CSM 3.x: Einrichten von Benutzerberechtigungen und -rollen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Berechtigungen und Rollen für die Benutzer im Cisco Security Manager (CSM) einrichten.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass das CSM installiert ist und ordnungsgemäß funktioniert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CSM 3.1.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Einrichten von Benutzerberechtigungen

Cisco Security Manager authentifiziert Ihren Benutzernamen und Ihr Kennwort, bevor Sie sich anmelden können. Nachdem sie authentifiziert wurden, legt der Security Manager Ihre Rolle innerhalb der Anwendung fest. Diese Rolle definiert Ihre Berechtigungen (auch als Berechtigungen bezeichnet), d. h. die Aufgaben oder Operationen, die Sie ausführen dürfen. Wenn Sie nicht für bestimmte Aufgaben oder Geräte autorisiert sind, werden die zugehörigen Menüelemente, TOC-Elemente und Schaltflächen ausgeblendet oder deaktiviert. Außerdem wird Ihnen eine Meldung angezeigt, dass Sie nicht über die Berechtigung zum Anzeigen der ausgewählten Informationen oder zum Ausführen der ausgewählten Operation verfügen.

Die Authentifizierung und Autorisierung für Security Manager erfolgt entweder über den CiscoWorks-Server oder den Cisco Secure Access Control Server (ACS). Standardmäßig verwaltet CiscoWorks Authentifizierung und Autorisierung. Sie können jedoch über die Seite "AAA Mode Setup" (AAA-Modus-Einrichtung) in CiscoWorks Common Services auf Cisco Secure ACS wechseln.

Die Hauptvorteile von Cisco Secure ACS sind die Möglichkeit, äußerst detaillierte Benutzerrollen mit speziellen Berechtigungssätzen zu erstellen (z. B. sodass der Benutzer bestimmte Richtlinientypen konfigurieren kann, andere jedoch nicht) und die Möglichkeit, Benutzer durch die Konfiguration von Netzwerkgerätegruppen (NDGs) auf bestimmte Geräte zu beschränken.

In den folgenden Themen werden Benutzerberechtigungen beschrieben:

- Sicherheitsmanager-Berechtigungen
- CiscoWorks-Rollen im Überblick
- Cisco Secure ACS-Rollen im Überblick
- Standardzuordnungen zwischen Berechtigungen und Rollen im Security Manager

Sicherheitsmanager-Berechtigungen

Der Security Manager klassifiziert Berechtigungen in die folgenden Kategorien:

1. **View** (**Ansicht**): Ermöglicht Ihnen, die aktuellen Einstellungen anzuzeigen. Weitere Informationen finden Sie unter Berechtigungen anzeigen.
2. **Modify** (**Ändern**) - Ermöglicht Ihnen, die aktuellen Einstellungen zu ändern. Weitere Informationen finden Sie unter Berechtigungen ändern.
3. **Zuweisen** - Ermöglicht die Zuweisung von Richtlinien zu Geräten und VPN-Topologien. Weitere Informationen finden Sie unter Berechtigungen zuweisen

4. **Genehmigen** - Ermöglicht die Genehmigung von Richtlinienänderungen und Bereitstellungsjobs. Weitere Informationen finden Sie unter Genehmigungen.
5. **Import** - Ermöglicht das Importieren der auf Geräten bereits bereitgestellten Konfigurationen in Security Manager.
6. **Deploy** (Bereitstellung): Ermöglicht die Bereitstellung von Konfigurationsänderungen für die Geräte im Netzwerk und das Zurücksetzen auf eine zuvor bereitgestellte Konfiguration.
7. **Control** - Ermöglicht Ihnen die Ausgabe von Befehlen an Geräte, z. B. Ping.
8. **Senden** - Ermöglicht Ihnen, Ihre Konfigurationsänderungen zur Genehmigung einzusenden.

- Wenn Sie Berechtigungen zum Ändern, Zuweisen, Genehmigen, Importieren, Steuern oder Bereitstellen auswählen, müssen Sie auch die entsprechenden Anzeigeberechtigungen auswählen. Andernfalls funktioniert der Security Manager nicht ordnungsgemäß.
- Wenn Sie Richtlinienberechtigungen ändern auswählen, müssen Sie auch die entsprechenden Berechtigungen zum Zuweisen und Anzeigen von Richtlinien auswählen.
- Wenn Sie eine Richtlinie zulassen, die Richtlinienobjekte als Teil ihrer Definition verwendet, müssen Sie diesen Objekttypen auch Anzeigeberechtigungen zuweisen. Wenn Sie beispielsweise die Berechtigung zum Ändern von Routingrichtlinien auswählen, müssen Sie auch die Berechtigungen zum Anzeigen von Netzwerkobjekten und Schnittstellenrollen auswählen. Dies sind die Objekttypen, die für Routingrichtlinien erforderlich sind.
- Dasselbe gilt, wenn ein Objekt zugelassen wird, das andere Objekte als Teil seiner Definition verwendet. Wenn Sie beispielsweise die Berechtigung zum Ändern von Benutzergruppen auswählen, müssen Sie auch die Berechtigungen zum Anzeigen von Netzwerkobjekten, ACL-Objekten und AAA-Servergruppen auswählen.

Berechtigungen anzeigen

Die Anzeigeberechtigungen (schreibgeschützt) in Security Manager sind wie gezeigt in die folgenden Kategorien unterteilt:

- Richtlinienberechtigungen anzeigen
- Objektberechtigungen anzeigen
- Zusätzliche Anzeigeberechtigungen

Richtlinienberechtigungen anzeigen

Der Security Manager umfasst die folgenden Anzeigeberechtigungen für Richtlinien:

1. **Ansicht > Richtlinien > Firewall.** Ermöglicht die Anzeige von Firewall-Service-Richtlinien (die sich in der Richtlinienauswahl unter Firewall befinden) auf PIX/ASA/FWSM-Geräten, IOS-Routern und Catalyst 6500/7600-Geräten. Beispiele für Firewall-Service-Richtlinien sind Zugriffsregeln, AAA-Regeln und Überprüfungsregeln.
2. **Zeigen Sie > Richtlinien > Intrusion Prevention System (Intrusion Prevention System) an.** Ermöglicht Ihnen die Anzeige von IPS-Richtlinien (im Richtlinienauswahl unter IPS), einschließlich Richtlinien für IPS, das auf IOS-Routern ausgeführt wird.
3. **Ansicht > Richtlinien > Bild.** Ermöglicht Ihnen die Auswahl eines Signatur-Aktualisierungspakets im Assistenten zum Anwenden von IPS-Updates (unter Extras > IPS-Update anwenden). Sie können das Paket jedoch nicht bestimmten Geräten zuweisen, es sei denn, Sie verfügen auch über die Berechtigung Ändern > Richtlinien > Bild.

4. **Anzeigen > Richtlinien > NAT**. Ermöglicht die Anzeige von Netzwerkadressenübersetzungsrichtlinien auf PIX/ASA/FWSM-Geräten und IOS-Routern. Beispiele für NAT-Richtlinien sind statische Regeln und dynamische Regeln.
5. **Ansicht > Richtlinien > Site-to-Site-VPN**. Ermöglicht die Anzeige von Site-to-Site-VPN-Richtlinien auf PIX/ASA/FWSM-Geräten, IOS-Routern und Catalyst 6500/7600-Geräten. Beispiele für Site-to-Site-VPN-Richtlinien sind IKE-Angebote, IPsec-Vorschläge und vorinstallierte Schlüssel.
6. **Ansicht > Richtlinien > VPN für Remote-Zugriff**. Ermöglicht die Anzeige von VPN-Richtlinien für den Remote-Zugriff auf PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte. Beispiele für VPN-Richtlinien für den Remote-Zugriff sind IKE-Vorschläge, IPsec-Vorschläge und PKI-Richtlinien.
7. **Ansicht > Richtlinien > SSL VPN**. Ermöglicht die Anzeige von SSL-VPN-Richtlinien auf PIX/ASA/FWSM-Geräten und IOS-Routern, z. B. dem SSL VPN-Assistenten.
8. **Anzeigen > Richtlinien > Schnittstellen**. Ermöglicht die Anzeige von Schnittstellenrichtlinien (die sich im Richtlinienauswahl unter Schnittstellen befindet) auf PIX/ASA/FWSM-Geräten, IOS-Routern, IPS-Sensoren und Catalyst 6500/7600-Geräten.Auf PIX/ASA/FWSM-Geräten umfasst diese Berechtigung Hardware-Ports und Schnittstelleneinstellungen.Bei IOS-Routern umfasst diese Berechtigung grundlegende und erweiterte Schnittstelleneinstellungen sowie andere schnittstellenbezogene Richtlinien, z. B. DSL-, PVC-, PPP- und Dialer-Richtlinien.Bei IPS-Sensoren umfasst diese Berechtigung physische Schnittstellen und Zusammenfassungszuordnungen.Auf Catalyst 6500/7600-Geräten umfasst diese Berechtigung Schnittstellen und VLAN-Einstellungen.
9. **Anzeigen > Richtlinien > Bridging**. Ermöglicht Ihnen die Anzeige von ARP-Tabellenrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Bridging befinden) auf PIX/ASA/FWSM-Geräten.
10. **Anzeigen > Richtlinien > Geräteverwaltung**. Ermöglicht die Anzeige von Gerätemanagement-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Device Admin befinden) für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte:Beispiele für PIX/ASA/FWSM-Geräte sind Zugriffsrichtlinien für Geräte, Serverzugriffsrichtlinien und Failover-Richtlinien.Bei IOS-Routern sind beispielsweise Richtlinien für den Gerätezugriff (einschließlich Leitungszugriff), Serverzugriffsrichtlinien, AAA und die sichere Gerätebereitstellung erforderlich.Auf IPS-Sensoren umfasst diese Berechtigung Zugriffsrichtlinien für Geräte und Serverzugriffsrichtlinien.Auf Catalyst 6500/7600-Geräten umfasst diese Berechtigung IDSM-Einstellungen und VLAN-Zugriffslisten.
11. **Anzeigen > Richtlinien > Identität**. Ermöglicht Ihnen die Anzeige von Identitätsrichtlinien (die sich im Richtlinienauswahl unter Plattform > Identität befinden) auf Cisco IOS-Routern, einschließlich 802.1x- und NAC-Richtlinien (Network Admission Control).
12. **Anzeigen > Richtlinien > Protokollierung**. Ermöglicht Ihnen die Anzeige von Protokollierungsrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Protokollierung befindet) für PIX/ASA/FWSM-Geräte, IOS-Router und IPS-Sensoren. Beispiele für Protokollierungsrichtlinien sind Protokollierungs-Setup, Server-Setup und Syslog-Serverrichtlinien.
13. **Anzeigen > Richtlinien > Multicast**. Ermöglicht die Anzeige von Multicast-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Multicast befinden) auf PIX/ASA/FWSM-Geräten. Beispiele für Multicast-Richtlinien sind Multicast-Routing und IGMP-Richtlinien.
14. **Anzeigen > Richtlinien > QoS**. Ermöglicht das Anzeigen von QoS-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Quality of Service (QoS-Richtlinien) auf Cisco IOS-

