



CHAPTER 2

Managing User Accounts

To use Security Manager, users must log into the product. Create individual accounts for each user. You can either create accounts that are unique to Security Manager, which are defined on the Security Manager server and are called local accounts, or you can use your enterprise ACS server to authenticate users. The following topics describe how to create and manage user accounts, and how to integrate the product with your ACS system:

- [Setting Up User Permissions, page 2-1](#)
- [Integrating Security Manager with Cisco Secure ACS, page 2-21](#)

Setting Up User Permissions

Cisco Security Manager authenticates your username and password before you can log in. After they are authenticated, Security Manager establishes your role within the application. This role defines your permissions (also called privileges), which are the set of tasks or operations that you are authorized to perform. If you are not authorized for certain tasks or devices, the related menu items, items in tables of contents, and buttons are hidden or disabled. In addition, a message tells you that you do not have permission to view the selected information or perform the selected operation.

Authentication and authorization for Security Manager is managed either by the CiscoWorks server or the Cisco Secure Access Control Server (ACS). By default, CiscoWorks manages authentication and authorization, but you can change to Cisco Secure ACS by using the AAA Mode Setup page in CiscoWorks Common Services. For more information about ACS integration, see [Integrating Security Manager with Cisco Secure ACS, page 2-21](#).

The major advantages of using Cisco Secure ACS are the ability to create highly granular user roles with specialized permissions sets (for example, allowing the user to configure certain policy types but not others) and the ability to restrict users to certain devices by configuring network device groups (NDGs). These granular privileges are not available for CiscoWorks local users.



Tip

To view the complete Security Manager permissions tree, log in to Cisco Secure ACS, then click **Share Profile Components** on the navigation bar. For more information, see [Customizing Cisco Secure ACS Roles, page 2-19](#).

The following topics describe user permissions:

- [Security Manager ACS Permissions, page 2-2](#)
- [Understanding CiscoWorks Roles, page 2-16](#)

- [Understanding Cisco Secure ACS Roles, page 2-18](#)
- [Default Associations Between Permissions and Roles in Security Manager, page 2-20](#)

Security Manager ACS Permissions

Cisco Security Manager provides default ACS roles and permissions. You can customize the default roles or create additional roles to suit your needs. However, when defining new roles or customizing default roles, make sure that the permissions you select are logical within the context of the Security Manager application. For example, if you assign modify permissions without view permissions, you will lock the user out of the application.

Security Manager classifies permissions into the following categories:

- **View**—Allows you to view the current settings.
- **Modify**—Allows you to change the current settings.
- **Assign**—Allows you to assign policies to devices and VPN topologies.
- **Approve**—Allows you to approve policy changes and deployment jobs.
- **Control**—Allows you to issue commands to devices, such as ping. This permission is used for connectivity diagnostics.
- **Deploy**—Allows you to deploy configuration changes to the devices in your network and perform rollback to return to a previously deployed configuration.
- **Import**—Allows you to import the configurations that are already deployed on devices into Security Manager. You must also have view device and modify device privileges.
- **Submit**—Allows you to submit your configuration changes for approval.

Tips

- When you select modify, assign, approve, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager will not function properly.
- When you select modify policy permissions, you must also select the corresponding assign and view policy permissions.
- When you permit a policy that uses policy objects as part of its definition, you must also grant view permissions to these object types. For example, if you select the permission for modifying routing policies, you must also select the permissions for viewing network objects and interface roles, which are the object types required by routing policies.
- The same holds true when permitting an object that uses other objects as part of its definition. For example, if you select the permission for modifying user groups, you must also select the permissions for viewing network objects, ACL objects, and AAA server groups.
- You can limit device permissions to particular sets of devices by configuring network device groups (NDGs). NDGs have the following effects on policy permissions:
 - To view a policy, you must have permissions for at least one device to which the policy is assigned.
 - To modify a policy, you must have permissions for all of the devices to which the policy is assigned.
 - To view, modify, or assign a VPN policy, you must have permissions for all of the devices in the VPN topology.

- To assign a policy to a device, you need permissions only for that device, regardless of whether you have permissions for any other devices to which the policy is assigned. (VPN policies are an exception, as noted above.) However, if a user assigns a policy to a device for which you do not have permissions, you will not be able to modify that policy.

View Permissions

View (read-only) permissions in Security Manager are divided into the following categories:

- [View Policies Permissions, page 2-3](#)
- [View Objects Permissions, page 2-4](#)
- [Additional View Permissions, page 2-8](#)

View Policies Permissions

Security Manager includes the following view permissions for policies:

- **View > Policies > Firewall.** Allows you to view firewall service policies (located in the Policy selector under Firewall) on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of firewall service policies include access rules, AAA rules, and inspection rules.
- **View > Policies > Intrusion Prevention System.** Allows you to view IPS policies (located in the Policy selector under IPS), including policies for IPS running on IOS routers.
- **View > Policies > Image.** Allows you to select a signature update package in the Apply IPS Updates wizard (located under Tools > Apply IPS Update), but does not allow you to assign the package to specific devices, unless you also have the Modify > Policies > Image permission.
- **View > Policies > NAT.** Allows you to view network address translation policies on PIX/ASA/FWSM devices and IOS routers. Examples of NAT policies include static rules and dynamic rules.
- **View > Policies > Site-to-Site VPN.** Allows you to view site-to-site VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of site-to-site VPN policies include IKE proposals, IPsec proposals, and preshared keys.
- **View > Policies > Remote Access VPN.** Allows you to view IPsec and SSL remote access VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of remote access VPN policies include IKE proposals, IPsec proposals, PKI policies, and the SSL VPN wizard.
- **View > Policies > Interfaces and Failover.** Allows you to view interface policies (located in the Policy selector under Interfaces) on PIX/ASA/FWSM devices, IOS routers, IPS sensors, and Catalyst devices:
 - On PIX/ASA/FWSM devices, this permission covers hardware ports and interface settings.
 - On IOS routers, this permission covers basic and advanced interface settings, as well as other interface-related policies, such as DSL, PVC, PPP, and dialer policies.
 - On IPS sensors, this permission covers physical interfaces and summary maps.
 - On Catalyst devices, this permission covers interfaces and VLAN settings.
- **View > Policies > Bridging.** Allows you to view ARP table policies (located in the Policy selector under Platform > Bridging) on PIX/ASA/FWSM devices.
- **View > Policies > Device Administration.** Allows you to view device administration policies (located in the Policy selector under Platform > Device Admin) on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices:

- On PIX/ASA/FWSM devices, examples include device access policies, server access policies, and failover policies.
- On IOS routers, examples include device access (including line access) policies, server access policies, AAA, and Secure Device Provisioning.
- On IPS sensors, this permission covers device access policies and server access policies.
- On Catalyst devices, this permission covers IDSM settings and VLAN access lists.
- **View > Policies > Identity.** Allows you to view identity policies (located in the Policy selector under Platform > Identity) on Cisco IOS routers, including 802.1x and Network Admission Control (NAC) policies.
- **View > Policies > Logging.** Allows you to view logging policies (located in the Policy selector under Platform > Logging) on PIX/ASA/FWSM devices, IOS routers, and IPS sensors. Examples of logging policies include logging setup, server setup, and syslog server policies.
- **View > Policies > Multicast.** Allows you to view multicast policies (located in the Policy selector under Platform > Multicast) on PIX/ASA/FWSM devices. Examples of multicast policies include multicast routing and IGMP policies.
- **View > Policies > QoS.** Allows you to view QoS policies (located in the Policy selector under Platform > Quality of Service) on Cisco IOS routers.
- **View > Policies > Routing.** Allows you to view routing policies (located in the Policy selector under Platform > Routing) on PIX/ASA/FWSM devices and IOS routers. Examples of routing policies include OSPF, RIP, and static routing policies.
- **View > Policies > Security.** Allows you to view security policies (located in the Policy selector under Platform > Security) on PIX/ASA/FWSM devices and IPS sensors:
 - On PIX/ASA/FWSM devices, security policies include anti-spoofing, fragment, and timeout settings.
 - On IPS sensors, security policies include blocking settings.
- **View > Policies > Service Policy Rules.** Allows you to view service policy rule policies (located in the Policy selector under Platform > Service Policy Rules) on PIX 7.x/ASA devices. Examples include priority queues and IPS, QoS, and connection rules.
- **View > Policies > User Preferences.** Allows you to view the Deployment policy (located in the Policy selector under Platform > User Preferences) on PIX/ASA/FWSM devices. This policy contains an option for clearing all NAT translations on deployment.
- **View > Policies > Virtual Device.** Allows you to view virtual sensor policies on IPS devices. This policy is used to create virtual sensors.
- **View > Policies > FlexConfig.** Allows you to view FlexConfigs, which are additional CLI commands and instructions that can be deployed to PIX/ASA/FWSM devices, IOS routers, and Catalyst devices.

View Objects Permissions

Security Manager includes the following view permissions for objects:

- **View > Objects > AAA Server Groups.** Allows you to view AAA server group objects. These objects are used in policies that require AAA services (authentication, authorization, and accounting).
- **View > Objects > AAA Servers.** Allows you to view AAA server objects. These objects represent individual AAA servers that are defined as part of a AAA server group.

