Cisco Application Networking Manager 1.2

Cisco® Application Networking Manager (ANM) software helps enable centralized provisioning, operations, and basic monitoring of Cisco data center networking equipment and services. Version 1.2 of Cisco ANM focuses on providing provisioning capability for Cisco Application Control Engine (ACE) devices, including ACE modules and ACE 4710 appliances. It also supports operations management and monitoring for ACE devices as well as for Cisco Content Services Switch (CSS), Cisco Content Switching Module (CSM), and Cisco Content Switching Module with SSL (CSM-S).

Product Overview

Cisco ANM helps manage multidevice data center network services effectively. Version 1.2 simplifies provisioning of the Cisco Application Control Engine virtualized environment, providing a unified interface for Cisco ACE configuration tasks. It also unifies the operations management and monitoring of real and virtual servers spanning a load-balancing infrastructure of ACE, CSS, CSM, and CSM-S devices.

Cisco ANM simplifies Cisco ACE provisioning through forms-based configuration management of Layer 4–7 virtualized network devices and services. With Cisco ANM, network managers can create, modify, and delete all virtual contexts of Cisco ACE, as well as control the allocation of resources among the virtual contexts. Within these virtual contexts, Cisco ANM helps enable complete configuration of the content networking and Secure Sockets Layer (SSL) services.

Cisco ANM facilitates rapid creation, modification, and prestaged or immediate deployment of common services by operators of all skill levels. Cisco ANM does this by including a varying set of provisioning forms for the basic, advanced, and expert user. Utilizing the basic forms, even operators new to the system can get value from their Cisco ACE systems "right out of the box" by provisioning the most common services quickly and easily (Figure 1).

Utilizing the advanced forms, a more knowledgeable user can easily exercise the more powerful features of Cisco ACE without having to master the Cisco ACE system itself. Even more advanced users can go a step beyond to Cisco ANM expert mode to implement the most intricate configurations of services while still gaining the security and error reduction afforded by performing these tasks though the Cisco ANM graphical user interface or building-block–based configuration management.

Figure 1. Cisco ANM Virtual Server Configuration
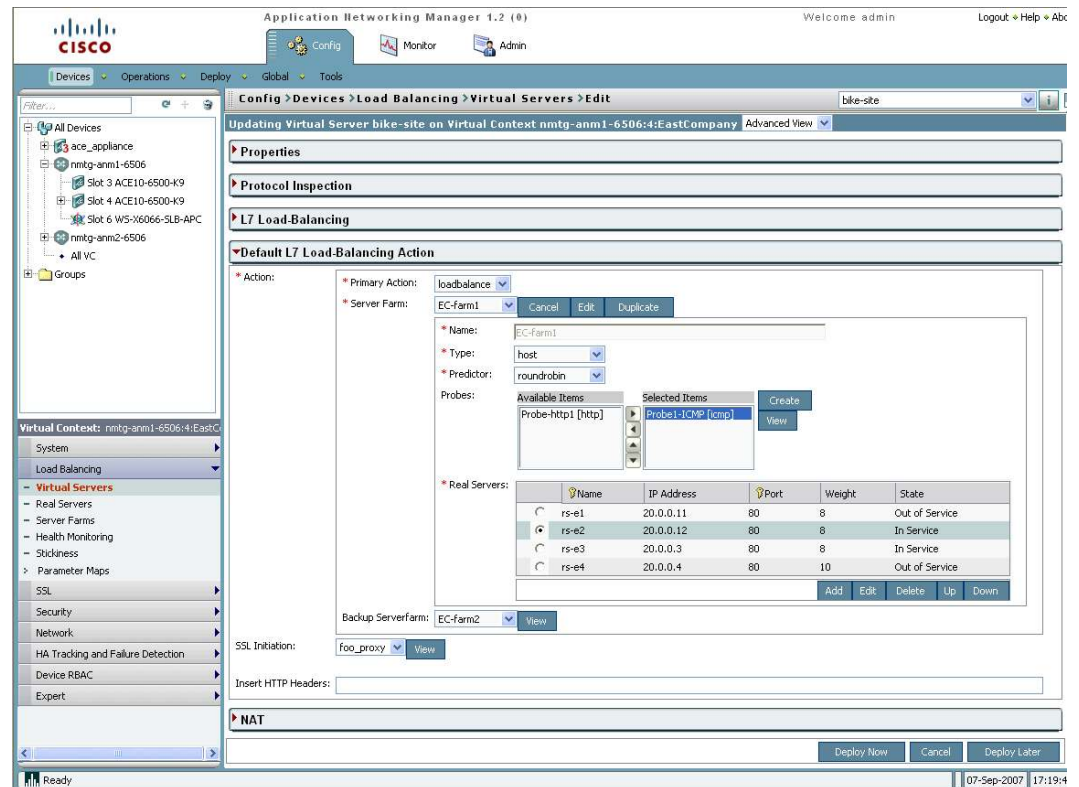
Cisco ANM provides information on the health, state, and utilization of all ANM managed devices, virtual contexts, and services that aid systems and applications managers, as well as operations staff, to help ensure availability of the services being supported by ANM managed devices, Cisco ANM 1.2 also includes the ability for operators to create user-defined threshold-crossing alerts for both device and service health, availability, and capacity monitoring for all managed devices (Figure 2).

