CSM 3.x: Configuración de permisos de usuario y funciones

Contenido

Introducción

Este documento describe cómo configurar los permisos y funciones para los usuarios en Cisco Security Manager (CSM).

Prerequisites

Requirements

Este documento asume que el CSM está instalado y funciona correctamente.

Componentes Utilizados

La información en este documento se basa en el 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar permisos de usuario

Cisco Security Manager autentica su nombre de usuario y contraseña antes de poder iniciar sesión. Después de autenticarse, el Administrador de seguridad establece su función dentro de la aplicación. Esta función define sus permisos (también denominados privilegios), que son el conjunto de tareas u operaciones que está autorizado a realizar. Si no está autorizado para ciertas tareas o dispositivos, los elementos de menú relacionados, los elementos de la tabla de contenido y los botones se ocultan o desactivan. Además, un mensaje indica que no tiene permiso para ver la información seleccionada o realizar la operación seleccionada.

La autenticación y la autorización para el administrador de seguridad la administra el servidor de CiscoWorks o el Cisco Secure Access Control Server (ACS). De forma predeterminada, CiscoWorks administra la autenticación y la autorización, pero puede cambiar a Cisco Secure ACS mediante la página AAA Mode Setup en CiscoWorks Common Services.

Las principales ventajas del uso de Cisco Secure ACS son la capacidad de crear funciones de usuario altamente granulares con conjuntos de permisos especializados (por ejemplo, permitir al usuario configurar determinados tipos de políticas, pero no otros) y la capacidad de restringir a los usuarios a determinados dispositivos mediante la configuración de grupos de dispositivos de red (NDG).

Los temas siguientes describen los permisos de usuario:

- Permisos de Security Manager
- Comprensión de las funciones de CiscoWorks
- Introducción a las funciones de Cisco Secure ACS
- Asociaciones predeterminadas entre permisos y funciones en el Administrador de seguridad

Permisos de Security Manager

Security Manager clasifica los permisos en las categorías como se muestra a continuación:

1. **Ver**: permite ver la configuración actual. Para obtener más información, vea Ver permisos.
2. **Modificar**: permite cambiar la configuración actual. Para obtener más información, vea Modificar permisos.
3. **Asignar**: permite asignar políticas a dispositivos y topologías VPN. Para obtener más información, vea Asignar permisos
4. **Aprobar**: permite aprobar cambios de políticas y trabajos de implementación. Para obtener más información, vea Aprobar permisos.
5. **Importar**: permite importar las configuraciones que ya se han implementado en los dispositivos al Administrador de seguridad.

6. **Implementar**: permite implementar cambios de configuración en los dispositivos de la red y realizar una reversión para volver a una configuración implementada anteriormente.
7. **Control**: permite ejecutar comandos en dispositivos, como ping.
8. **Enviar**: permite enviar los cambios de configuración para su aprobación.

- Cuando seleccione modificar, asignar, aprobar, importar, controlar o implementar permisos, también debe seleccionar los permisos de vista correspondientes; de lo contrario, el Administrador de seguridad no funcionará correctamente.
- Al seleccionar modificar permisos de directiva, también debe seleccionar los permisos de asignación y vista de directiva correspondientes.
- Cuando se permite una directiva que utiliza objetos de directiva como parte de su definición, también se deben conceder permisos de vista a estos tipos de objeto. Por ejemplo, si selecciona el permiso para modificar las políticas de enrutamiento, también debe seleccionar los permisos para ver los objetos de red y las funciones de interfaz, que son los tipos de objeto requeridos por las políticas de enrutamiento.
- Lo mismo se aplica a true cuando se permite un objeto que utiliza otros objetos como parte de su definición. Por ejemplo, si selecciona el permiso para modificar grupos de usuarios, también debe seleccionar los permisos para ver objetos de red, objetos ACL y grupos de servidores AAA.

Ver permisos

Los permisos de vista (sólo lectura) del Administrador de seguridad se dividen en las categorías como se muestra a continuación:

- Ver permisos de políticas
- Ver permisos de objetos
- Permisos de vista adicionales

Ver permisos de políticas

Security Manager incluye los siguientes permisos de vista para las políticas:

1. **Ver > Políticas > Firewall.** Permite ver las políticas de servicio de firewall (ubicadas en el selector de políticas en Firewall) en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Algunos ejemplos de políticas de servicio de firewall son las reglas de acceso, las reglas AAA y las reglas de inspección.
2. **Ver > Políticas > Sistema de prevención de intrusiones.** Permite ver las políticas IPS (situadas en el selector de políticas en IPS), incluidas las políticas para IPS que se ejecutan en routers IOS.
3. **Ver > Políticas > Imagen.** Permite seleccionar un paquete de actualización de firma en el asistente Aplicar actualizaciones de IPS (ubicado en Herramientas > Aplicar actualización de IPS), pero no permite asignar el paquete a dispositivos específicos, a menos que también tenga el permiso Modificar > Políticas > Imagen.
4. **Ver > Políticas > NAT**. Permite ver las políticas de traducción de direcciones de red en los dispositivos PIX/ASA/FWSM y los routers IOS. Algunos ejemplos de políticas NAT incluyen reglas estáticas y reglas dinámicas.
5. **View > Policies > Site-to-Site VPN**. Permite ver las políticas VPN de sitio a sitio en los

dispositivos PIX/ASA/FWSM, los routers IOS y los dispositivos Catalyst 6500/7600. Algunos ejemplos de políticas VPN de sitio a sitio incluyen propuestas IKE, propuestas IPsec y claves previamente compartidas.