- **View > Objects > Access Control Lists - Standard/Extended.** Allows you to view standard and extended ACL objects. Extended ACL objects are used for a variety of policies, such as NAT and NAC, and for establishing VPN access. Standard ACL objects are used for such policies as OSPF and SNMP, as well as for establishing VPN access.
- **View > Objects > Access Control Lists - Web.** Allows you to view web ACL objects. Web ACL objects are used to perform content filtering in SSL VPN policies.
- **View > Objects > ASA User Groups.** Allows you to view ASA user group objects. These objects are configured on ASA security appliances in Easy VPN, remote access VPN, and SSL VPN configurations.
- **View > Objects > Categories.** Allows you to view category objects. These objects help you easily identify rules and objects in rules tables through the use of color.
- **View > Objects > Credentials.** Allows you to view credential objects. These objects are used in Easy VPN configuration during IKE Extended Authentication (Xauth).
- **View > Objects > FlexConfigs.** Allows you to view FlexConfig objects. These objects, which contain configuration commands with additional scripting language instructions, can be used to configure commands that are not supported by the Security Manager user interface.
- **View > Objects > IKE Proposals.** Allows you to view IKE proposal objects. These objects contain the parameters required for IKE proposals in remote access VPN policies.
- **View > Objects > Inspect - Class Maps - DNS.** Allows you to view DNS class map objects. These objects match DNS traffic with specific criteria so that actions can be performed on that traffic.
- **View > Objects > Inspect - Class Maps - FTP.** Allows you to view FTP class map objects. These objects match FTP traffic with specific criteria so that actions can be performed on that traffic.
- **View > Objects > Inspect - Class Maps - HTTP.** Allows you to view HTTP class map objects. These objects match HTTP traffic with specific criteria so that actions can be performed on that traffic.
- **View > Objects > Inspect - Class Maps - IM.** Allows you to view IM class map objects. These objects match IM traffic with specific criteria so that actions can be performed on that traffic.
- **View > Objects > Inspect - Class Maps - SIP.** Allows you to view SIP class map objects. These objects match SIP traffic with specific criteria so that actions can be performed on that traffic.
- **View > Objects > Inspect - Policy Maps - DNS.** Allows you to view DNS policy map objects. These objects are used to create inspection maps for DNS traffic.
- **View > Objects > Inspect - Policy Maps - FTP.** Allows you to view FTP policy map objects. These objects are used to create inspection maps for FTP traffic.
- **View > Objects > Inspect - Policy Maps - GTP.** Allows you to view GTP policy map objects. These objects are used to create inspection maps for GTP traffic.
- **View > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS).** Allows you to view HTTP policy map objects created for ASA/PIX 7.1.x devices and IOS routers. These objects are used to create inspection maps for HTTP traffic.
- **View > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2).** Allows you to view HTTP policy map objects created for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for HTTP traffic.
- **View > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2).** Allows you to view IM policy map objects created for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for IM traffic.

- **View > Objects > Inspect - Policy Maps - IM (IOS).** Allows you to view IM policy map objects created for IOS devices. These objects are used to create inspection maps for IM traffic.
- **View > Objects > Inspect - Policy Maps - SIP.** Allows you to view SIP policy map objects. These objects are used to create inspection maps for SIP traffic.
- **View > Objects > Inspect - Regular Expressions.** Allows you to view regular expression objects. These objects represent individual regular expressions that are defined as part of a regular expression group.
- **View > Objects > Inspect - Regular Expressions Groups.** Allows you to view regular expression group objects. These objects are used by certain class maps and inspect maps to match text inside a packet.
- **View > Objects > Inspect - TCP Maps.** Allows you to view TCP map objects. These objects customize inspection on TCP flow in both directions.
- **View > Objects > Interface Roles.** Allows you to view interface role objects. These objects define naming patterns that can represent multiple interfaces on different types of devices. Interface roles enable you to apply policies to specific interfaces on multiple devices without having to manually define the name of each interface.
- **View > Objects > IPsec Transform Sets.** Allows you to view IPsec transform set objects. These objects comprise a combination of security protocols, algorithms and other settings that specify exactly how the data in the IPsec tunnel will be encrypted and authenticated.
- **View > Objects > LDAP Attribute Maps.** Allows you to view LDAP attribute map objects. These objects are used to map custom (user-defined) attribute names to Cisco LDAP attribute names.
- **View > Objects > Networks/Hosts.** Allows you to view network/host objects. These objects are logical collections of IP addresses that represent networks, hosts, or both. Network/host objects enable you to define policies without specifying each network or host individually.
- **View > Objects > PKI Enrollments.** Allows you to view PKI enrollment objects. These objects define the Certification Authority (CA) servers that operate within a public key infrastructure.
- **View > Objects > Port Forwarding Lists.** Allows you to view port forwarding list objects. These objects define the mappings of port numbers on a remote client to the application's IP address and port behind an SSL VPN gateway.
- **View > Objects > Smart Tunnel Lists.** Allows you to view SSL VPN smart tunnel list objects. These objects define the smart tunnel lists, each of which consists of one or more applications eligible for smart tunnel access.
- **View > Objects > Secure Desktop Configurations.** Allows you to view secure desktop configuration objects. These objects are reusable, named components that can be referenced by SSL VPN policies to provide a reliable means of eliminating all traces of sensitive data that is shared for the duration of an SSL VPN session.
- **View > Objects > Services - Port Lists.** Allows you to view port list objects. These objects, which contain one or more ranges of port numbers, are used to streamline the process of creating service objects.
- **View > Objects > Services/Service Groups.** Allows you to view service and service group objects. These objects are defined mappings of protocol and port definitions that describe network services used by policies, such as Kerberos, SSH, and POP3.
- **View > Objects > Single Sign On Servers.** Allows you to view single sign on server objects. Single Sign-On (SSO) lets SSL VPN users enter a username and password once and be able to access multiple protected services and web servers.

- **View > Objects > SLA Monitors.** Allows you to view SLA monitor objects. These objects are used by PIX/ASA security appliances running version 7.2 or later to perform route tracking. This feature provides a method to track the availability of a primary route and install a backup route if the primary route fails.
- **View > Objects > SSL VPN Customizations.** Allows you to view SSL VPN customization objects. These objects define how to change the appearance of SSL VPN pages that are displayed to users, such as Login/Logout and Home pages.
- **View > Objects > SSL VPN Gateways.** Allows you to view SSL VPN gateway objects. These objects define parameters that enable the gateway to be used as a proxy for connections to the protected resources in your SSL VPN.
- **View > Objects > Style Objects.** Allows you to view style objects. These objects let you configure style elements, such as font characteristics and colors, to customize the appearance of the SSL VPN page that appears to SSL VPN users when they connect to the security appliance.
- **View > Objects > Text Objects.** Allows you to view free-form text objects. These objects comprise a name and value pair, where the value can be a single string, a list of strings, or a table of strings.
- **View > Objects > Time Ranges.** Allows you to view time range objects. These objects are used when creating time-based ACLs and inspection rules. They are also used when defining ASA user groups to restrict VPN access to specific times during the week.
- **View > Objects > Traffic Flows.** Allows you to view traffic flow objects. These objects define specific traffic flows for use by PIX 7.x/ASA 7.x and higher devices.
- **View > Objects > URL Lists.** Allows you to view URL list objects. These objects define the URLs that are displayed on the portal page after a successful login. This enables users to access the resources available on SSL VPN websites when operating in Clientless access mode.
- **View > Objects > User Groups.** Allows you to view user group objects. These objects define groups of remote clients that are used in Easy VPN topologies, remote access VPNs, and SSL VPNs.
- **View > Objects > WINS Server Lists.** Allows you to view WINS server list objects. These objects represent WINS servers, which are used by SSL VPN to access or share files on remote systems.
- **View > Objects > Internal - DN Rules.** Allows you to view the DN rules used by DN policies. This is an internal object used by Security Manager that does not appear in the Policy Object Manager.
- **View > Objects > Internal - Client Updates.** This is an internal object required by user group objects that does not appear in the Policy Object Manager.
- **View > Objects > Internal - Standard ACE.** This is an internal object for standard access control entries, which are used by ACL objects.
- **View > Objects > Internal - Extended ACE.** This is an internal object for extended access control entries, which are used by ACL objects.
- **View > Objects > Inspect - Policy Maps - DCE/RPC.** Allows you to view DCE/RPC policy map objects. These objects are used to create inspection maps for DCE/RPC traffic.
- **View > Objects > Inspect - Policy Maps - H.323 (ASA 7.2/PIX 7.2).** Allows you to view H.323 policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for H.323 traffic.
- **View > Objects > Inspect - Class Maps - H.323 (ASA 7.2/PIX 7.2).** Allows you to view H.323 class map objects for ASA 7.2/PIX 7.2 and higher devices. These objects match H.323 traffic with specific criteria so that actions can be performed on that traffic.
- **View > Objects > Inspect - Policy Maps - IPSec Pass Through (ASA 7.2/PIX 7.2).** Allows you to view IPSec Pass Through policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for IPSec Pass Through traffic.

- **View > Objects > Inspect - Policy Maps - MGCP (ASA 7.2/PIX 7.2).** Allows you to view MGCP policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for MGCP traffic.
- **View > Objects > Inspect - Policy Maps - NetBIOS (ASA 7.2/PIX 7.2).** Allows you to view NetBIOS policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for NetBIOS traffic.
- **View > Objects > Inspect - Policy Maps - RADIUS (ASA 7.2/PIX 7.2).** Allows you to view RADIUS policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for RADIUS traffic.
- **View > Objects > Inspect - Policy Maps - SKINNY (ASA 7.2/PIX 7.2).** Allows you to view Skinny policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for Skinny traffic.
- **View > Objects > Inspect - Policy Maps - SNMP.** Allows you to view SNMP policy map objects. These objects are used to create inspection maps for SNMP traffic.
- **View > Objects > Inspect - Policy Maps - ESMTP.** Allows you to view ESMTP policy map objects. These objects are used to create inspection maps for ESMTP traffic.
- **View > Objects > File Objects.** Allows you to view file objects. These objects are used to identify files that are included in an SSL VPN configuration.

Additional View Permissions

Security Manager includes the following additional view permissions:

- **View > Admin.** Allows you to view Security Manager administrative settings.
- **View > CLI.** Allows you to view the CLI commands configured on a device and preview the commands that are about to be deployed.
- **View > Config Archive.** Allows you to view the list of configurations contained in the configuration archive. You cannot view the device configuration or any CLI commands.
- **View > Devices.** Allows you to view devices in Device view and all related information, including their device settings, properties, assignments, and so on. You can limit device permissions to particular sets of devices by configuring network device groups (NDGs).
- **View > Device Managers.** Allows you to launch read-only versions of the device managers for individual devices, such as the Cisco Router and Security Device Manager (SDM) for Cisco IOS routers.
- **View > Topology.** Allows you to view maps configured in Map view.

