可准确指定IPsec隧道中数据的加密和身份验证方式。
28. **视图>对象> LDAP属性映射**。允许您查看LDAP属性映射对象。这些对象用于将自定义（用户定义的）属性名称映射到思科LDAP属性名称。
29. **查看>对象>网络/主机**。允许您查看网络/主机对象。这些对象是IP地址的逻辑集合，代表网络、主机或两者。网络/主机对象使您能够定义策略，而无需单独指定每个网络或主机。
30. **View > Objects > PKI Enrollments**。允许您查看PKI注册对象。这些对象定义在公共密钥基础设施中运行的证书颁发机构(CA)服务器。
31. **查看>对象>端口转发列表**。允许您查看端口转发列表对象。这些对象定义远程客户端上的端口号与应用的IP地址和SSL VPN网关后面的端口的映射。
32. **查看>对象>安全桌面配置**。允许您查看安全桌面配置对象。这些对象是可重用的命名组件，SSL VPN策略可以引用这些组件，以提供消除在SSL VPN会话期间共享的所有敏感数据跟踪的可靠方法。
33. **查看>对象>服务 — 端口列表**。允许您查看端口列表对象。这些对象包含一个或多个端口号范围，用于简化创建服务对象的过程。
34. **查看>对象>服务/服务组**允许您查看服务和服务组对象。这些对象是协议和端口定义的映射，描述策略（如Kerberos、SSH和POP3）使用的网络服务。
35. **“视图”>“对象”>“单点登录服务器**”。允许您查看服务器对象上的单点登录。单点登录(SSO)使SSL VPN用户只需输入一次用户名和密码即可访问多个受保护的服务和Web服务器。

36. **View > Objects > SLA Monitors**。允许您查看SLA监控对象。运行版本7.2或更高版本的PIX/ASA安全设备使用这些对象执行路由跟踪。此功能提供了一种在主路由发生故障时跟踪主路由的可用性并安装备用路由的方法。
37. **查看>对象> SSL VPN自定义**。允许您查看SSL VPN自定义对象。这些对象定义如何更改向用户显示的SSL VPN页面的外观，如登录/注销和主页。
38. **View > Objects > SSL VPN Gateways**。允许您查看SSL VPN网关对象。这些对象定义了一些参数，这些参数使网关能够用作与SSL VPN中受保护资源的连接的代理。
39. **“视图”(View)>“对象”(Objects)>“样式对象**”(Style Objects)。允许您查看样式对象。这些对象允许您配置样式元素（如字体特征和颜色），以自定义SSL VPN用户在连接到安全设备时显示的SSL VPN页面的外观。
40. **视图>对象>文本对象**。允许您查看自由格式文本对象。这些对象包括名称和值对，其中值可以是单个字符串、字符串列表或字符串表。
41. **视图>对象>时间范围。**允许您查看时间范围对象。创建基于时间的ACL和检查规则时使用这些对象。在定义ASA用户组时，也会使用这些组来限制VPN访问在一周中的特定时间。
42. **View > Objects > Traffic Flows**。允许您查看流量对象。这些对象定义了供PIX 7.x/ASA 7.x设备使用的特定流量。
43. **视图>对象> URL列表**。允许您查看URL列表对象。这些对象定义成功登录后在门户页面上显示的URL。这使用户能够在无客户端访问模式下操作时访问SSL VPN网站上可用的资源。
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Easy VPN拓扑、远程访问VPN和SSL VPN中使用的远程客户端组。
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 VPN使用这些服务器访问或共享远程系统上的文件。
46. **查看>对象>内部 — DN规则**。允许您查看DN策略使用的DN规则。这是安全管理器使用的内部对象，不显示在策略对象管理器中。
47. **查看>对象>内部 — 客户端更新**。这是用户组对象所需的内部对象，不显示在策略对象管理器中。
48. **查看>对象>内部 — 标准ACE**。这是标准访问控制条目的内部对象，ACL对象使用它。
49. **视图>对象>内部 — 扩展ACE。**这是扩展访问控制条目的内部对象，ACL对象使用这些条目。