6. **Ver > Políticas > VPN de acceso remoto**. Permite ver las políticas de VPN de acceso remoto en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Entre los ejemplos de políticas de VPN de acceso remoto se incluyen las propuestas de IKE, las propuestas de IPSec y las políticas PKI.
7. **Ver > Políticas > SSL VPN**. Permite ver las políticas SSL VPN en los dispositivos PIX/ASA/FWSM y los routers IOS, como el asistente SSL VPN.
8. **Ver > Políticas > Interfaces**. Permite ver las políticas de interfaz (ubicadas en el selector de políticas en Interfaces) en dispositivos PIX/ASA/FWSM, routers IOS, sensores IPS y dispositivos Catalyst 6500/7600.En los dispositivos PIX/ASA/FWSM, este permiso cubre los puertos de hardware y la configuración de la interfaz.En los routers IOS, este permiso cubre la configuración básica y avanzada de la interfaz, así como otras políticas relacionadas con la interfaz, como las políticas DSL, PVC, PPP y dialer.En los sensores IPS, este permiso cubre las interfaces físicas y los mapas de resumen.En los dispositivos Catalyst 6500/7600, este permiso cubre las interfaces y la configuración de VLAN.
9. **Ver > Políticas > Puente**. Permite ver las políticas de tabla ARP (ubicadas en el selector de políticas en Plataforma > Puente) en los dispositivos PIX/ASA/FWSM.
10. **Ver > Políticas > Administración de dispositivos**. Permite ver las políticas de administración de dispositivos (ubicadas en el selector de políticas en Plataforma > Administrador de dispositivos) en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, los ejemplos incluyen políticas de acceso de dispositivos, políticas de acceso al servidor y políticas de conmutación por fallas.En los routers IOS, los ejemplos incluyen políticas de acceso de dispositivos (incluido el acceso a la línea), políticas de acceso al servidor, AAA y aprovisionamiento seguro de dispositivos.En los sensores IPS, este permiso cubre las políticas de acceso de dispositivos y las políticas de acceso al servidor.En los dispositivos Catalyst 6500/7600, este permiso cubre la configuración de IDSM y las listas de acceso de VLAN.
11. **Ver > Políticas > Identidad**. Permite ver las políticas de identidad (situadas en el selector de políticas en Plataforma > Identidad) en los routers Cisco IOS, incluidas las políticas 802.1x y Network Admission Control (NAC).
12. **Ver > Políticas > Registro**. Permite ver las políticas de registro (ubicadas en el selector de políticas en Plataforma > Registro) en dispositivos PIX/ASA/FWSM, routers IOS y sensores IPS. Algunos ejemplos de políticas de registro son: configuración de registro, configuración del servidor y políticas del servidor syslog.
13. **Ver > Políticas > Multicast**. Permite ver las políticas de multidifusión (ubicadas en el selector de políticas en Plataforma > Multidifusión) en los dispositivos PIX/ASA/FWSM. Algunos ejemplos de políticas de multidifusión son el routing de multidifusión y las políticas IGMP.
14. **Ver > Políticas > QoS**. Permite ver las políticas de QoS (situadas en el selector de políticas en Plataforma > Calidad de servicio) en los routers Cisco IOS.
15. **Ver > Políticas > Enrutamiento**. Permite ver las políticas de ruteo (ubicadas en el selector de políticas en Plataforma > Ruteo) en dispositivos PIX/ASA/FWSM y routers IOS. Algunos ejemplos de políticas de ruteo incluyen OSPF, RIP y políticas de ruteo estáticas.
16. **Ver > Políticas > Seguridad**. Permite ver las políticas de seguridad (ubicadas en el selector de políticas en Plataforma > Seguridad) en dispositivos PIX/ASA/FWSM y sensores IPS:En los dispositivos PIX/ASA/FWSM, las políticas de seguridad incluyen la configuración anti-

simulación, fragmento y tiempo de espera.En los sensores IPS, las políticas de seguridad incluyen la configuración de bloqueo.

17. **Ver > Políticas > Reglas de política de servicio**. Permite ver las políticas de regla de política de servicio (situadas en el selector de políticas en Plataforma > Reglas de política de servicio) en dispositivos PIX 7.x/ASA. Los ejemplos incluyen colas de prioridad e IPS, QoS y reglas de conexión.
18. **Ver > Políticas > Preferencias de usuario**. Permite ver la política de implementación (ubicada en el selector de políticas en Plataforma > Preferencias de usuario) en dispositivos PIX/ASA/FWSM. Esta política contiene una opción para borrar todas las traducciones NAT en la implementación.
19. **Ver > Políticas > Dispositivo virtual**. Permite ver las políticas de sensores virtuales en los dispositivos IPS. Esta política se utiliza para crear sensores virtuales.
20. **Ver > Políticas > FlexConfig**. Permite ver FlexConfigs, que son comandos e instrucciones CLI adicionales que se pueden implementar en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600.

Ver permisos de objetos

El Administrador de seguridad incluye los siguientes permisos de vista para los objetos:

1. **View > Objects > AAA Server Groups**. Permite ver los objetos de grupo de servidores AAA. Estos objetos se utilizan en políticas que requieren servicios AAA (autenticación, autorización y contabilidad).
2. **Ver > Objetos > Servidores AAA**. Permite ver objetos de servidor AAA. Estos objetos representan servidores AAA individuales que se definen como parte de un grupo de servidores AAA.
3. **View > Objects > Access Control Lists - Standard/Extended**. Permite ver objetos ACL estándar y extendidos. Los objetos de ACL extendidos se utilizan para una variedad de políticas, como NAT y NAC, y para establecer el acceso VPN. Los objetos ACL estándar se utilizan para políticas como OSPF y SNMP, así como para establecer el acceso VPN.
4. **View > Objects > Access Control Lists** - Web. Permite ver objetos de ACL web. Los objetos Web ACL se utilizan para realizar el filtrado de contenido en las políticas SSL VPN.
5. **Ver > Objetos > Grupos de usuarios ASA**. Permite ver los objetos de grupo de usuarios de ASA. Estos objetos se configuran en dispositivos de seguridad ASA en configuraciones Easy VPN, VPN de acceso remoto y VPN SSL.
6. **Ver > Objetos > Categorías**. Permite ver objetos de categoría. Estos objetos le ayudan a identificar fácilmente reglas y objetos en las tablas de reglas mediante el uso del color.
7. **Ver > Objetos > Credenciales**. Permite ver objetos de credenciales. Estos objetos se utilizan en la configuración de Easy VPN durante la autenticación ampliada IKE (Xauth).
8. **Ver > Objetos > FlexConfigs**. Permite ver objetos FlexConfig. Estos objetos, que contienen comandos de configuración con instrucciones de lenguaje de secuencias de comandos adicionales, se pueden utilizar para configurar comandos que no son compatibles con la interfaz de usuario del Administrador de seguridad.
9. **Ver > Objetos > Propuestas IKE**. Permite ver los objetos de propuesta IKE. Estos objetos contienen los parámetros requeridos para las propuestas IKE en las políticas VPN de acceso remoto.
10. **Ver > Objetos > Inspeccionar - Mapas de clase** - DNS. Permite ver objetos de mapa de clase DNS. Estos objetos coinciden con el tráfico DNS con criterios específicos para que se

puedan realizar acciones en ese tráfico.

11. **Ver > Objetos > Inspeccionar - Mapas de clase - FTP**. Permite ver objetos de mapa de clase FTP. Estos objetos coinciden con el tráfico FTP con criterios específicos para que se puedan realizar acciones en ese tráfico.
12. **Ver > Objetos > Inspeccionar - Mapas de clase - HTTP**. Permite ver objetos de mapa de clase HTTP. Estos objetos coinciden con el tráfico HTTP con criterios específicos para que se puedan realizar acciones en ese tráfico.
13. **View > Objects > Inspect - Class Maps - IM**. Permite ver objetos de mapa de clase de IM. Estos objetos coinciden con el tráfico de IM con criterios específicos, de modo que se puedan realizar acciones en ese tráfico.
14. **View > Objects > Inspect - Class Maps - SIP**. Permite ver objetos de mapa de clase SIP. Estos objetos coinciden con el tráfico SIP con criterios específicos para que se puedan realizar acciones en ese tráfico.
15. **View > Objects > Inspect - Policy Maps - DNS.** Permite ver objetos de mapa de políticas DNS. Estos objetos se utilizan para crear mapas de inspección para el tráfico DNS.
16. **View > Objects > Inspect - Policy Maps - FTP.** Permite ver objetos de mapa de políticas FTP. Estos objetos se utilizan para crear mapas de inspección para el tráfico FTP.
17. **Ver > Objetos > Inspeccionar - Policy Maps - GTP**. Permite ver los objetos de mapa de políticas GTP. Estos objetos se utilizan para crear mapas de inspección para el tráfico GTP.
18. **View > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite ver los objetos de mapa de política HTTP creados para dispositivos ASA/PIX 7.1.x y routers IOS. Estos objetos se utilizan para crear mapas de inspección para el tráfico HTTP.
19. **View > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)**. Permite ver los objetos de mapa de política HTTP creados para dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear mapas de inspección para el tráfico HTTP.
20. **View > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2)**. Permite ver los objetos de mapa de política de IM creados para dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear mapas de inspección para el tráfico de IM.
21. **View > Objects > Inspect - Policy Maps - IM (IOS)**. Permite ver los objetos de mapa de políticas de IM creados para los dispositivos IOS. Estos objetos se utilizan para crear mapas de inspección para el tráfico de IM.
22. **Ver > Objetos > Inspeccionar - Policy Maps - SIP**. Permite ver objetos de mapa de política SIP. Estos objetos se utilizan para crear mapas de inspección para el tráfico SIP.
23. **Ver > Objetos > Inspeccionar - Expresiones regulares**. Permite ver los objetos de expresión regular. Estos objetos representan expresiones regulares individuales que se definen como parte de un grupo de expresiones regulares.
24. **Ver > Objetos > Inspeccionar - Grupos de expresiones regulares**. Permite ver los objetos de grupo de expresiones regulares. Estos objetos son utilizados por ciertos mapas de clase e inspeccionan los mapas para que coincidan con el texto dentro de un paquete.
25. **Ver > Objetos > Inspeccionar - Mapas TCP**. Permite ver objetos de mapa TCP. Estos objetos personalizan la inspección en el flujo TCP en ambas direcciones.
26. **View > Objects > Interface Roles**. Permite ver objetos de rol de interfaz. Estos objetos definen patrones de nomenclatura que pueden representar varias interfaces en diferentes tipos de dispositivos. Las funciones de interfaz permiten aplicar políticas a interfaces específicas en varios dispositivos sin tener que definir manualmente el nombre de cada interfaz.
27. **Ver > Objetos > Conjuntos de transformación IPsec**. Permite ver los objetos del conjunto de

