CSM 3.x: Configurar permissões e funções de usuário

Contents

Introduction

Este documento descreve como configurar as permissões e funções para os usuários no Cisco Security Manager (CSM).

Prerequisites

Requirements

Este documento pressupõe que o CSM está instalado e funciona corretamente.

Componentes Utilizados

As informações neste documento são baseadas no CSM 3.1.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar permissões de usuário

O Cisco Security Manager autentica seu nome de usuário e sua senha antes de fazer login. Depois de serem autenticados, o Security Manager estabelece sua função no aplicativo. Essa função define suas permissões (também chamadas de privilégios), que são o conjunto de tarefas ou operações que você está autorizado a executar. Se você não estiver autorizado para determinadas tarefas ou dispositivos, os itens de menu relacionados, os itens de TOC e os botões serão ocultos ou desativados. Além disso, uma mensagem informa que você não tem permissão para exibir as informações selecionadas ou executar a operação selecionada.

A autenticação e a autorização do Security Manager são gerenciadas pelo servidor CiscoWorks ou pelo Cisco Secure Access Control Server (ACS). Por padrão, o CiscoWorks gerencia autenticação e autorização, mas você pode alterar para o Cisco Secure ACS usando a página AAA Mode Setup do CiscoWorks Common Services.

As principais vantagens do uso do Cisco Secure ACS são a capacidade de criar funções de usuário altamente granulares com conjuntos de permissões especializados (por exemplo, permitindo que o usuário configure determinados tipos de política, mas não outros) e a capacidade de restringir usuários a determinados dispositivos configurando grupos de dispositivos de rede (NDGs).

Os tópicos a seguir descrevem permissões de usuário:

- Permissões do Security Manager
- Entendendo as funções do CiscoWorks
- Entendendo as funções do Cisco Secure ACS
- Associações padrão entre permissões e funções no Gerenciador de segurança

Permissões do Security Manager

O Security Manager classifica as permissões nas categorias conforme mostrado:

1. **Exibir**—Permite que você veja as configurações atuais. Para obter mais informações, consulte Exibir permissões.
2. **Modificar** — Permite alterar as configurações atuais. Para obter mais informações, consulte Modificar permissões.
3. **Atribuir** —Permite atribuir políticas a dispositivos e topologias VPN. Para obter mais informações, consulte Atribuir permissões
4. **Aprovar** —Permite aprovar alterações de política e trabalhos de implantação. Para obter mais informações, consulte Aprovar permissões.
5. **Importar** — Permite importar as configurações que já estão implantadas em dispositivos

para o Security Manager.
6. **Implantar** — Permite implantar alterações de configuração nos dispositivos na rede e executar reversão para retornar a uma configuração previamente implantada.
7. **Controle** —Permite que você emita comandos para dispositivos, como ping.
8. **Submeter** — Permite submeter as alterações de configuração para aprovação.

- Ao selecionar as permissões de modificar, atribuir, aprovar, importar, controlar ou implantar, você também deve selecionar as permissões de exibição correspondentes; caso contrário, o Security Manager não funcionará corretamente.
- Ao selecionar modificar permissões de política, você também deve selecionar as permissões de política de atribuição e exibição correspondentes.
- Quando você permite uma política que usa objetos de política como parte de sua definição, também deve conceder permissões de exibição a esses tipos de objeto. Por exemplo, se você selecionar a permissão para modificar as políticas de roteamento, também deverá selecionar as permissões para exibir objetos de rede e funções de interface, que são os tipos de objetos exigidos pelas políticas de roteamento.
- O mesmo se aplica ao permitir um objeto que usa outros objetos como parte de sua definição. Por exemplo, se você selecionar a permissão para modificar grupos de usuários, também deverá selecionar as permissões para exibir objetos de rede, objetos de ACL e grupos de servidores AAA.

Exibir permissões

As permissões de visualização (somente leitura) no Gerenciador de segurança são divididas em categorias, conforme mostrado:

- Exibir permissões de políticas
- Exibir permissões de objetos
- Permissões adicionais de visualização

Exibir permissões de políticas

O Gerenciador de segurança inclui as seguintes permissões de exibição para políticas:

1. **Exibir > Políticas > Firewall.** Permite exibir políticas de serviço de firewall (localizadas no seletor de Política em Firewall) em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de serviço de firewall incluem regras de acesso, regras de AAA e regras de inspeção.
2. **Exibir > Políticas > Sistema de prevenção de intrusão.** Permite visualizar as políticas de IPS (localizadas no seletor de política em IPS), incluindo as políticas para IPS em execução em roteadores IOS.
3. **Exibir > Políticas > Imagem.** Permite selecionar um pacote de atualização de assinatura no assistente Aplicar atualizações de IPS (localizado em Ferramentas > Aplicar atualização de IPS), mas não permite que você atribua o pacote a dispositivos específicos, a menos que também tenha a permissão Modificar > Políticas > Imagem.
4. **Exibir > Políticas > NAT**. Permite visualizar as políticas de conversão de endereços de rede em dispositivos PIX/ASA/FWSM e roteadores IOS. Exemplos de políticas de NAT incluem regras estáticas e regras dinâmicas.

5. **Exibir > Políticas > VPN site a site**. Permite exibir políticas de VPN site a site em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de VPN site a site incluem propostas de IKE, propostas de IPsec e chaves pré-compartilhadas.
6. **Exibir > Políticas > VPN de acesso remoto**. Permite visualizar políticas de VPN de acesso remoto em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de VPN de acesso remoto incluem propostas de IKE, propostas de IPsec e políticas de PKI.
7. **Exibir > Políticas > SSL VPN**. Permite exibir políticas de VPN SSL em dispositivos PIX/ASA/FWSM e roteadores IOS, como o assistente de VPN SSL.
8. **Exibir > Políticas > Interfaces**. Permite visualizar as políticas de interface (localizadas no seletor de política em Interfaces) em dispositivos PIX/ASA/FWSM, roteadores IOS, sensores IPS e dispositivos Catalyst 6500/7600.Em dispositivos PIX/ASA/FWSM, essa permissão abrange as portas de hardware e as configurações de interface.Nos roteadores IOS, essa permissão abrange as configurações básicas e avançadas da interface, bem como outras políticas relacionadas à interface, como DSL, PVC, PPP e políticas de discador.Em sensores IPS, essa permissão abrange interfaces físicas e mapas de resumo.Nos dispositivos Catalyst 6500/7600, essa permissão abrange interfaces e configurações de VLAN.
9. **Exibir > Políticas > Bridging**. Permite exibir as políticas da tabela ARP (localizadas no seletor Política em Plataforma > Bridging) em dispositivos PIX/ASA/FWSM.
10. **Exibir > Políticas > Administração de dispositivo**. Permite visualizar as políticas de administração de dispositivos (localizadas no seletor de Política em Plataforma > Administrador de dispositivo) em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600:Em dispositivos PIX/ASA/FWSM, os exemplos incluem políticas de acesso a dispositivos, políticas de acesso a servidores e políticas de failover.Nos roteadores IOS, os exemplos incluem políticas de acesso ao dispositivo (incluindo acesso de linha), políticas de acesso ao servidor, AAA e Provisionamento de dispositivo seguro.Em sensores IPS, essa permissão abrange políticas de acesso a dispositivos e políticas de acesso a servidores.Nos dispositivos Catalyst 6500/7600, essa permissão abrange as configurações de IDSM e as listas de acesso de VLAN.
11. **Exibir > Políticas > Identidade**. Permite exibir políticas de identidade (localizadas no seletor de Política em Plataforma > Identidade) em roteadores Cisco IOS, incluindo políticas 802.1x e NAC (Network Admission Control).
12. **Exibir > Políticas > Registro**. Permite exibir políticas de registro (localizadas no seletor de política em Plataforma > Registro) em dispositivos PIX/ASA/FWSM, roteadores IOS e sensores IPS. Exemplos de políticas de registro incluem configuração de registro, configuração de servidor e políticas de servidor syslog.
13. **Exibir > Políticas > Multicast**. Permite exibir políticas multicast (localizadas no seletor de Política em Plataforma > Multicast) em dispositivos PIX/ASA/FWSM. Exemplos de políticas multicast incluem roteamento multicast e políticas IGMP.
14. **Exibir > Políticas > QoS**. Permite exibir as políticas de QoS (localizadas no seletor Política em Plataforma > Qualidade de Serviço) nos roteadores Cisco IOS.
15. **Exibir > Políticas > Roteamento**. Permite visualizar as políticas de roteamento (localizadas no seletor de Política em Plataforma > Roteamento) em dispositivos PIX/ASA/FWSM e roteadores IOS. Exemplos de políticas de roteamento incluem OSPF, RIP e políticas de roteamento estático.
16. **Exibir > Políticas > Segurança**. Permite visualizar as políticas de segurança (localizadas no

