

Cisco Security Manager 3.1

Cisco® Security Manager is a leading enterprise-class application for managing network security. Cisco Security Manager delivers provisioning of firewall, VPN, and intrusion prevention system (IPS) services across Cisco routers, security appliances, and switch services modules.

Cisco Security Manager is part of the Cisco Security Management Suite, which delivers comprehensive policy administration and enforcement for the Cisco Self-Defending Network. Unlike point security products from multiple vendors, which often do not work together and can leave vulnerable gaps, the suite provides a comprehensive solution for provisioning, monitoring, mitigation, and identity to keep networks safer, more resilient, and easier to operate. The suite also includes Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) for monitoring and mitigation.

Using powerful policy-based management techniques, Cisco Security Manager excels at efficiently managing networks of all sizes. Its rich-client GUI provides superior ease of use. Cisco Security Manager provides multiple views into the application to accommodate different tasks and user experience levels, such as the device-centric view shown in Figure 1 and the map-centric view shown in Figure 2.

Figure 1. The Device-Centric View Delivers a Simplified Interface to Add Devices and Edit and Deploy Security Policies

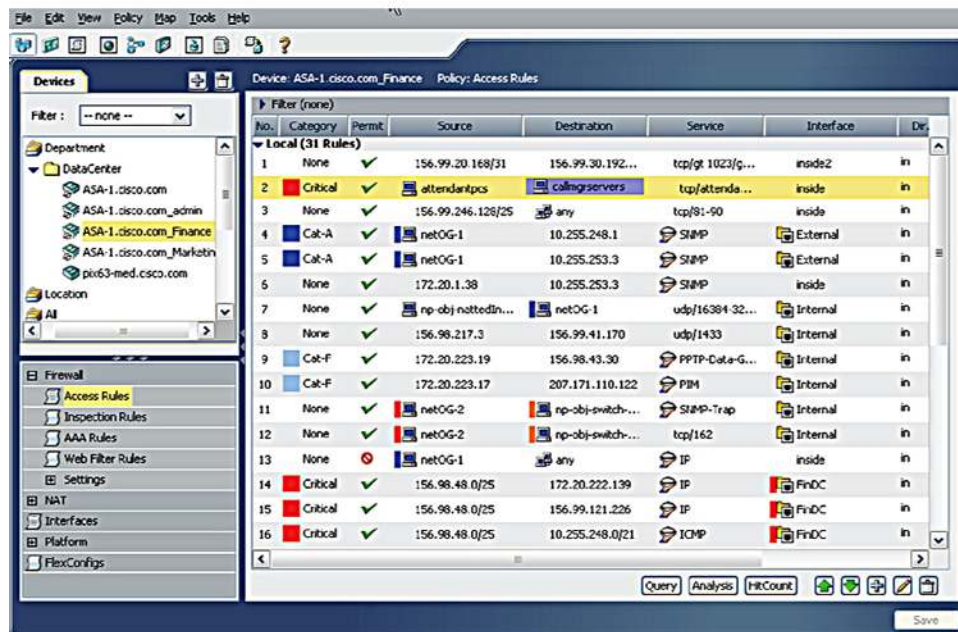
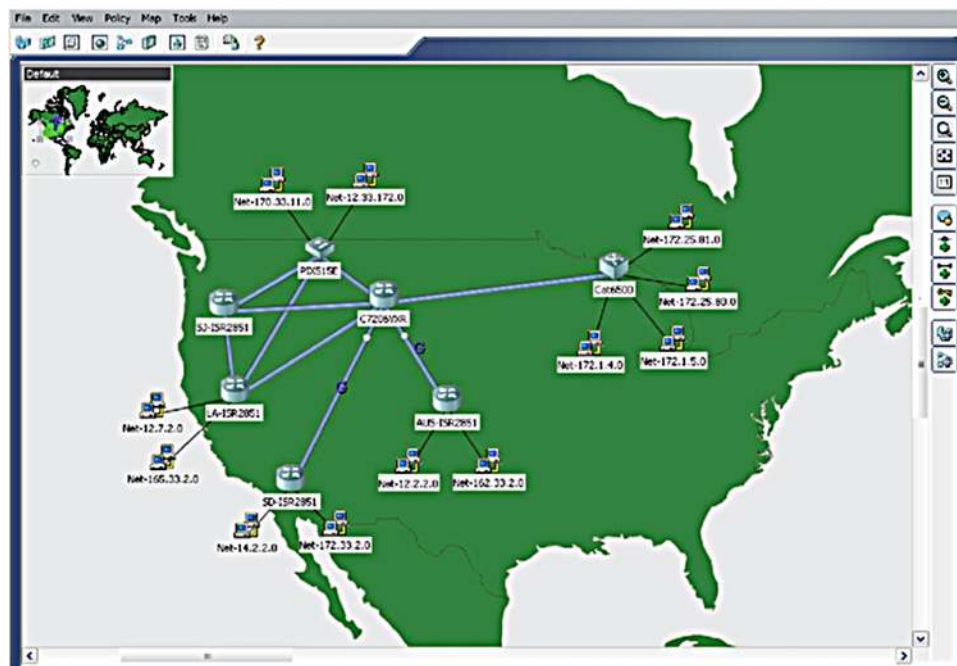
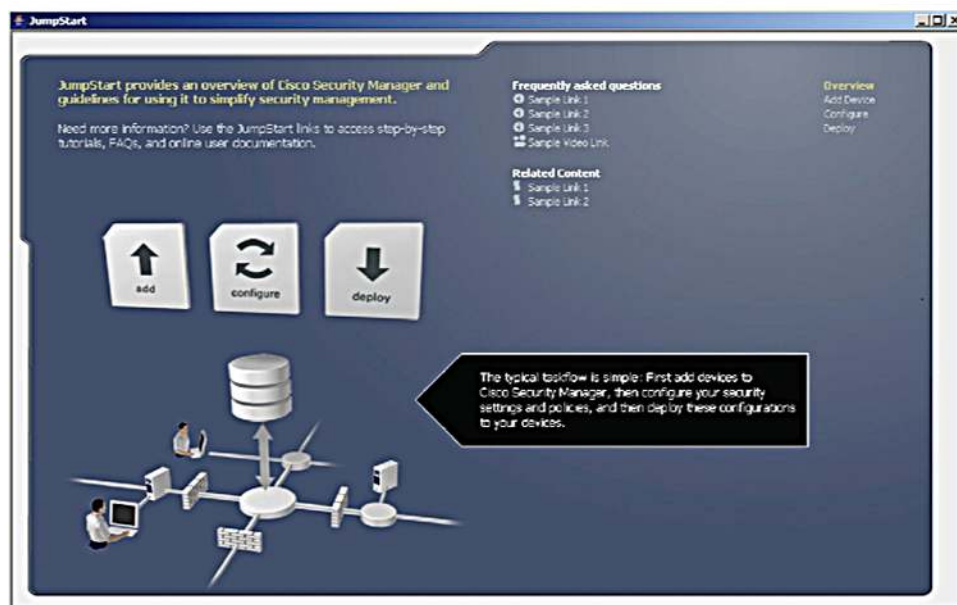


Figure 2. The Map-Centric View Allows You to Manage Policies and Devices Visually



Cisco Security Manager includes JumpStart, a built-in interactive tutorial that helps new users quickly learn about Cisco Security Manager features and concepts (Figure 3).

Figure 3. The Cisco Security Manager JumpStart Interactive Tutorial



Cisco Security Manager allows security policies to be configured per device, per device group, or globally. Security policies can be applied to Cisco ASA 5500 Series adaptive security appliances, Cisco PIX® security appliances, Cisco IPS 4200 Series sensors, Cisco Catalyst® 6500 Series services modules, and Cisco router platforms running a Cisco IOS® Software security software image.

Table 1 provides a list of features and benefits of Cisco Security Manager 3.1.