其他查看权限

安全管理器包括以下其他查看权限：

1. **查看>管理**。允许您查看安全管理器管理设置。
2. **查看> CLI**。允许您查看设备上配置的CLI命令并预览即将部署的命令。
3. **查看>配置存档**。允许您查看配置存档中包含的配置列表。您无法查看设备配置或任何CLI命令。
4. **查看>设备**。允许您在设备视图中查看设备和所有相关信息，包括设备设置、属性、分配等。
5. **查看>设备管理器**。允许您为单个设备启动只读版本的设备管理器，例如Cisco IOS路由器的Cisco路由器和安全设备管理器(SDM)。
6. **查看>拓扑**。允许您查看在“映射”视图中配置的映射。

修改权限

安全管理器中的修改（读写）权限分为以下类别：

- 修改策略权限

- 修改对象权限
- 其他修改权限

修改策略权限

注：指定修改策略权限时，请确保您也选择了相应的分配和查看策略权限。

安全管理器包括以下策略修改权限：

1. **修改>策略>防火墙**。允许您修改PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的防火墙服务策略（位于防火墙下的策略选择器中）。防火墙服务策略的示例包括访问规则、AAA规则和检查规则。
2. **Modify > Policies > Intrusion Prevention System**。允许您修改IPS策略（位于IPS下的Policy选择器中），包括IPS路由器上运行的策略。此权限还允许您在“签名更新”向导（位于“工具”>“应用IPS更新”下）中调整签名。
3. **修改>策略>映像**。允许您在Apply IPS Updates向导（位于Tools > Apply IPS Update下）中将签名更新包分配给设备。 此权限还允许您将自动更新设置分配给特定设备（位于Tools > Security Manager Administration > IPS Updates下）。
4. **修改>策略> NAT**。允许您修改PIX/ASA/FWSM设备和IOS路由器上的网络地址转换策略。NAT策略的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PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的站点到站点VPN策略。站点到站点VPN策略的示例包括IKE提议、IPsec提议和预共享密钥。
6. **Modify > Policies > Remote Access VPN**。允许您修改PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的远程访问VPN策略。远程访问VPN策略的示例包括IKE提议、IPsec提议和PKI策略。
7. **Modify > Policies > SSL VPN**。允许您修改PIX/ASA/FWSM设备和IOS路由器上的SSL VPN策略，如SSL VPN向导。
8. **修改>策略>接口**。允许您修改PIX/ASA/FWSM设备、IOS路由器、IPS传感器和Catalyst 6500/7600设备上的接口策略（位于Interfaces下的Policy选择器中）：在PIX/ASA/FWSM设备上，此权限涵盖硬件端口和接口设置。在IOS路由器上，此权限涵盖基本和高级接口设置，以及其他接口相关策略，如DSL、PVC、PPP和拨号器策略。在IPS传感器上，此权限涵盖物理接口和摘要映射。在Catalyst 6500/7600设备上，此权限涵盖接口和VLAN设置。
9. **修改>策略>桥接**。允许您修改PIX/ASA/FWSM设备上的ARP表策略（位于Platform > Bridging下的Policy选择器中）。
10. **修改>策略>设备管理**。允许您修改PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备上的设备管理策略（位于Platform > Device Admin下的策略选择器）：在PIX/ASA/FWSM设备上，示例包括设备访问策略、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）策略、服务器访问策略、AAA和安全设备调配。在IPS传感器上，此权限涵盖设备访问策略和服务器访问策略。在Catalyst 6500/7600设备上，此权限涵盖IDSM设置和VLAN访问列表。
11. **修改>策略>身份**。允许您修改Cisco IOS路由器上的身份策略（位于Platform > Identity下的Policy选择器中），包括802.1x和网络准入控制(NAC)策略。
12. **Modify > Policies > Logging**。允许您修改PIX/ASA/FWSM设备、IOS路由器和IPS传感器上的日志记录策略（位于Platform > Logging下的Policy选择器中）。日志记录策略的示例包括日志记录设置、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PIX/ASA/FWSM设备上的组播策略（位于Platform > Multicast下的Policy选择器中）。组播策略的示例包括组播路由和IGMP策略。