Routern befinden.

15. **Anzeigen > Richtlinien > Routing**. Ermöglicht die Anzeige von Routing-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Routing befinden) auf PIX/ASA/FWSM-Geräten und IOS-Routern. Beispiele für Routing-Richtlinien sind OSPF, RIP und statische Routing-Richtlinien.
16. **Anzeigen > Richtlinien > Sicherheit**. Ermöglicht die Anzeige von Sicherheitsrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Sicherheit befinden) auf PIX/ASA/FWSM-Geräten und IPS-Sensoren:Auf PIX/ASA/FWSM-Geräten beinhalten Sicherheitsrichtlinien Anti-Spoofing, Fragment und Timeout-Einstellungen.Auf IPS-Sensoren beinhalten Sicherheitsrichtlinien Blockierungseinstellungen.
17. **Anzeigen > Richtlinien > Regeln für Service-Richtlinien**. Ermöglicht das Anzeigen von Richtlinien für Service-Richtlinien (die sich in der Richtlinienauswahl unter Plattform > Service Policy Rules (Servicerichtlinienregeln) auf PIX 7.x-/ASA-Geräten befinden. Beispiele hierfür sind Prioritätswarteschlangen und IPS, QoS und Verbindungsregeln.
18. **Anzeigen > Richtlinien > Benutzervoreinstellungen**. Ermöglicht das Anzeigen der Bereitstellungsrichtlinie (die sich in der Richtlinienauswahl unter Plattform > Benutzereinstellungen befindet) auf PIX/ASA/FWSM-Geräten. Diese Richtlinie enthält eine Option zum Löschen aller NAT-Übersetzungen bei der Bereitstellung.
19. **Anzeigen > Richtlinien > Virtuelles Gerät**. Ermöglicht die Anzeige virtueller Sensorrichtlinien auf IPS-Geräten. Diese Richtlinie wird zur Erstellung virtueller Sensoren verwendet.
20. **Anzeigen > Richtlinien > FlexConfig**. Ermöglicht die Anzeige von FlexConfigs, bei denen es sich um zusätzliche CLI-Befehle und -Anweisungen handelt, die für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte bereitgestellt werden können.

Objektberechtigungen anzeigen

Der Security Manager umfasst die folgenden Ansichtsberechtigungen für Objekte:

1. **Ansicht > Objekte > AAA-Servergruppen**. Ermöglicht das Anzeigen von AAA-Servergruppenobjekten. Diese Objekte werden in Richtlinien verwendet, die AAA-Dienste (Authentifizierung, Autorisierung und Abrechnung) erfordern.
2. **Ansicht > Objekte > AAA-Server**. Ermöglicht die Anzeige von AAA-Serverobjekten. Diese Objekte stellen einzelne AAA-Server dar, die als Teil einer AAA-Servergruppe definiert sind.
3. **Ansicht > Objekte > Zugriffskontrolllisten - Standard/Erweitert**. Ermöglicht die Anzeige von Standard- und erweiterten ACL-Objekten. Erweiterte ACL-Objekte werden für eine Vielzahl von Richtlinien wie NAT und NAC sowie für die Einrichtung des VPN-Zugriffs verwendet. Standard-ACL-Objekte werden für Richtlinien wie OSPF und SNMP sowie für die Einrichtung des VPN-Zugriffs verwendet.
4. **Ansicht > Objekte > Zugriffskontrolllisten** - Web. Ermöglicht die Anzeige von Web-ACL-Objekten. Webbasierte ACL-Objekte werden zum Filtern von Inhalten in SSL VPN-Richtlinien verwendet.
5. **Anzeigen > Objekte > ASA-Benutzergruppen**. Ermöglicht Ihnen die Anzeige von ASA-Benutzergruppenobjekten. Diese Objekte werden auf ASA Security Appliances in Easy VPN-, Remote Access VPN- und SSL VPN-Konfigurationen konfiguriert.
6. **Ansicht > Objekte > Kategorien**. Ermöglicht das Anzeigen von Kategorieobjekten. Mit diesen Objekten können Sie Regeln und Objekte in Regeltabellen mithilfe von Farbe leicht identifizieren.
7. **Anzeigen > Objekte > Anmeldeinformationen**. Ermöglicht das Anzeigen von

Anmeldeinformationsobjekten. Diese Objekte werden in der Easy VPN-Konfiguration während der IKE Extended Authentication (Xauth) verwendet.

8. **Anzeigen > Objekte > FlexConfigs**. Ermöglicht die Anzeige von FlexConfig-Objekten. Diese Objekte, die Konfigurationsbefehle mit zusätzlichen Anweisungen zur Skriptsprache enthalten, können zum Konfigurieren von Befehlen verwendet werden, die von der Benutzeroberfläche des Sicherheitsmanagers nicht unterstützt werden.
9. **Ansicht > Objekte > IKE-Vorschläge**. Ermöglicht die Anzeige von IKE-Angebotsobjekten. Diese Objekte enthalten die Parameter, die für IKE-Vorschläge in VPN-Richtlinien für den Remote-Zugriff erforderlich sind.
10. **View > Objects > Inspect - Class Maps** - DNS Ermöglicht die Anzeige von Objekten für die DNS-Klassenzuordnung. Diese Objekte ordnen DNS-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr ausgeführt werden können.
11. **Ansicht > Objekte > Inspect - Class Maps - FTP**. Ermöglicht das Anzeigen von Objekten für die FTP-Klassenzuordnung. Diese Objekte ordnen FTP-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr ausgeführt werden können.
12. **Ansicht > Objekte > Inspect - Class Maps - HTTP**. Ermöglicht das Anzeigen von HTTP-Klassenzuordnungsobjekten. Diese Objekte ordnen HTTP-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr ausgeführt werden können.
13. **Ansicht > Objekte > Inspect - Class Maps - IM**. Ermöglicht die Anzeige von IM-Klassenzuordnungs-Objekten. Diese Objekte ordnen IM-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr durchgeführt werden können.
14. **Ansicht > Objekte > Inspect - Class Maps - SIP**. Ermöglicht das Anzeigen von SIP-Klassenzuordnungsobjekten. Diese Objekte ordnen SIP-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr durchgeführt werden können.
15. **View > Objects > Inspect - Policy Maps - DNS.** Ermöglicht die Anzeige von Objekten in der DNS-Richtlinienzuordnung. Diese Objekte werden zum Erstellen von Prüfzuordnungen für DNS-Datenverkehr verwendet.
16. **Ansicht > Objekte > Inspektion - Richtlinienzuordnungen - FTP.** Ermöglicht das Anzeigen von Objekten für die FTP-Richtlinienzuordnung. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für FTP-Datenverkehr verwendet.
17. **Ansicht > Objekte > Inspektion - Richtlinienzuordnungen - GTP**. Ermöglicht das Anzeigen von GTP-Richtlinienzuordnungsobjekten. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für den GTP-Datenverkehr verwendet.
18. **Ansicht > Objekte > Inspektion - Richtlinienzuordnungen - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Ermöglicht die Anzeige von HTTP-Richtlinienzuordnungsobjekten, die für ASA/PIX 7.1.x-Geräte und IOS-Router erstellt wurden. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für HTTP-Datenverkehr verwendet.
19. **Ansicht > Objekte > Inspektion - Richtlinienzuordnungen - HTTP (ASA7.2/PIX7.2)**. Ermöglicht die Anzeige von HTTP-Richtlinienzuordnungsobjekten, die für ASA 7.2-/PIX 7.2-Geräte erstellt wurden. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für HTTP-Datenverkehr verwendet.
20. **Ansicht > Objekte > Inspektion - Richtlinienzuordnungen - IM (ASA7.2/PIX7.2)**. Ermöglicht die Anzeige von IM-Richtlinienzuordnungsobjekten, die für ASA 7.2-/PIX 7.2-Geräte erstellt wurden. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für IM-Datenverkehr verwendet.
21. **Ansicht > Objekte > Inspektion - Richtlinienzuordnungen - IM (IOS)**. Ermöglicht die Anzeige von für IOS-Geräte erstellten IM-Richtlinienzuordnungsobjekten. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für IM-Datenverkehr verwendet.

