



## DATA SHEET

# CISCOVERKS VPN/SECURITY MANAGEMENT SOLUTION 2.3

## PRODUCT OVERVIEW

CiscoWorks VPN/Security Management Solution (VMS) is an integral part of the SAFE Blueprint from Cisco® and the flagship integrated security management solution from Cisco Systems®. It combines Web-based tools for configuring, monitoring, and troubleshooting:

- VPNs
- Firewalls
- Network Intrusion Prevention Systems (IPSs)
- Host-based Intrusion Prevention Systems (IPSs)
- Router-based IPSs

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments by helping to protect productivity gains and reduce operating costs. Unlike point security products from multiple vendors that can leave vulnerable gaps, CiscoWorks VMS provides a comprehensive solution that ties separate security and VPN technologies into a single secure network.

Today's business challenges require more than the ability to support numerous devices. Many customers have limited staffing, yet must manage several different types of security devices. They must manage the security and network infrastructure, frequently update remote devices, implement change control and auditing, enhance security without adding more staff, deploy remote-access VPNs to employees, and monitor the VPN service.

CiscoWorks VMS enables customers to deploy security infrastructures from small to large environments, using the following powerful features:

- Integrated management
  - CiscoWorks VMS manages both the security infrastructure and the network infrastructure. CiscoWorks VMS delivers integrated monitoring of Cisco firewalls, Cisco IOS® Software, network-based IPSs, and host-based IPSs, along with event correlation. Customers benefit from being able to manage these components through one solution.
- Scalable foundation
  - CiscoWorks VMS implements a foundation that makes it easy to scale management to many devices. CiscoWorks VMS provides users with a consistent GUI to reduce learning time, workflow to allow multiple administrators to work together and coordinate tasks, access control server (ACS) integration to precisely control access, support for Windows and Solaris platforms, use of a robust database engine, a new simplified installation, and more. A feature of this foundation is the Auto Update feature, which allows numerous devices to be updated easily and quickly. Auto Update enables devices, even remote and dynamically addressed devices, to periodically "call home" to an update server and pull the most current security configurations or Cisco PIX® operating system

- Auto Update is required to effectively scale remote-office firewall deployments across intermittent links or dynamic addresses. Prior policy updating methods relied on a “push” model. Although this model works for known devices, it does not work for remote devices with unknown addresses or devices that are not always active. Without Auto Update, a manual process is required to update each remote device. The Auto Update feature provides a dramatic scalability improvement for organizations that want to deploy devices with many remote and local locations.
- Consistent implementation of corporate security policy
  - CiscoWorks VMS enables organizations to easily implement corporate security policies across several locations. For example, the Smart Rules feature allows an administrator to define a device group for the New York sales office and deploy that same policy to all other sales offices quickly and consistently worldwide. The solution includes workflow processes for generating, approving, and deploying configurations. This can help organizations delegate tasks to different administrators while still functioning as a team. It is particularly important for customers who have separate groups for network and security operations. An audit of the changes can be maintained.
- Centralized role-based access control (RBAC)
  - CiscoWorks VMS allows RBAC and enables groups to have different access rights across different devices and applications, providing precise and secure control.

### **New Features in Version 2.3**

The management functions for firewalls, Network IPS, Cisco security agents, VPNs, security monitoring, and performance monitoring have been updated with new features and usability improvements such as streamlined installation. Management support for router-based IPS signatures has been added to extend security to the network infrastructure.

These details are listed in individual datasheets, available at: <http://www.cisco.com/go/vms>.

### **Features and Benefits**

CiscoWorks VMS is launched from the CiscoWorks dashboard and is organized into several functional areas:

- Firewall management
- Auto Update Server
- Network IPS and router-based IPS management
- Cisco Security Agent management
- VPN management
- Security monitoring
- Performance monitoring
- Operational management

The key functions of CiscoWorks VMS are outlined in Table 1. Further details on each function can viewed at: <http://www.cisco.com/go/vms>.