seletor de Política em Plataforma > Segurança) em dispositivos PIX/ASA/FWSM e sensores IPS:Em dispositivos PIX/ASA/FWSM, as políticas de segurança incluem configurações de anti-falsificação, fragmento e tempo limite.Nos sensores IPS, as políticas de segurança incluem configurações de bloqueio.

17. **Exibir > Políticas > Regras de Política de Serviço**. Permite exibir políticas de regra de política de serviço (localizadas no seletor de Política em Plataforma > Regras de Política de Serviço) em dispositivos PIX 7.x/ASA. Os exemplos incluem filas de prioridade e IPS, QoS e regras de conexão.
18. **Exibir > Políticas > Preferências do usuário**. Permite exibir a política de implantação (localizada no seletor Política em Plataforma > Preferências do usuário) em dispositivos PIX/ASA/FWSM. Essa política contém uma opção para limpar todas as conversões de NAT na implantação.
19. **Exibir > Políticas > Dispositivo virtual**. Permite visualizar políticas de sensor virtual em dispositivos IPS. Essa política é usada para criar sensores virtuais.
20. **Exibir > Políticas > FlexConfig**. Permite visualizar FlexConfigs, que são comandos e instruções CLI adicionais que podem ser implantados em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600.

Exibir permissões de objetos

O Gerenciador de segurança inclui as seguintes permissões de exibição para objetos:

1. **Exibir > Objetos > Grupos de servidores AAA**. Permite exibir objetos de grupo de servidores AAA. Esses objetos são usados em políticas que exigem serviços AAA (autenticação, autorização e contabilização).
2. **Exibir > Objetos > Servidores AAA**. Permite exibir objetos do servidor AAA. Esses objetos representam servidores AAA individuais que são definidos como parte de um grupo de servidores AAA.
3. **Exibir > Objetos > Listas de Controle de Acesso - Padrão/Estendido**. Permite visualizar objetos de ACL padrão e estendida. Os objetos de ACL estendida são usados para uma variedade de políticas, como NAT e NAC, e para estabelecer acesso VPN. Os objetos de ACL padrão são usados para políticas como OSPF e SNMP, bem como para estabelecer acesso VPN.
4. **Exibir > Objetos > Listas de Controle de Acesso** - Web. Permite exibir objetos da ACL da Web. Os objetos da ACL da Web são usados para executar a filtragem de conteúdo em políticas de VPN SSL.
5. **Exibir > Objetos > Grupos de usuários do ASA**. Permite exibir objetos de grupo de usuários do ASA. Esses objetos são configurados em dispositivos de segurança ASA em configurações de VPN Easy, VPN de acesso remoto e VPN SSL.
6. **Exibir > Objetos > Categorias**. Permite exibir objetos de categoria. Esses objetos ajudam a identificar regras e objetos facilmente em tabelas de regras por meio do uso de cores.
7. **Exibir > Objetos > Credenciais**. Permite exibir objetos de credencial. Esses objetos são usados na configuração do Easy VPN durante a autenticação estendida IKE (Xauth).
8. **Exibir > Objetos > FlexConfigs**. Permite exibir objetos FlexConfig. Esses objetos, que contêm comandos de configuração com instruções adicionais de linguagem de script, podem ser usados para configurar comandos que não são suportados pela interface de usuário do Security Manager.
9. **Exibir > Objetos > Propostas IKE**. Permite exibir objetos de proposta IKE. Esses objetos

contêm os parâmetros necessários para propostas de IKE em políticas de VPN de acesso remoto.

10. **View > Objects > Inspect - Class Maps** - DNS. Permite exibir objetos de mapa de classe DNS. Esses objetos correspondem ao tráfego DNS com critérios específicos para que as ações possam ser executadas nesse tráfego.
11. **View > Objects > Inspect - Class Maps - FTP**. Permite exibir objetos de mapa de classe FTP. Esses objetos correspondem ao tráfego FTP com critérios específicos para que as ações possam ser executadas nesse tráfego.
12. **View > Objects > Inspect - Class Maps - HTTP**. Permite exibir objetos de mapa de classe HTTP. Esses objetos correspondem ao tráfego HTTP com critérios específicos para que as ações possam ser executadas nesse tráfego.
13. **View > Objects > Inspect - Class Maps - IM**. Permite exibir objetos de mapa de classe IM. Esses objetos correspondem ao tráfego de IM com critérios específicos para que as ações possam ser executadas nesse tráfego.
14. **View > Objects > Inspect - Class Maps - SIP**. Permite exibir objetos de mapa de classe SIP. Esses objetos correspondem ao tráfego SIP com critérios específicos para que as ações possam ser executadas nesse tráfego.
15. **View > Objects > Inspect - Policy Maps - DNS (Exibir > Objetos > Inspecionar - Mapas de política - DNS).** Permite exibir objetos de mapa de política DNS. Esses objetos são usados para criar mapas de inspeção para o tráfego DNS.
16. **View > Objects > Inspect - Policy Maps - FTP.** Permite exibir objetos de mapa de políticas de FTP. Esses objetos são usados para criar mapas de inspeção para tráfego FTP.
17. **Exibir > Objetos > Inspecionar - Mapas de Política - GTP**. Permite exibir objetos de mapa de política GTP. Esses objetos são usados para criar mapas de inspeção para tráfego GTP.
18. **View > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite exibir objetos de mapa de política HTTP criados para dispositivos ASA/PIX 7.1.x e roteadores IOS. Esses objetos são usados para criar mapas de inspeção para tráfego HTTP.
19. **View > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)**. Permite exibir objetos de mapa de política HTTP criados para dispositivos ASA 7.2/PIX 7.2. Esses objetos são usados para criar mapas de inspeção para tráfego HTTP.
20. **View > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2)**. Permite exibir objetos de mapa de política de IM criados para dispositivos ASA 7.2/PIX 7.2. Esses objetos são usados para criar mapas de inspeção para tráfego IM.
21. **View > Objects > Inspect - Policy Maps - IM (IOS)**. Permite exibir objetos de mapa de políticas de IM criados para dispositivos IOS. Esses objetos são usados para criar mapas de inspeção para tráfego IM.
22. **Exibir > Objetos > Inspecionar - Mapas de Política - SIP**. Permite exibir objetos do mapa de políticas SIP. Esses objetos são usados para criar mapas de inspeção para o tráfego SIP.
23. **Exibir > Objetos > Inspecionar - Expressões Regulares**. Permite exibir objetos de expressão regular. Esses objetos representam expressões regulares individuais que são definidas como parte de um grupo de expressões regulares.
24. **Exibir > Objetos > Inspecionar - Grupos de Expressões Regulares**. Permite exibir objetos de grupo de expressões regulares. Esses objetos são usados por certos mapas de classe e inspecionam mapas para corresponder texto dentro de um pacote.
25. **Exibir > Objetos > Inspecionar - Mapas TCP**. Permite exibir objetos de mapa TCP. Esses objetos personalizam a inspeção no fluxo TCP em ambas as direções.
26. **Exibir > Objetos > Funções de Interface**. Permite exibir objetos de função de interface.