22. Ansicht > Objekte > Inspektion - Richtlinienzuordnungen - SIP. Ermöglicht die Anzeige von SIP-Richtlinienzuordnungsobjekten. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für SIP-Datenverkehr verwendet.
23. Anzeigen > Objekte > Überprüfen - Reguläre Ausdrücke. Ermöglicht das Anzeigen von Objekten für reguläre Ausdrücke. Diese Objekte stellen einzelne reguläre Ausdrücke dar, die als Teil einer Gruppe regulärer Ausdrücke definiert sind.
24. Ansicht > Objekte > Inspektion - Gruppen für reguläre Ausdrücke. Ermöglicht das Anzeigen von Gruppenobjekten für reguläre Ausdrücke. Diese Objekte werden von bestimmten Klassenzuordnungen verwendet und überprüfen Zuordnungen, um Text innerhalb eines Pakets zuzuordnen.
25. Ansicht > Objekte > Inspektion - TCP-Karten. Ermöglicht Ihnen, TCP-Zuordnungsobjekte anzuzeigen. Diese Objekte passen die Überprüfung des TCP-Datenflusses in beide Richtungen an.
26. Ansicht > Objekte > Schnittstellenrollen. Ermöglicht das Anzeigen von Objekten für Schnittstellenrollen. Diese Objekte definieren Benennungsmuster, die mehrere Schnittstellen auf verschiedenen Gerätetypen darstellen können. Mit Schnittstellenrollen können Sie Richtlinien auf bestimmte Schnittstellen auf mehreren Geräten anwenden, ohne den Namen der einzelnen Schnittstellen manuell definieren zu müssen.
27. View > Objects > IPsec Transform Sets. Ermöglicht die Anzeige von IPsec-Transformationssatz-Objekten. Diese Objekte umfassen eine Kombination aus Sicherheitsprotokollen, Algorithmen und anderen Einstellungen, die genau festlegen, wie die Daten im IPsec-Tunnel verschlüsselt und authentifiziert werden.
28. Ansicht > Objekte > LDAP-Attributzuordnungen. Ermöglicht die Anzeige von LDAP-Attributzuordnungs-Objekten. Diese Objekte werden verwendet, um benutzerdefinierten (benutzerdefinierten) Attributnamen Cisco LDAP-Attributnamen zuzuordnen.
29. Ansicht > Objekte > Netzwerke/Hosts. Ermöglicht die Anzeige von Netzwerk-/Hostobjekten. Diese Objekte sind logische Sammlungen von IP-Adressen, die Netzwerke, Hosts oder beide darstellen. Mit Netzwerk-/Hostobjekten können Sie Richtlinien definieren, ohne jedes Netzwerk oder jeden Host einzeln anzugeben.
30. Anzeigen > Objekte > PKI-Anmeldungen. Ermöglicht die Anzeige von PKI-Anmeldungsobjekten. Diese Objekte definieren die CA-Server (Certification Authority), die in einer Public Key-Infrastruktur arbeiten.
31. Ansicht > Objekte > Portweiterleitungslisten. Ermöglicht Ihnen die Anzeige von Objekten in der Portweiterleitungsliste. Diese Objekte definieren die Zuordnungen von Portnummern eines Remote-Clients zur IP-Adresse und zum Port der Anwendung hinter einem SSL VPN-Gateway.
32. Anzeigen > Objekte > Sichere Desktop-Konfigurationen. Ermöglicht die Anzeige sicherer Desktopkonfigurationsobjekte. Diese Objekte sind wiederverwendbare, benannte Komponenten, auf die durch SSL VPN-Richtlinien verwiesen werden kann, um alle Spuren von vertraulichen Daten zu löschen, die während der Dauer einer SSL VPN-Sitzung gemeinsam genutzt werden.
33. Ansicht > Objekte > Dienste - Portlisten. Ermöglicht die Anzeige von Portlistenobjekten. Diese Objekte, die einen oder mehrere Bereiche von Portnummern enthalten, werden verwendet, um den Prozess der Erstellung von Dienstobjekten zu rationalisieren.
34. Ansicht > Objekte > Dienste/Servicegruppen Zum Anzeigen von Service- und Servicegruppenobjekten. Diese Objekte sind definierte Zuordnungen von Protokoll- und Portdefinitionen, die die von Richtlinien verwendeten Netzwerkdienste beschreiben, z. B. Kerberos, SSH und POP3.

35. **Ansicht > Objekte > Server mit einmaliger Anmeldung**. Ermöglicht die Anzeige einzelner Serverobjekte, die sich auf einem Server befinden. Mit Single Sign-On (SSO) können SSL VPN-Benutzer einen Benutzernamen und ein Kennwort einmal eingeben und auf mehrere geschützte Dienste und Webserver zugreifen.
36. **Ansicht > Objekte > SLA-Monitore**. Ermöglicht die Anzeige von SLA-Monitorobjekten. Diese Objekte werden von PIX/ASA Security Appliances verwendet, die Version 7.2 oder höher ausführen, um die Routenverfolgung durchzuführen. Diese Funktion bietet eine Methode, um die Verfügbarkeit einer primären Route zu verfolgen und eine Backup-Route zu installieren, falls die primäre Route fehlschlägt.
37. **Ansicht > Objekte > SSL VPN-Anpassungen**. Ermöglicht die Anzeige von Objekten zur SSL VPN-Anpassung. Diese Objekte definieren, wie die Darstellung von SSL-VPN-Seiten, die Benutzern angezeigt werden, geändert wird, z. B. Anmelden/Abmelden und Startseiten.
38. **Ansicht > Objekte > SSL VPN-Gateways**. Ermöglicht die Anzeige von SSL VPN-Gateway-Objekten. Diese Objekte definieren Parameter, mit denen das Gateway als Proxy für Verbindungen zu den geschützten Ressourcen im SSL VPN verwendet werden kann.
39. **Ansicht > Objekte > Formatobjekte**. Ermöglicht das Anzeigen von Formatobjekten. Mit diesen Objekten können Sie Stilelemente wie Schriftartmerkmale und -farben konfigurieren, um die Darstellung der SSL VPN-Seite anzupassen, die SSL VPN-Benutzern bei der Verbindung mit der Sicherheitsappliance angezeigt wird.
40. **Ansicht > Objekte > Textobjekte**. Ermöglicht das Anzeigen von frei formatierten Textobjekten. Diese Objekte umfassen ein Name-Wert-Paar, wobei der Wert eine einzelne Zeichenfolge, eine Liste von Zeichenfolgen oder eine Tabelle von Zeichenfolgen sein kann.
41. **Ansicht > Objekte > Zeitbereiche.** Ermöglicht das Anzeigen von Objekten im Zeitbereich. Diese Objekte werden bei der Erstellung zeitbasierter ACLs und Prüfungsregeln verwendet. Sie werden auch bei der Definition von ASA-Benutzergruppen verwendet, um den VPN-Zugriff auf bestimmte Zeiten während der Woche zu beschränken.
42. **Ansicht > Objekte > Datenverkehrsflüsse**. Ermöglicht die Anzeige von Datenverkehrsflussobjekten. Diese Objekte definieren spezifische Datenverkehrsflüsse für PIX 7.x-/ASA 7.x-Geräte.
43. **Ansicht > Objekte > URL-Listen**. Ermöglicht die Anzeige von URL-Listenobjekten. Diese Objekte definieren die URLs, die nach erfolgreicher Anmeldung auf der Portalseite angezeigt werden. Dadurch können Benutzer auf die auf SSL VPN-Websites verfügbaren Ressourcen zugreifen, wenn sie im Clientless-Zugriffsmodus betrieben werden.
44. **Anzeigen > Objekte > Benutzergruppen**. Ermöglicht das Anzeigen von Benutzergruppenobjekten. Diese Objekte definieren Gruppen von Remote-Clients, die in Easy VPN-Topologien, Remote-Access-VPNs und SSL-VPNs verwendet werden.
45. **Ansicht > Objekte > WINS-Serverlisten**. Ermöglicht das Anzeigen von WINS-Serverlistenobjekten. Diese Objekte stellen WINS-Server dar, die von SSL VPN für den Zugriff auf Dateien oder die gemeinsame Nutzung von Dateien auf Remote-Systemen verwendet werden.
46. **Anzeigen > Objekte > Intern - DN-Regeln**. Ermöglicht die Anzeige der DN-Regeln, die von DN-Richtlinien verwendet werden. Dies ist ein internes Objekt, das vom Security Manager verwendet wird und nicht im Policy Object Manager angezeigt wird.
47. **Ansicht > Objekte > Intern - Client-Updates**. Dies ist ein internes Objekt, das von Benutzergruppenobjekten benötigt wird und nicht im Policy Object Manager angezeigt wird.
48. **Ansicht > Objekte > Intern - Standard-ACEs**. Dies ist ein internes Objekt für Standardeinträge zur Zugriffskontrolle, die von ACL-Objekten verwendet werden.
49. **View > Objects > Internal - Extended ACEs.** Dies ist ein internes Objekt für Einträge der

erweiterten Zugriffskontrolle, die von ACL-Objekten verwendet werden.