Figure 2. Cisco ANM Monitoring Virtual Servers and Monitoring Threshold Group Creation
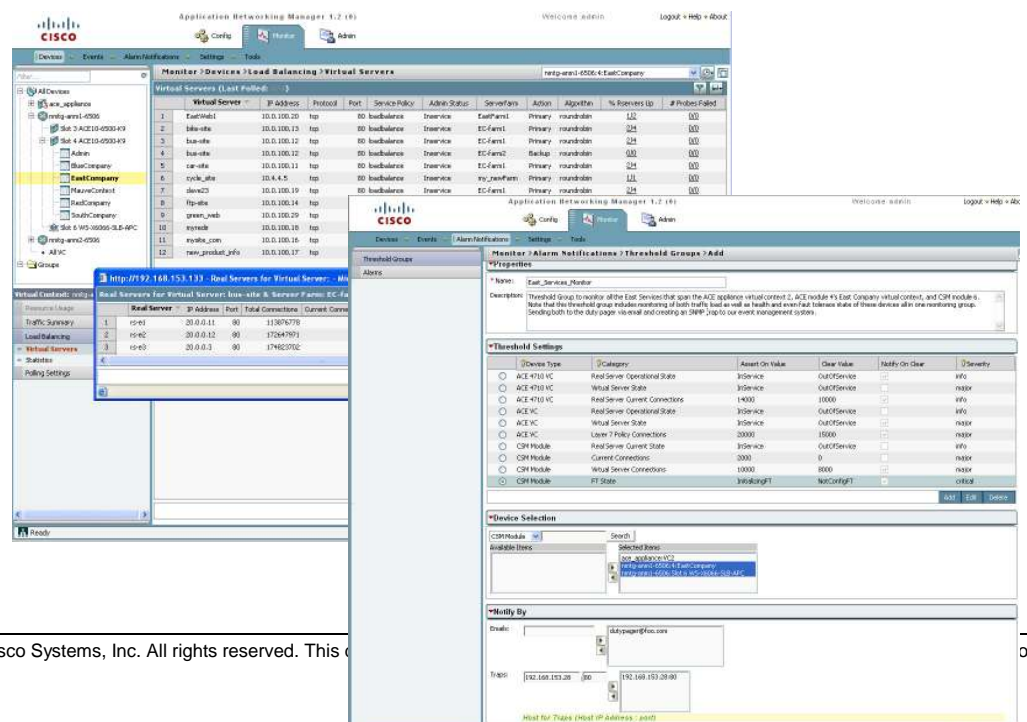
Throughout all functions, Cisco ANM uses an administrator-defined role-based access control (RBAC) security model that facilitates delegation of authority and responsibility for operations, administration, and monitoring of the managed devices, including activation and suspension of selected load-balanced servers. The Cisco ANM administrator can define with high granularity the tasks and options that are available to individual users or user groups.

By taking advantage of the ANM secure delegation capabilities, server managers can perform their daily management tasks, such as taking one or more real servers in or out of service, with options for graceful shutdown or cleared connections without needing to know the type of network device that is supporting their servers (ACE, CSS, CSM, or CSM-S), the network topology, or other network operations.

Cisco ANM is ideal for enterprises and service providers that implement Cisco ACE, as well as providing additional value to customers utilizing Cisco CSS, CSM, and CSM-S devices. These customers range from data center infrastructure providers, application service providers, and large enterprises to e-business data centers. Even small and medium-sized enterprises with small deployments of Cisco ACE can take advantage of the benefits of Cisco ANM through the entry-point offering.