Esses objetos definem padrões de nomenclatura que podem representar várias interfaces em diferentes tipos de dispositivos. As funções de interface permitem que você aplique políticas a interfaces específicas em vários dispositivos sem precisar definir manualmente o nome de cada interface.

27. **Exibir > Objetos > Conjuntos de Transformação IPsec**. Permite exibir objetos do conjunto de transformações IPsec. Esses objetos compreendem uma combinação de protocolos de segurança, algoritmos e outras configurações que especificam exatamente como os dados no túnel IPsec serão criptografados e autenticados.
28. **View > Objects > LDAP Attribute Maps**. Permite exibir objetos de mapa de atributos LDAP. Esses objetos são usados para mapear nomes de atributos personalizados (definidos pelo usuário) para nomes de atributos do Cisco LDAP.
29. **Exibir > Objetos > Redes/Hosts**. Permite exibir objetos de rede/host. Esses objetos são coleções lógicas de endereços IP que representam redes, hosts ou ambos. Os objetos de rede/host permitem definir políticas sem especificar cada rede ou host individualmente.
30. **Exibir > Objetos > Inscrições PKI**. Permite exibir objetos de inscrição PKI. Esses objetos definem os servidores da Autoridade de Certificação (CA) que operam em uma infraestrutura de chave pública.
31. **Exibir > Objetos > Listas de encaminhamento de portas**. Permite exibir objetos da lista de encaminhamento de portas. Esses objetos definem os mapeamentos de números de porta em um cliente remoto para o endereço IP e a porta do aplicativo atrás de um gateway de VPN SSL.
32. **Exibir > Objetos > Configurações Seguras de Desktop**. Permite exibir objetos de configuração de área de trabalho seguros. Esses objetos são reutilizáveis, componentes nomeados que podem ser referenciados pelas políticas de VPN SSL para fornecer um meio confiável de eliminar todos os rastreamentos de dados confidenciais compartilhados durante uma sessão de VPN SSL.
33. **Exibir > Objetos > Serviços - Listas de Portas**. Permite exibir objetos de lista de portas. Esses objetos, que contêm um ou mais intervalos de números de porta, são usados para simplificar o processo de criação de objetos de serviço.
34. **Exibir > Objetos > Serviços/Grupos de Serviços** Permite que você exiba objetos de serviços e grupos de serviços. Esses objetos são mapeamentos definidos de definições de protocolo e porta que descrevem os serviços de rede usados por políticas, como Kerberos, SSH e POP3.
35. **Exibir > Objetos > Servidores de Logon Único**. Permite exibir objetos de servidor de logon único. O SSO (Single Sign-On, login único) permite que os usuários de VPN SSL insiram um nome de usuário e uma senha uma vez e possam acessar vários serviços protegidos e servidores Web.
36. **Exibir > Objetos > Monitores SLA**. Permite exibir objetos do monitor SLA. Esses objetos são usados por dispositivos de segurança PIX/ASA que executam a versão 7.2 ou posterior para executar o rastreamento de rota. Esse recurso fornece um método para rastrear a disponibilidade de uma rota primária e instalar uma rota de backup se a rota primária falhar.
37. **Exibir > Objetos > Personalizações de VPN SSL**. Permite exibir objetos de personalização de VPN SSL. Esses objetos definem como alterar a aparência das páginas VPN SSL exibidas aos usuários, como Login/Logoff e páginas iniciais.
38. **View > Objects > SSL VPN Gateways**. Permite exibir objetos de gateway de VPN SSL. Esses objetos definem parâmetros que permitem que o gateway seja usado como proxy para conexões com os recursos protegidos em sua VPN SSL.
39. **Exibir > Objetos > Objetos de Estilo**. Permite exibir objetos de estilo. Esses objetos

permitem configurar elementos de estilo, como características de fonte e cores, para personalizar a aparência da página VPN SSL que aparece para usuários de VPN SSL quando eles se conectam ao Security Appliance.

40. **Exibir > Objetos > Objetos de Texto**. Permite exibir objetos de texto em forma livre. Esses objetos compreendem um par de nome e valor, em que o valor pode ser uma única string, uma lista de strings ou uma tabela de strings.
41. **Exibir > Objetos > Intervalos de Tempo.** Permite exibir objetos de intervalo de tempo. Esses objetos são usados ao criar ACLs com base no tempo e regras de inspeção. Eles também são usados ao definir grupos de usuários do ASA para restringir o acesso VPN a horários específicos durante a semana.
42. **Exibir > Objetos > Fluxos de Tráfego**. Permite exibir objetos de fluxo de tráfego. Esses objetos definem fluxos de tráfego específicos para uso pelos dispositivos PIX 7.x/ASA 7.x.
43. **Exibir > Objetos > Listas de URL**. Permite exibir objetos de lista de URLs. Esses objetos definem os URLs exibidos na página do portal após um login bem-sucedido. Isso permite que os usuários acessem os recursos disponíveis em sites de VPN SSL ao operarem no modo de acesso sem cliente.
44. **Exibir > Objetos > Grupos de usuários**. Permite exibir objetos de grupo de usuários. Esses objetos definem grupos de clientes remotos usados em topologias Easy VPN, VPNs de acesso remoto e VPNs SSL.
45. **Exibir > Objetos > Listas de Servidores WINS**. Permite exibir objetos de lista de servidores WINS. Esses objetos representam servidores WINS, que são usados por VPN SSL para acessar ou compartilhar arquivos em sistemas remotos.
46. **Exibir > Objetos > Interno - Regras de DN**. Permite exibir as regras de DN usadas pelas políticas de DN. Este é um objeto interno usado pelo Gerenciador de segurança que não aparece no Gerenciador de objetos de política.
47. **Exibir > Objetos > Interno - Atualizações de Cliente**. Este é um objeto interno exigido por objetos de grupo de usuários que não aparecem no Gerenciador de Objetos de Política.
48. **View > Objects > Internal - Standard ACEs**. Este é um objeto interno para entradas de controle de acesso padrão, que são usadas por objetos de ACL.
49. **Exibir > Objetos > Interno - ACEs Estendidas.** Este é um objeto interno para entradas de controle de acesso estendido, que são usadas por objetos de ACL.