Zusätzliche Anzeigeberechtigungen

Security Manager umfasst die folgenden zusätzlichen Ansichtsberechtigungen:

1. **Ansicht > Verwaltung**. Ermöglicht das Anzeigen von Verwaltungseinstellungen für den Sicherheitsmanager.
2. **Ansicht > CLI**. Hier können Sie die auf einem Gerät konfigurierten CLI-Befehle anzeigen und eine Vorschau der Befehle anzeigen, die in Kürze bereitgestellt werden sollen.
3. **Ansicht > Konfigurationsarchiv**. Ermöglicht das Anzeigen der Konfigurationsliste im Konfigurationsarchiv. Sie können die Gerätekonfiguration oder CLI-Befehle nicht anzeigen.
4. **Anzeigen > Geräte**. Ermöglicht die Anzeige von Geräten in der Geräteansicht und aller zugehörigen Informationen, einschließlich der Geräteeinstellungen, Eigenschaften, Zuweisungen usw.
5. **Ansicht > Gerätemanager**. Ermöglicht das Starten von schreibgeschützten Versionen der Gerätemanager für einzelne Geräte, z. B. den Cisco Router und Security Device Manager (SDM) für Cisco IOS-Router.
6. **Ansicht > Topologie**. Ermöglicht die Anzeige von Karten, die in der Ansicht Karte konfiguriert sind.

Berechtigungen ändern

Die Berechtigungen zum Ändern (Lese-/Schreibzugriff) in Security Manager werden wie gezeigt in die folgenden Kategorien unterteilt:

- Ändern von Richtlinienberechtigungen
- Ändern von Objektberechtigungen
- Zusätzliche Berechtigungen ändern

Ändern von Richtlinienberechtigungen

Hinweis: Wenn Sie Richtlinienberechtigungen ändern möchten, stellen Sie sicher, dass Sie auch die entsprechenden Berechtigungen zum Zuweisen und Anzeigen von Richtlinien ausgewählt haben.

Security Manager umfasst die folgenden Änderungsberechtigungen für Richtlinien:

1. **Ändern > Richtlinien > Firewall**. Ermöglicht das Ändern von Firewall-Service-Richtlinien (die sich in der Richtlinienauswahl unter Firewall befinden) für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte. Beispiele für Firewall-Service-Richtlinien sind Zugriffsregeln, AAA-Regeln und Überprüfungsregeln.
2. **Ändern > Policies > Intrusion Prevention System (Richtlinien > Intrusion Prevention System)**. Ermöglicht das Ändern von IPS-Richtlinien (die sich im Richtlinienauswahl unter IPS befinden), einschließlich Richtlinien für IPS, das auf IOS-Routern ausgeführt wird. Mit dieser Berechtigung können Sie auch Signaturen im Signature Update-Assistenten abstimmen (unter Extras > IPS-Update anwenden).
3. **Ändern > Richtlinien > Bild**. Ermöglicht Ihnen, Geräten im Assistenten zum Anwenden von

IPS-Updates ein Signatur-Update-Paket zuzuweisen (unter Extras > IPS-Update anwenden). Mit dieser Berechtigung können Sie außerdem bestimmten Geräten Auto-Update-Einstellungen zuweisen (unter Extras > Security Manager Administration > IPS Updates).

4. **Ändern > Richtlinien > NAT**. Ermöglicht die Änderung der Richtlinien für die Netzwerkadressenübersetzung auf PIX/ASA/FWSM-Geräten und IOS-Routern. Beispiele für NAT-Richtlinien sind statische Regeln und dynamische Regeln.
5. **Ändern > Richtlinien > Site-to-Site-VPN**. Ermöglicht die Änderung von Site-to-Site-VPN-Richtlinien für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte. Beispiele für Site-to-Site-VPN-Richtlinien sind IKE-Angebote, IPsec-Vorschläge und vorinstallierte Schlüssel.
6. **Ändern > Richtlinien > Remotezugriffs-VPN**. Ermöglicht die Änderung von VPN-Richtlinien für Remote-Zugriff auf PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte. Beispiele für VPN-Richtlinien für den Remote-Zugriff sind IKE-Vorschläge, IPsec-Vorschläge und PKI-Richtlinien.
7. **Ändern > Richtlinien > SSL VPN**. Ermöglicht die Änderung von SSL VPN-Richtlinien auf PIX/ASA/FWSM-Geräten und IOS-Routern, z. B. dem SSL VPN-Assistenten.
8. **Ändern > Richtlinien > Schnittstellen**. Ermöglicht das Ändern von Schnittstellenrichtlinien (die sich im Richtlinienauswahl unter Schnittstellen befindet) für PIX/ASA/FWSM-Geräte, IOS-Router, IPS-Sensoren und Catalyst 6500/7600-Geräte:Auf PIX/ASA/FWSM-Geräten umfasst diese Berechtigung Hardware-Ports und Schnittstelleneinstellungen.Bei IOS-Routern umfasst diese Berechtigung grundlegende und erweiterte Schnittstelleneinstellungen sowie andere schnittstellenbezogene Richtlinien, z. B. DSL-, PVC-, PPP- und Dialer-Richtlinien.Bei IPS-Sensoren umfasst diese Berechtigung physische Schnittstellen und Zusammenfassungszuordnungen.Auf Catalyst 6500/7600-Geräten umfasst diese Berechtigung Schnittstellen und VLAN-Einstellungen.
9. **Ändern > Richtlinien > Bridging**. Ermöglicht das Ändern von ARP-Tabellenrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Bridging befinden) auf PIX/ASA/FWSM-Geräten.
10. **Ändern > Richtlinien > Geräteverwaltung**. Ermöglicht das Ändern von Geräteverwaltungsrichtlinien (die sich im Richtlinienauswahl unter Plattform > Geräteadministrator befinden) für PIX-/ASA-/FWSM-Geräte, IOS-Router und Catalyst 6500-/7600-Geräte:Beispiele für PIX/ASA/FWSM-Geräte sind Zugriffsrichtlinien für Geräte, Serverzugriffsrichtlinien und Failover-Richtlinien.Bei IOS-Routern sind beispielsweise Richtlinien für den Gerätezugriff (einschließlich Leitungszugriff), Serverzugriffsrichtlinien, AAA und die sichere Gerätebereitstellung erforderlich.Auf IPS-Sensoren umfasst diese Berechtigung Zugriffsrichtlinien für Geräte und Serverzugriffsrichtlinien.Auf Catalyst 6500/7600-Geräten umfasst diese Berechtigung die IDSM-Einstellungen und die VLAN-Zugriffsliste.
11. **Ändern > Richtlinien > Identität**. Ermöglicht das Ändern von Identitätsrichtlinien (die sich im Richtlinienauswahl unter Plattform > Identität befindet) auf Cisco IOS-Routern, einschließlich 802.1x- und NAC-Richtlinien (Network Admission Control).
12. **Ändern > Richtlinien > Protokollierung**. Ermöglicht das Ändern von Protokollierungsrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Protokollierung befindet) für PIX/ASA/FWSM-Geräte, IOS-Router und IPS-Sensoren. Beispiele für Protokollierungsrichtlinien sind Protokollierungs-Setup, Server-Setup und Syslog-Serverrichtlinien.
13. **Ändern > Richtlinien > Multicast**. Ermöglicht das Ändern von Multicast-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Multicast befinden) für PIX/ASA/FWSM-Geräte. Beispiele für Multicast-Richtlinien sind Multicast-Routing und IGMP-Richtlinien.