Key Features and Benefits

The following sections describe the key features and benefits of Cisco. Cisco ANM's primary function is providing for the provisioning and administration of ACE devices' virtual contexts and the services implemented within those virtual contexts. It also provides a unifying operations capability for delegated server management for ACE, CSS, CSM, and CSM-S devices. These functions are supported by a granular RBAC, a secure access model, and device and service monitoring features.

Device and Service Provisioning

The introduction of virtual contexts, up to 250 per Cisco ACE, allows exceptional control of the application-delivery infrastructure. For each virtual context, administrators can tune the processing resources—such as bandwidth, connection setup rate, SSL transaction rate, or syslog rate—as well as many memory resources, such as the number of concurrent connections or access control lists (ACLs). Thus, business organizations, customers, subscribers, and applications can all share a physical Cisco ACE with complete isolation from each other.

Cisco ANM empowers multiple concurrent operators and administrators with the ability to turn on a new application or service within these virtual contexts, or modify an existing one, with a few clicks rather than going through tedious, time-consuming processes of selecting, qualifying, deploying, and troubleshooting a new device.

Cisco ANM supports robust Layer 4–7 configuration of Cisco ACE devices. To accomplish this, Cisco ANM employs forms from which users can select the features and functions to invoke for the particular service being implemented. For each feature or function selected, Cisco ANM guides the user through the configuration by presenting only the appropriate configuration selections that may

apply, offering default configuration choices as well as options for the user to customize the configuration.

These forms support configuration of virtual contexts, resource class management, and load-balancing services including ACLs, real servers, server farms, sticky groups, and health monitoring along with the service bindings to the hosting Cisco Catalyst® 6500 Series Switch and Cisco 7600 VLAN interfaces for the Cisco ACE module. The forms also support configuration of SSL services including key management, chain groups, certificate signing requests, and proxy services. Cisco ANM extends these configuration capabilities to the configuration of redundant Cisco ACE devices.

The Cisco ANM global "building-blocks" feature speeds deployment of common configuration components and supports the standardization of those configurations for devices, virtual contexts of devices, and services.

For systems established prior to the deployment of Cisco ANM, it provides the capability to discover all chassis, modules, virtual contexts, and service definitions across a large number of systems.

All of these configuration tasks can be performed using a secure Web-based GUI, eliminating the need to use the Cisco ACE command-line interface (CLI).

Operations—Delegated Server Management

Cisco ANM provides productivity gains for services and server managers by offering two operations-specific displays where they can monitor their assigned virtual and real servers. On a single screen, operators can monitor the administrative and operational state of all their servers (that is, the servers' health), as well as the number of connections active on the servers (that is, the servers' utilization).

For administrators who manage large numbers of devices, these displays include the ability to toggle on and off filters on any displayed data elements, as well as custom configuration options—a customization feature common to almost all Cisco ANM displays.

From the virtual server and real server operations displays, server managers can also perform their daily management tasks, such as taking one or more servers in and out of service, with options for graceful shutdown or cleared connections. This delegated activation and suspension of servers eliminates the need for server managers to know the network topology or operations. Since this functionality spans not only ACE devices, but also CSS, CSM, and CSM-S devices, operators need not utilize different systems or views to perform this common task.

A significant advantage to the Cisco ANM virtual server and real server operations displays, as with all features in Cisco ANM, is that RBAC can be used to securely delegate access to view or modify operations of any virtual or real servers.

Granular RBAC and Secure Access

A granular user access model, RBAC, is used to administratively grant user authorization to access network resources such as virtual contexts of Cisco ACE modules, content networking and load balancing, and SSL services, as well as individual application services. This removes unnecessary overhead between network administrators, network operations center (NOC) staff, systems operators, and server managers, which allows faster service deployment, simplifies workflow within IT, and reduces configuration errors.

RBAC allows each virtual context in Cisco ACE to be managed by the appropriate business or IT team. Using Cisco ANM, an unlimited number of administratively defined domains can be created within each virtual context, providing further granularity for controlling resources within that virtual context or spanning multiple virtual contexts. Similarly, Cisco ANM administrators can define and assign user roles that specify which of 32 defined actions a user can take against the network resources they can reach, such as configuration creation, editing, and modification, or device and service monitoring. A set of predefined roles is provided with the product to speed implementation and provide examples that administrators can tailor to their specific needs.