Modify Permissions

Modify (read-write) permissions in Security Manager are divided into the following categories:

- [Modify Policies Permissions, page 2-9](#)
- [Modify Objects Permissions, page 2-10](#)
- [Additional Modify Permissions, page 2-14](#)

Modify Policies Permissions

Security Manager includes the following modify permissions for policies. When you specify modify policy permissions, make sure that you have selected the corresponding assign and view policy permissions as well.

- **Modify > Policies > Firewall.** Allows you to modify firewall service policies (located in the Policy selector under Firewall) on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of firewall service policies include access rules, AAA rules, and inspection rules.
- **Modify > Policies > Intrusion Prevention System.** Allows you to modify IPS policies (located in the Policy selector under IPS), including policies for IPS running on IOS routers. This permission also allows you to tune signatures in the Signature Update wizard (located under Tools > Apply IPS Update).
- **Modify > Policies > Image.** Allows you to assign a signature update package to devices in the Apply IPS Updates wizard (located under Tools > Apply IPS Update). This permission also allows you to assign auto update settings to specific devices (located under Tools > Security Manager Administration > IPS Updates).
- **Modify > Policies > NAT.** Allows you to modify network address translation policies on PIX/ASA/FWSM devices and IOS routers. Examples of NAT policies include static rules and dynamic rules.
- **Modify > Policies > Site-to-Site VPN.** Allows you to modify site-to-site VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of site-to-site VPN policies include IKE proposals, IPsec proposals, and preshared keys.
- **Modify > Policies > Remote Access VPN.** Allows you to modify IPsec and SSL remote access VPN policies on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of remote access VPN policies include IKE proposals, IPsec proposals, PKI policies, and the SSL VPN wizard.
- **Modify > Policies > Interfaces and Failover.** Allows you to modify interface policies (located in the Policy selector under Interfaces) on PIX/ASA/FWSM devices, IOS routers, IPS sensors, and Catalyst devices:
 - On PIX/ASA/FWSM devices, this permission covers hardware ports and interface settings.
 - On IOS routers, this permission covers basic and advanced interface settings, as well as other interface-related policies, such as DSL, PVC, PPP, and dialer policies.
 - On IPS sensors, this permission covers physical interfaces and summary maps.
 - On Catalyst devices, this permission covers interfaces and VLAN settings.
- **Modify > Policies > Bridging.** Allows you to modify ARP table policies (located in the Policy selector under Platform > Bridging) on PIX/ASA/FWSM devices.
- **Modify > Policies > Device Administration.** Allows you to modify device administration policies (located in the Policy selector under Platform > Device Admin) on PIX/ASA/FWSM devices, IOS routers, and Catalyst devices:
 - On PIX/ASA/FWSM devices, examples include device access policies, server access policies, and failover policies.
 - On IOS routers, examples include device access (including line access) policies, server access policies, AAA, and Secure Device Provisioning.
 - On IPS sensors, this permission covers device access policies and server access policies.
 - On Catalyst devices, this permission covers IDSM settings and VLAN access lists.

- **Modify > Policies > Identity.** Allows you to modify identity policies (located in the Policy selector under Platform > Identity) on Cisco IOS routers, including 802.1x and Network Admission Control (NAC) policies.
- **Modify > Policies > Logging.** Allows you to modify logging policies (located in the Policy selector under Platform > Logging) on PIX/ASA/FWSM devices, IOS routers, and IPS sensors. Examples of logging policies include logging setup, server setup, and syslog server policies.
- **Modify > Policies > Multicast.** Allows you to modify multicast policies (located in the Policy selector under Platform > Multicast) on PIX/ASA/FWSM devices. Examples of multicast policies include multicast routing and IGMP policies.
- **Modify > Policies > QoS.** Allows you to modify QoS policies (located in the Policy selector under Platform > Quality of Service) on Cisco IOS routers.
- **Modify > Policies > Routing.** Allows you to modify routing policies (located in the Policy selector under Platform > Routing) on PIX/ASA/FWSM devices and IOS routers. Examples of routing policies include OSPF, RIP, and static routing policies.
- **Modify > Policies > Security.** Allows you to modify security policies (located in the Policy selector under Platform > Security) on PIX/ASA/FWSM devices and IPS sensors:
 - On PIX/ASA/FWSM devices, security policies include anti-spoofing, fragment, and timeout settings.
 - On IPS sensors, security policies include blocking settings.
- **Modify > Policies > Service Policy Rules.** Allows you to modify service policy rule policies (located in the Policy selector under Platform > Service Policy Rules) on PIX 7.x/ASA devices. Examples include priority queues and IPS, QoS, and connection rules.
- **Modify > Policies > User Preferences.** Allows you to modify the Deployment policy (located in the Policy selector under Platform > User Preferences) on PIX/ASA/FWSM devices. This policy contains an option for clearing all NAT translations on deployment.
- **Modify > Policies > Virtual Device.** Allows you to modify virtual sensor policies on IPS devices. Use this policy to create virtual sensors.
- **Modify > Policies > FlexConfig.** Allows you to modify FlexConfigs, which are additional CLI commands and instructions that can be deployed to PIX/ASA/FWSM devices, IOS routers, and Catalyst devices.

Modify Objects Permissions

Security Manager includes the following modify permissions for objects:

- **Modify > Objects > AAA Server Groups.** Allows you to modify AAA server group objects. These objects are used in policies that require AAA services (authentication, authorization, and accounting).
- **Modify > Objects > AAA Servers.** Allows you to modify AAA server objects. These objects represent individual AAA servers that are defined as part of a AAA server group.
- **Modify > Objects > Access Control Lists - Standard/Extended.** Allows you to modify standard and extended ACL objects. Extended ACL objects are used for a variety of policies, such as NAT and NAC, and for establishing VPN access. Standard ACL objects are used for such policies as OSPF and SNMP, as well as for establishing VPN access.
- **Modify > Objects > Access Control Lists - Web.** Allows you to modify web ACL objects. Web ACL objects are used to perform content filtering in SSL VPN policies.

- **Modify > Objects > ASA User Groups.** Allows you to modify ASA user group objects. These objects are configured on ASA security appliances in Easy VPN, remote access VPN, and SSL VPN configurations.
- **Modify > Objects > Categories.** Allows you to modify category objects. These objects help you easily identify rules and objects in rules tables through the use of color.
- **Modify > Objects > Credentials.** Allows you to modify credential objects. These objects are used in Easy VPN configuration during IKE Extended Authentication (Xauth).
- **Modify > Objects > FlexConfigs.** Allows you to modify FlexConfig objects. These objects, which contain configuration commands with additional scripting language instructions, can be used to configure commands that are not supported by the Security Manager user interface.
- **Modify > Objects > IKE Proposals.** Allows you to modify IKE proposal objects. These objects contain the parameters required for IKE proposals in remote access VPN policies.
- **Modify > Objects > Inspect - Class Maps - DNS.** Allows you to modify DNS class map objects. These objects match DNS traffic with specific criteria so that actions can be performed on that traffic.
- **Modify > Objects > Inspect - Class Maps - FTP.** Allows you to modify FTP class map objects. These objects match FTP traffic with specific criteria so that actions can be performed on that traffic.
- **Modify > Objects > Inspect - Class Maps - HTTP.** Allows you to modify HTTP class map objects. These objects match HTTP traffic with specific criteria so that actions can be performed on that traffic.
- **Modify > Objects > Inspect - Class Maps - IM.** Allows you to modify IM class map objects. These objects match IM traffic with specific criteria so that actions can be performed on that traffic.
- **Modify > Objects > Inspect - Class Maps - SIP.** Allows you to modify SIP class map objects. These objects match SIP traffic with specific criteria so that actions can be performed on that traffic.
- **Modify > Objects > Inspect - Policy Maps - DNS.** Allows you to modify DNS policy map objects. These objects are used to create inspection maps for DNS traffic.
- **Modify > Objects > Inspect - Policy Maps - FTP.** Allows you to modify FTP policy map objects. These objects are used to create inspection maps for FTP traffic.
- **Modify > Objects > Inspect - Policy Maps - GTP.** Allows you to modify GTP policy map objects. These objects are used to create inspection maps for GTP traffic.
- **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS).** Allows you to modify HTTP policy map objects created for ASA/PIX 7.x devices and IOS routers. These objects are used to create inspection maps for HTTP traffic.
- **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2).** Allows you to modify HTTP policy map objects created for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for HTTP traffic.
- **Modify > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2).** Allows you to modify IM policy map objects created for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for IM traffic.
- **Modify > Objects > Inspect - Policy Maps - IM (IOS).** Allows you to modify IM policy map objects created for IOS devices. These objects are used to create inspection maps for IM traffic.
- **Modify > Objects > Inspect - Policy Maps - SIP.** Allows you to modify SIP policy map objects. These objects are used to create inspection maps for SIP traffic.