14. **Ändern > Richtlinien > QoS**. Ermöglicht das Ändern von QoS-Richtlinien (die sich in der Richtlinienauswahl unter Plattform > Quality of Service (QoS-Richtlinien) auf Cisco IOS-Routern befinden.
15. **Ändern > Richtlinien > Routing**. Ermöglicht das Ändern von Routing-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Routing befinden) für PIX-/ASA-/FWSM-Geräte und IOS-Router. Beispiele für Routing-Richtlinien sind OSPF, RIP und statische Routing-Richtlinien.
16. **Ändern > Richtlinien > Sicherheit**. Ermöglicht das Ändern von Sicherheitsrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Sicherheit befinden) für PIX-/ASA-/FWSM-Geräte und IPS-Sensoren:Auf PIX/ASA/FWSM-Geräten beinhalten Sicherheitsrichtlinien Anti-Spoofing, Fragment und Timeout-Einstellungen.Auf IPS-Sensoren beinhalten Sicherheitsrichtlinien Blockierungseinstellungen.
17. **Ändern > Richtlinien > Regeln für Service-Richtlinien**. Ermöglicht das Ändern von Richtlinien für Service-Richtlinien (die sich in der Richtlinienauswahl unter Plattform > Service Policy Rules (Servicerichtlinienregeln) auf PIX 7.x-/ASA-Geräten befinden. Beispiele hierfür sind Prioritätswarteschlangen und IPS, QoS und Verbindungsregeln.
18. **Ändern > Richtlinien > Benutzervoreinstellungen**. Ermöglicht das Ändern der Bereitstellungsrichtlinie (die sich in der Richtlinienauswahl unter Plattform > Benutzereinstellungen befindet) für PIX/ASA/FWSM-Geräte. Diese Richtlinie enthält eine Option zum Löschen aller NAT-Übersetzungen bei der Bereitstellung.
19. **Ändern > Richtlinien > Virtuelles Gerät**. Ermöglicht Ihnen die Änderung von Richtlinien für virtuelle Sensoren auf IPS-Geräten. Verwenden Sie diese Richtlinie, um virtuelle Sensoren zu erstellen.
20. **Ändern > Richtlinien > FlexConfig**. Ermöglicht die Änderung von FlexConfigs, d. h. zusätzlichen CLI-Befehlen und Anweisungen, die für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte bereitgestellt werden können.

Ändern von Objektberechtigungen

Der Security Manager umfasst die folgenden Ansichtsberechtigungen für Objekte:

1. **Ändern > Objekte > AAA-Servergruppen**. Ermöglicht das Anzeigen von AAA-Servergruppenobjekten. Diese Objekte werden in Richtlinien verwendet, die AAA-Dienste (Authentifizierung, Autorisierung und Abrechnung) erfordern.
2. **Ändern > Objekte > AAA-Server**. Ermöglicht die Anzeige von AAA-Serverobjekten. Diese Objekte stellen einzelne AAA-Server dar, die als Teil einer AAA-Servergruppe definiert sind.
3. **Ändern > Objekte > Zugriffskontrolllisten - Standard/Extended**. Ermöglicht die Anzeige von Standard- und erweiterten ACL-Objekten. Erweiterte ACL-Objekte werden für eine Vielzahl von Richtlinien wie NAT und NAC sowie für die Einrichtung des VPN-Zugriffs verwendet. Standard-ACL-Objekte werden für Richtlinien wie OSPF und SNMP sowie für die Einrichtung des VPN-Zugriffs verwendet.
4. **Ändern > Objekte > Zugriffskontrolllisten - Web**. Ermöglicht die Anzeige von Web-ACL-Objekten. Webbasierte ACL-Objekte werden zum Filtern von Inhalten in SSL VPN-Richtlinien verwendet.
5. **Ändern > Objekte > ASA-**Benutzergruppen. Ermöglicht Ihnen die Anzeige von ASA-Benutzergruppenobjekten. Diese Objekte werden auf ASA Security Appliances in Easy VPN-, Remote Access VPN- und SSL VPN-Konfigurationen konfiguriert.
6. **Ändern > Objekte > Kategorien**. Ermöglicht das Anzeigen von Kategorieobjekten. Mit diesen

Objekten können Sie Regeln und Objekte in Regeltabellen mithilfe von Farbe leicht identifizieren.

7. **Ändern > Objekte > Anmeldeinformationen**. Ermöglicht das Anzeigen von Anmeldeinformationsobjekten. Diese Objekte werden in der Easy VPN-Konfiguration während der IKE Extended Authentication (Xauth) verwendet.
8. **Ändern > Objekte > FlexConfigs**. Ermöglicht die Anzeige von FlexConfig-Objekten. Diese Objekte, die Konfigurationsbefehle mit zusätzlichen Anweisungen zur Skriptsprache enthalten, können zum Konfigurieren von Befehlen verwendet werden, die von der Benutzeroberfläche des Sicherheitsmanagers nicht unterstützt werden.
9. **Ändern > Objekte > IKE-Angebote**. Ermöglicht die Anzeige von IKE-Angebotsobjekten. Diese Objekte enthalten die Parameter, die für IKE-Vorschläge in VPN-Richtlinien für den Remote-Zugriff erforderlich sind.
10. **Ändern > Objekte > Inspect - Class Maps - DNS**. Ermöglicht die Anzeige von Objekten für die DNS-Klassenzuordnung. Diese Objekte ordnen DNS-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr ausgeführt werden können.
11. **Ändern > Objekte > Inspect - Class Maps - FTP**. Ermöglicht das Anzeigen von Objekten für die FTP-Klassenzuordnung. Diese Objekte ordnen FTP-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr ausgeführt werden können.
12. **Ändern > Objekte > Inspect - Class Maps - HTTP**. Ermöglicht das Anzeigen von HTTP-Klassenzuordnungsobjekten. Diese Objekte ordnen HTTP-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr ausgeführt werden können.
13. **Ändern > Objekte > Inspect - Class Maps - IM**. Ermöglicht die Anzeige von IM-Klassenzuordnungs-Objekten. Diese Objekte ordnen IM-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr durchgeführt werden können.
14. **Ändern > Objekte > Inspect - Class Maps - SIP**. Ermöglicht das Anzeigen von SIP-Klassenzuordnungsobjekten. Diese Objekte ordnen SIP-Datenverkehr bestimmten Kriterien zu, sodass Aktionen für diesen Datenverkehr durchgeführt werden können.
15. **Ändern > Objekte > Inspektion - Richtlinienzuordnungen - DNS**. Ermöglicht die Anzeige von Objekten in der DNS-Richtlinienzuordnung. Diese Objekte werden zum Erstellen von Prüfzuordnungen für DNS-Datenverkehr verwendet.
16. **Ändern > Objekte > Inspect - Policy Maps - FTP**. Ermöglicht das Anzeigen von Objekten für die FTP-Richtlinienzuordnung. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für FTP-Datenverkehr verwendet.
17. **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Ermöglicht die Anzeige von HTTP-Richtlinienzuordnungsobjekten, die für ASA/PIX 7.x-Geräte und IOS-Router erstellt wurden. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für HTTP-Datenverkehr verwendet.
18. **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)**. Ermöglicht die Anzeige von HTTP-Richtlinienzuordnungsobjekten, die für ASA 7.2-/PIX 7.2-Geräte erstellt wurden. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für HTTP-Datenverkehr verwendet.
19. **Modify > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2)**. Ermöglicht die Anzeige von IM-Richtlinienzuordnungsobjekten, die für ASA 7.2-/PIX 7.2-Geräte erstellt wurden. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für IM-Datenverkehr verwendet.
20. **Ändern > Objekte > Inspect - Policy Maps - IM (IOS)**. Ermöglicht die Anzeige von für IOS-Geräte erstellten IM-Richtlinienzuordnungsobjekten. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für IM-Datenverkehr verwendet.

21. **Ändern > Objekte > Inspect - Policy Maps - SIP**. Ermöglicht die Anzeige von SIP-Richtlinienzuordnungsobjekten. Diese Objekte werden zum Erstellen von Inspektionszuordnungen für SIP-Datenverkehr verwendet.
22. **Ändern > Objekte > Überprüfen - Reguläre Ausdrücke**. Ermöglicht das Anzeigen von Objekten für reguläre Ausdrücke. Diese Objekte stellen einzelne reguläre Ausdrücke dar, die als Teil einer Gruppe regulärer Ausdrücke definiert sind.
23. **Ändern > Objekte > Inspektion - Gruppen für reguläre Ausdrücke**. Ermöglicht das Anzeigen von Gruppenobjekten für reguläre Ausdrücke. Diese Objekte werden von bestimmten Klassenzuordnungen verwendet und überprüfen Zuordnungen, um Text innerhalb eines Pakets zuzuordnen.
24. **Ändern > Objekte > Inspect - TCP-Karten**. Ermöglicht Ihnen, TCP-Zuordnungsobjekte anzuzeigen. Diese Objekte passen die Überprüfung des TCP-Datenflusses in beide Richtungen an.
25. **Ändern > Objekte > Schnittstellenrollen**. Ermöglicht das Anzeigen von Objekten für Schnittstellenrollen. Diese Objekte definieren Benennungsmuster, die mehrere Schnittstellen auf verschiedenen Gerätetypen darstellen können. Mit Schnittstellenrollen können Sie Richtlinien auf bestimmte Schnittstellen auf mehreren Geräten anwenden, ohne den Namen der einzelnen Schnittstellen manuell definieren zu müssen.
26. **Ändern > Objekte > IPsec-Transformationssätze**. Ermöglicht die Anzeige von IPsec-Transformationssatz-Objekten. Diese Objekte umfassen eine Kombination aus Sicherheitsprotokollen, Algorithmen und anderen Einstellungen, die genau festlegen, wie die Daten im IPsec-Tunnel verschlüsselt und authentifiziert werden.
27. **Ändern > Objekte > LDAP-Attributzuordnungen**. Ermöglicht die Anzeige von LDAP-Attributzuordnungs-Objekten. Diese Objekte werden verwendet, um benutzerdefinierten (benutzerdefinierten) Attributnamen Cisco LDAP-Attributnamen zuzuordnen.
28. **Ändern > Objekte > Netzwerke/Hosts**. Ermöglicht die Anzeige von Netzwerk-/Hostobjekten. Diese Objekte sind logische Sammlungen von IP-Adressen, die Netzwerke, Hosts oder beide darstellen. Mit Netzwerk-/Hostobjekten können Sie Richtlinien definieren, ohne jedes Netzwerk oder jeden Host einzeln anzugeben.
29. **Ändern > Objekte > PKI-Anmeldungen**. Ermöglicht die Anzeige von PKI-Anmeldungsobjekten. Diese Objekte definieren die CA-Server (Certification Authority), die in einer Public Key-Infrastruktur arbeiten.
30. **Ändern > Objekte > Portweiterleitungslisten**. Ermöglicht Ihnen die Anzeige von Objekten in der Portweiterleitungsliste. Diese Objekte definieren die Zuordnungen von Portnummern eines Remote-Clients zur IP-Adresse und zum Port der Anwendung hinter einem SSL VPN-Gateway.
31. **Ändern > Objekte > Sichere Desktop-Konfigurationen**. Ermöglicht die Anzeige sicherer Desktopkonfigurationsobjekte. Diese Objekte sind wiederverwendbare, benannte Komponenten, auf die durch SSL VPN-Richtlinien verwiesen werden kann, um alle Spuren von vertraulichen Daten zu löschen, die während der Dauer einer SSL VPN-Sitzung gemeinsam genutzt werden.
32. **Ändern > Objekte > Dienste - Portlisten**. Ermöglicht die Anzeige von Portlistenobjekten. Diese Objekte, die einen oder mehrere Bereiche von Portnummern enthalten, werden verwendet, um den Prozess der Erstellung von Dienstobjekten zu rationalisieren.
33. **Ändern > Objekte > Dienste/Servicegruppen.** Ermöglicht die Anzeige von Service- und Service-Gruppen-Objekten. Diese Objekte sind definierte Zuordnungen von Protokoll- und Portdefinitionen, die die von Richtlinien verwendeten Netzwerkdienste beschreiben, z. B. Kerberos, SSH und POP3.