transformación IPsec. Estos objetos comprenden una combinación de protocolos de seguridad, algoritmos y otros ajustes que especifican exactamente cómo se cifrarán y autenticarán los datos del túnel IPsec.

28. **View > Objects > LDAP Attribute Maps**. Permite ver objetos de mapa de atributos LDAP. Estos objetos se utilizan para asignar nombres de atributos personalizados (definidos por el usuario) a nombres de atributos de Cisco LDAP.
29. **Ver > Objetos > Redes/Hosts**. Permite ver objetos de host/red. Estos objetos son colecciones lógicas de direcciones IP que representan redes, hosts o ambos. Los objetos de red/host permiten definir políticas sin especificar cada red o host individualmente.
30. **Ver > Objetos > Inscripciones PKI**. Permite ver los objetos de inscripción PKI. Estos objetos definen los servidores de la Autoridad de certificación (CA) que funcionan dentro de una infraestructura de clave pública.
31. **View > Objects > Port Forwarding Lists**. Permite ver los objetos de la lista de reenvío de puertos. Estos objetos definen las asignaciones de números de puerto en un cliente remoto a la dirección IP de la aplicación y al puerto detrás de un gateway VPN SSL.
32. **View > Objects > Secure Desktop Configurations**. Permite ver objetos de configuración de escritorio seguros. Estos objetos son reutilizables, componentes con nombre a los que las políticas SSL VPN pueden hacer referencia para proporcionar un medio fiable de eliminar todos los rastros de datos confidenciales que se comparten durante la duración de una sesión SSL VPN.
33. **Ver > Objetos > Servicios - Listas de puertos**. Permite ver los objetos de la lista de puertos. Estos objetos, que contienen uno o más rangos de números de puerto, se utilizan para simplificar el proceso de creación de objetos de servicio.
34. **View > Objects > Services/Service Groups** Permite ver los objetos de servicio y de grupo de servicios. Estos objetos son asignaciones definidas de definiciones de protocolo y puerto que describen los servicios de red utilizados por las políticas, como Kerberos, SSH y POP3.
35. **View > Objects > Single Sign On Servers**. Permite ver el inicio de sesión único en los objetos del servidor. Single Sign-On (SSO) permite a los usuarios de SSL VPN introducir un nombre de usuario y una contraseña una vez y acceder a varios servicios protegidos y servidores web.
36. **Ver > Objetos > Monitores SLA**. Permite ver objetos de supervisión SLA. Estos objetos son utilizados por los dispositivos de seguridad PIX/ASA que ejecutan la versión 7.2 o posterior para realizar el seguimiento de la ruta. Esta función proporciona un método para realizar un seguimiento de la disponibilidad de una ruta principal e instalar una ruta de respaldo si la ruta principal falla.
37. **Ver > Objetos > Personalizaciones SSL VPN**. Permite ver los objetos de personalización de VPN SSL. Estos objetos definen cómo cambiar el aspecto de las páginas SSL VPN que se muestran a los usuarios, como Login/Logout y páginas de inicio.
38. **Ver > Objetos > Gateways SSL VPN**. Permite ver objetos de gateway VPN SSL. Estos objetos definen parámetros que permiten que el gateway se utilice como proxy para las conexiones a los recursos protegidos en su SSL VPN.
39. **Ver > Objetos > Objetos de estilo**. Permite ver objetos de estilo. Estos objetos le permiten configurar elementos de estilo, como las características de fuente y los colores, para personalizar el aspecto de la página SSL VPN que aparece para los usuarios SSL VPN cuando se conectan al dispositivo de seguridad.
40. **Ver > Objetos > Objetos de texto**. Permite ver objetos de texto de formato libre. Estos objetos comprenden un par de nombre y valor, donde el valor puede ser una única cadena,

una lista de cadenas o una tabla de cadenas.

41. **Ver > Objetos > Rangos de tiempo.** Permite ver objetos de intervalo de tiempo. Estos objetos se utilizan al crear ACL basadas en tiempo y reglas de inspección. También se utilizan al definir grupos de usuarios ASA para restringir el acceso VPN a horas específicas durante la semana.
42. **Ver > Objetos > Flujos de tráfico**. Permite ver los objetos de flujo de tráfico. Estos objetos definen flujos de tráfico específicos para su uso por los dispositivos PIX 7.x/ASA 7.x.
43. **Ver > Objetos > Listas de URL**. Permite ver objetos de lista de URL. Estos objetos definen las URL que se muestran en la página del portal después de un inicio de sesión correcto. Esto permite a los usuarios acceder a los recursos disponibles en los sitios web de SSL VPN cuando funcionan en modo de acceso sin cliente.
44. **Ver > Objetos > Grupos de usuarios**. Permite ver los objetos de grupo de usuarios. Estos objetos definen grupos de clientes remotos que se utilizan en topologías Easy VPN, VPN de acceso remoto y VPN SSL.
45. **Ver > Objetos > Listas de Servidores WINS**. Permite ver los objetos de lista del servidor WINS. Estos objetos representan servidores WINS, que utilizan SSL VPN para acceder o compartir archivos en sistemas remotos.
46. **Ver > Objetos > Reglas internas - DN**. Permite ver las reglas DN que utilizan las políticas DN. Se trata de un objeto interno que utiliza el Administrador de seguridad y que no aparece en el Administrador de objetos de directiva.
47. **View > Objects > Internal - Client Updates**. Se trata de un objeto interno requerido por los objetos de grupo de usuarios que no aparece en el Administrador de objetos de directiva.
48. **View > Objects > Internal - Standard ACEs**. Se trata de un objeto interno para las entradas de control de acceso estándar, que utilizan los objetos ACL.
49. **View > Objects > Internal - Extended ACE.** Se trata de un objeto interno para las entradas de control de acceso extendido que utilizan los objetos ACL.