14. **修改>策略> QoS**。允许您修改Cisco IOS路由器上的QoS策略（位于Platform > Quality of Service下的Policy选择器中）。
15. **修改>策略>路由**。允许您修改PIX/ASA/FWSM设备和IOS路由器上的路由策略（位于Platform > Routing下的Policy选择器中）。路由策略的示例包括OSPF、RIP和静态路由策略。
16. **修改>策略>安全**。允许您修改PIX/ASA/FWSM设备和IPS传感器上的安全策略（位于Platform > Security下的Policy选择器中）：在PIX/ASA/FWSM设备上，安全策略包括反欺骗、分段和超时设置。在IPS传感器上，安全策略包括阻止设置。
17. **修改>策略>服务策略规则**。允许您修改PIX 7.x/ASA设备上的服务策略规则策略（位于Platform > Service Policy Rules下的Policy选择器中）。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PIX/ASA/FWSM设备上的部署策略（位于Platform > User Preferences下的Policy选择器中）。此策略包含用于清除部署上所有NAT转换的选项。
19. **修改>策略>虚拟设备**。允许您修改IPS设备上的虚拟传感器策略。使用此策略创建虚拟传感器。
20. **修改>策略> FlexConfig**。允许您修改FlexConfigs，这些是可部署到PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备的附加CLI命令和说明。

修改对象权限

安全管理器包括对象的以下视图权限：

1. **Modify > Objects > AAA Server Groups**。允许您查看AAA服务器组对象。这些对象用于需要AAA服务（身份验证、授权和记帐）的策略。
2. **Modify > Objects > AAA Servers**。允许您查看AAA服务器对象。这些对象代表定义为AAA服务器组一部分的单个AAA服务器。
3. **修改>对象>访问控制列表 — 标准/扩展**。允许您查看标准ACL对象和扩展ACL对象。扩展ACL对象用于各种策略（如NAT和NAC）和建立VPN访问。标准ACL对象用于OSPF和SNMP等策略，以及建立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对象用于在SSL VPN策略中执行内容过滤。
5. **Modify > Objects > ASA** User Groups。允许您查看ASA用户组对象。这些对象在ASA安全设备上以Easy VPN、远程访问VPN和SSL VPN配置进行配置。
6. **修改>对象>类别**。允许您查看类别对象。这些对象通过使用颜色帮助您轻松识别规则表中的规则和对象。
7. **修改>对象>凭据**。允许您查看凭证对象。在IKE扩展身份验证(Xauth)期间，这些对象在Easy VPN配置中使用。
8. **修改>对象> FlexConfigs**。允许您查看FlexConfig对象。这些对象包含配置命令和其他脚本语言说明，可用于配置安全管理器用户界面不支持的命令。
9. **Modify > Objects > IKE Proposals**。允许您查看IKE建议对象。这些对象包含远程访问VPN策略中IKE提议所需的参数。
10. **修改>对象>检查 — 类映射 — DNS**。允许您查看DNS类映射对象。这些对象与具有特定条件的DNS流量匹配，以便对该流量执行操作。
11. **Modify > Objects > Inspect - Class Maps - FTP**。允许您查看FTP类映射对象。这些对象与具有特定条件的FTP流量匹配，以便对该流量执行操作。
12. **修改>对象>检查 — 类映射 — HTTP**。允许您查看HTTP类映射对象。这些对象与具有特定条件的HTTP流量匹配，以便对该流量执行操作。
13. **Modify > Objects > Inspect - Class Maps - IM**。允许您查看IM类映射对象。这些对象与具有