Permissões adicionais de visualização

O Gerenciador de segurança inclui as seguintes permissões de exibição adicionais:

1. **Exibir > Admin**. Permite visualizar as definições administrativas do Security Manager.
2. **Exibir > CLI**. Permite visualizar os comandos CLI configurados em um dispositivo e visualizar os comandos que estão prestes a ser implantados.
3. **Exibir > Arquivo de configuração**. Permite exibir a lista de configurações contidas no arquivo de configuração. Você não pode exibir a configuração do dispositivo ou qualquer comando CLI.
4. **Exibir > Dispositivos**. Permite exibir dispositivos na exibição Dispositivo e todas as informações relacionadas, incluindo configurações, propriedades, atribuições e assim por diante.
5. **Exibir > Gerenciador de dispositivos**. Permite iniciar versões somente leitura dos gerenciadores de dispositivos para dispositivos individuais, como o Cisco Router e o Security Device Manager (SDM) para roteadores Cisco IOS.

6. **Exibir > Topologia**. Permite exibir mapas configurados na exibição Mapa.

Modificar permissões

As permissões de modificação (leitura/gravação) no Gerenciador de segurança são divididas em categorias, conforme mostrado:

- Modificar permissões de políticas
- Modificar permissões de objetos
- Outras permissões de modificação

Modificar permissões de políticas

Nota: Ao especificar as permissões de modificação de política, certifique-se de ter selecionado as permissões de atribuição e exibição correspondentes também.

O Gerenciador de segurança inclui as seguintes permissões de modificação para políticas:

1. **Modificar > Políticas > Firewall**. Permite modificar políticas de serviço de firewall (localizadas no seletor de Política em Firewall) em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de serviço de firewall incluem regras de acesso, regras de AAA e regras de inspeção.
2. **Modificar > Políticas > Sistema de prevenção de intrusão**. Permite modificar as políticas de IPS (localizadas no seletor de política em IPS), incluindo políticas para IPS em execução em roteadores IOS. Essa permissão também permite que você ajuste assinaturas no assistente de Atualização de assinatura (localizado em Ferramentas > Aplicar atualização de IPS).
3. **Modificar > Políticas > Imagem**. Permite atribuir um pacote de atualização de assinatura a dispositivos no assistente Aplicar atualizações de IPS (localizado em Ferramentas > Aplicar atualização de IPS). Essa permissão também permite atribuir configurações de atualização automática a dispositivos específicos (localizados em Ferramentas > Administração do Gerenciador de Segurança > Atualizações de IPS).
4. **Modificar > Políticas > NAT**. Permite modificar as políticas de conversão de endereços de rede em dispositivos PIX/ASA/FWSM e roteadores IOS. Exemplos de políticas de NAT incluem regras estáticas e regras dinâmicas.
5. **Modificar > Políticas > VPN site a site**. Permite modificar políticas de VPN site a site em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de VPN site a site incluem propostas de IKE, propostas de IPsec e chaves pré-compartilhadas.
6. **Modificar > Políticas > VPN de acesso remoto**. Permite modificar políticas de VPN de acesso remoto em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de VPN de acesso remoto incluem propostas de IKE, propostas de IPsec e políticas de PKI.
7. **Modificar > Políticas > SSL VPN**. Permite modificar políticas de VPN SSL em dispositivos PIX/ASA/FWSM e roteadores IOS, como o assistente de VPN SSL.
8. **Modificar > Políticas > Interfaces**. Permite modificar políticas de interface (localizadas no seletor de política em Interfaces) em dispositivos PIX/ASA/FWSM, roteadores IOS, sensores IPS e dispositivos Catalyst 6500/7600:Em dispositivos PIX/ASA/FWSM, essa permissão abrange as portas de hardware e as configurações de interface.Nos roteadores IOS, essa

permissão abrange as configurações básicas e avançadas da interface, bem como outras políticas relacionadas à interface, como DSL, PVC, PPP e políticas de discador.Em sensores IPS, essa permissão abrange interfaces físicas e mapas de resumo.Nos dispositivos Catalyst 6500/7600, essa permissão abrange interfaces e configurações de VLAN.

9. **Modificar > Políticas > Bridging**. Permite modificar as políticas da tabela ARP (localizadas no seletor Política em Plataforma > Bridging) em dispositivos PIX/ASA/FWSM.
10. **Modificar > Políticas > Administração de dispositivo**. Permite modificar as políticas de administração de dispositivos (localizadas no seletor Política em Plataforma > Administrador de dispositivo) em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600:Em dispositivos PIX/ASA/FWSM, os exemplos incluem políticas de acesso a dispositivos, políticas de acesso a servidores e políticas de failover.Nos roteadores IOS, os exemplos incluem políticas de acesso ao dispositivo (incluindo acesso de linha), políticas de acesso ao servidor, AAA e Provisionamento de dispositivo seguro.Em sensores IPS, essa permissão abrange políticas de acesso a dispositivos e políticas de acesso a servidores.Nos dispositivos Catalyst 6500/7600, essa permissão abrange as configurações de IDSM e a lista de acesso de VLAN.
11. **Modificar > Políticas > Identidade**. Permite modificar políticas de identidade (localizadas no seletor de Política em Plataforma > Identidade) em roteadores Cisco IOS, incluindo políticas 802.1x e NAC (Network Admission Control).
12. **Modificar > Políticas > Registro**. Permite modificar as políticas de registro (localizadas no seletor de Política em Plataforma > Registro) em dispositivos PIX/ASA/FWSM, roteadores IOS e sensores IPS. Exemplos de políticas de registro incluem configuração de registro, configuração de servidor e políticas de servidor syslog.
13. **Modificar > Políticas > Multicast**. Permite modificar políticas multicast (localizadas no seletor de Política em Plataforma > Multicast) em dispositivos PIX/ASA/FWSM. Exemplos de políticas multicast incluem roteamento multicast e políticas IGMP.
14. **Modificar > Políticas > QoS**. Permite modificar as políticas de QoS (localizadas no seletor Política em Plataforma > Qualidade de Serviço) nos roteadores Cisco IOS.
15. **Modificar > Políticas > Roteamento**. Permite modificar as políticas de roteamento (localizadas no seletor Política em Plataforma > Roteamento) em dispositivos PIX/ASA/FWSM e roteadores IOS. Exemplos de políticas de roteamento incluem OSPF, RIP e políticas de roteamento estático.
16. **Modificar > Políticas > Segurança**. Permite modificar políticas de segurança (localizadas no seletor de Política em Plataforma > Segurança) em dispositivos PIX/ASA/FWSM e sensores IPS:Em dispositivos PIX/ASA/FWSM, as políticas de segurança incluem configurações de anti-falsificação, fragmento e tempo limite.Nos sensores IPS, as políticas de segurança incluem configurações de bloqueio.
17. **Modificar > Políticas > Regras de Política de Serviço**. Permite modificar políticas de regra de política de serviço (localizadas no seletor Política em Plataforma > Regras de Política de Serviço) em dispositivos PIX 7.x/ASA. Os exemplos incluem filas de prioridade e IPS, QoS e regras de conexão.
18. **Modificar > Políticas > Preferências do usuário**. Permite modificar a política de Implantação (localizada no seletor Política em Plataforma > Preferências do usuário) em dispositivos PIX/ASA/FWSM. Essa política contém uma opção para limpar todas as conversões de NAT na implantação.
19. **Modificar > Políticas > Dispositivo virtual**. Permite modificar políticas de sensor virtual em dispositivos IPS. Use essa política para criar sensores virtuais.