34. **Ändern > Objekte > Server mit einmaliger Anmeldung.** Ermöglicht die Anzeige einzelner Serverobjekte, die sich auf einem Server befinden. Mit Single Sign-On (SSO) können SSL VPN-Benutzer einen Benutzernamen und ein Kennwort einmal eingeben und auf mehrere geschützte Dienste und Webserver zugreifen.
35. **Ändern > Objekte > SLA-Monitore**. Ermöglicht die Anzeige von SLA-Monitorobjekten. Diese Objekte werden von PIX/ASA Security Appliances verwendet, die Version 7.2 oder höher ausführen, um die Routenverfolgung durchzuführen. Diese Funktion bietet eine Methode, um die Verfügbarkeit einer primären Route zu verfolgen und eine Backup-Route zu installieren, falls die primäre Route fehlschlägt.
36. **Ändern > Objekte > SSL VPN-Anpassungen**. Ermöglicht die Anzeige von Objekten zur SSL VPN-Anpassung. Diese Objekte definieren, wie die Darstellung von SSL-VPN-Seiten, die Benutzern angezeigt werden, geändert wird, z. B. Anmelden/Abmelden und Startseiten.
37. **Ändern > Objekte > SSL VPN-Gateways**. Ermöglicht die Anzeige von SSL VPN-Gateway-Objekten. Diese Objekte definieren Parameter, mit denen das Gateway als Proxy für Verbindungen zu den geschützten Ressourcen im SSL VPN verwendet werden kann.
38. **Ändern > Objekte > Formatobjekte**. Ermöglicht das Anzeigen von Formatobjekten. Mit diesen Objekten können Sie Stilelemente wie Schriftartmerkmale und -farben konfigurieren, um die Darstellung der SSL VPN-Seite anzupassen, die SSL VPN-Benutzern bei der Verbindung mit der Sicherheitsappliance angezeigt wird.
39. **Ändern > Objekte > Textobjekte**. Ermöglicht das Anzeigen von frei formatierten Textobjekten. Diese Objekte umfassen ein Name-Wert-Paar, wobei der Wert eine einzelne Zeichenfolge, eine Liste von Zeichenfolgen oder eine Tabelle von Zeichenfolgen sein kann.
40. **Ändern > Objekte > Zeitbereiche.** Ermöglicht das Anzeigen von Objekten im Zeitbereich. Diese Objekte werden bei der Erstellung zeitbasierter ACLs und Prüfungsregeln verwendet. Sie werden auch bei der Definition von ASA-Benutzergruppen verwendet, um den VPN-Zugriff auf bestimmte Zeiten während der Woche zu beschränken.
41. **Ändern > Objekte > Datenverkehrsflüsse**. Ermöglicht die Anzeige von Datenverkehrsflussobjekten. Diese Objekte definieren spezifische Datenverkehrsflüsse für PIX 7.x-/ASA 7.x-Geräte.
42. **Ändern > Objekte > URL-Listen**. Ermöglicht die Anzeige von URL-Listenobjekten. Diese Objekte definieren die URLs, die nach erfolgreicher Anmeldung auf der Portalseite angezeigt werden. Dadurch können Benutzer auf die auf SSL VPN-Websites verfügbaren Ressourcen zugreifen, wenn sie im Clientless-Zugriffsmodus betrieben werden.
43. **Ändern > Objekte > Benutzergruppen**. Ermöglicht das Anzeigen von Benutzergruppenobjekten. Diese Objekte definieren Gruppen von Remote-Clients, die in Easy VPN-Topologien, Remote-Access-VPNs und SSL VPNs verwendet werden
44. **Ändern > Objekte > WINS-Serverlisten**. Ermöglicht das Anzeigen von WINS-Serverlistenobjekten. Diese Objekte stellen WINS-Server dar, die von SSL VPN für den Zugriff auf Dateien oder die gemeinsame Nutzung von Dateien auf Remote-Systemen verwendet werden.
45. **Ändern > Objekte > Intern - DN-Regeln.** Ermöglicht die Anzeige der DN-Regeln, die von DN-Richtlinien verwendet werden. Dies ist ein internes Objekt, das vom Security Manager verwendet wird und nicht im Policy Object Manager angezeigt wird.
46. **Ändern > Objekte > Intern - Client-Updates**. Dies ist ein internes Objekt, das von Benutzergruppenobjekten benötigt wird und nicht im Policy Object Manager angezeigt wird.
47. **Ändern > Objekte > Intern - Standard-ACE**. Dies ist ein internes Objekt für Standardeinträge zur Zugriffskontrolle, die von ACL-Objekten verwendet werden.
48. **Ändern > Objekte > Intern - Erweiterter ACE**. Dies ist ein internes Objekt für Einträge der

erweiterten Zugriffskontrolle, die von ACL-Objekten verwendet werden.

Zusätzliche Berechtigungen ändern

Der Security Manager umfasst die folgenden zusätzlichen Änderungsberechtigungen:

1. **Ändern > Admin**. Ermöglicht Ihnen das Ändern der Verwaltungseinstellungen von Security Manager.
2. **Ändern > Konfigurationsarchiv**. Ermöglicht das Ändern der Gerätekonfiguration im Konfigurationsarchiv. Darüber hinaus können Sie dem Archiv Konfigurationen hinzufügen und das Tool "Konfigurationsarchiv" anpassen.
3. **Ändern > Geräte**. Ermöglicht das Hinzufügen und Löschen von Geräten sowie das Ändern von Geräteeigenschaften und -attributen. Um die Richtlinien auf dem hinzugefügten Gerät zu ermitteln, müssen Sie auch die Import-Berechtigung aktivieren. Wenn Sie die Berechtigung Ändern > Geräte aktivieren, müssen Sie außerdem die Berechtigung Zuweisen > Richtlinien > Schnittstellen aktivieren.
4. **Ändern > Hierarchie**. Ermöglicht das Ändern von Gerätegruppen.
5. **Ändern > Topologie**. Ermöglicht Ihnen, Karten in der Map-Ansicht zu ändern.