Permisos de vista adicionales

Security Manager incluye los siguientes permisos de vista adicionales:

1. **Ver > Admin**. Permite ver la configuración administrativa del Administrador de seguridad.
2. **Ver > CLI**. Permite ver los comandos CLI configurados en un dispositivo y obtener una vista previa de los comandos que se van a implementar.
3. **Ver > Archivo de configuración**. Permite ver la lista de configuraciones contenidas en el archivo de configuración. No puede ver la configuración del dispositivo ni ningún comando CLI.
4. **Ver > Dispositivos**. Permite ver los dispositivos en la vista Dispositivo y toda la información relacionada, incluida la configuración del dispositivo, las propiedades, las asignaciones, etc.
5. **Ver > Administradores de dispositivos**. Permite iniciar versiones de sólo lectura de los administradores de dispositivos para dispositivos individuales, como el router de Cisco y el administrador de dispositivos de seguridad (SDM) para los routers Cisco IOS.
6. **Ver > Topología**. Permite ver mapas configurados en la vista de mapa.

Modificar permisos

Los permisos de modificación (lectura y escritura) del Administrador de seguridad se dividen en categorías como se muestra a continuación:

- Modificar permisos de políticas
- Modificar permisos de objetos
- Permisos de modificación adicionales

Modificar permisos de políticas

Nota: Cuando especifique modificar permisos de directivas, asegúrese de que también ha seleccionado los correspondientes permisos de asignación y vista de directivas.

El Administrador de seguridad incluye los siguientes permisos de modificación para las políticas:

1. **Modificar > Políticas > Firewall**. Permite modificar las políticas de servicio de firewall (ubicadas en el selector de políticas en Firewall) en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Algunos ejemplos de políticas de servicio de firewall son las reglas de acceso, las reglas AAA y las reglas de inspección.
2. **Modificar > Políticas > Sistema de prevención de intrusiones**. Permite modificar las políticas IPS (situadas en el selector de políticas en IPS), incluidas las políticas para IPS que se ejecutan en routers IOS. Este permiso también le permite ajustar firmas en el Asistente de actualización de firmas (ubicado en Herramientas > Aplicar actualización de IPS).
3. **Modificar > Políticas > Imagen**. Permite asignar un paquete de actualización de firma a los dispositivos en el asistente Aplicar actualizaciones de IPS (ubicado en Herramientas > Aplicar actualización de IPS). Este permiso también le permite asignar la configuración de actualización automática a dispositivos específicos (ubicados en Herramientas > Administración del administrador de seguridad > Actualizaciones IPS).
4. **Modificar > Políticas > NAT**. Permite modificar las políticas de traducción de direcciones de red en los dispositivos PIX/ASA/FWSM y los routers IOS. Algunos ejemplos de políticas NAT incluyen reglas estáticas y reglas dinámicas.
5. **Modifique > Políticas > VPN de sitio a sitio**. Permite modificar las políticas VPN de sitio a sitio en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Algunos ejemplos de políticas VPN de sitio a sitio incluyen propuestas IKE, propuestas IPsec y claves previamente compartidas.
6. **Modify > Policies > Remote Access VPN**. Permite modificar las políticas de VPN de acceso remoto en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Entre los ejemplos de políticas de VPN de acceso remoto se incluyen las propuestas de IKE, las propuestas de IPSec y las políticas PKI.
7. **Modifique > Políticas > SSL VPN**. Permite modificar las políticas SSL VPN en los dispositivos PIX/ASA/FWSM y los routers IOS, como el asistente SSL VPN.
8. **Modificar > Políticas > Interfaces**. Permite modificar las políticas de interfaz (ubicadas en el selector de políticas en Interfaces) en dispositivos PIX/ASA/FWSM, routers IOS, sensores IPS y dispositivos Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, este permiso cubre los puertos de hardware y la configuración de la interfaz.En los routers IOS, este permiso cubre la configuración básica y avanzada de la interfaz, así como otras políticas relacionadas con la interfaz, como las políticas DSL, PVC, PPP y dialer.En los sensores IPS, este permiso cubre las interfaces físicas y los mapas de resumen.En los dispositivos Catalyst 6500/7600, este permiso cubre las interfaces y la configuración de VLAN.
9. **Modificar > Políticas > Puente**. Permite modificar las políticas de tabla ARP (ubicadas en el selector de políticas en Plataforma > Puente) en dispositivos PIX/ASA/FWSM.
10. **Modificar > Políticas > Administración de dispositivos**. Permite modificar las políticas de

administración de dispositivos (situadas en el selector de políticas en Plataforma > Administrador de dispositivos) en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, los ejemplos incluyen políticas de acceso de dispositivos, políticas de acceso al servidor y políticas de conmutación por fallas.En los routers IOS, los ejemplos incluyen políticas de acceso de dispositivos (incluido el acceso a la línea), políticas de acceso al servidor, AAA y aprovisionamiento seguro de dispositivos.En los sensores IPS, este permiso cubre las políticas de acceso de dispositivos y las políticas de acceso al servidor.En los dispositivos Catalyst 6500/7600, este permiso cubre la configuración de IDSM y la lista de acceso de VLAN.

11. **Modificar > Políticas > Identidad**. Permite modificar las políticas de identidad (que se encuentran en el selector de políticas en Plataforma > Identidad) en los routers Cisco IOS, incluidas las políticas 802.1x y Network Admission Control (NAC).
12. **Modificar > Políticas > Registro**. Permite modificar las políticas de registro (ubicadas en el selector de políticas en Plataforma > Registro) en dispositivos PIX/ASA/FWSM, routers IOS y sensores IPS. Algunos ejemplos de políticas de registro son: configuración de registro, configuración del servidor y políticas del servidor syslog.
13. **Modificar > Políticas > Multicast**. Permite modificar las políticas de multidifusión (situadas en el selector de políticas en Plataforma > Multidifusión) en dispositivos PIX/ASA/FWSM. Algunos ejemplos de políticas de multidifusión son el routing de multidifusión y las políticas IGMP.
14. **Modificar > Políticas > QoS**. Permite modificar las políticas de QoS (situadas en el selector de políticas en Plataforma > Calidad de servicio) en los routers Cisco IOS.
15. **Modificar > Políticas > Enrutamiento**. Le permite modificar las políticas de ruteo (ubicadas en el selector de políticas en Plataforma > Ruteo) en los dispositivos PIX/ASA/FWSM y los routers IOS. Algunos ejemplos de políticas de ruteo incluyen OSPF, RIP y políticas de ruteo estáticas.
16. **Modificar > Políticas > Seguridad**. Permite modificar las políticas de seguridad (ubicadas en el selector de políticas en Plataforma > Seguridad) en dispositivos PIX/ASA/FWSM y sensores IPS:En los dispositivos PIX/ASA/FWSM, las políticas de seguridad incluyen la configuración anti-simulación, fragmento y tiempo de espera.En los sensores IPS, las políticas de seguridad incluyen la configuración de bloqueo.
17. **Modificar > Políticas > Reglas de política de servicio**. Permite modificar las políticas de regla de política de servicio (situadas en el selector de políticas en Plataforma > Reglas de política de servicio) en dispositivos PIX 7.x/ASA. Los ejemplos incluyen colas de prioridad e IPS, QoS y reglas de conexión.
18. **Modificar > Políticas > Preferencias de usuario**. Permite modificar la política de implementación (ubicada en el selector de políticas en Plataforma > Preferencias de usuario) en dispositivos PIX/ASA/FWSM. Esta política contiene una opción para borrar todas las traducciones NAT en la implementación.
19. **Modificar > Políticas > Dispositivo virtual**. Permite modificar las políticas de sensores virtuales en los dispositivos IPS. Utilice esta política para crear sensores virtuales.
20. **Modificar > Políticas > FlexConfig**. Permite modificar FlexConfigs, que son comandos e instrucciones CLI adicionales que se pueden implementar en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600.