- **Modify > Objects > Inspect - Regular Expressions.** Allows you to modify regular expression objects. These objects represent individual regular expressions that are defined as part of a regular expression group.
- **Modify > Objects > Inspect - Regular Expressions Groups.** Allows you to modify regular expression group objects. These objects are used by certain class maps and inspect maps to match text inside a packet.
- **Modify > Objects > Inspect - TCP Maps.** Allows you to modify TCP map objects. These objects customize inspection on TCP flow in both directions.
- **Modify > Objects > Interface Roles.** Allows you to modify interface role objects. These objects define naming patterns that can represent multiple interfaces on different types of devices. Interface roles enable you to apply policies to specific interfaces on multiple devices without having to manually define the name of each interface.
- **Modify > Objects > IPsec Transform Sets.** Allows you to modify IPsec transform set objects. These objects comprise a combination of security protocols, algorithms and other settings that specify exactly how the data in the IPsec tunnel will be encrypted and authenticated.
- **Modify > Objects > LDAP Attribute Maps.** Allows you to modify LDAP attribute map objects. These objects are used to map custom (user-defined) attribute names to Cisco LDAP attribute names.
- **Modify > Objects > Networks/Hosts.** Allows you to modify network/host objects. These objects are logical collections of IP addresses that represent networks, hosts, or both. Network/host objects enable you to define policies without specifying each network or host individually.
- **Modify > Objects > PKI Enrollments.** Allows you to modify PKI enrollment objects. These objects define the Certification Authority (CA) servers that operate within a public key infrastructure.
- **Modify > Objects > Port Forwarding Lists.** Allows you to modify port forwarding list objects. These objects define the mappings of port numbers on a remote client to the application's IP address and port behind an SSL VPN gateway.
- **Modify > Objects > Smart Tunnel Lists.** Allows you to modify SSL VPN smart tunnel list objects. These objects define the smart tunnel lists, each of which consists of one or more applications eligible for smart tunnel access.
- **Modify > Objects > Secure Desktop Configurations.** Allows you to modify secure desktop configuration objects. These objects are reusable, named components that can be referenced by SSL VPN policies to provide a reliable means of eliminating all traces of sensitive data that is shared for the duration of an SSL VPN session.
- **Modify > Objects > Services - Port Lists.** Allows you to modify port list objects. These objects, which contain one or more ranges of port numbers, are used to streamline the process of creating service objects
- **Modify > Objects > Services/Service Groups.** Allows you to modify service and service group objects. These objects are defined mappings of protocol and port definitions that describe network services used by policies, such as Kerberos, SSH, and POP3.
- **Modify > Objects > Single Sign On Servers.** Allows you to modify single sign on server objects. Single Sign-On (SSO) lets SSL VPN users enter a username and password once and be able to access multiple protected services and web servers.
- **Modify > Objects > SLA Monitors.** Allows you to modify SLA monitor objects. These objects are used by PIX/ASA security appliances running version 7.2 or later to perform route tracking. This feature provides a method to track the availability of a primary route and install a backup route if the primary route fails.

- **Modify > Objects > SSL VPN Customizations.** Allows you to modify SSL VPN customization objects. These objects define how to change the appearance of SSL VPN pages that are displayed to users, such as Login/Logout and Home pages.
- **Modify > Objects > SSL VPN Gateways.** Allows you to modify SSL VPN gateway objects. These objects define parameters that enable the gateway to be used as a proxy for connections to the protected resources in your SSL VPN.
- **Modify > Objects > Style Objects.** Allows you to modify style objects. These objects let you configure style elements, such as font characteristics and colors, to customize the appearance of the SSL VPN page that appears to SSL VPN users when they connect to the security appliance.
- **Modify > Objects > Text Objects.** Allows you to modify free-form text objects. These objects comprise a name and value pair, where the value can be a single string, a list of strings, or a table of strings.
- **Modify > Objects > Time Ranges.** Allows you to modify time range objects. These objects are used when creating time-based ACLs and inspection rules. They are also used when defining ASA user groups to restrict VPN access to specific times during the week.
- **Modify > Objects > Traffic Flows.** Allows you to modify traffic flow objects. These objects define specific traffic flows for use by PIX 7.x/ASA 7.x and higher devices.
- **Modify > Objects > URL Lists.** Allows you to modify URL list objects. These objects define the URLs that are displayed on the portal page after a successful login. This enables users to access the resources available on SSL VPN websites when operating in Clientless access mode.
- **Modify > Objects > User Groups.** Allows you to modify user group objects. These objects define groups of remote clients that are used in Easy VPN topologies, remote access VPNs, and SSL VPNs.
- **Modify > Objects > WINS Server Lists.** Allows you to modify WINS server list objects. These objects represent WINS servers, which are used by SSL VPN to access or share files on remote systems.
- **Modify > Objects > Internal - DN Rules.** Allows you to modify the DN rules used by DN policies. This is an internal object used by Security Manager that does not appear in the Policy Object Manager.
- **Modify > Objects > Internal - Client Updates.** This is an internal object required by user group objects that does not appear in the Policy Object Manager.
- **Modify > Objects > Internal - Standard ACE.** This is an internal object for standard access control entries, which are used by ACL objects.
- **Modify > Objects > Internal - Extended ACE.** This is an internal object for extended access control entries, which are used by ACL objects.
- **Modify > Objects > Inspect - Policy Maps - DCE/RPC.** Allows you to modify DCE/RPC policy map objects. These objects are used to create inspection maps for DCE/RPC traffic.
- **Modify > Objects > Inspect - Policy Maps - H.323 (ASA 7.2/PIX 7.2).** Allows you to modify H.323 policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for H.323 traffic.
- **Modify > Objects > Inspect - Class Maps - H.323 (ASA 7.2/PIX 7.2).** Allows you to modify H.323 class map objects for ASA 7.2/PIX 7.2 and higher devices. These objects match H.323 traffic with specific criteria so that actions can be performed on that traffic.
- **Modify > Objects > Inspect - Policy Maps - IPSec Pass Through (ASA 7.2/PIX 7.2).** Allows you to modify IPSec Pass Through policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for IPSec Pass Through traffic.

- **Modify > Objects > Inspect - Policy Maps - MGCP (ASA 7.2/PIX 7.2).** Allows you to modify MGCP policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for MGCP traffic.
- **Modify > Objects > Inspect - Policy Maps - NetBIOS (ASA 7.2/PIX 7.2).** Allows you to modify NetBIOS policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for NetBIOS traffic.
- **Modify > Objects > Inspect - Policy Maps - RADIUS (ASA 7.2/PIX 7.2).** Allows you to modify RADIUS policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for RADIUS traffic.
- **Modify > Objects > Inspect - Policy Maps - SKINNY (ASA 7.2/PIX 7.2).** Allows you to modify Skinny policy map objects for ASA 7.2/PIX 7.2 and higher devices. These objects are used to create inspection maps for Skinny traffic.
- **Modify > Objects > Inspect - Policy Maps - SNMP.** Allows you to modify SNMP policy map objects. These objects are used to create inspection maps for SNMP traffic.
- **Modify > Objects > Inspect - Policy Maps - ESMTP.** Allows you to modify ESMTP policy map objects. These objects are used to create inspection maps for ESMTP traffic.
- **Modify > Objects > File Objects.** Allows you to modify file objects. These objects are used to identify files that are included in an SSL VPN configuration.

Additional Modify Permissions

Security Manager includes the following additional modify permissions:

- **Modify > Admin.** Allows you to modify Security Manager administrative settings.
- **Modify > Config Archive.** Allows you to modify the device configuration in the Configuration Archive. In addition, it allows you to add configurations to the archive and customize the Configuration Archive tool.
- **Modify > Devices.** Allows you to add and delete devices, as well as modify device properties and attributes. To discover the policies on the device being added, you must also enable the Import permission. In addition, if you enable the Modify > Devices permission, make sure that you also enable the Assign > Policies > Interfaces permission. You can limit device permissions to particular sets of devices by configuring network device groups (NDGs).
- **Modify > Hierarchy.** Allows you to modify device groups.
- **Modify > Topology.** Allows you to modify maps in Map view.

Assign Permissions

Security Manager includes the following policy assignment permissions. When you specify assign permissions, make sure that you have selected the corresponding view permissions as well.

- **Assign > Policies > Firewall.** Allows you to assign firewall service policies (located in the Policy selector under Firewall) to PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of firewall service policies include access rules, AAA rules, and inspection rules.
- **Assign > Policies > Intrusion Prevention System.** Allows you to assign IPS policies (located in the Policy selector under IPS), including policies for IPS running on IOS routers.
- **Assign > Policies > Image.** This permission is currently not used by Security Manager.

- **Assign > Policies > NAT.** Allows you to assign network address translation policies to PIX/ASA/FWSM devices and IOS routers. Examples of NAT policies include static rules and dynamic rules.
- **Assign > Policies > Site-to-Site VPN.** Allows you to assign site-to-site VPN policies to PIX/ASA/FWSM devices, IOS routers, and Catalyst 6500/7600 devices. Examples of site-to-site VPN policies include IKE proposals, IPsec proposals, and preshared keys.
- **Assign > Policies > Remote Access VPN.** Allows you to assign IPsec and SSL remote access VPN policies to PIX/ASA/FWSM devices, IOS routers, and Catalyst devices. Examples of remote access VPN policies include IKE proposals, IPsec proposals, PKI policies, and the SSL VPN wizard.
- **Assign > Policies > Interfaces.** Allows you to assign interface policies (located in the Policy selector under Interfaces) to PIX/ASA/FWSM devices, IOS routers, IPS sensors, and Catalyst devices:
 - On PIX/ASA/FWSM devices, this permission covers hardware ports and interface settings.
 - On IOS routers, this permission covers basic and advanced interface settings, as well as other interface-related policies, such as DSL, PVC, PPP, and dialer policies.
 - On IPS sensors, this permission covers physical interfaces and summary maps.
 - On Catalyst devices, this permission covers interfaces and VLAN settings.
- **Assign > Policies > Bridging.** Allows you to assign ARP table policies (located in the Policy selector under Platform > Bridging) to PIX/ASA/FWSM devices.
- **Assign > Policies > Device Administration.** Allows you to assign device administration policies (located in the Policy selector under Platform > Device Admin) to PIX/ASA/FWSM devices, IOS routers, and Catalyst devices:
 - On PIX/ASA/FWSM devices, examples include device access policies, server access policies, and failover policies.
 - On IOS routers, examples include device access (including line access) policies, server access policies, AAA, and Secure Device Provisioning.
 - On IPS sensors, this permission covers device access policies and server access policies.
 - On Catalyst devices, this permission covers IDSM settings and VLAN access lists.
- **Assign > Policies > Identity.** Allows you to assign identity policies (located in the Policy selector under Platform > Identity) to Cisco IOS routers, including 802.1x and Network Admission Control (NAC) policies.
- **Assign > Policies > Logging.** Allows you to assign logging policies (located in the Policy selector under Platform > Logging) to PIX/ASA/FWSM devices and IOS routers. Examples of logging policies include logging setup, server setup, and syslog server policies.
- **Assign > Policies > Multicast.** Allows you to assign multicast policies (located in the Policy selector under Platform > Multicast) to PIX/ASA/FWSM devices. Examples of multicast policies include multicast routing and IGMP policies.
- **Assign > Policies > QoS.** Allows you to assign QoS policies (located in the Policy selector under Platform > Quality of Service) to Cisco IOS routers.
- **Assign > Policies > Routing.** Allows you to assign routing policies (located in the Policy selector under Platform > Routing) to PIX/ASA/FWSM devices and IOS routers. Examples of routing policies include OSPF, RIP, and static routing policies.
- **Assign > Policies > Security.** Allows you to assign security policies (located in the Policy selector under Platform > Security) to PIX/ASA/FWSM devices. Security policies include anti-spoofing, fragment, and timeout settings.