Table 1. Cisco Security Manager 3.1 Features and Benefits

Feature	Benefit
Scalable Network Management	Cisco Security Manager is suitable for efficiently managing networks that range from a few devices to thousands of devices. Scalability is achieved through powerful policy-based management techniques, which allow defining settings once and then optionally assigning the settings to individual devices, groups of devices, or across the enterprise. When a setting is changed, Cisco Security Manager automatically applies the change to all affected network devices. The firewall or VPN policies are platform-neutral, and can be applied across different device platforms such as Cisco routers, security appliances, or services modules. Cisco Security Manager also provides flexible device-level overrides; this allows policy re-use and sharing while retaining the ability to customize device-specific settings as necessary.
VPN Provisioning	<p>A VPN wizard provides easy configuration of site-to-site, hub-and-spoke, full-mesh, and extranet VPNs.</p> <ul style="list-style-type: none"> • Cisco Security Manager supports Dynamic Multipoint VPN (DMVPN) and generic routing encapsulation (GRE) IP Security (IPsec), both with dynamic IP and hierarchical certificates. • VPN and Easy VPN services can be configured remotely. • The support of secure device provisioning enables zero-touch deployment. • Configurations for automatic failover and load-balancing for headends are supported.
Firewall Provisioning	<p>Cisco Security Manager enables administrators to configure policies for Cisco ASA 5500 Series appliances, Cisco PIX appliances, Cisco Catalyst 6500 Series firewall services modules, and Cisco integrated services router platforms running a Cisco IOS Software security image.</p> <ul style="list-style-type: none"> • The software provides a single rule table for all platforms. Customers benefit from being able to manage these devices through one solution. • The rule analysis feature reports firewall rules that overlap or conflict with other rules. • The object grouping feature dramatically compresses the number of access rules required to implement a particular security policy. Object grouping uses an algorithm to group objects of a similar type so that a single access rule can apply to all objects in the group. • The software helps identify and delete rules that have no effect on the network. • The access control list (ACL) hit count feature checks to ensure traffic is flowing correctly. • The policy query feature displays which rules match a specific source, destination, and service flow, including wildcards. • To ease configuration, device information can be imported from a device repository, imported from a configuration file, or added in the software. Additionally, firewall policies can be discovered from the device itself. • Interface roles allow a user to apply a rule policy on groups of interfaces in a scalable manner.