**Table 1.** Coverage of Functions in CiscoWorks VMS

| Function   | Description  |
|--|--|
| <b>Firewall Management</b>                               | <ul style="list-style-type: none"> <li>• CiscoWorks VMS provides coverage for centralized management of Cisco firewalls. Using Smart Rules, a user can configure a common rule (such as allowing all HTTP traffic) one time and can apply this rule globally to all firewalls. The software supports an extensive list of device settings, all of which can be defined globally and inherited by all applicable firewalls.</li> </ul>  |
| <b>Auto Update Server for Firewall Management</b>        | <ul style="list-style-type: none"> <li>• CiscoWorks VMS allows Cisco firewalls periodically and automatically to contact the update server for any security configuration, Cisco PIX operating system and Cisco PIX Device Manager updates.</li> </ul>   |
| <b>Network-Based IPS and Router-Based IPS Management</b> | <ul style="list-style-type: none"> <li>• Administrators can use CiscoWorks VMS to configure network IPS and router-based IPS. Many sensors can be configured quickly using group profiles. Additionally, a powerful signature management feature is included to increase the accuracy and specificity of detection.</li> <li>• Improvements include dramatically improved configuration deployment times and a real-time progress bar to track deployments and signature updates. Hierarchical configuration is now available for signatures, allowing group and global policy changes with minimal keystrokes.</li> </ul>   |
| <b>Cisco Security Agent Management</b>                   | <ul style="list-style-type: none"> <li>• CiscoWorks VMS delivers management for Cisco security agents that protect servers and desktops, also known as “endpoints”. Cisco Security Agent technology goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. The management solution is scalable to thousands of agents to support large enterprise deployments.</li> </ul>  |
| <b>VPN Router Management</b>                             | <ul style="list-style-type: none"> <li>• CiscoWorks VMS includes functions for the setup and maintenance of large deployments of VPN connections and provides users with a point-and-click interface for setting up and deploying connections. This component is intended for scalable configuration of site-to-site VPN connections in a hub-and-spoke topology for centralized, multidevice configuration and deployment of Internet Key Exchange (IKE) and IP Security (IPSec) tunneling policies on VPN routers.</li> </ul>  |
| <b>Security Monitoring</b>                               | <ul style="list-style-type: none"> <li>• CiscoWorks VMS provides integrated monitoring to minimize the number of security monitoring consoles required.</li> <li>• The software increases the accuracy of threat detection, lowers the operational costs for event monitoring, The software delivers event correlation to identify attacks that are not easily recognizable from a single event, a flexible notification scheme, and automated responses to critical events.</li> <li>• CiscoWorks VMS offers a Security Device Event Exchange (SDEE) server through which other management systems may retrieve security events. Sustained event throughput performance has been improved significantly.</li> </ul> |
| <b>Performance Monitoring</b>                            | <ul style="list-style-type: none"> <li>• CiscoWorks VMS provides improved functions for monitoring and troubleshooting the performance of services that contribute to enterprise network security. The software enables users, without requiring expertise with IPSec or other security technologies, to increase service availability by isolating and troubleshooting significant events in their networks as they occur.</li> </ul>   |

| Function               | Description   |
|------------------------|---|
| Operational Management | <ul style="list-style-type: none"> <li>• CiscoWorks VMS provides the operational management for the network, allowing network managers to quickly build a complete network inventory and monitor and report on hardware, software, configuration, and inventory changes. CiscoWorks Resource Manager Essentials 3.5 is the operational management component of CiscoWorks VMS.</li> </ul> |

Table 2 lists the minimum hardware requirements for CiscoWorks VMS. The CiscoWorks VMS deployment guide documentation lists recommended guidelines for hardware based on different deployment sizes which are often higher than the minimum.

**Table 2.** System Requirements

| Hardware and Operating System Support  | Requirement   |
|--|---|
| Server Hardware (minimum requirements) | <p>CiscoWorks VMS requires one of these servers:</p> <ul style="list-style-type: none"> <li>• PC with 1 GHz or faster Pentium processor</li> <li>• Sun UltraSPARC 60 MP with 440 MHz or faster processor</li> <li>• Sun UltraSPARC III</li> </ul> <p>Server hardware needs to be equipped with at least these attributes:</p> <ul style="list-style-type: none"> <li>• CD-ROM drive</li> <li>• 100BASE-T or faster connection</li> <li>• 1 GB RAM</li> <li>• 9 GB available disk drive space</li> <li>• 2 GB virtual memory</li> <li>• Color monitor with video card capable of 16-bit color</li> </ul> |
| Server Operating System                | <p>CiscoWorks VMS requires one of these operating systems:</p> <ul style="list-style-type: none"> <li>• Windows 2000 Professional, Server, and Advanced Server (Service Pack 4). Supported on US English and Japanese operating systems.</li> </ul> <p><b>Note:</b> Support for Advanced Server requires that Terminal Services be uninstalled.</p> <ul style="list-style-type: none"> <li>• Sun Solaris 2.8 with selected patches listed in the Quick Start Guide documentation</li> </ul>   |

|                            |   |
|----------------------------|---|
| <b>Client Requirements</b> | <p><b>Client Hardware</b></p> <ul style="list-style-type: none"> <li>• PC with 300 MHz or faster Pentium processor</li> </ul> <p><b>Client Operating System</b></p> <ul style="list-style-type: none"> <li>• Windows 2000 Server, Professional Edition with Service Pack 4, or Windows XP with Service Pack 2</li> </ul> <p><b>Client Browser</b></p> <ul style="list-style-type: none"> <li>• All CiscoWorks VMS components support Internet Explorer 6 with Service Pack 1 and Netscape Navigator 7.1 on Windows platforms</li> </ul> |
|----------------------------|---|

## ORDERING INFORMATION

CiscoWorks VMS is available for purchase through regular Cisco sales and distribution channels worldwide. To place an order, visit the [Cisco Ordering Home Page](#).

CiscoWorks VMS licensing options are described in the CiscoWorks VMS product bulletin, available at:

<http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html>

## 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](#).

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based, 24-hour access to the Cisco Technical Assistance Center (TAC), full [Cisco.com](#) privileges, and software maintenance updates. A Cisco SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

## FOR MORE INFORMATION

For more information about the CiscoWorks VPN/Security Management Solution, visit: <http://www.cisco.com/go/vms>, contact your local account representative, or send e-mail to: [ciscoworks@cisco.com](mailto:ciscoworks@cisco.com).



#### **Corporate 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: 408 526-4100

#### **European Headquarters**

Cisco Systems International  
BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

#### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

#### **Asia Pacific Headquarters**

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R) KW/LW9004 08/05