20. **Modificar > Políticas > FlexConfig**. Permite modificar FlexConfigs, que são comandos e instruções CLI adicionais que podem ser implantados em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600.

Modificar permissões de objetos

O Gerenciador de segurança inclui as seguintes permissões de exibição para objetos:

1. **Modificar > Objetos > Grupos de servidores AAA**. Permite exibir objetos de grupo de servidores AAA. Esses objetos são usados em políticas que exigem serviços AAA (autenticação, autorização e contabilização).
2. **Modificar > Objetos > Servidores AAA**. Permite exibir objetos do servidor AAA. Esses objetos representam servidores AAA individuais que são definidos como parte de um grupo de servidores AAA.
3. **Modificar > Objetos > Listas de Controle de Acesso - Padrão/Estendido**. Permite visualizar objetos de ACL padrão e estendida. Os objetos de ACL estendida são usados para uma variedade de políticas, como NAT e NAC, e para estabelecer acesso VPN. Os objetos de ACL padrão são usados para políticas como OSPF e SNMP, bem como para estabelecer acesso VPN.
4. **Modificar > Objetos > Listas de Controle de Acesso - Web**. Permite exibir objetos da ACL da Web. Os objetos da ACL da Web são usados para executar a filtragem de conteúdo em políticas de VPN SSL.
5. **Modificar > Objetos > ASA** User Groups. Permite exibir objetos de grupo de usuários do ASA. Esses objetos são configurados em dispositivos de segurança ASA em configurações de VPN Easy, VPN de acesso remoto e VPN SSL.
6. **Modificar > Objetos > Categorias**. Permite exibir objetos de categoria. Esses objetos ajudam a identificar regras e objetos facilmente em tabelas de regras por meio do uso de cores.
7. **Modificar > Objetos > Credenciais**. Permite exibir objetos de credencial. Esses objetos são usados na configuração do Easy VPN durante a autenticação estendida IKE (Xauth).
8. **Modificar > Objetos > FlexConfigs**. Permite exibir objetos FlexConfig. Esses objetos, que contêm comandos de configuração com instruções adicionais de linguagem de script, podem ser usados para configurar comandos que não são suportados pela interface de usuário do Security Manager.
9. **Modificar > Objetos > Propostas IKE**. Permite exibir objetos de proposta IKE. Esses objetos contêm os parâmetros necessários para propostas de IKE em políticas de VPN de acesso remoto.
10. **Modificar > Objetos > Inspecionar - Mapas de Classe - DNS**. Permite exibir objetos de mapa de classe DNS. Esses objetos correspondem ao tráfego DNS com critérios específicos para que as ações possam ser executadas nesse tráfego.
11. **Modificar > Objetos > Inspecionar - Mapas de Classe - FTP**. Permite exibir objetos de mapa de classe FTP. Esses objetos correspondem ao tráfego FTP com critérios específicos para que as ações possam ser executadas nesse tráfego.
12. **Modificar > Objetos > Inspecionar - Mapas de Classe - HTTP**. Permite exibir objetos de mapa de classe HTTP. Esses objetos correspondem ao tráfego HTTP com critérios específicos para que as ações possam ser executadas nesse tráfego.
13. **Modificar > Objetos > Inspecionar - Mapas de Classe - IM**. Permite exibir objetos de mapa de classe IM. Esses objetos correspondem ao tráfego de IM com critérios específicos para que as ações possam ser executadas nesse tráfego.

14. **Modificar > Objetos > Inspecionar - Mapas de Classe - SIP**. Permite exibir objetos de mapa de classe SIP. Esses objetos correspondem ao tráfego SIP com critérios específicos para que as ações possam ser executadas nesse tráfego.
15. **Modificar > Objetos > Inspecionar - Mapas de política - DNS**. Permite exibir objetos de mapa de política DNS. Esses objetos são usados para criar mapas de inspeção para o tráfego DNS.
16. **Modificar > Objetos > Inspecionar - Mapas de Política - FTP**. Permite exibir objetos de mapa de políticas de FTP. Esses objetos são usados para criar mapas de inspeção para tráfego FTP.
17. **Modificar > Objetos > Inspecionar - Mapa de Política - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite exibir objetos de mapa de política HTTP criados para dispositivos ASA/PIX 7.x e roteadores IOS. Esses objetos são usados para criar mapas de inspeção para tráfego HTTP.
18. **Modificar > Objetos > Inspecionar - Mapa de Política - HTTP (ASA7.2/PIX7.2)**. Permite exibir objetos de mapa de política HTTP criados para dispositivos ASA 7.2/PIX 7.2. Esses objetos são usados para criar mapas de inspeção para tráfego HTTP.
19. **Modificar > Objetos > Inspecionar - Mapas de Política - IM (ASA7.2/PIX7.2)**. Permite exibir objetos de mapa de política de IM criados para dispositivos ASA 7.2/PIX 7.2. Esses objetos são usados para criar mapas de inspeção para tráfego IM.
20. **Modificar > Objetos > Inspecionar - Mapas de Política - IM (IOS)**. Permite exibir objetos de mapa de políticas de IM criados para dispositivos IOS. Esses objetos são usados para criar mapas de inspeção para tráfego IM.
21. **Modificar > Objetos > Inspecionar - Mapas de Política - SIP**. Permite exibir objetos do mapa de políticas SIP. Esses objetos são usados para criar mapas de inspeção para o tráfego SIP.
22. **Modificar > Objetos > Inspecionar - Expressões Regulares**. Permite exibir objetos de expressão regular. Esses objetos representam expressões regulares individuais que são definidas como parte de um grupo de expressões regulares.
23. **Modificar > Objetos > Inspecionar - Grupos De Expressões Regulares**. Permite exibir objetos de grupo de expressões regulares. Esses objetos são usados por certos mapas de classe e inspecionam mapas para corresponder texto dentro de um pacote.
24. **Modificar > Objetos > Inspecionar - Mapas TCP**. Permite exibir objetos de mapa TCP. Esses objetos personalizam a inspeção no fluxo TCP em ambas as direções.
25. **Modificar > Objetos > Funções de Interface**. Permite exibir objetos de função de interface. Esses objetos definem padrões de nomenclatura que podem representar várias interfaces em diferentes tipos de dispositivos. As funções de interface permitem que você aplique políticas a interfaces específicas em vários dispositivos sem precisar definir manualmente o nome de cada interface.
26. **Modificar > Objetos > Conjuntos de Transformação IPsec**. Permite exibir objetos do conjunto de transformações IPsec. Esses objetos compreendem uma combinação de protocolos de segurança, algoritmos e outras configurações que especificam exatamente como os dados no túnel IPsec serão criptografados e autenticados.
27. **Modificar > Objetos > Mapas de atributos LDAP**. Permite exibir objetos de mapa de atributos LDAP. Esses objetos são usados para mapear nomes de atributos personalizados (definidos pelo usuário) para nomes de atributos do Cisco LDAP.
28. **Modificar > Objetos > Redes/Hosts**. Permite exibir objetos de rede/host. Esses objetos são coleções lógicas de endereços IP que representam redes, hosts ou ambos. Os objetos de rede/host permitem definir políticas sem especificar cada rede ou host individualmente.