Feature	Benefit
IPS Provisioning	<p>Cisco Security Manager enables administrators to easily and effectively manage IPS solution-based configuration and update policies for Cisco IPS 4200 Series sensors that support Cisco IPS Sensor Software Versions 5.1 and 6.0, the Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM), the Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM-2), the Cisco IDS Network Module, and Cisco IOS IPS.</p> <ul style="list-style-type: none"> • Cisco IPS Sensor Software Versions 5.1 and 6.0—The Cisco IPS solution combines an inline, intrusion prevention service with innovative technologies that improve accuracy. Cisco IPS Sensor Software accurately identifies, classifies, and stops malicious traffic, including worms, spyware and adware, network viruses, and application abuse, before it affects business continuity. • Cisco IOS IPS is an inline, deep-packet-inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. As a core facet of the Self-Defending Network, Cisco IOS IPS enables the network to defend itself with the intelligence to accurately identify, classify, and stop or block malicious or damaging traffic in real time. • Insight into Cisco IPS signature updates allows for incremental provisioning of new and updated signatures, as well as insight into Cisco Security Center (formerly MySDN) before deploying to your enterprise. This allows for immediate insight into the Cisco IPS Security Research Team's recommended defaults, and allows customers to tune their environment before distributing the signature update. • The Cisco IPS Update Wizard allows efficient automatic updates, scheduling, and distribution with status and details notification. • IPS management is fully integrated into Cisco Security Manager. This includes IPS device and policy views with context-sensitive menus, as well as content-based common IPS policies that allow the creation of enterprisewide policies that can be configured once and deployed to many. • To ease configuration, device information can be imported from a device repository, imported from a configuration file, or added in the software. Additionally, IPS policies can be discovered from the device itself. • IPS signature policies and event action filters can be inheritable and assignable to any device. All other IPS policies can be assignable and shared with other IPS devices. IPS management also includes policy rollback, a configuration archive, and cloning or creation of signatures. Copying policies between devices allows for effective management and lowers TCO by reducing deployment efforts. • IPS update administration and IPS subscription licensing updates streamline the distribution and allow users to manage IPS software, signature updates, and licensing based on local and shared policies.
Integrated Security Services Management	Cisco Security Manager enables the management of integrated security services, including quality of service (QoS) for VPN, routing, Network Admission Control (NAC), and more.
Flexible Device Grouping Options	Users can create and define device groups based on business function or location to accurately represent their organizational structure. All devices in a group can be managed as easily as a single device.
Multiple Application Views	Cisco Security Manager provides multiple views into the application to support different use cases and experience levels. The device-centric view is useful for novice users or those more familiar with using single-device managers. The map-centric view helps in visualizing the topologies of VPNs or containment relationships between Cisco Catalyst 6500 Series services modules and security contexts. The policy-centric view excels at performing highly efficient and scalable multidevice management.
Policy Object Manager	Re-usable objects can be created (for example, to represent network addresses, services, device settings, time ranges, or VPN parameters). Objects can be defined once and used any number of times to avoid manually entering values.
Deployment Manager—Flexible Deployment Options	Cisco Security Manager supports both on-demand and scheduled deployments to a device or to files.
Rollback	Cisco Security Manager provides the ability to roll back to a previous configuration, if required.
Role-Based Access Control	With Cisco Security Manager, access rights can be defined for multiple administrators, with appropriate controls. Cisco Security Manager is delivered with five user roles; additional roles are available with the optional Cisco Secure Access Control Server (ACS).
Workflow	Cisco Security Manager optionally allows assigning specific tasks to each administrator during the deployment of a policy, with formal change control and tracking. The workflow helps improve staff collaboration (for example, between network and security operations).
Distributed Deployment Methodologies—Auto Update Server, Cisco Network Services Configuration Engine	Cisco Security Manager simplifies updates to large numbers of remote firewalls, which may have dynamic addresses or Network Address Translation (NAT) addresses. This is a valuable feature for customers that have remote locations with intermittent network links and minimal technical staff at the remote site.

Feature	Benefit
Operational Management	Cisco Security Manager helps with operational functions such as software distribution or device inventory reporting. The software integrates with the Device and Credentials Repository (DCR) and CiscoWorks Resource Manager Essentials (RME).
Health and Performance Monitoring	Customers with a Cisco Security Manager service contract can download the CiscoWorks Monitoring Center for Performance application, available from Cisco.com. This application provides health and performance monitoring data for Cisco network devices and specific security services.

Changes in Cisco Security Manager 3.1

Cisco Security Manager 3.1 is an update that makes the following enhancements to Cisco Security Manager 3.0 and 3.0.1:

- Integrated IPS management
- Native, integrated Cisco Catalyst 6500 Series/Cisco 7600 Series router and VLAN ACL management
- Ability to discover site-to-site and remote-access VPNs
- Ability to discover Cisco IOS Software-based router configurations
- High availability
- Embedded read-only access to Cisco Router and Security Device Manager (SDM), Cisco Adaptive Security Device Manager (ASDM), Cisco IDS Device Manager, and Cisco IDS Event Viewer for monitoring of individual devices
- Enhanced reporting features, including device-centric policy reports and inventory reports
- Device, interface, and VPN up/down status reported in inventory report
- Detailed activity report for firewall and IDS devices
- Ability to configure Secure Sockets Layer (SSL) VPN on devices based on Cisco IOS Software and Cisco ASA Software Versions 7.1/7.2
- Cross-launch of Cisco RME Software Image Management for OS management.
- Ability to use Cisco Security Manager user login credentials to connect to devices
- Ability to use Telnet as a transport protocol to communicate with Cisco IOS Software-based devices and Cisco Catalyst 6500/7600 devices.
- Enhanced device certificate retrieval support, including bulk retrieval through CLIs
- Support following additional features on Cisco IOS Software-based devices:
 - SSL VPN
 - Additional Easy VPN features
 - Line access
 - Secure Shell (SSH) configuration
 - Local time
 - Comprehensive authentication, authorization, and accounting (AAA) support
 - HTTP server
 - Point to Point Protocol (PPP)
 - DSL/ATM
 - Domain Name System (DNS)
 - NFP (Network Foundation Protection)