Berechtigungen zuweisen

Der Security Manager umfasst die Richtlinienzuweisungsberechtigungen, wie gezeigt:

1. **Zuweisen > Richtlinien > Firewall**. Ermöglicht Ihnen die Zuweisung von Firewall-Service-Richtlinien (die sich in der Richtlinienauswahl unter Firewall befinden) für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte. Beispiele für Firewall-Service-Richtlinien sind Zugriffsregeln, AAA-Regeln und Überprüfungsregeln.
2. **Zuweisen > Richtlinien > Intrusion Prevention System (Intrusion Prevention System)**. Ermöglicht die Zuweisung von IPS-Richtlinien (im Richtlinienauswahl unter IPS), einschließlich Richtlinien für IPS, das auf IOS-Routern ausgeführt wird.
3. **Zuweisen > Richtlinien > Bild**. Diese Berechtigung wird derzeit nicht von Security Manager verwendet.
4. **Zuweisen > Richtlinien > NAT**. Ermöglicht Ihnen die Zuweisung von Netzwerkadressenübersetzungsrichtlinien an PIX/ASA/FWSM-Geräte und IOS-Router. Beispiele für NAT-Richtlinien sind statische Regeln und dynamische Regeln.
5. **Zuweisen > Richtlinien > Site-to-Site-VPN**. Ermöglicht die Zuweisung von Site-to-Site-VPN-Richtlinien für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte. Beispiele für Site-to-Site-VPN-Richtlinien sind IKE-Angebote, IPsec-Vorschläge und vorinstallierte Schlüssel.
6. **Zuweisen > Richtlinien > VPN für Remote-Zugriff**. Ermöglicht Ihnen die Zuweisung von VPN-Richtlinien für Remote-Zugriff an PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte. Beispiele für VPN-Richtlinien für den Remote-Zugriff sind IKE-Vorschläge, IPsec-Vorschläge und PKI-Richtlinien.
7. **Zuweisen > Richtlinien > SSL VPN**. Ermöglicht die Zuweisung von SSL VPN-Richtlinien für PIX/ASA/FWSM-Geräte und IOS-Router, z. B. den SSL VPN-Assistenten.
8. **Zuweisen > Richtlinien > Schnittstellen**. Ermöglicht die Zuweisung von Schnittstellenrichtlinien (die sich im Richtlinienauswahl unter Schnittstellen befindet) für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte:Auf PIX/ASA/FWSM-

Geräten umfasst diese Berechtigung Hardware-Ports und Schnittstelleneinstellungen.Bei IOS-Routern umfasst diese Berechtigung grundlegende und erweiterte Schnittstelleneinstellungen sowie andere schnittstellenbezogene Richtlinien, z. B. DSL-, PVC-, PPP- und Dialer-Richtlinien.Auf Catalyst 6500/7600-Geräten umfasst diese Berechtigung Schnittstellen und VLAN-Einstellungen.

9. **Zuweisen > Richtlinien > Bridging**. Ermöglicht Ihnen, PIX/ASA/FWSM-Geräten ARP-Tabellenrichtlinien zuzuweisen (in der Richtlinienauswahl unter Plattform > Bridging).
10. **Zuweisen > Richtlinien > Geräteverwaltung**. Ermöglicht Ihnen die Zuweisung von Gerätemanagement-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Geräteadministrator befinden) für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte:Beispiele für PIX/ASA/FWSM-Geräte sind Zugriffsrichtlinien für Geräte, Serverzugriffsrichtlinien und Failover-Richtlinien.Bei IOS-Routern sind beispielsweise Richtlinien für den Gerätezugriff (einschließlich Leitungszugriff), Serverzugriffsrichtlinien, AAA und die sichere Gerätebereitstellung erforderlich.Auf IPS-Sensoren umfasst diese Berechtigung Zugriffsrichtlinien für Geräte und Serverzugriffsrichtlinien.Auf Catalyst 6500/7600-Geräten umfasst diese Berechtigung IDSM-Einstellungen und VLAN-Zugriffslisten.
11. **Zuweisen > Richtlinien > Identität**. Ermöglicht Ihnen die Zuweisung von Identitätsrichtlinien (die Sie im Richtlinienauswahl unter Plattform > Identität finden) zu Cisco IOS-Routern, einschließlich 802.1x- und NAC-Richtlinien (Network Admission Control).
12. **Zuweisen > Richtlinien > Protokollierung**. Ermöglicht Ihnen die Zuweisung von Protokollierungsrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Protokollierung befindet) zu PIX/ASA/FWSM-Geräten und IOS-Routern. Beispiele für Protokollierungsrichtlinien sind Protokollierungs-Setup, Server-Setup und Syslog-Serverrichtlinien.
13. **Zuweisen > Richtlinien > Multicast**. Ermöglicht Ihnen, PIX/ASA/FWSM-Geräten Multicast-Richtlinien (die sich im Richtlinienauswahl unter Plattform > Multicast befinden) zuzuweisen. Beispiele für Multicast-Richtlinien sind Multicast-Routing und IGMP-Richtlinien.
14. **Zuweisen > Richtlinien > QoS**. Ermöglicht Ihnen, Cisco IOS-Routern QoS-Richtlinien (die sich in der Richtlinienauswahl unter Plattform > Quality of Service befinden) zuzuweisen.
15. **Zuweisen > Richtlinien > Routing**. Ermöglicht Ihnen die Zuweisung von Routingrichtlinien (die sich in der Richtlinienauswahl unter Plattform > Routing befinden) zu PIX/ASA/FWSM-Geräten und IOS-Routern. Beispiele für Routing-Richtlinien sind OSPF, RIP und statische Routing-Richtlinien.
16. **Zuweisen > Richtlinien > Sicherheit**. Ermöglicht Ihnen, PIX/ASA/FWSM-Geräten Sicherheitsrichtlinien zuzuweisen (in der Richtlinienauswahl unter Plattform > Sicherheit). Zu den Sicherheitsrichtlinien gehören Anti-Spoofing, Fragment und Timeout-Einstellungen.
17. **Zuweisen > Richtlinien > Service-Richtlinienregeln**. Ermöglicht Ihnen, PIX 7.x-/ASA-Geräten Richtlinien für Service-Richtlinien (in der Richtlinienauswahl unter Plattform > Service Policy Rules enthalten) zuzuweisen. Beispiele hierfür sind Prioritätswarteschlangen und IPS, QoS und Verbindungsregeln.
18. **Zuweisen > Richtlinien > Benutzervoreinstellungen**. Ermöglicht Ihnen die Zuweisung der Bereitstellungsrichtlinie (die sich in der Richtlinienauswahl unter Plattform > Benutzereinstellungen befindet) zu PIX/ASA/FWSM-Geräten. Diese Richtlinie enthält eine Option zum Löschen aller NAT-Übersetzungen bei der Bereitstellung.
19. **Zuweisen > Richtlinien > Virtuelles Gerät**. Ermöglicht Ihnen die Zuweisung virtueller Sensorrichtlinien zu IPS-Geräten. Verwenden Sie diese Richtlinie, um virtuelle Sensoren zu erstellen.

20. **Zuweisen > Richtlinien > FlexConfig**. Ermöglicht die Zuweisung von FlexConfigs, d. h. zusätzlichen CLI-Befehlen und Anweisungen, die für PIX/ASA/FWSM-Geräte, IOS-Router und Catalyst 6500/7600-Geräte bereitgestellt werden können.

Hinweis: Wenn Sie Berechtigungen zuweisen, stellen Sie sicher, dass Sie auch die entsprechenden Ansichtsberechtigungen ausgewählt haben.

Berechtigungen genehmigen

Der Security Manager stellt die genehmigten Berechtigungen wie gezeigt bereit:

1. **Genehmigen > CLI**. Ermöglicht die Genehmigung der CLI-Befehlsänderungen, die in einem Bereitstellungsauftrag enthalten sind.
2. **Genehmigen > Richtlinien**. Ermöglicht Ihnen die Genehmigung der Konfigurationsänderungen, die in den Richtlinien enthalten sind, die in einer Workflowaktivität konfiguriert wurden.

CiscoWorks-Rollen im Überblick

Wenn Benutzer in CiscoWorks Common Services erstellt werden, wird ihnen eine oder mehrere Rollen zugewiesen. Die den einzelnen Rollen zugeordneten Berechtigungen bestimmen die Vorgänge, die die einzelnen Benutzer im Security Manager ausführen dürfen.

In den folgenden Themen werden CiscoWorks-Rollen beschrieben:

- CiscoWorks Common Services-Standardrollen
- Zuweisen von Rollen zu Benutzern in CiscoWorks Common Services

CiscoWorks Common Services-Standardrollen

CiscoWorks Common Services enthält die folgenden Standardrollen:

1. **Helpdesk** - Helpdesk-Benutzer können Geräte, Richtlinien, Objekte und Topologiezuordnungen anzeigen (aber nicht ändern).
2. **Network Operator**: Netzwerkbetreiber können neben Berechtigungen auch CLI-Befehle und Verwaltungseinstellungen des Sicherheitsmanagers anzeigen. Netzwerkbetreiber können außerdem das Konfigurationsarchiv ändern und Befehle (wie Ping) an Geräte senden.
3. **Genehmiger** - Zusätzlich zu den Berechtigungen können Genehmiger Bereitstellungsaufträge genehmigen oder ablehnen. Sie können die Bereitstellung nicht durchführen.
4. **Netzwerkadministrator** - Netzwerkadministratoren verfügen über vollständige Berechtigungen zum Anzeigen und Ändern von Berechtigungen, mit Ausnahme der Änderung von Verwaltungseinstellungen. Sie können Geräte und die auf diesen Geräten konfigurierten Richtlinien erkennen, Geräten Richtlinien zuweisen und Geräten Befehle zuweisen. Netzwerkadministratoren können Tätigkeiten oder Bereitstellungsaufgaben nicht genehmigen. Sie können jedoch Jobs bereitstellen, die von anderen genehmigt wurden.
5. **Systemadministrator** - Systemadministratoren haben vollständigen Zugriff auf alle Security Manager-Berechtigungen, einschließlich Änderungen, Richtlinienzuweisung, Aktivität- und Aufgabengenehmigung, Erkennung, Bereitstellung und Ausgabe von Befehlen an Geräte.

Hinweis: Zusätzliche Rollen, z. B. Exportdaten, können in Common Services angezeigt werden, wenn zusätzliche Anwendungen auf dem Server installiert werden. Die Exportdatenrolle ist für Entwickler von Drittanbietern bestimmt und wird nicht von Security Manager verwendet.