Modificar permisos de objetos

El Administrador de seguridad incluye los siguientes permisos de vista para los objetos:

1. **Modify > Objects > AAA Server Groups**. Permite ver los objetos de grupo de servidores AAA. Estos objetos se utilizan en políticas que requieren servicios AAA (autenticación, autorización y contabilidad).
2. **Modificar > Objetos > Servidores AAA**. Permite ver objetos de servidor AAA. Estos objetos representan servidores AAA individuales que se definen como parte de un grupo de servidores AAA.
3. **Modify > Objects > Access Control Lists - Standard/Extended**. Permite ver objetos ACL estándar y extendidos. Los objetos de ACL extendidos se utilizan para una variedad de políticas, como NAT y NAC, y para establecer el acceso VPN. Los objetos ACL estándar se utilizan para políticas como OSPF y SNMP, así como para establecer el acceso VPN.
4. **Modificar > Objetos > Listas de Control de Acceso - Web**. Permite ver objetos de ACL web. Los objetos Web ACL se utilizan para realizar el filtrado de contenido en las políticas SSL VPN.
5. **Modify > Objects > ASA** User Groups. Permite ver los objetos de grupo de usuarios de ASA. Estos objetos se configuran en dispositivos de seguridad ASA en configuraciones Easy VPN, VPN de acceso remoto y VPN SSL.
6. **Modificar > Objetos > Categorías**. Permite ver objetos de categoría. Estos objetos le ayudan a identificar fácilmente reglas y objetos en las tablas de reglas mediante el uso del color.
7. **Modificar > Objetos > Credenciales**. Permite ver objetos de credenciales. Estos objetos se utilizan en la configuración de Easy VPN durante la autenticación ampliada IKE (Xauth).
8. **Modificar > Objetos > FlexConfigs**. Permite ver objetos FlexConfig. Estos objetos, que contienen comandos de configuración con instrucciones de lenguaje de secuencias de comandos adicionales, se pueden utilizar para configurar comandos que no son compatibles con la interfaz de usuario del Administrador de seguridad.
9. **Modificar > Objetos > Propuestas IKE**. Permite ver los objetos de propuesta IKE. Estos objetos contienen los parámetros requeridos para las propuestas IKE en las políticas VPN de acceso remoto.
10. **Modify > Objects > Inspect - Class Maps - DNS**. Permite ver objetos de mapa de clase DNS. Estos objetos coinciden con el tráfico DNS con criterios específicos para que se puedan realizar acciones en ese tráfico.
11. **Modify > Objects > Inspect - Class Maps - FTP**. Permite ver objetos de mapa de clase FTP. Estos objetos coinciden con el tráfico FTP con criterios específicos para que se puedan realizar acciones en ese tráfico.
12. **Modify > Objects > Inspect - Class Maps - HTTP**. Permite ver objetos de mapa de clase HTTP. Estos objetos coinciden con el tráfico HTTP con criterios específicos para que se puedan realizar acciones en ese tráfico.
13. **Modify > Objects > Inspect - Class Maps - IM**. Permite ver objetos de mapa de clase de IM. Estos objetos coinciden con el tráfico de IM con criterios específicos, de modo que se puedan realizar acciones en ese tráfico.
14. **Modify > Objects > Inspect - Class Maps - SIP**. Permite ver objetos de mapa de clase SIP. Estos objetos coinciden con el tráfico SIP con criterios específicos para que se puedan realizar acciones en ese tráfico.
15. **Modify > Objects > Inspect - Policy Maps - DNS**. Permite ver objetos de mapa de políticas DNS. Estos objetos se utilizan para crear mapas de inspección para el tráfico DNS.
16. **Modify > Objects > Inspect - Policy Maps - FTP**. Permite ver objetos de mapa de políticas FTP. Estos objetos se utilizan para crear mapas de inspección para el tráfico FTP.
17. **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite ver los objetos de mapa de política HTTP creados para dispositivos ASA/PIX 7.x y routers IOS.

Estos objetos se utilizan para crear mapas de inspección para el tráfico HTTP.

18. **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)**. Permite ver los objetos de mapa de política HTTP creados para dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear mapas de inspección para el tráfico HTTP.
19. **Modify > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2)**. Permite ver los objetos de mapa de política de IM creados para dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear mapas de inspección para el tráfico de IM.
20. **Modify > Objects > Inspect - Policy Maps - IM (IOS)**. Permite ver los objetos de mapa de políticas de IM creados para los dispositivos IOS. Estos objetos se utilizan para crear mapas de inspección para el tráfico de IM.
21. **Modify > Objects > Inspect - Policy Maps - SIP**. Permite ver objetos de mapa de política SIP. Estos objetos se utilizan para crear mapas de inspección para el tráfico SIP.
22. **Modificar > Objetos > Inspeccionar - Expresiones regulares**. Permite ver los objetos de expresión regular. Estos objetos representan expresiones regulares individuales que se definen como parte de un grupo de expresiones regulares.
23. **Modificar > Objetos > Inspeccionar - Grupos de expresiones regulares**. Permite ver los objetos de grupo de expresiones regulares. Estos objetos son utilizados por ciertos mapas de clase e inspeccionan los mapas para que coincidan con el texto dentro de un paquete.
24. **Modificar > Objetos > Inspeccionar - Mapas TCP**. Permite ver objetos de mapa TCP. Estos objetos personalizan la inspección en el flujo TCP en ambas direcciones.
25. **Modify > Objects > Interface Roles**. Permite ver objetos de rol de interfaz. Estos objetos definen patrones de nomenclatura que pueden representar varias interfaces en diferentes tipos de dispositivos. Las funciones de interfaz permiten aplicar políticas a interfaces específicas en varios dispositivos sin tener que definir manualmente el nombre de cada interfaz.
26. **Modificar > Objetos > Conjuntos de transformación IPsec**. Permite ver los objetos del conjunto de transformación IPsec. Estos objetos comprenden una combinación de protocolos de seguridad, algoritmos y otros ajustes que especifican exactamente cómo se cifrarán y autenticarán los datos del túnel IPsec.
27. **Modify > Objects > LDAP Attribute Maps**. Permite ver objetos de mapa de atributos LDAP. Estos objetos se utilizan para asignar nombres de atributos personalizados (definidos por el usuario) a nombres de atributos de Cisco LDAP.
28. **Modificar > Objetos > Redes/Hosts**. Permite ver objetos de host/red. Estos objetos son colecciones lógicas de direcciones IP que representan redes, hosts o ambos. Los objetos de red/host permiten definir políticas sin especificar cada red o host individualmente.
29. **Modificar > Objetos > Inscripciones PKI**. Permite ver los objetos de inscripción PKI. Estos objetos definen los servidores de la Autoridad de certificación (CA) que funcionan dentro de una infraestructura de clave pública.
30. **Modify > Objects > Port Forwarding Lists**. Permite ver los objetos de la lista de reenvío de puertos. Estos objetos definen las asignaciones de números de puerto en un cliente remoto a la dirección IP de la aplicación y al puerto detrás de un gateway VPN SSL.
31. **Modificar > Objetos > Configuraciones de escritorio seguro**. Permite ver objetos de configuración de escritorio seguros. Estos objetos son reutilizables, componentes con nombre a los que las políticas SSL VPN pueden hacer referencia para proporcionar un medio fiable de eliminar todos los rastros de datos confidenciales que se comparten durante la duración de una sesión SSL VPN.
32. **Modify > Objects > Services - Port Lists**. Permite ver los objetos de la lista de puertos. Estos objetos, que contienen uno o más rangos de números de puerto, se utilizan para

simplificar el proceso de creación de objetos de servicio.