29. **Modificar > Objetos > Inscrições PKI**. Permite exibir objetos de inscrição PKI. Esses objetos definem os servidores da Autoridade de Certificação (CA) que operam em uma infraestrutura de chave pública.
30. **Modificar > Objetos > Listas de encaminhamento de portas**. Permite exibir objetos da lista de encaminhamento de portas. Esses objetos definem os mapeamentos de números de porta em um cliente remoto para o endereço IP e a porta do aplicativo atrás de um gateway de VPN SSL.
31. **Modificar > Objetos > Configurações Seguras de Desktop**. Permite exibir objetos de configuração de área de trabalho seguros. Esses objetos são reutilizáveis, componentes nomeados que podem ser referenciados pelas políticas de VPN SSL para fornecer um meio confiável de eliminar todos os rastreamentos de dados confidenciais compartilhados durante uma sessão de VPN SSL.
32. **Modificar > Objetos > Serviços - Listas de Portas**. Permite exibir objetos de lista de portas. Esses objetos, que contêm um ou mais intervalos de números de porta, são usados para simplificar o processo de criação de objetos de serviço.
33. **Modificar > Objetos > Serviços/Grupos de Serviços.** Permite exibir objetos de grupo de serviços e serviços. Esses objetos são mapeamentos definidos de definições de protocolo e porta que descrevem os serviços de rede usados por políticas, como Kerberos, SSH e POP3.
34. **Modificar > Objetos > Servidores de Logon Único.** Permite exibir objetos de servidor de logon único. O SSO (Single Sign-On, login único) permite que os usuários de VPN SSL insiram um nome de usuário e uma senha uma vez e possam acessar vários serviços protegidos e servidores Web.
35. **Modificar > Objetos > Monitores SLA**. Permite exibir objetos do monitor SLA. Esses objetos são usados por dispositivos de segurança PIX/ASA que executam a versão 7.2 ou posterior para executar o rastreamento de rota. Esse recurso fornece um método para rastrear a disponibilidade de uma rota primária e instalar uma rota de backup se a rota primária falhar.
36. **Modificar > Objetos > Personalizações de VPN SSL**. Permite exibir objetos de personalização de VPN SSL. Esses objetos definem como alterar a aparência das páginas VPN SSL exibidas aos usuários, como Login/Logoff e páginas iniciais.
37. **Modificar > Objetos > Gateways VPN SSL**. Permite exibir objetos de gateway de VPN SSL. Esses objetos definem parâmetros que permitem que o gateway seja usado como proxy para conexões com os recursos protegidos em sua VPN SSL.
38. **Modificar > Objetos > Objetos de Estilo**. Permite exibir objetos de estilo. Esses objetos permitem configurar elementos de estilo, como características de fonte e cores, para personalizar a aparência da página VPN SSL que aparece para usuários de VPN SSL quando eles se conectam ao Security Appliance.
39. **Modificar > Objetos > Objetos de Texto**. Permite exibir objetos de texto em forma livre. Esses objetos compreendem um par de nome e valor, em que o valor pode ser uma única string, uma lista de strings ou uma tabela de strings.
40. **Modificar > Objetos > Intervalos de Tempo.** Permite exibir objetos de intervalo de tempo. Esses objetos são usados ao criar ACLs com base no tempo e regras de inspeção. Eles também são usados ao definir grupos de usuários do ASA para restringir o acesso VPN a horários específicos durante a semana.
41. **Modificar > Objetos > Fluxos de Tráfego**. Permite exibir objetos de fluxo de tráfego. Esses objetos definem fluxos de tráfego específicos para uso pelos dispositivos PIX 7.x/ASA 7.x.
42. **Modificar > Objetos > Listas de URL**. Permite exibir objetos de lista de URLs. Esses objetos definem os URLs exibidos na página do portal após um login bem-sucedido. Isso permite

que os usuários acessem os recursos disponíveis em sites de VPN SSL ao operarem no modo de acesso sem cliente.

43. **Modificar > Objetos > Grupos de usuários**. Permite exibir objetos de grupo de usuários. Esses objetos definem grupos de clientes remotos usados em topologias Easy VPN, VPNs de acesso remoto e VPN SSL
44. **Modificar > Objetos > Listas de Servidores WINS**. Permite exibir objetos de lista de servidores WINS. Esses objetos representam servidores WINS, que são usados por VPN SSL para acessar ou compartilhar arquivos em sistemas remotos.
45. **Modificar > Objetos > Interno - Regras de DN.** Permite exibir as regras de DN usadas pelas políticas de DN. Este é um objeto interno usado pelo Gerenciador de segurança que não aparece no Gerenciador de objetos de política.
46. **Modificar > Objetos > Interno - Atualizações de Cliente**. Este é um objeto interno exigido por objetos de grupo de usuários que não aparecem no Gerenciador de Objetos de Política.
47. **Modificar > Objetos > Interno - Padrão ACE**. Este é um objeto interno para entradas de controle de acesso padrão, que são usadas por objetos de ACL.
48. **Modificar > Objetos > Interno - ACE Estendida**. Este é um objeto interno para entradas de controle de acesso estendido, que são usadas por objetos de ACL.

Outras permissões de modificação

O Gerenciador de segurança inclui as permissões de modificação adicionais conforme mostrado:

1. **Modificar > Admin**. Permite modificar as definições administrativas do Security Manager.
2. **Modificar > Arquivo de configuração**. Permite modificar a configuração do dispositivo no Arquivo de configuração. Além disso, permite adicionar configurações ao arquivo e personalizar a ferramenta Arquivo de configuração.
3. **Modificar > Dispositivos**. Permite adicionar e excluir dispositivos, bem como modificar propriedades e atributos do dispositivo. Para descobrir as políticas no dispositivo que está sendo adicionado, você também deve habilitar a permissão Importar. Além disso, se você habilitar a permissão Modificar > Dispositivos, certifique-se de habilitar também a permissão Atribuir > Políticas > Interfaces.
4. **Modificar > Hierarquia**. Permite modificar grupos de dispositivos.
5. **Modificar > Topologia**. Permite modificar mapas na exibição Mapa.

Atribuir permissões

O Gerenciador de segurança inclui as permissões de atribuição de política conforme mostrado:

1. **Atribuir > Políticas > Firewall**. Permite atribuir políticas de serviço de firewall (localizadas no seletor de Política em Firewall) a dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de serviço de firewall incluem regras de acesso, regras de AAA e regras de inspeção.
2. **Atribuir > Políticas > Sistema de prevenção de intrusão**. Permite atribuir políticas de IPS (localizadas no seletor de política em IPS), incluindo políticas para IPS em execução em roteadores IOS.
3. **Atribuir > Políticas > Imagem**. Esta permissão não é usada no momento pelo Gerenciador de segurança.

