



Data Sheet

Cisco Security Auditor 1.0

The Cisco Security Auditor software enables customers to cost-effectively audit their network infrastructure against corporate security policies and industry best practices.

Product Overview

Cisco® Security Auditor is part of the Cisco overall security management portfolio. Cisco Security Auditor focuses specifically on the problem of determining whether Cisco network devices have been configured in accordance with defined security policies. Demands from new legislation and industry requirements concerning protection of sensitive data and accountability have heightened the need for security compliance auditing. Cisco Security Auditor provides new levels of security assurance by enabling the cost-effective auditing of Cisco network devices against defined security policies and industry best practices. Cisco Security Auditor is built on a scalable and flexible auditing framework that allows auditing a large number and variety of Cisco network devices.

Cisco Security Auditor allows users to select from a wide range of pre-defined best practice policies, customize those policies, and audit the network for compliance to those policies. The Cisco Security Auditor reporting framework provides a wide-variety of audit results reports which can be used to demonstrate the overall compliance of the network and also pinpoint specific issues for resolution. Cisco Security Auditor provides security improvement recommendations that simplify the process of addressing network security vulnerabilities. The automated auditing capabilities eliminate costly, time-consuming manual auditing operations for large scale networks, drastically reducing the time required to perform an audit, while also improving the accuracy and reliability of the results.

Cisco Security Auditor plays an important role in the continuous process of managing network security. Cisco Security Auditor can help define how to secure the network by selecting from the defined security policies, helps to monitor compliance to the defined security policies, and can make recommendations on how to improve network security by highlighting non-compliances and providing recommended corrective actions. In short, the use of Cisco Security Auditor can make a dramatic improvement in the security posture of the network, which results in improved protection of sensitive data and resources and improved overall network availability.

Features and Benefits

Key product features include:

- An extensive built-in library of security policies based on guidelines from the National Security Agency (NSA), SAFE Blueprints from Cisco, and the Center for Internet Security (CIS)
- Ability to import device list from various sources (for example, RME, DCR, local directory, CSV, XML, other Network Management platforms) on an on-demand or scheduled basis
- Ability to group devices into static/dynamic device groups based on device attributes
- Ability to assign a weight to a security policy to reflect its importance; both raw and weighted results reflected in audit reports
- Ability to define which specific policies to check or not check for a defined group of devices; for those policies checked, the ability to customize the policy parameters
- Ability to conduct audits online on a live network or offline using locally stored or remotely accessible configuration files

- Ability to conduct audits on demand or automatically according to a defined schedule
- A wide variety of standard reports from executive-summary graphical reports down to specific policy pass/fail results with recommended corrective actions
- Bottom 10 device report to quickly identify the devices with the poorest security policy compliance
- Bottom 10 policy report to quickly identify the security policies with the poorest compliance
- Trending reports to visualize compliance of the network over time
- Ability to export reports in PDF or CSV format

Network Device Support

Cisco Security Auditor supports auditing:

- Cisco PIX® 500 Series Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco IOS® routers
- Cisco IOS switches
- Cisco Firewall Services Module

For detailed device support information refer to the [Compatibility Information](#) on Cisco.com.

Supported Operating Systems

The Cisco Security Auditor server is supported on Microsoft Windows 2000 and 2003 and Sun Solaris 8 and 9. The Cisco Security Auditor client is Web-browser based and supported on Windows, using Internet Explorer 6.0 or Netscape Navigator 7.1. For further details refer to the [Cisco Security Auditor Installation Guide](#) for Windows or Solaris.

Ordering Information

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

Cisco Security Auditor part numbers and licensing options are described in the Cisco Security Auditor 1.0 product bulletin, viewed at: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6263/ps6383/prod_bulletin0900aecd8029d16f.html.

Service and Support

Cisco Systems® 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 Security Auditor, visit: <http://www.cisco.com/go/secauditor>, contact your local account representative, or send e-mail to: secauditor@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.**

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

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks or 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. (0502R)

KW/LW9171 08/05