33. **Modify > Objects > Services/Service Groups.** Permite ver los objetos de servicio y de grupo de servicios. Estos objetos son asignaciones definidas de definiciones de protocolo y puerto que describen los servicios de red utilizados por las políticas, como Kerberos, SSH y POP3.
34. **Modify > Objects > Single Sign On Servers.** Permite ver el inicio de sesión único en los objetos del servidor. Single Sign-On (SSO) permite a los usuarios de SSL VPN introducir un nombre de usuario y una contraseña una vez y acceder a varios servicios protegidos y servidores web.
35. **Modificar > Objetos > Monitores SLA**. Permite ver objetos de supervisión SLA. Estos objetos son utilizados por los dispositivos de seguridad PIX/ASA que ejecutan la versión 7.2 o posterior para realizar el seguimiento de la ruta. Esta función proporciona un método para realizar un seguimiento de la disponibilidad de una ruta principal e instalar una ruta de respaldo si la ruta principal falla.
36. **Modificar > Objetos > Personalizaciones SSL VPN**. Permite ver los objetos de personalización de VPN SSL. Estos objetos definen cómo cambiar el aspecto de las páginas SSL VPN que se muestran a los usuarios, como Login/Logout y páginas de inicio.
37. **Modify > Objects > SSL VPN Gateways**. Permite ver objetos de gateway VPN SSL. Estos objetos definen parámetros que permiten que el gateway se utilice como proxy para las conexiones a los recursos protegidos en su SSL VPN.
38. **Modificar > Objetos > Objetos de estilo**. Permite ver objetos de estilo. Estos objetos le permiten configurar elementos de estilo, como las características de fuente y los colores, para personalizar el aspecto de la página SSL VPN que aparece para los usuarios SSL VPN cuando se conectan al dispositivo de seguridad.
39. **Modificar > Objetos > Objetos de Texto**. Permite ver objetos de texto de formato libre. Estos objetos comprenden un par de nombre y valor, donde el valor puede ser una única cadena, una lista de cadenas o una tabla de cadenas.
40. **Modify > Objects > Time Ranges (Modificar > Objetos > Rangos de tiempo).** Permite ver objetos de intervalo de tiempo. Estos objetos se utilizan al crear ACL basadas en tiempo y reglas de inspección. También se utilizan al definir grupos de usuarios ASA para restringir el acceso VPN a horas específicas durante la semana.
41. **Modificar > Objetos > Flujos de tráfico**. Permite ver los objetos de flujo de tráfico. Estos objetos definen flujos de tráfico específicos para su uso por los dispositivos PIX 7.x/ASA 7.x.
42. **Modificar > Objetos > Listas de URL**. Permite ver objetos de lista de URL. Estos objetos definen las URL que se muestran en la página del portal después de un inicio de sesión correcto. Esto permite a los usuarios acceder a los recursos disponibles en los sitios web de SSL VPN cuando funcionan en modo de acceso sin cliente.
43. **Modificar > Objetos > Grupos de usuarios**. Permite ver los objetos de grupo de usuarios. Estos objetos definen grupos de clientes remotos que se utilizan en topologías Easy VPN, VPN de acceso remoto y VPN SSL
44. **Modify > Objects > WINS Server Lists**. Permite ver los objetos de lista del servidor WINS. Estos objetos representan servidores WINS, que utilizan SSL VPN para acceder o compartir archivos en sistemas remotos.
45. **Modify > Objects > Internal - DN Rules.** Permite ver las reglas DN que utilizan las políticas DN. Se trata de un objeto interno que utiliza el Administrador de seguridad y que no aparece en el Administrador de objetos de directiva.
46. **Modify > Objects > Internal - Client Updates**. Se trata de un objeto interno requerido por los

objetos de grupo de usuarios que no aparece en el Administrador de objetos de directiva.
47. **Modify > Objects > Internal - Standard ACE**. Se trata de un objeto interno para las entradas de control de acceso estándar, que utilizan los objetos ACL.
48. **Modify > Objects > Internal - Extended ACE**. Se trata de un objeto interno para las entradas de control de acceso extendido que utilizan los objetos ACL.

Permisos de modificación adicionales

Security Manager incluye los permisos de modificación adicionales como se muestra a continuación:

1. **Modify > Admin**. Permite modificar la configuración administrativa del Administrador de seguridad.
2. **Modificar > Archivo de configuración**. Permite modificar la configuración del dispositivo en el Archivo de configuración. Además, permite agregar configuraciones al archivo y personalizar la herramienta Archivo de configuración.
3. **Modificar > Dispositivos**. Permite agregar y eliminar dispositivos, así como modificar propiedades y atributos del dispositivo. Para detectar las directivas del dispositivo que se va a agregar, también debe habilitar el permiso Importar. Además, si habilita el permiso Modificar > Dispositivos, asegúrese de habilitar también el permiso Asignar > Políticas > Interfaces.
4. **Modificar > Jerarquía**. Permite modificar grupos de dispositivos.
5. **Modificar > Topología**. Permite modificar mapas en la vista Mapa.

Asignar permisos

Security Manager incluye los permisos de asignación de directivas como se muestra a continuación:

1. **Asignar > Políticas > Firewall**. Permite asignar políticas de servicio de firewall (situadas en el selector de políticas en Firewall) a dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Algunos ejemplos de políticas de servicio de firewall son las reglas de acceso, las reglas AAA y las reglas de inspección.
2. **Asignar > Políticas > Sistema de prevención de intrusiones**. Permite asignar políticas IPS (situadas en el selector de políticas en IPS), incluidas las políticas para IPS que se ejecutan en routers IOS.
3. **Asignar > Políticas > Imagen**. El Administrador de seguridad no utiliza actualmente este permiso.
4. **Asignar > Políticas > NAT**. Permite asignar políticas de traducción de direcciones de red a dispositivos PIX/ASA/FWSM y routers IOS. Algunos ejemplos de políticas NAT incluyen reglas estáticas y reglas dinámicas.
5. **Asignar > Políticas > VPN de sitio a sitio**. Permite asignar políticas VPN de sitio a sitio a dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Algunos ejemplos de políticas VPN de sitio a sitio incluyen propuestas IKE, propuestas IPsec y claves previamente compartidas.
6. **Asignar > Políticas > VPN de acceso remoto**. Permite asignar políticas VPN de acceso remoto a dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600. Entre los ejemplos de políticas de VPN de acceso remoto se incluyen las propuestas de IKE, las

propuestas de IPSec y las políticas PKI.

