DATA SHEET

CISCO CONFIGURATION ASSURANCE SOLUTION VERSION 1.0

Cisco® Configuration Assurance Solution (CAS) increases network availability and security, helps ensure efficient application delivery, and documents compliance with important regulatory and IT governance requirements. Cisco CAS automatically performs regular, systematic audits of the production network to diagnose device misconfigurations, configuration policy violations, performance inefficiencies, and security gaps.

PRODUCT OVERVIEW

Organizations need the visibility and ability to avoid costly network and application services disruptions. The network has become a critical business resource by enabling organizations to develop and introduce new services and applications, improve productivity and accessibility, and increase business opportunities and market competitiveness. As such, organizations must plan and implement strategies that strengthen business continuity through improved network and application resilience while reducing operational expenses.

The Cisco Configuration Assurance Solution (CAS) is a vital tool for improving network availability as well as application and service continuity. The Cisco CAS examines the production IP network for a broad scope of configuration problems, including addressing and routing, protocol configurations, route maps and access control lists (ACLs), Simple Network Management Protocol (SNMP), system logging, IP quality of service (QoS), custom policies, and more. Cisco CAS intelligently processes and interprets device configurations during audits the same way that production network devices do during operation. Expert knowledge of network devices, protocols, and routing behavior enables networkwide analysis of connectivity and resiliency, unlike other tools that are limited to simple syntax checks on a single device at a time. Actionable information derived from analysis is used to facilitate automated or guided changes in the network and to meet business objectives. With Cisco CAS, network reliability increases while operating costs decrease. Cisco CAS helps users to:

- **Reduce network outages**—Detect configuration problems before they disrupt network operations. An extensive rules library provides configurable rules to analyze individual devices, groups of devices, topology, and routing information.
- **Ensure network security**—Verify that network security policies have been implemented effectively. Cisco CAS "tests" network security non-intrusively by simulating unauthorized traffic flows in a virtual model of the production network, identifying security gaps and pinpointing misconfigured nodes that block valid connectivity.
- **Verify network resiliency**—Inspect complex backup configurations across the network, diagnosing latent problems. Cisco CAS can simulate network failures to test network resiliency and predict the impact on applications, resources, and security.
- **Demonstrate regulatory compliance**—Document compliance with regulatory requirements such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Federal Information Security Management Act (FISMA), and others. Cisco CAS supports critical processes from popular IT Governance frameworks including ITIL/BS15000 and ISO 17799.
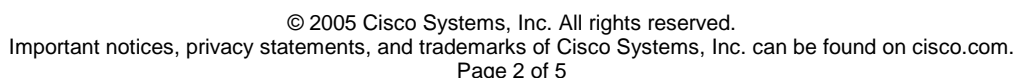
HIGH-FIDELITY NETWORK DATA MODEL

Cisco CAS includes a Virtual Network Data Server that automatically maintains a detailed, near real-time data model of the production network, including topology, configuration, and traffic. It collects and intelligently merges detailed network data from a broad range of sources, reconciling conflicts based on user-configurable priorities. Information can be obtained online from network devices including Cisco routers, Cisco Catalyst® switches, the Cisco PIX® Security Appliance, and third-party devices. Data can also be imported from CiscoWorks, Cisco Network Connectivity Center, Cisco NetFlow FlowCollector, and numerous third-party sources. The Virtual Network Data Server can integrate with event-management platforms, including Cisco Info Center, to obtain real-time awareness of configuration changes, helping ensure network data integrity.

AUDITING THE NETWORK CONFIGURATION

Cisco CAS completely automates the end-to-end workflow for network configuration audits. The operation of the core Audit and Analysis engine can be scheduled to run multiple regular audits that vary in terms of network scope, frequency, and target analyses.

Cisco CAS is provided with hundreds of standard checks that reflect industry best practices published by Cisco Systems®, U.S. government agencies, and others. Standard checks encompass:

- IP addressing and routing
- Protocol configurations, including Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Border Gateway Protocol (BGP)
- Route maps and ACLs
- Hot Standby Router Protocol (HSRP)
- SNMP, system logging, and router administration
- Firewall configurations and security protocols including authentication, authorization, and accounting (AAA), Kerberos Protocol, Network Address Translation (NAT), RADIUS and TACACS+
- VPNs, tunnels, and VLANs
- QoS and more

Rules are provided with source code, sample policy templates, and an integrated authoring environment to enable incorporation of your organization's best practices.

COMMUNICATING RESULTS

Cisco CAS automatically publishes results to an integrated Web-based Report Server, a central repository for reports encompassing documents, charts, tables, and images (Figure 1). These provide detailed results of the network audit, including informational reports summarizing network configuration characteristics such as deployed software releases and patch levels. Access can be restricted by username and password. Cisco CAS can also be configured to notify users of critical errors through e-mail or pager.

Figure 1. Network Audit Reports Generated by the Cisco CAS Report Server

SYSTEM REQUIREMENTS

Cisco CAS comprises: an Audit and Analysis engine; a Virtual Network Data Server that is generally implemented on a dual-processor platform with the prerequisite database environment; and a Web-based Report Server. The Audit and Analysis engine and Report Server can be implemented on the same (dual-processor) platform, or separate platforms per the following (Table 1).

Table 1. System Requirements

	Audit and Analysis	Virtual Network Data Server	Report Server
Disk Space	20 GB	80 GB (or larger depending on network size and data-retention practices)	60 GB (or larger depending on report-retention practices)
Hardware	3.0+ GHz Intel Pentium 4, M, or Xeon with 800-MHz front side bus (FSB)	Dual 3.0+ GHz Intel Pentium 4 or Xeon with 800-MHz FSB	1.5 GHz Intel Pentium 4 or Xeon
Memory	2 GB (Min)	4 GB (minimum)	1 GB (minimum)
Software	Only English language versions are supported: • Windows Server 2003 • Windows 2000 Server • Windows 2000 Professional	Only English language versions are supported: • Windows Server 2003 • Windows 2000 Server • Windows XP Professional • Windows 2000 Professional	Only English language versions are supported: • Windows Server 2003 • Windows 2000 Server • Windows 2000 Professional
Prerequisites (Not included with Cisco CAS 1.0)		Only English language versions are supported: • Oracle 9i Database • Oracle 9i Application Server TopLink patched to Release 9.0.3.5	

ORDERING INFORMATION

Cisco CAS 1.0 is available for purchase through regular Cisco sales and distribution channels worldwide. To place an order, visit the Cisco Ordering Home Page.

Cisco CAS 1.0 licensing options are described in the Cisco CAS 1.0 product bulletin, available at:
http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6341/ps6364/prod_bulletin0900aecd802c8487.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.

FOR MORE INFORMATION

For more information about the Cisco Configuration Assurance Solution, visit http://www.cisco.com/en/US/products/ps6364/index.html or contact your local account representative.

CISCO SYSTEMS

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