特定条件的即时消息流量匹配，以便对该流量执行操作。

14. **Modify > Objects > Inspect - Class Maps - SIP**。允许您查看SIP类映射对象。这些对象与具有特定条件的SIP流量匹配，以便对该流量执行操作。
15. **Modify > Objects > Inspect - Policy Maps - DNS**。允许您查看DNS策略映射对象。这些对象用于为DNS流量创建检测映射。
16. **Modify > Objects > Inspect - Policy Maps - FTP**。允许您查看FTP策略映射对象。这些对象用于为FTP流量创建检测映射。
17. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.1.x/PIX7.1.x/IOS)**。 允许您查看为ASA/PIX 7.x设备和IOS路由器创建的HTTP策略映射对象。这些对象用于为HTTP流量创建检测映射。
18. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.2/PIX7.2)**。 允许您查看为ASA 7.2/PIX 7.2设备创建的HTTP策略映射对象。这些对象用于为HTTP流量创建检测映射。
19. **修改>对象>检查 — 策略映射 — IM(ASA7.2/PIX7.2)**。 允许您查看为ASA 7.2/PIX 7.2设备创建的IM策略映射对象。这些对象用于为IM流量创建检测映射。
20. **Modify > Objects > Inspect - Policy Maps - IM(IOS)**。 允许您查看为IOS设备创建的IM策略映射对象。这些对象用于为IM流量创建检测映射。
21. **Modify > Objects > Inspect - Policy Maps - SIP**。允许您查看SIP策略映射对象。这些对象用于为SIP流量创建检测映射。
22. **Modify > Objects > Inspect - Regular Expressions**。允许您查看正则表达式对象。这些对象表示作为正则表达式组一部分定义的各个正则表达式。
23. **修改>对象>检查 — 正则表达式组**。允许您查看正则表达式组对象。某些类映射使用这些对象并检查映射以匹配数据包中的文本。
24. **Modify > Objects > Inspect - TCP Maps**。允许您查看TCP映射对象。这些对象自定义对TCP流双向的检查。
25. **修改>对象>接口角色**。允许您查看接口角色对象。这些对象定义可代表不同类型设备上多个接口的命名模式。接口角色使您能够将策略应用到多台设备上的特定接口，而无需手动定义每个接口的名称。
26. **修改>对象> IPsec转换集**。允许您查看IPsec转换集对象。这些对象包括安全协议、算法和其他设置的组合，这些设置可准确指定IPsec隧道中数据的加密和身份验证方式。
27. **Modify > Objects > LDAP Attribute Maps**。允许您查看LDAP属性映射对象。这些对象用于将自定义（用户定义的）属性名称映射到思科LDAP属性名称。
28. **修改>对象>网络/主机**。允许您查看网络/主机对象。这些对象是IP地址的逻辑集合，代表网络、主机或两者。网络/主机对象使您能够定义策略，而无需单独指定每个网络或主机。
29. **Modify > Objects > PKI Enrollments**。允许您查看PKI注册对象。这些对象定义在公共密钥基础设施中运行的证书颁发机构(CA)服务器。
30. **修改>对象>端口转发列表**。允许您查看端口转发列表对象。这些对象定义远程客户端上的端口号与应用的IP地址和SSL VPN网关后面的端口的映射。
31. **修改>对象>安全桌面配置**。允许您查看安全桌面配置对象。这些对象是可重用的命名组件，SSL VPN策略可以引用这些组件，以提供消除在SSL VPN会话期间共享的所有敏感数据跟踪的可靠方法。
32. **修改>对象>服务 — 端口列表**。允许您查看端口列表对象。这些对象包含一个或多个端口号范围，用于简化创建服务对象的过程。
33. **修改>对象>服务/服务组。**允许您查看服务和服务组对象。这些对象是协议和端口定义的映射，描述策略（如Kerberos、SSH和POP3）使用的网络服务。
34. **Modify > Objects > Single Sign On Servers。**允许您查看服务器对象上的单点登录。单点登录(SSO)使SSL VPN用户只需输入一次用户名和密码即可访问多个受保护的服务和Web服务器。
35. **Modify > Objects > SLA Monitors**。允许您查看SLA监控对象。运行版本7.2或更高版本的