7. **Asignar > Políticas > SSL VPN**. Permite asignar políticas SSL VPN a dispositivos PIX/ASA/FWSM y routers IOS, como el asistente SSL VPN.
8. **Asignar > Políticas > Interfaces**. Permite asignar políticas de interfaz (situadas en el selector de políticas en Interfaces) a dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, este permiso cubre los puertos de hardware y la configuración de la interfaz.En los routers IOS, este permiso cubre la configuración básica y avanzada de la interfaz, así como otras políticas relacionadas con la interfaz, como las políticas DSL, PVC, PPP y dialer.En los dispositivos Catalyst 6500/7600, este permiso cubre las interfaces y la configuración de VLAN.
9. **Asignar > Políticas > Puente**. Permite asignar políticas de tabla ARP (situadas en el selector de políticas en Plataforma > Puente) a dispositivos PIX/ASA/FWSM.
10. **Asignar > Políticas > Administración de dispositivos**. Permite asignar políticas de administración de dispositivos (situadas en el selector de políticas en Plataforma > Administrador de dispositivos) a dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, los ejemplos incluyen políticas de acceso de dispositivos, políticas de acceso al servidor y políticas de conmutación por fallas.En los routers IOS, los ejemplos incluyen políticas de acceso de dispositivos (incluido el acceso a la línea), políticas de acceso al servidor, AAA y aprovisionamiento seguro de dispositivos.En los sensores IPS, este permiso cubre las políticas de acceso de dispositivos y las políticas de acceso al servidor.En los dispositivos Catalyst 6500/7600, este permiso cubre la configuración de IDSM y las listas de acceso de VLAN.
11. **Asignar > Políticas > Identidad**. Permite asignar políticas de identidad (situadas en el selector de políticas en Plataforma > Identidad) a los routers Cisco IOS, incluidas las políticas 802.1x y Network Admission Control (NAC).
12. **Asignar > Políticas > Registro**. Permite asignar políticas de registro (situadas en el selector de políticas en Plataforma > Registro) a dispositivos PIX/ASA/FWSM y routers IOS. Algunos ejemplos de políticas de registro son: configuración de registro, configuración del servidor y políticas del servidor syslog.
13. **Asignar > Políticas > Multicast**. Permite asignar políticas de multidifusión (situadas en el selector de políticas en Plataforma > Multidifusión) a dispositivos PIX/ASA/FWSM. Algunos ejemplos de políticas de multidifusión son el routing de multidifusión y las políticas IGMP.
14. **Asignar > Políticas > QoS**. Permite asignar políticas de QoS (situadas en el selector de políticas en Plataforma > Calidad de servicio) a los routers Cisco IOS.
15. **Asignar > Políticas > Enrutamiento**. Permite asignar políticas de ruteo (situadas en el selector de políticas en Plataforma > Ruteo) a dispositivos PIX/ASA/FWSM y routers IOS. Algunos ejemplos de políticas de ruteo incluyen OSPF, RIP y políticas de ruteo estáticas.
16. **Asignar > Políticas > Seguridad**. Permite asignar políticas de seguridad (situadas en el selector de políticas en Plataforma > Seguridad) a dispositivos PIX/ASA/FWSM. Las políticas de seguridad incluyen la configuración de tiempo de espera, fragmentos y antisimulación.
17. **Asignar > Políticas > Reglas de política de servicio**. Permite asignar políticas de regla de política de servicio (situadas en el selector de políticas en Plataforma > Reglas de política de servicio) a dispositivos PIX 7.x/ASA. Los ejemplos incluyen colas de prioridad e IPS, QoS y reglas de conexión.
18. **Asignar > Políticas > Preferencias de usuario**. Permite asignar la política de implementación (ubicada en el selector de políticas en Plataforma > Preferencias de usuario) a dispositivos PIX/ASA/FWSM. Esta política contiene una opción para borrar todas

las traducciones NAT en la implementación.

19. **Asignar > Políticas > Dispositivo virtual**. Permite asignar políticas de sensores virtuales a dispositivos IPS. Utilice esta política para crear sensores virtuales.
20. **Asignar > Políticas > FlexConfig**. Permite asignar FlexConfigs, que son comandos e instrucciones CLI adicionales que se pueden implementar en dispositivos PIX/ASA/FWSM, routers IOS y dispositivos Catalyst 6500/7600.

Nota: Cuando especifique permisos de asignación, asegúrese de que también ha seleccionado los permisos de vista correspondientes.

Aprobar permisos

Security Manager proporciona los permisos de aprobación como se muestra:

1. **Aprobar > CLI**. Permite aprobar los cambios del comando CLI contenidos en un trabajo de implementación.
2. **Aprobar > Política**. Permite aprobar los cambios de configuración contenidos en las políticas configuradas en una actividad de flujo de trabajo.

Comprensión de las funciones de CiscoWorks

Cuando se crean usuarios en CiscoWorks Common Services, se les asigna una o más funciones. Los permisos asociados a cada función determinan las operaciones que cada usuario está autorizado a realizar en el Administrador de seguridad.

Los temas siguientes describen las funciones de CiscoWorks:

- Funciones predeterminadas de CiscoWorks Common Services
- Asignación de roles a usuarios en CiscoWorks Common Services

Funciones predeterminadas de CiscoWorks Common Services

CiscoWorks Common Services contiene las siguientes funciones predeterminadas:

1. **Help Desk**: los usuarios del soporte técnico pueden ver (pero no modificar) dispositivos, políticas, objetos y mapas de topología.
2. **Operador de red**: además de ver permisos, los operadores de red pueden ver los comandos CLI y la configuración administrativa de Security Manager. Los operadores de red también pueden modificar el archivo de configuración y ejecutar comandos (como ping) en los dispositivos.
3. **Aprobador**: además de ver permisos, los aprobadores pueden aprobar o rechazar trabajos de implementación. No pueden realizar la implementación.
4. **Administrador de red**: los administradores de red tienen permisos completos de visualización y modificación, excepto para modificar la configuración administrativa. Pueden detectar dispositivos y las políticas configuradas en estos dispositivos, asignar políticas a los dispositivos y ejecutar comandos en los dispositivos. Los administradores de red no pueden aprobar actividades ni trabajos de implementación; sin embargo, pueden implementar trabajos aprobados por otros.
5. **Administrador del sistema**: los administradores del sistema tienen acceso completo a todos

los permisos del Administrador de seguridad, incluidas la modificación, la asignación de políticas, la aprobación de actividades y tareas, la detección, la implementación y la ejecución de comandos en los dispositivos.

Nota: Es posible que se muestren funciones adicionales, como datos de exportación, en Common Services si se instalan aplicaciones adicionales en el servidor. El rol de datos de exportación es para desarrolladores de terceros y no lo utiliza el Administrador de seguridad.

Sugerencia: Aunque no puede cambiar la definición de las funciones de CiscoWorks, puede definir qué funciones se asignan a cada usuario. Para obtener más información, vea Asignación de Funciones a los Usuarios en CiscoWorks Common Services.

Asignación de roles a usuarios en CiscoWorks Common Services

CiscoWorks Common Services permite definir las funciones asignadas a cada usuario. Al cambiar la definición de rol de un usuario, cambia los tipos de operaciones que este usuario está autorizado a realizar en el Administrador de seguridad. Por ejemplo, si asigna la función de Help Desk, el usuario se limita a ver las operaciones y no puede modificar ningún dato. Sin embargo, si asigna la función de operador de red, el usuario también puede modificar el archivo de configuración. Puede asignar varias funciones a cada usuario.