- **Assign > Policies > Service Policy Rules.** Allows you to assign service policy rule policies (located in the Policy selector under Platform > Service Policy Rules) to PIX 7.x/ASA devices. Examples include priority queues and IPS, QoS, and connection rules.
- **Assign > Policies > User Preferences.** Allows you to assign the Deployment policy (located in the Policy selector under Platform > User Preferences) to PIX/ASA/FWSM devices. This policy contains an option for clearing all NAT translations on deployment.
- **Assign > Policies > Virtual Device.** Allows you to assign virtual sensor policies to IPS devices. Use this policy to create virtual sensors.
- **Assign > Policies > FlexConfig.** Allows you to assign FlexConfigs, which are additional CLI commands and instructions that can be deployed to PIX/ASA/FWSM devices, IOS routers, and Catalyst devices.

Approve Permissions

Security Manager provides the following approve permissions:

- **Approve > CLI.** Allows you to approve the CLI command changes contained in a deployment job.
- **Approve > Policy.** Allows you to approve the configuration changes contained in the policies that were configured in a workflow activity.

Understanding CiscoWorks Roles

When users are created in CiscoWorks Common Services, they are assigned one or more roles. The permissions associated with each role determine the operations that each user is authorized to perform in Security Manager.

The following topics describe CiscoWorks roles:

- [CiscoWorks Common Services Default Roles, page 2-16](#)
- [Assigning Roles to Users in CiscoWorks Common Services, page 2-17](#)

CiscoWorks Common Services Default Roles

CiscoWorks Common Services contains the following default roles For Security Manager:

- **Help Desk**—Help desk users can view (but not modify) devices, policies, objects, and topology maps.
- **Approver**—In addition to view permissions, approvers can approve or reject deployment jobs. They cannot perform deployment.
- **Network Operator**—In addition to view permissions, network operators can view CLI commands and Security Manager administrative settings. Network operators can also modify the configuration archive and issue commands (such as ping) to devices.
- **Network Administrator**—Network administrators have complete view and modify permissions, except for modifying administrative settings. They can discover devices and the policies configured on these devices, assign policies to devices, and issue commands to devices. Network administrators cannot approve activities or deployment jobs; however, they can deploy jobs that were approved by others.



Note Cisco Secure ACS features a default role called Network Administrator that contains a different set of permissions. For more information, see [Understanding Cisco Secure ACS Roles, page 2-18](#).

- **System Administrator**—System administrators have complete access to all Security Manager permissions, including modification, policy assignment, activity and job approval, discovery, deployment, and issuing commands to devices.

For details about which Security Manager permissions are associated with each CiscoWorks role, see [Default Associations Between Permissions and Roles in Security Manager, page 2-20](#).

Tips

- Additional roles, such as Export Data, might be displayed in Common Services if additional applications are installed on the server. The Export Data role is for third-party developers and is not used by Security Manager.
- Although you cannot change the definition of CiscoWorks roles, you can define which roles are assigned to each user. For more information, see [Assigning Roles to Users in CiscoWorks Common Services, page 2-17](#).
- To generate a permissions table in CiscoWorks, select **Server > Reports > Permission Report** and click **Generate Report**.

Assigning Roles to Users in CiscoWorks Common Services

When you define a user in CiscoWorks Common Services, you must select the roles that the user should have. By changing the role definition for a user, you change the types of operations this user is authorized perform in Security Manager. For example, if you assign the Help Desk role, the user is limited to view operations and cannot modify any data. However, if you assign the Network Operator role, the user is also able to modify the configuration archive. You can assign multiple roles to each user.



Tip

You must restart Security Manager after making changes to user permissions.

Related Topics

- [Security Manager ACS Permissions, page 2-2](#)
- [Default Associations Between Permissions and Roles in Security Manager, page 2-20](#)
- [Understanding CiscoWorks Roles, page 2-16](#)

Procedure

-
- Step 1** In Common Services, select **Server > Security**, then select **Single-Server Trust Management > Local User Setup** from the table of contents.



Tip

To reach the Local User Setup page from within Security Manager, select **Tools > Security Manager Administration > Server Security**, then click **Local User Setup**.

- Step 2** Do one of the following:
- To create a new user, click **Add** and enter the user name, password, and e-mail address.
 - To change the roles of an existing user, select the check box next to the user and click **Edit**.
- Step 3** On the User Information page, select the roles to assign to this user. For more information about each role, see [CiscoWorks Common Services Default Roles, page 2-16](#).
- Step 4** Click **OK** to save your changes.
- Step 5** Restart Security Manager.
-

Understanding Cisco Secure ACS Roles

Cisco Secure ACS provides greater flexibility for managing Security Manager permissions than does CiscoWorks because it supports application-specific roles that you can configure. Each role is made up of a set of permissions that determine the level of authorization to Security Manager tasks. In Cisco Secure ACS, you assign a role to each user group (and optionally, to individual users as well), which enables each user in that group to perform the operations authorized by the permissions defined for that role.

In addition, you can assign these roles to Cisco Secure ACS device groups, allowing permissions to be differentiated on different sets of devices.



Note

Cisco Secure ACS device groups are independent of Security Manager device groups.

The following topics describe Cisco Secure ACS roles:

- [Cisco Secure ACS Default Roles, page 2-18](#)
- [Customizing Cisco Secure ACS Roles, page 2-19](#)

Cisco Secure ACS Default Roles

Cisco Secure ACS includes the same roles as CiscoWorks (see [Understanding CiscoWorks Roles, page 2-16](#)), plus these additional roles:

- Security Approver**—Security approvers can view (but not modify) devices, policies, objects, maps, CLI commands, and administrative settings. In addition, security approvers can approve or reject the configuration changes contained in an activity. They cannot approve or reject the deployment job, nor can they perform deployment.
- Security Administrator**—In addition to having view permissions, security administrators can modify devices, device groups, policies, objects, and topology maps. They can also assign policies to devices and VPN topologies, and perform discovery to import new devices into the system.
- Network Administrator**—In addition to view permissions, network administrators can modify the configuration archive, perform deployment, and issue commands to devices.



Note

The permissions contained in the Cisco Secure ACS network administrator role are different from those contained in the CiscoWorks network administrator role. For more information, see [Understanding CiscoWorks Roles, page 2-16](#).

Unlike CiscoWorks, Cisco Secure ACS enables you to customize the permissions associated with each Security Manager role. For more information about modifying the default roles, see [Customizing Cisco Secure ACS Roles, page 2-19](#).

For details about which Security Manager permissions are associated with each Cisco Secure ACS role, see [Default Associations Between Permissions and Roles in Security Manager, page 2-20](#).

Related Topics

- [Integrating Security Manager with Cisco Secure ACS, page 2-21](#)
- [Setting Up User Permissions, page 2-1](#)

Customizing Cisco Secure ACS Roles

Cisco Secure ACS enables you to modify the permissions associated with each Security Manager role. You can also customize Cisco Secure ACS by creating specialized user roles with permissions that are targeted to particular Security Manager tasks.




Note

You must restart Security Manager after making changes to user permissions.

Related Topics

- [Security Manager ACS Permissions, page 2-2](#)
- [Default Associations Between Permissions and Roles in Security Manager, page 2-20](#)

Procedure

-
- Step 1** In Cisco Secure ACS, click **Shared Profile Components** on the navigation bar.
- Step 2** Click **Cisco Security Manager** on the Shared Components page. The roles that are configured for Security Manager are displayed.
- Step 3** Do one of the following:
- To create a role, click **Add**. Enter a name for the role and, optionally, a description.
 - To modify an existing role, click the role.
- Step 4** Select and deselect the check boxes in the permissions tree to define the permissions for this role. Selecting the check box for a branch of the tree selects all permissions in that branch. For example, selecting **Assign** selects all the assign permissions.
- For a complete list of Security Manager permissions, see [Security Manager ACS Permissions, page 2-2](#).
-  **Tip** When you select modify, approve, assign, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager will not function properly.
-
- Step 5** Click **Submit** to save your changes.
- Step 6** Restart Security Manager.
-

Default Associations Between Permissions and Roles in Security Manager

Table 2-1 shows how Security Manager permissions are associated with CiscoWorks Common Services roles and the default roles in Cisco Secure ACS. For information about the specific permissions, see [Security Manager ACS Permissions, page 2-2](#).