PIX/ASA安全设备使用这些对象执行路由跟踪。此功能提供了一种在主路由发生故障时跟踪主路由的可用性并安装备用路由的方法。

36. **修改>对象> SSL VPN自定义**。允许您查看SSL VPN自定义对象。这些对象定义如何更改向用户显示的SSL VPN页面的外观，如登录/注销和主页。
37. **Modify > Objects > SSL VPN Gateways**。允许您查看SSL VPN网关对象。这些对象定义了一些参数，这些参数使网关能够用作与SSL VPN中受保护资源的连接的代理。
38. **“修改”(Modify)>“对象”(Objects)>“样式对象**”(Style Objects)。允许您查看样式对象。这些对象允许您配置样式元素（如字体特征和颜色），以自定义SSL VPN用户在连接到安全设备时显示的SSL VPN页面的外观。
39. **修改>对象>文本对象**。允许您查看自由格式文本对象。这些对象包括名称和值对，其中值可以是单个字符串、字符串列表或字符串表。
40. **修改>对象>时间范围。**允许您查看时间范围对象。创建基于时间的ACL和检查规则时使用这些对象。在定义ASA用户组时，也会使用这些组来限制VPN访问在一周中的特定时间。
41. **修改>对象>流量**。允许您查看流量对象。这些对象定义了供PIX 7.x/ASA 7.x设备使用的特定流量。
42. **修改>对象> URL列表**。允许您查看URL列表对象。这些对象定义成功登录后在门户页面上显示的URL。这使用户能够在无客户端访问模式下操作时访问SSL VPN网站上可用的资源。
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Easy VPN拓扑、远程访问VPN和SSL VPN中使用的远程客户端组
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 VPN使用这些服务器访问或共享远程系统上的文件。
45. **修改>对象>内部 — DN规则。**允许您查看DN策略使用的DN规则。这是安全管理器使用的内部对象，不显示在策略对象管理器中。
46. **修改>对象>内部 — 客户端更新**。这是用户组对象所需的内部对象，不显示在策略对象管理器中。
47. **修改>对象>内部 — 标准ACE**。这是标准访问控制条目的内部对象，ACL对象使用它。
48. **修改>对象>内部 — 扩展ACE**。这是扩展访问控制条目的内部对象，ACL对象使用这些条目。

其他修改权限

安全管理器包括其他修改权限，如图所示：

1. **修改>管理**。允许您修改安全管理器管理设置。
2. **修改>配置存档**。允许您修改配置存档中的设备配置。此外，它还允许您向存档添加配置并自定义配置存档工具。
3. **修改>设备**。允许您添加和删除设备，以及修改设备属性和属性。要发现所添加设备上的策略，还必须启用导入权限。此外，如果启用Modify > Devices权限，请确保还启用Assign > Policies > Interfaces权限。
4. **“修改”>“层次结构**”。允许您修改设备组。
5. **修改>拓扑**。允许您修改映射视图中的映射。

分配权限

安全管理器包括策略分配权限，如图所示：

1. **分配>策略>防火墙**。允许您将防火墙服务策略（位于防火墙下的策略选择器中）分配给PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备。防火墙服务策略的示例包括访