- Bridging (wireless)
- Enhancements to QoS
- Authentication proxy enhancements
- Additional interface settings, such as IP redirect, IP reply, and virtual reassembly
- Additional firewall features, such as support for IM blocking, Java list, DoS settings, and voice service inspection
- Additional IPsec VPN features, such as large-scale DMVPN, AIM III
- Support for the following additional features on the Cisco Catalyst 6500 Series Firewall Services Module (FWSM3.1 and FWSM3.2):
 - More than one pair of Layer 2 interfaces
 - Simple Network Management Protocol (SNMP) v2c
 - Skinny video
 - Asymmetric routing
 - FTP authentication challenge
 - Destination NAT for multicast
 - 4000 global statements
 - Layer 2 Network and Port Address Translation (NAT/PAT)
 - TACACS+ command enhancements
 - Xlate table bypass
 - H.323 Gatekeeper Update Protocol (GUP) support
 - Cut through proxy enhancements
 - Real-Time Streaming Protocol (RTSP) PAT
- Support for the following features on Cisco ASA and PIX devices:
 - Easy VPN hardware client parity with Cisco PIX 501 and 506 Security Appliances and Cisco VPN 3002 Concentrators
 - Dual ISP support
 - PPP over Ethernet (PPPoE)
 - Home/business VLAN support
 - Enhanced auto-update support
 - Dynamic DNS
 - High availability; subsecond failover
 - Virtualization; resource manager
 - Extended use of DNS domain names
 - Generic input rate limiting
 - Multiprocessor Forwarding (MPF)-based regular expression classification map
 - N2H2 HTTPS/FTP filtering support
- Support for AIM III (IPsec/SSL VPN)
- Support for Cisco ASA 5505 Adaptive Security Appliances
- Support for legacy routers running Cisco IOS Software 12.1 and 12.2 for Layer 3 ACL management

- Support for Cisco IPS Sensor Software Versions 5.1/6.0 and Cisco IOS IPS in Cisco IOS Software Release 12.4(11)T2 and later
- Support for the following features on Cisco IPS Sensor Software 6.0-based devices:
 - Virtual sensors
 - Anomaly detection
 - Passive OS fingerprinting
 - Simplified custom signature creation
 - Signature update wizard; preview and tuning of new signatures
 - IPS signature update license management
 - External product interface (linking IPS sensor with Management Center for Cisco Security Agents)

Cisco Security Manager 3.1 also enforces the licensing key, which controls how many devices can be added in the software. If the license limit is exceeded in Version 3.0, an upgrade to Version 3.1 will prevent a new device from being added in the management software. Operators can purchase an increased license key to allow management of more devices. This does not require a re-installation of the software. Operators can use the Cisco Security Manager administrator options to easily add a new key. The licensing purchase options are listed in the product bulletin at http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html.

Table 2 lists the minimum server requirements for Cisco Security Manager. Table 3 provides the minimum client requirements.

Table 2. Server Requirements and Restrictions

Component	Minimum Requirement
System Hardware	<ul style="list-style-type: none"> • IBM PC-compatible with a 2-GHz or faster processor • Color monitor with at least 1024 x 768 resolution and a video card capable of 16-bit colors • DVD-ROM drive • 100BASE-T (100 Mbps) or faster network connection; single interface only • Keyboard • Mouse
File system	NTFS
Memory (RAM)	2 GB
System Software	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Windows 2003 Server: <ul style="list-style-type: none"> ◦ Enterprise Edition with SP1 ◦ Standard Edition with SP1 • Microsoft Windows 2000: <ul style="list-style-type: none"> ◦ Advanced Server with SP4 ◦ Server with SP4 ◦ Professional with SP4 <p>Note: Cisco Security Manager supports only the U.S. English and Japanese versions of Windows. Microsoft ODBC Driver Manager 3.510 or later is also required, so your server can work with Sybase database files.</p>
Browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 6.0 (6.0.2600) • Microsoft Internet Explorer 6.0 with SP1 (6.0.2800) • Mozilla 1.7 or 1.7.5
Compression Software	WinZip 9.0 or compatible
Hard Drive Space	20 GB

Component	Minimum Requirement
IP Address	One static IP address If the server has more than one IP address, disable all but one address. The Cisco Security Manager installer displays a warning if it detects any dynamic IP addresses on the target server. Dynamic addresses are not supported.