Table 2-1 Default Permission to Role Associations in Security Manager

Permissions	Roles							
	System Admin.	Security Admin. (ACS)	Security Approver (ACS)	Network Admin. (CW)	Network Admin. (ACS)	Approver	Network Operator	Help Desk
View Permissions								
View Device	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Topology	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View CLI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
View Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
View Config Archive	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Device Managers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Modify Permissions								
Modify Device	Yes	Yes	No	Yes	No	No	No	No
Modify Hierarchy	Yes	Yes	No	Yes	No	No	No	No
Modify Policy	Yes	Yes	No	Yes	No	No	No	No
Modify Image	Yes	Yes	No	Yes	No	No	No	No
Modify Objects	Yes	Yes	No	Yes	No	No	No	No
Modify Topology	Yes	Yes	No	Yes	No	No	No	No
Modify Admin	Yes	No	No	No	No	No	No	No
Modify Config Archive	Yes	Yes	No	Yes	Yes	No	Yes	No
Additional Permissions								
Assign Policy	Yes	Yes	No	Yes	No	No	No	No
Approve Policy	Yes	No	Yes	No	No	No	No	No
Approve CLI	Yes	No	No	No	No	Yes	No	No
Discover (Import)	Yes	Yes	No	Yes	No	No	No	No
Deploy	Yes	No	No	Yes	Yes	No	No	No

Table 2-1 Default Permission to Role Associations in Security Manager (Continued)

Permissions	Roles							
	System Admin.	Security Admin. (ACS)	Security Approver (ACS)	Network Admin. (CW)	Network Admin. (ACS)	Approver	Network Operator	Help Desk
Control	Yes	No	No	Yes	Yes	No	Yes	No
Submit	Yes	Yes	No	Yes	No	No	No	No

Integrating Security Manager with Cisco Secure ACS

This section describes how to integrate your Cisco Secure ACS with Cisco Security Manager.

Cisco Secure ACS provides command authorization for users who are using management applications, such as Security Manager, to configure managed network devices. Support for command authorization is provided by unique command authorization set types (called roles in Security Manager) that contain a set of permissions. These permissions (also called privileges) determine the actions that users with particular roles can perform within Security Manager.

Cisco Secure ACS uses TACACS+ to communicate with management applications. For Security Manager to communicate with Cisco Secure ACS, you must configure the CiscoWorks server in Cisco Secure ACS as a AAA client that uses TACACS+. In addition, you must provide the CiscoWorks server with the administrator name and password that you use to log in to the Cisco Secure ACS. Fulfilling these requirements ensures the validity of communications between Security Manager and Cisco Secure ACS.



Note

For an understanding of TACACS+ security advantages, see [User Guide for Cisco Secure Access Control Server](#).

When Security Manager initially communicates with Cisco Secure ACS, it dictates to Cisco ACS the creation of default roles, which appear in the Shared Profile Components section of the Cisco Secure ACS HTML interface. It also dictates a custom service to be authorized by TACACS+. This custom service appears on the TACACS+ (Cisco IOS) page in the Interface Configuration section of the HTML interface. You can then modify the permissions included in each Security Manager role and apply these roles to users and user groups.

The following topics describe how to use Cisco Secure ACS with Security Manager:

- [ACS Integration Requirements, page 2-22](#)
- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)
- [Integration Procedures Performed in Cisco Secure ACS, page 2-23](#)
- [Integration Procedures Performed in CiscoWorks, page 2-30](#)
- [Restarting the Daemon Manager, page 2-33](#)
- [Assigning Roles to User Groups in Cisco Secure ACS, page 2-33](#)

ACS Integration Requirements

To use Cisco Secure ACS, make sure that:

- You defined roles that include the permissions required to perform necessary functions in Security Manager.
- The Network Access Restriction (NAR) includes the device group (or the devices) that you want to administer, if you apply a NAR to the profile.
- Managed device names are spelled and capitalized identically in Cisco Secure ACS and in Security Manager.

Tips

- We highly recommend that you create a fault-tolerant infrastructure that utilizes multiple Cisco Secure ACS servers. Having multiple servers helps to ensure your ability to continue work in Security Manager even if connectivity is lost to one of the ACS servers.
- You can integrate only one version of Security Manager with a Cisco Secure ACS. Therefore, if your organization is using two different versions of Security Manager at the same time, you must perform integration with two different Cisco Secure ACS servers. You can, however, upgrade to a new version of Security Manager without having to use a different ACS.
- Even when Cisco Secure ACS authentication is used, CiscoWorks Common Services software uses local authorization for CiscoWorks Common Services-specific utilities, such as Compact Database and Database Checkpoint. To use these utilities, you must be defined locally and be assigned the appropriate permissions.

Related Topics

- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)
- [Integrating Security Manager with Cisco Secure ACS, page 2-21](#)

Procedural Overview for Initial Cisco Secure ACS Setup

The following procedure summarizes the overall tasks you need to perform to use Cisco Secure ACS with Security Manager. The procedure contains references to more specific procedures used to perform each step.

Related Topics

- [ACS Integration Requirements, page 2-22](#)
- [Integrating Security Manager with Cisco Secure ACS, page 2-21](#)

Procedure

Step 1 Plan your administrative authentication and authorization model.

You should decide on your administrative model before using Security Manager. This includes defining the administrative roles and accounts that you plan to use.



Tip

When defining the roles and permissions of potential administrators, you should also consider whether to enable Workflow. This selection affects how you can restrict access.

For more information, see:

- [Understanding Cisco Secure ACS Roles, page 2-18](#)
- [Selecting a Workflow Mode, page 1-12](#)
- [User Guide for Cisco Secure Access Control Server](#)

Step 2 Install Cisco Secure ACS, Cisco Security Manager, and CiscoWorks Common Services.

Install Cisco Secure ACS. Install CiscoWorks Common Services and Cisco Security Manager on a different server. Do not run Cisco Secure ACS and Security Manager on the same server.

For more information, see:

- [Supported Devices and Software Versions for Cisco Security Manager](#) (for information on the supported versions of Cisco Secure ACS)
- [Installation Guide for Cisco Security Manager](#)
- [Installation Guide for Cisco Secure ACS for Windows Server](#)

Step 3 Perform integration procedures in Cisco Secure ACS.

Define Security Manager users as ACS users and assign them to user groups based on their planned role, add all your managed devices (as well as the CiscoWorks/Security Manager server) as AAA clients, and create an administration control user.

For more information, see [Integration Procedures Performed in Cisco Secure ACS, page 2-23](#).

Step 4 Perform integration procedures in CiscoWorks Common Services.

Configure a local user that matches the administrator defined in Cisco Secure ACS, define that same user for the system identity setup, and configure ACS as the AAA setup mode.

For more information, see [Integration Procedures Performed in CiscoWorks, page 2-30](#).

Step 5 Restart the Daemon Manager.

You must restart the Security Manager server Daemon Manager for the AAA settings you configured to take effect.

For more information, see [Restarting the Daemon Manager, page 2-33](#).

Step 6 Assign roles to user groups in Cisco Secure ACS.

Assign roles to each user group configured in Cisco Secure ACS. The procedure you should use depends on whether you have configured network device groups (NDGs).

For more information, see [Assigning Roles to User Groups in Cisco Secure ACS, page 2-33](#).

Integration Procedures Performed in Cisco Secure ACS

The following topics describe the procedures to perform in Cisco Secure ACS when integrating it with Cisco Security Manager. Perform the tasks in the listed order. For more information about the procedures described in these sections, see [User Guide for Cisco Secure Access Control Server](#).

1. [Defining Users and User Groups in Cisco Secure ACS, page 2-24](#)
2. [Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 2-25](#)
3. [Creating an Administration Control User in Cisco Secure ACS, page 2-29](#)

Defining Users and User Groups in Cisco Secure ACS

All users of Security Manager must be defined in Cisco Secure ACS and assigned a role appropriate to their job function. The easiest way to do this is to divide the users into different groups based on each default role available in ACS, for example, assigning all the system administrators to one group, all the network operators to another group, and so on. For more information about the default roles in ACS, see [Cisco Secure ACS Default Roles, page 2-18](#).

You must create an additional user that is assigned the system administrator role with full permissions. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See [Defining the System Identity User, page 2-31](#).

Please note that at this stage you are merely assigning users to different groups. The actual assignment of roles to these groups is performed later, after CiscoWorks, Security Manager, and any other applications have been registered to Cisco Secure ACS.



Tip

This procedure explains how to create user accounts during the initial Cisco Secure ACS integration. After you complete the integration, when you create a new user account, you can assign it to the appropriate group as you create the account.

Related Topics

- [ACS Integration Requirements, page 2-22](#)
- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)
- [Assigning Roles to User Groups in Cisco Secure ACS, page 2-33](#)

Procedure

-
- Step 1** Log in to Cisco Secure ACS.
- Step 2** Configure a user with full permissions using the following procedure. For more information about the options available when configuring users and user groups, see [User Guide for Cisco Secure Access Control Server](#).
- a. Click **User Setup** on the navigation bar.
 - b. On the User Setup page, enter a name for the new user and click **Add/Edit**.



Tip

Do not create a user named **admin**. The admin user is the fall-back user in Security Manager. If the ACS system stops working for some reason, you can still log into CiscoWorks Common Services on the Security Manager server using the admin account to change the AAA mode to CiscoWorks local authentication and continue using the product.

- c. Select an authentication method from the Password Authentication list under User Setup.
- d. Enter and confirm the password for the new user.
- e. Select **Group 1** as the group to which the user should be assigned.
- f. Click **Submit** to create the user account.

Step 3 Repeat this process for each Security Manager user. We recommend dividing the users into groups based on the role each user will be assigned:

- Group 1—System Administrators
- Group 2—Security Administrators
- Group 3—Security Approvers
- Group 4—Network Administrators
- Group 5—Approvers
- Group 6—Network Operators
- Group 7—Help Desk

For more information about the default permissions associated with each role, see [Default Associations Between Permissions and Roles in Security Manager, page 2-20](#). For more information about customizing user roles, see [Customizing Cisco Secure ACS Roles, page 2-19](#).



Note At this stage, the groups themselves are collections of users without any role definitions. You will assign roles to each group after completing the integration process. See [Assigning Roles to User Groups in Cisco Secure ACS, page 2-33](#).

Step 4 Create an additional user and assign this user to the system administrators group. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See [Defining the System Identity User, page 2-31](#).

Step 5 Continue with [Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 2-25](#).

Adding Managed Devices as AAA Clients in Cisco Secure ACS

Before you can begin importing devices into Security Manager, you must first configure each device as a AAA client in your Cisco Secure ACS. In addition, you must configure the CiscoWorks/Security Manager server as a AAA client.

If Security Manager is managing security contexts configured on firewall devices, including security contexts configured on FWSMs for Catalyst 6500/7600 devices, each context must be added individually to Cisco Secure ACS. Likewise, all virtual sensors defined on IPS devices must also be added.