问规则、AAA规则和检查规则。

2. **Assign > Policies > Intrusion Prevention System**。允许您分配IPS策略（位于IPS下的Policy选择器中），包括在IOS路由器上运行的IPS的策略。
3. **分配>策略>映像**。安全管理器当前未使用此权限。
4. **分配>策略> NAT**。允许您将网络地址转换策略分配给PIX/ASA/FWSM设备和IOS路由器。NAT策略的示例包括静态规则和动态规则。
5. **分配>策略>站点到站点VPN**。允许您将站点到站点VPN策略分配给PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备。站点到站点VPN策略的示例包括IKE提议、IPsec提议和预共享密钥。
6. **Assign > Policies > Remote Access VPN**。允许您将远程访问VPN策略分配给PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备。远程访问VPN策略的示例包括IKE提议、IPsec提议和PKI策略。
7. **Assign > Policies > SSL VPN**。允许您将SSL VPN策略分配给PIX/ASA/FWSM设备和IOS路由器，如SSL VPN向导。
8. **分配>策略>接口**。允许您将接口策略（位于Interfaces下的Policy选择器中）分配给PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备：在PIX/ASA/FWSM设备上，此权限涵盖硬件端口和接口设置。在IOS路由器上，此权限涵盖基本和高级接口设置，以及其他接口相关策略，如DSL、PVC、PPP和拨号器策略。在Catalyst 6500/7600设备上，此权限涵盖接口和VLAN设置。
9. **分配>策略>桥接**。允许您将ARP表策略（位于Platform > Bridging下的Policy选择器中）分配给PIX/ASA/FWSM设备。
10. **分配>策略>设备管理**。允许您将设备管理策略（位于Platform > Device Admin下的Policy选择器中）分配给PIX/ASA/FWSM设备、IOS路由器和Catalyst 6500/7600设备：在PIX/ASA/FWSM设备上，示例包括设备访问策略、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）策略、服务器访问策略、AAA和安全设备调配。在IPS传感器上，此权限涵盖设备访问策略和服务器访问策略。在Catalyst 6500/7600设备上，此权限涵盖IDSM设置和VLAN访问列表。
11. **分配>策略>身份**。允许您将身份策略（位于Platform > Identity下的Policy选择器中）分配给Cisco IOS路由器，包括802.1x和网络准入控制(NAC)策略。
12. **分配>策略>日志记录**。允许您将日志记录策略（位于Platform > Logging下的Policy选择器中）分配给PIX/ASA/FWSM设备和IOS路由器。日志记录策略的示例包括日志记录设置、服务器设置和系统日志服务器策略。
13. **分配>策略>组播**。允许您将组播策略（位于Platform > Multicast下的Policy选择器中）分配给PIX/ASA/FWSM设备。组播策略的示例包括组播路由和IGMP策略。
14. **分配>策略> QoS**。允许您将QoS策略（位于Platform > Quality of Service下的Policy选择器中）分配给Cisco IOS路由器。
15. **分配>策略>路由**。允许您将路由策略（位于Platform > Routing下的Policy选择器中）分配给PIX/ASA/FWSM设备和IOS路由器。路由策略的示例包括OSPF、RIP和静态路由策略。
16. **分配>策略>安全**。允许您将安全策略（位于Platform > Security下的Policy选择器中）分配给PIX/ASA/FWSM设备。安全策略包括反欺骗、分段和超时设置。
17. **分配>策略>服务策略规则**。允许您将服务策略规则策略（位于Platform > Service Policy Rules下的Policy选择器中）分配给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**。允许您将部署策略（位于Platform > User Preferences下的Policy选择器中）分配给PIX/ASA/FWSM设备。此策略包含用于清除部署上所有NAT转换的选项。
19. **分配>策略>虚拟设备**。允许您将虚拟传感器策略分配给IPS设备。使用此策略创建虚拟传感器。
20. **分配>策略> FlexConfig**。允许您分配FlexConfigs，这些是可部署到PIX/ASA/FWSM设备、