Used in combination, these domains and roles make it possible to control access and allow tasks based on application, business organization, or user. For example, network managers can be allowed to configure all operations variables while the application and server owners can be allowed only to monitor, report on, and take specific virtual servers in or out of service for maintenance without risk to other IT configurations.

All user access to Cisco ANM is secured. Between the user's Web browser and the Cisco ANM server, 128-bit full encryption Secure Sockets Layer 2 (SSL2) is used so that authorized users can monitor, activate, and configure Layer 4–7 services remotely, even through firewalls.

During login to Cisco ANM, users are authenticated either by local accounts created on Cisco ANM or (preferably) by TACACS+ or RADIUS remote authentication. Also by taking advantage of the "Organizations" concept in ANM, the administrator may segment the managed devices and services into a set of organizations based on the user's affiliations to company, business unit, division, or work group or other security relationship. Separate remote authentication servers can be utilized for of each defined organization, thus facilitating segmentation even of administration of secure access. For many enterprise organizations, this feature adds much desired flexibility; for many managed hosting providers, this feature is a core requirement to be able to offer fully "hard walled," secure services across shared tenancy clients.

Monitoring

Cisco ANM provides a series of health and performance monitoring displays of the managed device infrastructure, saving time and resources in daily operations while also aiding in troubleshooting and problem resolution.

Monitoring provides a system view, traffic summary, resource usage view, Virtual IP (VIP) address, service path, load-balancing statistics, and application acceleration views. These views are available for each virtual context (for ACE) as well as at the device group level. Monitoring views are supported for ACE, CSS, CSM, and CSM-S devices. In the same manner, the chassis management display shows device status along with the model and Cisco IOS® Software version data for the hosting Cisco Catalyst 6500 Series and Cisco 7600 chassis.

User-definable threshold-crossing alerts can be set that span multiple devices and virtual services, so that health, availability, fault tolerant status, utilization, and resource capacity can be monitored with both crossing and clearing notifications generated through Simple Network Management Protocol (SNMP) traps, e-mail, or both.

Product Specifications

Table 1 lists the product specifications for Cisco Application Networking Manager 1.2.

Table 1.   Product Specifications

Product Parameter	Specification
Product compatibility	Cisco ACE Service Module (both ACE10-6500-K9 and ACE20-MOD-K9) installed in Cisco Catalyst 6500 Series Switches and Cisco 7600 Routers, Cisco ACE 4710 appliance, Cisco Content Services Switch, Cisco Content Switching Module, and Cisco Content Switching Module with SSL as specified in Supported Devices Table for the Cisco Application Networking Manager 1.2
Protocols	For Web client: • HTTP or HTTPS For communication to Cisco ACE module: • HTTPS/Secure Shell (SSH) Protocol version 2/XML (read and write) • SNMPv2c (read-only) • Syslog over User Datagram Protocol (UDP) or TCP (inbound notifications only) For communication to chassis (Catalyst 6500/Cisco 7600) and CSM/CSM-S: • SSH version 2 and Telnet (read and write) • SNMPv2c (read-only) • Syslog over UDP (inbound notifications only) For communication to CSS: • Telnet (read and write) • SNMPv2c (read-only) • Syslog over UDP (inbound notifications only) For details refer to Supported Devices Table for the Cisco Application Networking Manager 1.2.
Reliability and availability	ANM high availability is a configuration option for implementing Cisco ANM servers in a highly available, active/standby mode. In this configuration, the active Cisco ANM server maintains a stateful synchronization with the standby Cisco ANM server so that if the active server fails, or an administrative action "failover" occurs, the standby server can seamlessly take over operations.

System Capacity

Cisco ANM 1.2 is designed for a single ANM server to support up to 50 Cisco ACE devices, 25 Catalyst 6500 Switch or 7600 Series Router chassis, and 40 CSS, CSM, or CSM-S devices for delegated activation or suspension of real and virtual servers with monitoring. The exact number of modules supported depends upon the scale of operations on each module as weighted by the number of virtual contexts per module and the number of configured components and services within each virtual context (servers, server farms, health monitoring probes, and complexity of service configurations).

Up to 25 simultaneous users can be logged in to an ANM server to perform provisioning, operations, and monitoring tasks.