Nota: Debe reiniciar el Administrador de seguridad después de realizar cambios en los permisos de usuario.

Procedimiento:

1. En Common Services, seleccione **Server > Security** y, a continuación, seleccione **Single-Server Trust Management > Local User Setup** en la TOC.**Sugerencia:** Para acceder a la página Local User Setup desde dentro del Administrador de seguridad, seleccione Tools > Security Manager Administration > Server Security y, a continuación, haga clic en Local User Setup (Configuración de usuario local).
2. Active la casilla de verificación junto a un usuario existente y, a continuación, haga clic en **Editar**.
3. En la página User Information (Información de usuario), active las funciones que desea asignar a este usuario haciendo clic en las casillas de verificación.Para obtener más información sobre cada función, vea Funciones predeterminadas de CiscoWorks Common Services.
4. Haga clic en **Aceptar** para guardar los cambios.
5. Reinicie el Administrador de seguridad.

Introducción a las funciones de Cisco Secure ACS

Cisco Secure ACS proporciona mayor flexibilidad para gestionar los permisos de Security Manager que CiscoWorks, ya que admite funciones específicas de la aplicación que puede configurar. Cada función consta de un conjunto de permisos que determinan el nivel de autorización de las tareas del Administrador de seguridad. En Cisco Secure ACS, asigna una función a cada grupo de usuarios (y opcionalmente, también a usuarios individuales), lo que permite a cada usuario de ese grupo realizar las operaciones autorizadas por los permisos definidos para esa función.

Además, puede asignar estas funciones a los grupos de dispositivos Cisco Secure ACS, lo que permite diferenciar los permisos en diferentes conjuntos de dispositivos.

Nota: Los grupos de dispositivos Cisco Secure ACS son independientes de los grupos de dispositivos de Security Manager.

Los siguientes temas describen las funciones de Cisco Secure ACS:

- Funciones predeterminadas de Cisco Secure ACS
- Personalización de las Funciones de Cisco Secure ACS

Funciones predeterminadas de Cisco Secure ACS

Cisco Secure ACS incluye las mismas funciones que CiscoWorks (consulte Introducción a las funciones de CiscoWorks), además de estas funciones adicionales:

1. **Aprobador de seguridad**: los aprobadores de seguridad pueden ver (pero no modificar) dispositivos, políticas, objetos, mapas, comandos CLI y configuraciones administrativas. Además, los aprobadores de seguridad pueden aprobar o rechazar los cambios de configuración contenidos en una actividad. No pueden aprobar ni rechazar el trabajo de implementación, ni tampoco pueden realizar la implementación.
2. **Administrador de seguridad**: además de tener permisos de vista, los administradores de seguridad pueden modificar dispositivos, grupos de dispositivos, políticas, objetos y mapas de topología. También pueden asignar políticas a dispositivos y topologías VPN, y realizar la detección para importar nuevos dispositivos al sistema.
3. **Administrador de red**: además de ver permisos, los administradores de red pueden modificar el archivo de configuración, realizar la implementación y ejecutar comandos en los dispositivos.

Nota: Los permisos contenidos en la función de administrador de red de Cisco Secure ACS son diferentes de los incluidos en la función de administrador de red de CiscoWorks. Para obtener más información, vea Comprensión de las Funciones de CiscoWorks.

A diferencia de CiscoWorks, Cisco Secure ACS permite personalizar los permisos asociados a cada función del administrador de seguridad. Para obtener más información sobre la modificación de las funciones predeterminadas, vea Personalización de las Funciones ACS Seguras de Cisco.

Nota: Cisco Secure ACS 3.3 o posterior debe estar instalado para la autorización del Administrador de seguridad.

Personalización de las Funciones de Cisco Secure ACS

Cisco Secure ACS le permite modificar los permisos asociados a cada función del administrador de seguridad. También puede personalizar Cisco Secure ACS creando funciones de usuario especializadas con permisos dirigidos a tareas específicas de Security Manager.

Nota: Debe reiniciar el Administrador de seguridad después de realizar cambios en los permisos de usuario.

Procedimiento:

1. En Cisco Secure ACS, haga clic en **Shared Profile Components** en la barra de navegación.
2. Haga clic en **Cisco Security Manager** en la página Componentes compartidos. Se muestran las funciones configuradas para el Administrador de seguridad.
3. Siga uno de los siguientes pasos:Para crear una función, haga clic en **Agregar**. Vaya al paso 4.Para modificar una función existente, haga clic en la función. Vaya al paso 5.
4. Introduzca un nombre para la función y, opcionalmente, una descripción.
5. Seleccione y anule la selección de las casillas del árbol de permisos para definir los permisos para esta funciónAl activar la casilla de verificación de una rama del árbol, se seleccionan todos los permisos de esa rama. Por ejemplo, al seleccionar **Asignar** se seleccionan todos los permisos de asignación.Para obtener una lista completa de los permisos del Administrador de seguridad, vea Permisos del Administrador de seguridad.**Nota:** Al seleccionar permisos de modificación, aprobación, asignación, importación, control o implementación, también debe seleccionar los permisos de vista correspondientes; de lo contrario, el Administrador de seguridad no funcionará correctamente.
6. Haga clic en **Enviar** para guardar los cambios.
7. Reinicie el Administrador de seguridad.

Asociaciones predeterminadas entre permisos y funciones en el Administrador de seguridad

Esta tabla muestra cómo los permisos del Administrador de seguridad están asociados a las funciones de CiscoWorks Common Services y a las funciones predeterminadas de Cisco Secure ACS.

Permisos	Funciones							
	Administrador del sistema	Administrador de seguridad (ACS)	Aprobador de seguridad (ACS)	Administrador de red (CW)	Administrador de red (ACS)	Aprobador	Operador de red	Help Desk
Ver permisos								
Ver dispositivo	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ver política	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ver objetos	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ver topología	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ver CLI	Ye	Ye	Ye	Ye	Ye	Ye	Ye	No

	s	s	s	s	s	s	s	
View Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Ver archivo de configuración	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ver administradores de dispositivos	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Modificar permisos								
Modificar dispositivo	Yes	Yes	No	Yes	No	No	No	No
Modificar jerarquía	Yes	Yes	No	Yes	No	No	No	No
Modificar política	Yes	Yes	No	Yes	No	No	No	No
Modificar imagen	Yes	Yes	No	Yes	No	No	No	No
Modificar objetos	Yes	Yes	No	Yes	No	No	No	No
Modificar topología	Yes	Yes	No	Yes	No	No	No	No
Modificar administrador	Yes	No	No	No	No	No	No	No
Modificar archivo de configuración	Yes	Yes	No	Yes	Yes	No	Yes	No
Permisos adicionales								
Asignar política	Yes	Yes	No	Yes	No	No	No	No
Aprobar política	Yes	No	Yes	No	No	No	No	No
Aprobar CLI	Yes	No	No	No	No	Yes	No	No
Detectar (importar)	Yes	Yes	No	Yes	No	No	No	No
Implementar	Yes	No	No	Yes	Yes	No	No	No
Control	Yes	No	No	Yes	Yes	No	Yes	No
Enviar	Yes	Yes	No	Yes	No	No	No	No

Información Relacionada

- Página de soporte de Cisco Security Manager
- Soporte Técnico y Documentación - Cisco Systems