IOS路由器和Catalyst 6500/7600设备的附加CLI命令和说明。

注：指定分配权限时，请确保您也选择了相应的视图权限。

批准权限

安全管理器提供审批权限，如下所示：

1. **批准> CLI**。允许您批准部署作业中包含的CLI命令更改。
2. **批准>策略**。允许您批准工作流程活动中配置的策略中包含的配置更改。

了解CiscoWorks角色

当用户在CiscoWorks Common Services中创建时，会为其分配一个或多个角色。与每个角色关联的权限决定了每个用户有权在安全管理器中执行的操作。

以下主题介绍CiscoWorks角色：

- CiscoWorks Common Services默认角色
- 在CiscoWorks公共服务中为用户分配角色

CiscoWorks Common Services默认角色

CiscoWorks Common Services包含以下默认角色：

1. **帮助台** — 帮助台用户可以查看（但不能修改）设备、策略、对象和拓扑图。
2. **Network Operator** — 除了查看权限外，网络操作员还可以查看CLI命令和安全管理器管理设置。网络操作员还可以修改配置存档并向设备发出命令（如ping）。
3. **审批人** — 除查看权限外，审批人还可以批准或拒绝部署作业。他们无法执行部署。
4. **网络管理**员 — 除修改管理设置外，网络管理员具有完整的查看和修改权限。他们可以发现这些设备上配置的设备和策略，为设备分配策略，并向设备发出命令。网络管理员无法批准活动或部署作业；但是，他们可以部署其他人批准的作业。
5. **系统管理**员 — 系统管理员可以完全访问所有安全管理员权限，包括修改、策略分配、活动和作业批准、发现、部署和向设备发出命令。

注意：如果服务器上安装了其他应用程序，Common Services中可能会显示其他角色，如导出数据。导出数据角色适用于第三方开发人员，不由安全管理器使用。

提示： 虽然您不能更改CiscoWorks角色的定义，但您可以定义分配给每个用户的角色。有关详细信息，请参阅在CiscoWorks Common Services中为用户分配角色。

在CiscoWorks公共服务中为用户分配角色

CiscoWorks Common Services使您能够定义将哪些角色分配给每个用户。通过更改用户的角色定义，可以更改此用户在安全管理器中授权执行的操作的类型。例如，如果分配帮助台角色，则用户只能查看操作，无法修改任何数据。但是，如果分配网络操作员角色，用户也可以修改配置存档。您可以为每个用户分配多个角色。

注意：在更改用户权限后必须重新启动安全管理器。

步骤:

1. 在Common Services中，选择**Server > Security**，然后从TOC**中选择Single-Server Trust Management > Local User Setup。提示：要**从安全管理器内访问“本地用户设置”页，请选择工具>安全管理器管理>服务器安全，然后单击本地用户设置。
2. 选中现有用户旁边的复选框，然后单击“**编辑”**。
3. 在“用户信息”(User Information)页面上，通过单击复选框选择要分配给此用户的角色。有关每个角色的详细信息，请参阅CiscoWorks Common Services默认角色。
4. 单击**确定**保存更改。
5. 重新启动安全管理器。

了解Cisco Secure ACS角色

与CiscoWorks相比，Cisco Secure ACS在管理安全管理器权限方面提供了更大的灵活性，因为它支持您可以配置的应用特定角色。每个角色都由一组权限组成，这些权限确定对安全管理器任务的授权级别。在Cisco Secure ACS中，您为每个用户组（或者，也可为单个用户）分配角色，这样，该组中的每个用户就能够执行由为该角色定义的权限授权的操作。

此外，您可以将这些角色分配给Cisco Secure ACS设备组，从而允许在不同设备集上区分权限。

注意：思科安全ACS设备组独立于安全管理器设备组。

以下主题介绍Cisco Secure ACS角色：

- 思科安全ACS默认角色
- 自定义Cisco Secure ACS角色

思科安全ACS默认角色

Cisco Secure ACS包括与CiscoWorks相同的角色(请参阅了解CiscoWorks角色)，以及以下附加角色：

1. **安全审批**人 — 安全审批人可以查看（但不能修改）设备、策略、对象、映射、CLI命令和管理设置。此外，安全审批人可以批准或拒绝活动中包含的配置更改。他们不能批准或拒绝部署作业，也不能执行部署。
2. **安全管理**员 — 除了具有查看权限外，安全管理员还可以修改设备、设备组、策略、对象和拓扑图。它们还可以为设备和VPN拓扑分配策略，并执行发现以将新设备导入系统。
3. **网络管**理员 — 除了查看权限外，网络管理员还可以修改配置存档、执行部署和向设备发出命令。