Table 3. Client Requirements and Restrictions

Component	Minimum Requirement
System Hardware	<ul style="list-style-type: none"> • IBM PC-compatible with a 1-GHz or faster processor • Color monitor with video card set to 24-bit color depth • Keyboard • Mouse
Memory (RAM)	1 GB
Virtual Memory/ Swap Space	512 MB
Hard Drive Space	10 GB
Operating System	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Windows XP Professional with SP1 or higher • Microsoft Windows 2003: <ul style="list-style-type: none"> ◦ Server Edition with SP1 ◦ Enterprise Edition with SP1 • Microsoft Windows 2000: <ul style="list-style-type: none"> ◦ Advanced Server with SP4 ◦ Professional with SP4 <p>Note: The Cisco Security Manager Client supports only the U.S. English and Japanese versions of Windows. It does not support any other language version.</p>
Browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 6.0 (6.0.2600) • Microsoft Internet Explorer 6.0 with SP1 (6.0.2800) • Mozilla 1.7 or 1.7.5
Java	<p>The Cisco Security Manager Client includes an embedded and completely isolated version of Java. This Java version does not interfere with your browser settings or with other Java-based applications.</p> <p>If you try to open Cisco Security Manager but do not have the required version of Java, your Cisco Security Manager server will display a message that tells you how to download and install the required Java version.</p>

For more information on Cisco Security Manager hardware and software requirements, refer to the Cisco Security Manager Installation Guide at <http://www.cisco.com/go/csmanager>.

Table 4 lists some of the device product families supported by Cisco Security Manager. For a full list, refer to the document **Supported Devices and OS Versions for Cisco Security Manager**.

This document is available at

http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Table 4. Overview of Cisco Devices Supported by Cisco Security Manager

Supported Devices
Cisco PIX Security Appliances
Cisco ASA 5500 Series Adaptive Security Appliances
Cisco Integrated Services Routers
Cisco 7600 Series Routers
Cisco 7500 Series Routers
Cisco 7300 Series Routers

Supported Devices
Cisco 7200 Series Routers
Cisco 7100 Series Routers
Cisco Catalyst 6500 Series Firewall Services Modules (FWSMs)
Cisco Catalyst 6500 Series VPN Services Modules
Cisco 7600 Series/Catalyst 6500 Series IPsec VPN Shared Port Adapters
Cisco Catalyst 6500 Series IDSM-2
Cisco IPS 4200 Series Sensors
Cisco IPS Module for Access Routers

For a list of devices supported by the optional CiscoWorks RME 4.05, view the compatibility documentation at http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html.

Ordering Information

The Cisco Security Manager product bulletin describes the licensing options and the ordering details. The bulletin is published at <http://www.cisco.com/go/csmanager>.

Cisco Services

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit <http://www.cisco.com/go/services/security>.

Cisco Security Manager software is eligible for technical support service coverage under Cisco Software Application Support (SAS). Cisco SAS service agreement features include:

- Unlimited access to the Cisco Technical Assistance Center (TAC) for award-winning support. Technical assistance is provided by Cisco software application experts who are trained in Cisco security software applications. Support is available 24 hours per day, 7 days per week, 365 days per year worldwide.
- Registered access to Cisco.com, a robust repository of application tools and technical documents to assist in diagnosing network security problems, understanding new technologies, and staying current with innovative software enhancements. Utilities, white papers, application design data sheets, configuration documents, and case management tools help expand your in-house technical capabilities.
- Access to application software bug fixes and maintenance and minor software releases.

Existing Cisco Works VPN/Security Management Solution (VMS) products covered by an active SAS or Software Application Support plus Upgrades (SASU) contract might be eligible to migrate to Cisco Security Manager.