The method for adding managed devices depends on whether you want to restrict users to managing a particular set of devices by creating network device groups (NDGs). Proceed as follows:

- If you want users to have access to all devices, add the devices as described in [Adding Devices as AAA Clients Without NDGs, page 2-25](#).
- If you want users to have access only to certain NDGs, add the devices as described in [Configuring Network Device Groups for Use in Security Manager, page 2-26](#).

Adding Devices as AAA Clients Without NDGs

This procedure describes how to add devices as AAA clients of a Cisco Secure ACS. For complete information about all available options, see [User Guide for Cisco Secure Access Control Server](#).



Tip

Remember to add the CiscoWorks/Security Manager server as a AAA client.

Related Topics

- [ACS Integration Requirements, page 2-22](#)
- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)

Procedure

-
- Step 1** Click **Network Configuration** on the Cisco Secure ACS navigation bar.
- Step 2** Click **Add Entry** beneath the AAA Clients table.
- Step 3** Enter the AAA client hostname (up to 32 characters) on the Add AAA Client page. The hostname of the AAA client *must* match the display name you plan to use for the device in Security Manager.

For example, if you intend to append a domain name to the device name in Security Manager, the AAA client hostname in ACS must be **<device_name>.<domain_name>**.

When naming the CiscoWorks server, we recommend using the fully-qualified hostname. Be sure to spell the hostname correctly. (The hostname is not case sensitive.)

Additional naming conventions include:

- PIX or ASA security context, or FWSM security context when discovered through the FWSM: **<parent_display_name>_<context_name>**
- FWSM blade: **<chassis_name>_FW_<slot_number>**
- FWSM security context when discovered through the chassis: **<chassis_name>_FW_<slot_number>_<context_name>**
- IPS sensor: **<IPSParentName>_<virtualSensorName>**

- Step 4** Enter the IP address of the network device in the AAA Client IP Address field. If the device does not have an IP address (for example, a virtual sensor or a virtual context), enter the word **dynamic** instead of an address.



Note If you are adding a multi-homed device (a device with multiple NICs), enter the IP address of each NIC. Press **Enter** between each address. In addition, you must modify the gatekeeper.cfg file on the Security Manager server. For more information, see the chapter on post-installation server tasks in the [Installation Guide for Cisco Security Manager](#).

- Step 5** Enter the shared secret in the Key field.
- Step 6** Select **TACACS+ (Cisco IOS)** from the Authenticate Using list.
- Step 7** Click **Submit** to save your changes. The device you added is displayed in the AAA Clients table.
- Step 8** Repeat the process to add additional devices.
- Step 9** To save the devices you have added, click **Submit + Restart**.
- Step 10** Continue with [Creating an Administration Control User in Cisco Secure ACS, page 2-29](#).
-

Configuring Network Device Groups for Use in Security Manager

Cisco Secure ACS enables you to configure network device groups (NDGs) that contain specific devices to be managed. For example, you can create NDGs for each geographic region or NDGs that match your organizational structure. When used with Security Manager, NDGs enable you to provide users with different levels of permissions, depending on the devices they need to manage. For example, by using

NDGs you can assign User A system administrator permissions to the devices located in Europe and Help Desk permissions to the devices located in Asia. You can then assign the opposite permissions to User B.

NDGs are not assigned directly to users. Rather, NDGs are assigned to the roles that you define for each user group. Each NDG can be assigned to a single role only, but each role can include multiple NDGs. These definitions are saved as part of the configuration for the selected user group.

Tips

- Each device can be a member of only one NDG.
- NDGs are *not* related to the device groups that you can configure in Security Manager. See [Understanding Device Grouping, page 6-28](#).
- For complete details about managing NDGs, see *User Guide for Cisco Secure Access Control Server*

The following topics outline the basic information and steps for configuring NDGs:

- [NDGs and User Permissions, page 2-27](#)
- [Activating the NDG Feature, page 2-28](#)
- [Creating NDGs, page 2-28](#)
- [Associating NDGs and Roles with User Groups, page 2-34](#)

NDGs and User Permissions

Because NDGs limit users to particular sets of devices, they affect policy permissions, as follows:

- To view a policy, you must have permissions for at least *one* device to which the policy is assigned.
- To modify a policy, you must have permissions for *all* of the devices to which the policy is assigned.
- To view, modify, or assign a VPN policy, you must have permissions for *all* of the devices in the VPN topology.
- To assign a policy to a device, you need permissions only for that device, regardless of whether you have permissions for any other devices to which the policy is assigned. (VPN policies are an exception, as noted above.) However, if a user assigns a policy to a device for which you do not have permissions, you will not be able to modify that policy. See [Modify Policies Permissions, page 2-9](#).



Note

To modify an object, a user does *not* need modify permissions for all the devices that are using the object. However, a user must have modify permissions for a particular device in order to modify a device-level object override defined on that device.

Related Topics

- [Configuring Network Device Groups for Use in Security Manager, page 2-26](#)
- [View Policies Permissions, page 2-3](#)
- [Modify Policies Permissions, page 2-9](#)
- [Setting Up User Permissions, page 2-1](#)

Activating the NDG Feature

You must activate the NDG feature before you can create NDGs and populate them with devices.

Related Topics

- [Creating NDGs, page 2-28](#)
- [Associating NDGs and Roles with User Groups, page 2-34](#)
- [NDGs and User Permissions, page 2-27](#)
- [Configuring Network Device Groups for Use in Security Manager, page 2-26](#)

Procedure

-
- Step 1** Click **Interface Configuration** on the Cisco Secure ACS navigation bar.
- Step 2** Click **Advanced Options**.
- Step 3** Scroll down, then select the **Network Device Groups** check box.
- Step 4** Click **Submit**.
- Step 5** Continue with [Creating NDGs, page 2-28](#).
-

Creating NDGs

This procedure describes how to create NDGs and populate them with devices. Each device can belong to only one NDG.



Tip

We highly recommend creating a special NDG that contains the CiscoWorks/Security Manager servers.

Before You Begin

Activate the NDG feature as described in [Activating the NDG Feature, page 2-28](#)

Related Topics

- [Associating NDGs and Roles with User Groups, page 2-34](#)
- [NDGs and User Permissions, page 2-27](#)
- [Configuring Network Device Groups for Use in Security Manager, page 2-26](#)

Procedure

-
- Step 1** Click **Network Configuration** on the navigation bar.
- All devices are initially placed under Not Assigned, which holds all devices that were not placed in an NDG. Please note that Not Assigned is *not* an NDG.
- Step 2** Create NDGs:
- Click **Add Entry**.
 - Enter a name for the NDG on the New Network Device Group page. The maximum length is 24 characters. Spaces are permitted.

- c. (Optional) Enter a key to be used by all devices in the NDG. If you define a key for the NDG, it overrides any keys defined for the individual devices in the NDG.
 - d. Click **Submit** to save the NDG.
 - e. Repeat the process to create more NDGs.
- Step 3** Populate the NDGs with devices. Keep in mind that each device can be a member of only one NDG.
- a. Click the name of the NDG in the Network Device Groups area.
 - b. Click **Add Entry** in the AAA Clients area.
 - c. Define the particulars of the device to add to the NDG, then click **Submit**. For more information, see [Adding Devices as AAA Clients Without NDGs, page 2-25](#).
 - d. Repeat the process to add the remaining devices to NDGs. The only device you should consider leaving in the Not Assigned category is the default AAA server.
 - e. After you configure the last device, click **Submit + Restart**.
- Step 4** Continue with [Creating an Administration Control User in Cisco Secure ACS, page 2-29](#).



Tip You can associate roles with each NDG only after completing the integration procedures in Cisco Secure ACS and CiscoWorks Common Services. See [Associating NDGs and Roles with User Groups, page 2-34](#).

Creating an Administration Control User in Cisco Secure ACS

Use the Administration Control page in Cisco Secure ACS to define the administrator account that is used when defining the AAA setup mode in CiscoWorks Common Services. For more information, see [Configuring the AAA Setup Mode in CiscoWorks, page 2-31](#).

Related Topics

- [ACS Integration Requirements, page 2-22](#)
- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)

Procedure

-
- Step 1** Click **Administration Control** on the Cisco Secure ACS navigation bar.
 - Step 2** Click **Add Administrator**.
 - Step 3** On the Add Administrator page, enter a name and password for the administrator.
 - Step 4** Click **Grant All** in the Administrator Privileges area to provide full administrative permissions to this administrator.
 - Step 5** Click **Submit** to create the administrator.



Note For more information about the options available when configuring an administrator, see [User Guide for Cisco Secure Access Control Server](#).

Integration Procedures Performed in CiscoWorks

After you complete the integration tasks in Cisco Secure ACS (described in [Integration Procedures Performed in Cisco Secure ACS, page 2-23](#)), you must complete some tasks in CiscoWorks Common Services. Common Services performs the actual registration of any installed applications, such as Cisco Security Manager and Auto-Update Server, into Cisco Secure ACS.

The following topics describe the procedures to perform in CiscoWorks Common Services when integrating it with Cisco Security Manager:

- [Creating a Local User in CiscoWorks, page 2-30](#)
- [Defining the System Identity User, page 2-31](#)
- [Configuring the AAA Setup Mode in CiscoWorks, page 2-31](#)

Creating a Local User in CiscoWorks

Use the Local User Setup page in CiscoWorks Common Services to create a local user account that duplicates the administrator you previously created in Cisco Secure ACS. This local user account is later used for the system identity setup. For more information, see [Defining the System Identity User, page 2-31](#).

Before You Begin

Create an administrator in Cisco Secure ACS. See [Defining Users and User Groups in Cisco Secure ACS, page 2-24](#).

Related Topics

- [ACS Integration Requirements, page 2-22](#)
- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)
- [Logging In to the Cisco Security Management Suite Server, page 1-8](#)

Procedure

-
- Step 1** Log in to CiscoWorks using the **admin** user account.
- Step 2** Select **Server > Security** from Common Services, then select **Local User Setup** from the TOC.