注意：Cisco Secure ACS网络管理员角色中包含的权限与CiscoWorks网络管理员角色中包含的权限不同。有关详细信息，请参阅了解CiscoWorks角色。

与CiscoWorks不同，Cisco Secure ACS允许您自定义与每个安全管理器角色关联的权限。有关修改默认角色的详细信息，请参阅自定义Cisco Secure ACS角色。

注意：必须安装Cisco Secure ACS 3.3或更高版本才能进行安全管理器授权。

自定义Cisco Secure ACS角色

Cisco Secure ACS允许您修改与每个安全管理器角色关联的权限。您还可以通过创建具有针对特定安全管理器任务的权限的专用用户角色来自定义Cisco Secure ACS。

注意：在更改用户权限后必须重新启动安全管理器。

步骤:

1. 在Cisco Secure ACS中，单击导**航栏上的**共享配置文件组件。
2. 在“共**享组件”**页面上单击“思科安全管理器”。系统将显示为安全管理器配置的角色。
3. 执行以下操作之一：要创建角色，请单击“添**加”**。转到第 4 步。要修改现有角色，请点击该角色。转到第 5 步。
4. 输入角色的名称，或者输入说明。
5. 选择并取消选择权限树中的复选框以定义此角色的权限选中树分支的复选框可选择该分支中的所有权限。例如，选择“分配”**会**选择所有分配权限。有关安全管理器权限的完整列表，请参阅安全管理器权限。**注：在**选择修改、批准、分配、导入、控制或部署权限时，还必须选择相应的查看权限；否则，安全管理器将无法正常运行。
6. 单击 **Submit 以保存更改。**
7. 重新启动安全管理器。

安全管理器中权限和角色之间的默认关联

此表显示安全管理器权限如何与CiscoWorks Common Services角色和Cisco Secure ACS中的默认角色相关联。

权限	角色							
	系统管理员	安全管理员(ACS)	安全审批人(ACS)	网络管理员(CW)	网络管理员(ACS)	审批人	网络操作员	帮助台
查看权限								
查看设备	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
查看策略	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
查看对象	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
查看拓扑	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
查看CLI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	无
查看管理员	Yes	Yes	Yes	Yes	Yes	Yes	Yes	无
查看配置存档	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

查看设备管理器	Yes	Yes	Yes	Yes	Yes	Yes	Yes	无
修改权限								
修改设备	Yes	Yes	无	Yes	无	无	无	无
修改层次结构	Yes	Yes	无	Yes	无	无	无	无
修改策略	Yes	Yes	无	Yes	无	无	无	无
修改映像	Yes	Yes	无	Yes	无	无	无	无
修改对象	Yes	Yes	无	Yes	无	无	无	无
修改拓扑	Yes	Yes	无	Yes	无	无	无	无
修改管理员	Yes	无	无	无	无	无	无	无
修改配置存档	Yes	Yes	无	Yes	Yes	无	Yes	无
其他权限								
分配策略	Yes	Yes	无	Yes	无	无	无	无
批准策略	Yes	无	Yes	无	无	无	无	无
批准CLI	Yes	无	无	无	无	Yes	无	无
发现（导入）	Yes	Yes	无	Yes	无	无	无	无
部署	Yes	无	无	Yes	Yes	无	无	无
控制	Yes	无	无	Yes	Yes	无	Yes	无
提交	Yes	Yes	无	Yes	无	无	无	无

相关信息

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