Features

Cisco ANM 1.2 provides facilities for device and service discovery, provisioning, operations, and monitoring, in addition to global features. Cisco ANM 1.2 features include:

Discovery and device management

- IP/network discovery (ping sweep, IP range)
- Credential discovery (SSH, TACACS, SNMP)
- Layer 2 and 3 connectivity
- Chassis and module discovery (physical/inventory, logical)
- Device import through add/delete operation
- Management of device access credentials

Provisioning

- Virtual context administration and resource assignment

- Forms-based configuration (server load balancing, application acceleration, SSL, security, and Cisco Catalyst 6500 Series Switch and Cisco 7600 connectivity)
- Service activation and suspension
- Monitoring
- Monitoring of health, utilization, and performance of virtual contexts and services
- Monitoring through syslog, trap, SNMP, and CLI polling
- Threshold-crossing alerts (to alerts page and external notification through traps, e-mail, or both)
- Monitoring of alarms and events (to monitoring and notifications pages)

Global

- RBAC role and domain support
- Debugging tool: Simple creation of a system "Lifeline," a single file snapshot of running Cisco ANM system and devices
- System failover support and high availability
- System backup and restore

System Requirements

Table 2 lists the system requirements for Cisco Application Networking Manager.

Table 2. System Requirements

Description	Specification
Server hardware requirements	• Generic PC • Equivalent of 3 GHz Pentium III CPU performance (dual processors or dual-core CPUs are supported) • 2 GB of RAM • 60 GB minimum, 80 GB+ recommended hard drive/fixed storage • CD-ROM drive • One 100-Mbps Ethernet interface for single Cisco ANM configuration, two full-duplex interfaces for Cisco ANM high-availability configuration
Server software requirements	Server OS requirements: • Red Hat Enterprise Linux AS 4 Update 2 or 5 (4.2 or 4.5) 32-bit Server Edition (Linux 2.6 Kernel) **Note:** Cisco Application Networking Manager 1.2 does not support the 64-bit version of Red Hat Linux Enterprise AS 4 Update 2 or 5.
Client hardware requirements	As specified in Supported Devices Table for the Cisco Application Networking Manager 1.2
Client software requirements	As specified in Supported Devices Table for the Cisco Application Networking Manager 1.2

Ordering Information

To place an order, visit the [Cisco Ordering Homepage](#). Table 3 lists ordering information.

Table 3. Ordering Information

Part Number	Product Description
ANM-SERVER-12-K9	ANM Server Software
ANM-AD-005	ANM License For 5 ACE Devices
ANM-AD-010	ANM License For 10 ACE Devices
ANM-AD-020	ANM License For 20 ACE Devices
ANM-AD-050	ANM License For 50 ACE Devices

ANM-AV-020	ANM License For 20 VC On One ACE Device
ANM-AV-050	ANM License For 50 VC On One ACE Device
ANM-AV-100	ANM License For 100 VC On One ACE Device
ANM-AV-250	ANM License For 250 VC On One ACE Device
ANM-CD-010	ANM License For 10 CSS, CSM, or CSM-S Devices
ANM-CD-040	ANM License For 40 CSS, CSM, or CSM-S Devices
ANM-AV-UP1=	Upgrade ANM License – AV-020 To AV-050
ANM-AV-UP2=	Upgrade ANM License – AV-050 To AV-100
ANM-AV-UP3=	Upgrade ANM License – AV-100 To AV-250
ANM-SERVER-12-H-K9	ANM HA Server Software
ANM-AD-005-H	ANM HA License For 5 ACE Devices
ANM-AD-010-H	ANM HA License For 10 ACE Devices
ANM-AD-020-H	ANM HA License For 20 ACE Devices
ANM-AD-050-H	ANM HA License For 50 ACE Devices
ANM-AV-020-H	ANM HA License For 20 VC On One ACE Device
ANM-AV-050-H	ANM HA License For 50 VC On One ACE Device
ANM-AV-100-H	ANM HA License For 100 VC On One ACE Device
ANM-AV-250-H	ANM HA License For 250 VC On One ACE Device
ANM-CD-010-H	ANM HA License For 10 CSS, CSM, or CSM-S Devices
ANM-CD-040-H	ANM HA License For 40 CSS, CSM, or CSM-S Devices
ANM-AV-UP1-H=	Upgrade ANM HA License – AV-020 To AV-050
ANM-AV-UP2-H=	Upgrade ANM HA License – AV-050 To AV-100
ANM-AV-UP3-H=	Upgrade ANM HA License – AV-100 To AV-250

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique 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 the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about Cisco Application Networking Manager, visit

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C78-440408-00 11/07