4. **Atribuir > Políticas > NAT**. Permite atribuir políticas de conversão de endereços de rede a dispositivos PIX/ASA/FWSM e roteadores IOS. Exemplos de políticas de NAT incluem regras estáticas e regras dinâmicas.
5. **Atribuir > Políticas > VPN site a site**. Permite atribuir políticas de VPN site a site a dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de VPN site a site incluem propostas de IKE, propostas de IPsec e chaves pré-compartilhadas.
6. **Atribuir > Políticas > VPN de acesso remoto**. Permite atribuir políticas de VPN de acesso remoto a dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600. Exemplos de políticas de VPN de acesso remoto incluem propostas de IKE, propostas de IPsec e políticas de PKI.
7. **Atribuir > Políticas > SSL VPN**. Permite atribuir políticas de VPN SSL a dispositivos PIX/ASA/FWSM e roteadores IOS, como o assistente de VPN SSL.
8. **Atribuir > Políticas > Interfaces**. Permite atribuir políticas de interface (localizadas no seletor de Política em Interfaces) a dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600:Em dispositivos PIX/ASA/FWSM, essa permissão abrange as portas de hardware e as configurações de interface.Nos roteadores IOS, essa permissão abrange as configurações básicas e avançadas da interface, bem como outras políticas relacionadas à interface, como DSL, PVC, PPP e políticas de discador.Nos dispositivos Catalyst 6500/7600, essa permissão abrange interfaces e configurações de VLAN.
9. **Atribuir > Políticas > Bridging**. Permite atribuir políticas de tabela ARP (localizadas no seletor Política em Plataforma > Bridging) a dispositivos PIX/ASA/FWSM.
10. **Atribuir > Políticas > Administração de dispositivo**. Permite atribuir políticas de administração de dispositivos (localizadas no seletor Política em Plataforma > Administrador de dispositivo) a dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600:Em dispositivos PIX/ASA/FWSM, os exemplos incluem políticas de acesso a dispositivos, políticas de acesso a servidores e políticas de failover.Nos roteadores IOS, os exemplos incluem políticas de acesso ao dispositivo (incluindo acesso de linha), políticas de acesso ao servidor, AAA e Provisionamento de dispositivo seguro.Em sensores IPS, essa permissão abrange políticas de acesso a dispositivos e políticas de acesso a servidores.Nos dispositivos Catalyst 6500/7600, essa permissão abrange as configurações de IDSM e as listas de acesso de VLAN.
11. **Atribuir > Políticas > Identidade**. Permite atribuir políticas de identidade (localizadas no seletor de Política em Plataforma > Identidade) aos roteadores Cisco IOS, incluindo políticas 802.1x e NAC (Network Admission Control).
12. **Atribuir > Políticas > Registro**. Permite atribuir políticas de registro (localizadas no seletor de política em Plataforma > Registro) a dispositivos PIX/ASA/FWSM e roteadores IOS. Exemplos de políticas de registro incluem configuração de registro, configuração de servidor e políticas de servidor syslog.
13. **Atribuir > Políticas > Multicast**. Permite atribuir políticas multicast (localizadas no seletor de Política em Plataforma > Multicast) a dispositivos PIX/ASA/FWSM. Exemplos de políticas multicast incluem roteamento multicast e políticas IGMP.
14. **Atribuir > Políticas > QoS**. Permite atribuir políticas de QoS (localizadas no seletor Política em Plataforma > Qualidade de Serviço) aos roteadores Cisco IOS.
15. **Atribuir > Políticas > Roteamento**. Permite atribuir políticas de roteamento (localizadas no seletor Política em Plataforma > Roteamento) a dispositivos PIX/ASA/FWSM e roteadores IOS. Exemplos de políticas de roteamento incluem OSPF, RIP e políticas de roteamento estático.

16. **Atribuir > Políticas > Segurança**. Permite atribuir políticas de segurança (localizadas no seletor Política em Plataforma > Segurança) a dispositivos PIX/ASA/FWSM. As políticas de segurança incluem configurações de anti-falsificação, fragmento e tempo limite.
17. **Atribuir > Políticas > Regras de Política de Serviço**. Permite atribuir políticas de regra de política de serviço (localizadas no seletor Política em Plataforma > Regras de Política de Serviço) a dispositivos PIX 7.x/ASA. Os exemplos incluem filas de prioridade e IPS, QoS e regras de conexão.
18. **Atribuir > Políticas > Preferências do usuário**. Permite atribuir a política de implantação (localizada no seletor Política em Plataforma > Preferências do usuário) aos dispositivos PIX/ASA/FWSM. Essa política contém uma opção para limpar todas as conversões de NAT na implantação.
19. **Atribuir > Políticas > Dispositivo virtual**. Permite atribuir políticas de sensor virtual a dispositivos IPS. Use essa política para criar sensores virtuais.
20. **Atribuir > Políticas > FlexConfig**. Permite atribuir FlexConfigs, que são comandos e instruções CLI adicionais que podem ser implantados em dispositivos PIX/ASA/FWSM, roteadores IOS e dispositivos Catalyst 6500/7600.

Observação: ao especificar permissões de atribuição, certifique-se de que você também selecionou as permissões de exibição correspondentes.

Aprovar permissões

O Security Manager fornece as permissões de aprovação conforme mostrado:

1. **Aprovar > CLI**. Permite aprovar as alterações do comando CLI contidas em um trabalho de implantação.
2. **Aprovar > Política**. Permite aprovar as alterações de configuração contidas nas políticas que foram configuradas em uma atividade de fluxo de trabalho.

Entendendo as funções do CiscoWorks

Quando os usuários são criados no CiscoWorks Common Services, uma ou mais funções são atribuídas a eles. As permissões associadas a cada função determinam as operações que cada usuário está autorizado a executar no Gerenciador de segurança.

Os tópicos a seguir descrevem as funções do CiscoWorks:

- Funções padrão do CiscoWorks Common Services
- Atribuindo funções a usuários do CiscoWorks Common Services

Funções padrão do CiscoWorks Common Services

O CiscoWorks Common Services contém as seguintes funções padrão:

1. **Help Desk** — Os usuários do Help Desk podem exibir (mas não modificar) dispositivos, políticas, objetos e mapas de topologia.
2. **Operador de Rede** —Além de exibir permissões, os operadores de rede podem exibir comandos CLI e configurações administrativas do Security Manager. Os operadores de rede também podem modificar o arquivo de configuração e emitir comandos (como ping) para

dispositivos.

3. **Aprovador** — Além de exibir permissões, os aprovadores podem aprovar ou rejeitar trabalhos de implantação. Eles não podem executar a implantação.
4. **Administrador de rede** — Os administradores de rede têm permissões de visualização e modificação completas, exceto para modificar configurações administrativas. Eles podem descobrir dispositivos e as políticas configuradas nesses dispositivos, atribuir políticas a dispositivos e emitir comandos a dispositivos. Os administradores de rede não podem aprovar atividades ou trabalhos de implantação; no entanto, eles podem implantar trabalhos que foram aprovados por outros.
5. **Administrador do sistema** — Os administradores do sistema têm acesso completo a todas as permissões do Gerenciador de segurança, incluindo modificação, atribuição de política, aprovação de atividade e trabalho, descoberta, implantação e emissão de comandos para os dispositivos.

Observação: funções adicionais, como dados de exportação, podem ser exibidas em Common Services se aplicativos adicionais estiverem instalados no servidor. A função de exportação de dados é para desenvolvedores terceirizados e não é usada pelo Security Manager.

Dica: embora você não possa alterar a definição das funções do CiscoWorks, você pode definir quais funções são atribuídas a cada usuário. Para obter mais informações, consulte Atribuindo Funções a Usuários nos Serviços Comuns do CiscoWorks.