Tipp: Obwohl Sie die Definition von CiscoWorks-Rollen nicht ändern können, können Sie festlegen, welche Rollen den einzelnen Benutzern zugewiesen sind. Weitere Informationen finden Sie unter Zuweisen von Rollen zu Benutzern in CiscoWorks Common Services.

Zuweisen von Rollen zu Benutzern in CiscoWorks Common Services

Mit CiscoWorks Common Services können Sie festlegen, welche Rollen den einzelnen Benutzern zugewiesen werden. Wenn Sie die Rollendefinition für einen Benutzer ändern, ändern Sie die Arten von Vorgängen, die dieser Benutzer in Security Manager ausführen darf. Wenn Sie beispielsweise die Helpdesk-Rolle zuweisen, ist der Benutzer auf die Anzeige von Vorgängen beschränkt und kann keine Daten ändern. Wenn Sie jedoch die Rolle Netzwerkbetreiber zuweisen, kann der Benutzer auch das Konfigurationsarchiv ändern. Sie können jedem Benutzer mehrere Rollen zuweisen.

Hinweis: Sie müssen Security Manager neu starten, nachdem Sie Änderungen an den Benutzerberechtigungen vorgenommen haben.

Verfahren:

1. Wählen Sie unter Common Services **Server > Security (Server > Sicherheit) aus**, und wählen Sie dann **Single-Server Trust Management > Local User Setup (Verwaltung** der **Vertrauenswürdigkeit eines Servers > Lokales Benutzereinrichtung** im Inhaltsverzeichnis aus.**Tipp:** Um die Seite für die lokale Benutzereinrichtung im Sicherheitsmanager zu öffnen, wählen Sie Extras > Security Manager Administration > Server Security aus, und klicken Sie dann auf Local User Setup (Lokale Benutzereinrichtung).
2. Aktivieren Sie das Kontrollkästchen neben einem vorhandenen Benutzer, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie auf der Seite Benutzerinformationen die Rollen aus, die diesem Benutzer zugewiesen werden sollen, indem Sie die Kontrollkästchen aktivieren.Weitere Informationen zu den einzelnen Rollen finden Sie unter CiscoWorks Common Services-Standardrollen.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.
5. Starten Sie Security Manager neu.

Cisco Secure ACS-Rollen im Überblick

Cisco Secure ACS bietet mehr Flexibilität bei der Verwaltung von Security Manager-Berechtigungen als CiscoWorks, da es anwendungsspezifische Rollen unterstützt, die Sie konfigurieren können. Jede Rolle besteht aus einer Reihe von Berechtigungen, die die Berechtigungsstufe für Security Manager-Aufgaben festlegen. In Cisco Secure ACS weisen Sie jeder Benutzergruppe (und optional auch einzelnen Benutzern) eine Rolle zu, sodass jeder Benutzer in dieser Gruppe die Vorgänge ausführen kann, die durch die für diese Rolle definierten Berechtigungen autorisiert wurden.

Darüber hinaus können Sie diese Rollen den Cisco Secure ACS-Gerätegruppen zuweisen, sodass Berechtigungen auf verschiedenen Gerätesätzen differenziert werden können.

Hinweis: Cisco Secure ACS-Gerätegruppen sind unabhängig von Security Manager-Gerätegruppen.

In den folgenden Themen werden Cisco Secure ACS-Rollen beschrieben:

- Cisco Secure ACS-Standardrollen
- Anpassen von Cisco Secure ACS-Rollen

Cisco Secure ACS-Standardrollen

Cisco Secure ACS umfasst dieselben Rollen wie CiscoWorks (siehe Understanding CiscoWorks Roles) sowie folgende zusätzliche Rollen:

1. **Sicherheitsgenehmiger**: Sicherheitsgenehmiger können Geräte, Richtlinien, Objekte, Karten, CLI-Befehle und Verwaltungseinstellungen anzeigen (jedoch nicht ändern). Darüber hinaus können Sicherheitsgenehmiger die in einer Aktivität enthaltenen Konfigurationsänderungen genehmigen oder ablehnen. Sie können den Bereitstellungsauftrag nicht genehmigen oder ablehnen oder die Bereitstellung durchführen.
2. **Sicherheitsadministrator** - Sicherheitsadministratoren können nicht nur Zugriffsrechte anzeigen, sondern auch Geräte, Gerätegruppen, Richtlinien, Objekte und Topologiezuordnungen ändern. Sie können auch Geräten und VPN-Topologien Richtlinien zuweisen und diese ermitteln, um neue Geräte in das System zu importieren.
3. **Netzwerkadministrator**: Netzwerkadministratoren können nicht nur Berechtigungen anzeigen, sondern auch das Konfigurationsarchiv ändern, die Bereitstellung durchführen und Befehle an Geräte senden.

Hinweis: Die Berechtigungen in der Cisco Secure ACS-Netzwerkadministratorrolle unterscheiden sich von denen in der CiscoWorks-Netzwerkadministratorrolle. Weitere Informationen finden Sie unter Grundlagen zu CiscoWorks-Rollen.

Im Gegensatz zu CiscoWorks können Sie mit Cisco Secure ACS die Berechtigungen anpassen, die den einzelnen Security Manager-Rollen zugeordnet sind. Weitere Informationen zum Ändern der Standardrollen finden Sie unter Anpassen von Cisco Secure ACS-Rollen.

Hinweis: Cisco Secure ACS 3.3 oder höher muss für die Security Manager-Autorisierung installiert werden.

Anpassen von Cisco Secure ACS-Rollen

Mit Cisco Secure ACS können Sie die Berechtigungen ändern, die jeder Security Manager-Rolle zugewiesen sind. Sie können Cisco Secure ACS auch anpassen, indem Sie spezielle Benutzerrollen mit Berechtigungen erstellen, die auf bestimmte Security Manager-Aufgaben zugeschnitten sind.

Hinweis: Sie müssen Security Manager neu starten, nachdem Sie Änderungen an den Benutzerberechtigungen vorgenommen haben.

Verfahren:

1. Klicken Sie in Cisco Secure ACS in der Navigationsleiste auf **Shared Profile Components** (**Komponenten** für **freigegebene Profile**).

2. Klicken Sie auf der Seite "Gemeinsam genutzte Komponenten" auf **Cisco Security Manager**. Die für Security Manager konfigurierten Rollen werden angezeigt.
3. Führen Sie einen der folgenden Schritte aus:Zum Erstellen einer Rolle klicken Sie auf **Hinzufügen**. Fahren Sie mit Schritt 4 fort.Um eine vorhandene Rolle zu ändern, klicken Sie auf die Rolle. Fahren Sie mit Schritt 5 fort.
4. Geben Sie einen Namen für die Rolle und optional eine Beschreibung ein.
5. Aktivieren und deaktivieren Sie die Kontrollkästchen in der Berechtigungsstruktur, um die Berechtigungen für diese Rolle zu definieren.Wenn Sie das Kontrollkästchen für eine Verzweigung der Struktur aktivieren, werden alle Berechtigungen in dieser Verzweigung ausgewählt. Wenn Sie beispielsweise **Zuweisen** auswählen, werden alle Berechtigungen für die Zuweisung ausgewählt.Eine vollständige Liste der Security Manager-Berechtigungen finden Sie unter Security Manager-Berechtigungen.**Hinweis:** Wenn Sie Berechtigungen zum Ändern, Genehmigen, Zuweisen, Importieren, Steuern oder Bereitstellen auswählen, müssen Sie auch die entsprechenden Anzeigeberechtigungen auswählen. Andernfalls funktioniert der Security Manager nicht ordnungsgemäß.
6. Klicken Sie auf **Senden**, um die Änderungen zu speichern.
7. Starten Sie Security Manager neu.

Standardzuordnungen zwischen Berechtigungen und Rollen im Security Manager

In dieser Tabelle wird gezeigt, wie Berechtigungen für Security Manager den CiscoWorks Common Services-Rollen und den Standardrollen in Cisco Secure ACS zugeordnet sind.

Berechtigungen	Rollen							
	Systemadministrator	Sicherheitsadministrator (ACS)	Security-Genehmiger (ACS)	Netzwerkadministrator (CW)	Netzwerkadministrator (ACS)	Genehmiger	Netzwerkbetreiber	Helpdesk
Berechtigungen anzeigen								
Gerät anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Richtlinie anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Objekte anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Topologie anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
CLI anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein

Administrator anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein
Konfigurationsarchiv anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Geräteman ager anzeigen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein
Berechtigungen ändern								
Gerät ändern	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Hierarchie ändern	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Policy ändern	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Bild ändern	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Objekte ändern	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Topologie ändern	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Admin ändern	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Konfigurationsarchiv ändern	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Nein
Zusätzliche Berechtigungen								
Policy zuweisen	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Richtlinie genehmigen	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein
CLI genehmigen	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Nein
Ermittlung (Import)	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Bereitstellen	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Nein
Kontrolle	Ja	Nein	Nein	Ja	Ja	Nein	Ja	Nein
Senden	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein

Zugehörige Informationen

- Support-Seite für Cisco Security Manager

- Technischer Support und Dokumentation - Cisco Systems