Tip To get to this page from the Security Manager client, select **Tools > Security Manager Administration > Server Security** and click **Local User Setup**.

- Step 3** Click **Add**.
- Step 4** Enter the same name and password that you entered when creating the administrator in Cisco Secure ACS. See [Defining Users and User Groups in Cisco Secure ACS, page 2-24](#).
- Step 5** Select all check boxes under Roles.
- Step 6** Click **OK** to create the user.
-

Defining the System Identity User

Use the System Identity Setup page in CiscoWorks Common Services to create a trust user (called the System Identity user) that enables communication between servers that are part of the same domain and application processes that are located on the same server. Applications use the System Identity user to authenticate processes on local or remote CiscoWorks servers. This is especially useful when the applications must synchronize before any users have logged in.

In addition, the System Identity user is often used to perform a subtask when the primary task has already been authorized for the logged in user.

The System Identity user you configure here must be identical to the administrator with full permissions that you configured in ACS. Failure to do so could result in your being unable to view all the devices and policies configured in Security Manager.

Before You Begin

Create a local user with the same name and password as this administrator in CiscoWorks Common Services. See [Creating a Local User in CiscoWorks](#), page 2-30.

Related Topics

- [ACS Integration Requirements](#), page 2-22
- [Procedural Overview for Initial Cisco Secure ACS Setup](#), page 2-22
- [Logging In to the Cisco Security Management Suite Server](#), page 1-8

Procedure

Step 1 In Common Services, select **Server > Security**, then select **Multi-Server Trust Management > System Identity Setup** from the TOC.



Tip To get to this page from the Security Manager client, select **Tools > Security Manager Administration > Server Security** and click **System Identity Setup**.

Step 2 Enter the name of the administrator that you created for Cisco Secure ACS. See [Defining Users and User Groups in Cisco Secure ACS](#), page 2-24.

Step 3 Enter and verify the password for this user.

Step 4 Click **Apply**.

Configuring the AAA Setup Mode in CiscoWorks

Use the AAA Setup Mode page in CiscoWorks Common Services to define your Cisco Secure ACS as the AAA server, including the required port and shared secret key. In addition, you can define up to two backup servers.

This procedure performs the actual registration of CiscoWorks and Security Manager (and optionally, Auto-Update Server) into Cisco Secure ACS.

**Tip**

The AAA setup configured here is not retained if you uninstall CiscoWorks Common Services or Cisco Security Manager. In addition, this configuration cannot be backed up and restored after reinstallation. Therefore, if you upgrade to a new version of either application, you must reconfigure the AAA setup mode and reregister Security Manager with ACS. This process is not required for incremental updates. If you install additional applications, such as AUS, on top of CiscoWorks, you must reregister the new applications and Cisco Security Manager.

Related Topics

- [ACS Integration Requirements, page 2-22](#)
- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)
- [Logging In to the Cisco Security Management Suite Server, page 1-8](#)

Procedure

Step 1 In Common Services, select **Server > Security**, then select **AAA Mode Setup** from the TOC.

**Tip**

To get to this page from the Security Manager client, select **Tools > Security Manager Administration > Server Security** and click **AAA Mode Setup**.

Step 2 Select the **TACACS+** check box under Available Login Modules.

Step 3 Select **ACS** as the AAA type.

Step 4 Enter the IP addresses of up to three Cisco Secure ACS servers in the Server Details area. The secondary and tertiary servers act as backups in case the primary server fails. All servers must be running the same version of Cisco Secure ACS.

**Note**

If all the configured TACACS+ servers fail to respond, you must log in using the *admin* CiscoWorks Local account, then change the AAA mode back to Non-ACS/CiscoWorks Local. After the TACACS+ servers are restored to service, you must change the AAA mode back to ACS.

Step 5 In the Login area, enter the name of the administrator that you defined on the Administration Control page of Cisco Secure ACS. For more information, see [Creating an Administration Control User in Cisco Secure ACS, page 2-29](#).

Step 6 Enter and verify the password for this administrator.

Step 7 Enter and verify the shared secret key that you entered when you added the Security Manager server as a AAA client of Cisco Secure ACS. See [Adding Devices as AAA Clients Without NDGs, page 2-25](#).

Step 8 Select the **Register all installed applications with ACS** check box to register Security Manager and any other installed applications with Cisco Secure ACS.

Step 9 Click **Apply** to save your settings. A progress bar displays the progress of the registration. A message is displayed when registration is complete.

Step 10 Restart the Cisco Security Manager Daemon Manager service. See [Restarting the Daemon Manager, page 2-33](#).

- Step 11** Log back in to Cisco Secure ACS to assign roles to each user group. See [Assigning Roles to User Groups in Cisco Secure ACS, page 2-33](#).
-

Restarting the Daemon Manager

This procedure describes how to restart the Daemon Manager of the Security Manager server. You must do this so the AAA settings that you configured take effect. You can then log back in to CiscoWorks using the credentials defined in Cisco Secure ACS.

Related Topics

- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)
- [ACS Integration Requirements, page 2-22](#)

Procedure

- Step 1** Log in to the machine on which the Security Manager server is installed.
- Step 2** Select **Start > Programs > Administrative Tools > Services** to open the Services window.
- Step 3** From the list of services displayed in the right pane, select **Cisco Security Manager Daemon Manager**.
- Step 4** Click the **Restart Service** button on the toolbar.
- Step 5** Continue with [Assigning Roles to User Groups in Cisco Secure ACS, page 2-33](#).
-

Assigning Roles to User Groups in Cisco Secure ACS

After you have registered CiscoWorks, Security Manager and other installed applications to Cisco Secure ACS, you can assign roles to each of the user groups that you previously configured in Cisco Secure ACS. These roles determine the actions that the users in each group are permitted to perform in Security Manager.

The procedure for assigning roles to user groups depends on whether NDGs are being used:

- [Assigning Roles to User Groups Without NDGs, page 2-33](#)
- [Associating NDGs and Roles with User Groups, page 2-34](#)

Assigning Roles to User Groups Without NDGs

This procedure describes how to assign the default roles to user groups when NDGs have not been defined. For more information, see [Cisco Secure ACS Default Roles, page 2-18](#).

Before You Begin

- Create a user group for each default role. See [Defining Users and User Groups in Cisco Secure ACS, page 2-24](#).
- Complete the procedures described in these topics:
 - [Integration Procedures Performed in Cisco Secure ACS, page 2-23](#)

- [Integration Procedures Performed in CiscoWorks, page 2-30](#)

Related Topics

- [Understanding CiscoWorks Roles, page 2-16](#)
- [Understanding Cisco Secure ACS Roles, page 2-18](#)

Procedure

-
- Step 1** Log in to Cisco Secure ACS.
- Step 2** Click **Group Setup** on the navigation bar.
- Step 3** Select the user group for system administrators from the list (see [Defining Users and User Groups in Cisco Secure ACS, page 2-24](#)), then click **Edit Settings**.



Tip You can rename the groups with a more meaningful name to make it easier to identify the correct groups. Select a group and click **Rename Group** to change the name.

- Step 4** Assign the system administrator role to this group:
- Scroll down to the CiscoWorks area under TACACS+ Settings.
 - Select the first **Assign** option, then select **System Administrator** from the list of CiscoWorks roles.
 - Scroll down to the Cisco Security Manager Shared Services area.
 - Select the first **Assign** option, then select **System Administrator** from the list of Cisco Secure ACS roles.
 - Click **Submit** to save the group settings.
- Step 5** Repeat the process for the remaining roles, assigning each role to the appropriate user group.
- When selecting the Security Approver or Security Administrator roles in Cisco Secure ACS, we recommend selecting Network Administrator as the closest equivalent CiscoWorks role.
- For more information about customizing the default roles in ACS, see [Customizing Cisco Secure ACS Roles, page 2-19](#).
-

Associating NDGs and Roles with User Groups

When you associate NDGs with roles for use in Security Manager, you must create definitions in two places on the Group Setup page:

- CiscoWorks area
- Cisco Security Manager area

The definitions in each area should match as closely as possible. When associating custom roles or ACS roles that do not exist in CiscoWorks Common Services, try to define as close an equivalent as possible based on the permissions assigned to that role.

You must create associations for each user group that will be used with Security Manager. For example, if you have a user group containing support personnel for the Western region, you can select that user group, then associate the NDG containing the devices in that region with the Help Desk role.

Before You Begin

Activate the NDG feature and create NDGs. See [Configuring Network Device Groups for Use in Security Manager, page 2-26](#).

Related Topics

- [ACS Integration Requirements, page 2-22](#)
- [Procedural Overview for Initial Cisco Secure ACS Setup, page 2-22](#)

Procedure

Step 1 Click **Group Setup** on the navigation bar.

Step 2 Select a user group from the Group list, then click **Edit Settings**.



Tip You can rename the groups with a more meaningful name to make it easier to identify the correct groups. Select a group and click **Rename Group** to change the name.

Step 3 Map NDGs and roles for use in CiscoWorks:

- a. On the Group Setup page, scroll down to the CiscoWorks area under TACACS+ Settings.
- b. Select **Assign a Ciscoworks on a per Network Device Group Basis**.
- c. Select an NDG from the Device Group list.
- d. Select the role to which this NDG should be associated from the second list.
- e. Click **Add Association**. The association appears in the Device Group box.
- f. Repeat the process to create additional associations.

To remove an association, select it from the Device Group, then click **Remove Association**.

Step 4 Scroll down to the Cisco Security Manager area and create associations that match as closely as possible the associations defined in the previous step.



Note When selecting the Security Approver or Security Administrator roles in Cisco Secure ACS, we recommend selecting Network Administrator as the closest equivalent CiscoWorks role.

Step 5 Click **Submit** to save your settings.

Step 6 Repeat the process to define NDGs for the remaining user groups.

Step 7 To save the associations that you have created, click **Submit + Restart**.

For more information about customizing the default roles in ACS, see [Customizing Cisco Secure ACS Roles, page 2-19](#).