Atribuindo funções a usuários do CiscoWorks Common Services

O CiscoWorks Common Services permite definir quais funções são atribuídas a cada usuário. Ao alterar a definição de função de um usuário, você altera os tipos de operações que esse usuário está autorizado a executar no Gerenciador de segurança. Por exemplo, se você atribuir a função Help Desk, o usuário será limitado a exibir operações e não poderá modificar nenhum dado. No entanto, se você atribuir a função Operador de Rede, o usuário também poderá modificar o arquivo de configuração. Você pode atribuir várias funções a cada usuário.

Nota: Tem de reiniciar o Gestor de Segurança depois de efetuar alterações às permissões de utilizador.

Procedimento:

1. Em Common Services, selecione **Server > Security** e, em seguida, selecione **Single-Server Trust Management > Local User Setup** no TOC.**Dica:** para acessar a página Configuração de usuário local no Gerenciador de segurança, selecione Ferramentas > Administração do Gerenciador de segurança > Segurança do servidor e clique em Configuração de usuário local.
2. Marque a caixa de seleção ao lado de um usuário existente e clique em **Editar**.
3. Na página Informações do usuário, selecione as funções a serem atribuídas a esse usuário clicando nas caixas de seleção.Para obter mais informações sobre cada função, consulte Funções padrão do CiscoWorks Common Services.
4. Clique em **OK** para salvar suas alterações.
5. Reinicie o Gerenciador de segurança.

Entendendo as funções do Cisco Secure ACS

O Cisco Secure ACS oferece maior flexibilidade para gerenciar permissões do Security Manager do que o CiscoWorks, pois ele suporta funções específicas de aplicativos que você pode configurar. Cada função é composta por um conjunto de permissões que determinam o nível de autorização para tarefas do Gerenciador de Segurança. No Cisco Secure ACS, você atribui uma função a cada grupo de usuários (e, opcionalmente, a usuários individuais também), o que permite que cada usuário desse grupo execute as operações autorizadas pelas permissões definidas para essa função.

Além disso, você pode atribuir essas funções aos grupos de dispositivos Cisco Secure ACS, permitindo que as permissões sejam diferenciadas em diferentes conjuntos de dispositivos.

Observação: os grupos de dispositivos do Cisco Secure ACS são independentes dos grupos de dispositivos do Security Manager.

Os tópicos a seguir descrevem as funções do Cisco Secure ACS:

Funções padrão do Cisco Secure ACS

O Cisco Secure ACS inclui as mesmas funções do CiscoWorks (consulte Compreendendo as Funções do CiscoWorks), além destas funções adicionais:

1. **Aprovador de segurança** —Os aprovadores de segurança podem exibir (mas não modificar) dispositivos, políticas, objetos, mapas, comandos CLI e configurações administrativas. Além disso, os aprovadores de segurança podem aprovar ou rejeitar as alterações de configuração contidas em uma atividade. Eles não podem aprovar ou rejeitar o trabalho de implantação, nem podem executar a implantação.
2. **Administrador de segurança** —Além de ter permissões de exibição, os administradores de segurança podem modificar dispositivos, grupos de dispositivos, políticas, objetos e mapas de topologia. Eles também podem atribuir políticas a dispositivos e topologias de VPN e executar a descoberta para importar novos dispositivos para o sistema.
3. **Administrador de rede** —Além de exibir permissões, os administradores de rede podem modificar o arquivo de configuração, executar implantação e emitir comandos para os dispositivos.

Observação: as permissões contidas na função de administrador de rede do Cisco Secure ACS são diferentes das contidas na função de administrador de rede do CiscoWorks. Para obter mais informações, consulte Entendendo as funções do CiscoWorks.

Ao contrário do CiscoWorks, o Cisco Secure ACS permite personalizar as permissões associadas a cada função do Security Manager. Para obter mais informações sobre como modificar as funções padrão, consulte Personalizar funções do Cisco Secure ACS.

Observação: o Cisco Secure ACS 3.3 ou posterior deve ser instalado para autorização do Security Manager.

Personalizando as funções do Cisco Secure ACS

O Cisco Secure ACS permite que você modifique as permissões associadas a cada função do

Gerenciador de segurança. Você também pode personalizar o Cisco Secure ACS criando funções de usuário especializadas com permissões direcionadas a tarefas específicas do Security Manager.

Nota: Tem de reiniciar o Gestor de Segurança depois de efetuar alterações às permissões de utilizador.

Procedimento:

1. No Cisco Secure ACS, clique em **Shared Profile Components** na barra de navegação.
2. Clique em **Cisco Security Manager** na página Componentes compartilhados. As funções configuradas para o Gerenciador de segurança são exibidas.
3. Escolha fazer entre o seguinte:Para criar uma função, clique em **Adicionar**. Vá para a Etapa 4.Para modificar uma função existente, clique na função. Vá para a Etapa 5.
4. Insira um nome para a função e, opcionalmente, uma descrição.
5. Marque e desmarque as caixas de seleção na árvore de permissões para definir as permissões para essa funçãoMarcar a caixa de seleção de uma ramificação da árvore seleciona todas as permissões nessa ramificação. Por exemplo, selecionar **Atribuir** seleciona todas as permissões de atribuição.Para obter uma lista completa de permissões do Security Manager, consulte Permissões do Security Manager.**Nota:** Ao selecionar modificar, aprovar, atribuir, importar, controlar ou implantar permissões, você também deve selecionar as permissões de exibição correspondentes; caso contrário, o Security Manager não funcionará corretamente.
6. Clique em **Enviar** para salvar suas alterações.
7. Reinicie o Gerenciador de segurança.

Associações padrão entre permissões e funções no Gerenciador de segurança

Esta tabela mostra como as permissões do Security Manager são associadas às funções do CiscoWorks Common Services e às funções padrão no Cisco Secure ACS.

Permissões	Funções							
	System Admin	Administrador de segurança (ACS)	Aprovador de segurança (ACS)	Administrador de rede (CW)	Administrador de rede (ACS)	Aprovador	Operador de rede	Help desk
Exibir permissões								
Exibir dispositivo	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Exibir política	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Exibir objetos	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Exibir topologia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Exibir CLI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Exibir administrador	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Exibir arquivo de configuração	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Exibir gerentes de dispositivos	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Modificar permissões								
Modificar dispositivo	Yes	Yes	No	Yes	No	No	No	No
Modificar hierarquia	Yes	Yes	No	Yes	No	No	No	No
Modificar política	Yes	Yes	No	Yes	No	No	No	No
Modificar imagem	Yes	Yes	No	Yes	No	No	No	No
Modificar objetos	Yes	Yes	No	Yes	No	No	No	No
Modificar topologia	Yes	Yes	No	Yes	No	No	No	No
Modificar administrador	Yes	No	No	No	No	No	No	No
Modificar arquivo de configuração	Yes	Yes	No	Yes	Yes	No	Yes	No
Permissões adicionais								
Atribuir política	Yes	Yes	No	Yes	No	No	No	No
Aprovar política	Yes	No	Yes	No	No	No	No	No
Aprovar CLI	Yes	No	No	No	No	Yes	No	No
Descobrir (Importar)	Yes	Yes	No	Yes	No	No	No	No
Implantar	Ye	No	No	Ye	Ye	No	No	No

	s			s	s			
Controle	Yes	No	No	Yes	Yes	No	Yes	No
Enviar	Yes	Yes	No	Yes	No	No	No	No

Informações Relacionadas

- Página de suporte do Cisco Security Manager
- Suporte Técnico e Documentação - Cisco Systems