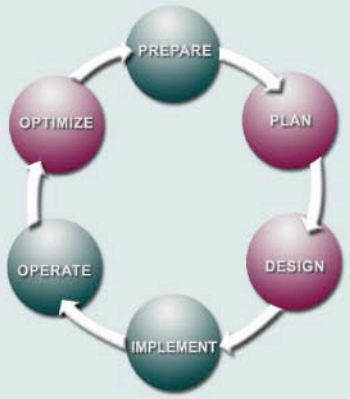
Cisco Security Unified Communications Services

Planning and Design Services to Help Ensure the Integrity, Privacy, and Availability of Cisco Unified Communications

THE CISCO LIFECYCLE SERVICES APPROACH



The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

Network Lifecycle Phases

- **Prepare**—Develop a business case for a technology investment
- **Plan**—Assess readiness to support proposed solution
- **Design**—Create a detailed design to address business and technical requirements
- **Implement**—Deploy new technology
- **Operate**—Maintain network health through day-to-day operations
- **Optimize**—Achieve operational excellence through ongoing improvements

SERVICE OVERVIEW

Many organizations have discovered that IP Communications – the convergence of data, voice, and video onto a single network – can enhance employee productivity and mobility, while dramatically reducing communication costs. But the key to attaining these advantages is the confidence that IP Communications are secure and protected from disruption.

Numerous threats, from device failures to malicious attacks, can affect the integrity, privacy, and availability of IP Communications. To increase protection, Cisco Systems® recommends an approach in which multiple layers of security are integrated throughout Cisco Unified Communications applications and systems.

As part of the plan, design, and optimize phases of the Cisco® Lifecycle Services approach, Cisco Systems offers detailed Security Unified Communications services designed for large enterprises. Through these services, Cisco consultants apply a consistent, proven methodology to the analysis of Cisco Unified Communications systems and deliver recommendations for comprehensive, system-level protection.

Through Cisco Security Unified Communications services, expert Cisco unified communications and security engineers evaluate your organization's communications security policy, the security of your Cisco Unified Communications system itself, and the underlying security embedded in your network. The consultants identify vulnerabilities and deviations from corporate security policy and industry best practices and provide you with detailed recommendations to strengthen the security of Cisco Unified Communications and avoid costly implementation delays and poor service quality.

Cisco Security Unified Communications services include the following service components:

- Cisco Unified Communications Security Policy and Procedure Review
- Cisco Unified Communications System Security Design Review
- Cisco Unified Communications Network Security Design Review
- Cisco Unified Communications Vulnerability Test

BENEFITS

With Cisco Security Unified Communications services, your organization can:

- **Mitigate Cisco Unified Communication security threats** – Identify security vulnerabilities and deviations from your corporate security policy and industry best practices

- **Improve the integrity, privacy, and availability of Cisco Unified Communications**–Recommend improvements to your communication infrastructure and systems to enable multilayer, integrated security
- **Increase your network administration and IT staff productivity** – Enable your organization to enforce consistent, efficient Cisco Unified Communications security policies and procedures
- **Lower your total cost of ownership (TCO) for Cisco Unified Communications** – Improve your IP communication system operating procedures through the consistent deployment of security controls, such as revision update processes, system configuration, and server hardening
- **Reduce your network TCO** – Extend the security capabilities already in place for data network to communication services and allow your organization to better prepare for future Cisco Unified Communications deployment initiatives

CISCO UNIFIED COMMUNICATIONS SECURITY POLICY AND PROCEDURE REVIEW

Analyzing Operational Policies and Procedures Enhance Secure, Cisco Unified Communications

Through the Cisco Unified Communications Security Policy and Procedure Review, Cisco consultants perform an in-depth review of your organization's Cisco Unified Communications security policies and operational procedures. (See Table 1.)

Table 1. Cisco Unified Communications Security Policy and Procedure Review Activities, Methodology, and Deliverable

Activities	Methodology and Deliverable
• Review security policy documentation for Cisco Unified Communications, such as access control, virus checking, incident reporting and recovery, security monitoring, and data integrity • Analyze Cisco Unified Communications operational procedures for virus protection, incident management, network backup/restore, security monitoring, and application revision procedures • Review Cisco Unified Communications and network access control procedures, including privilege management, user authentication, password protection, and remote access • Analyze organizational procedures for managing network security, including roles and responsibilities, cross-functional decision making, and change management	**Methodology** • Hold a pre-assessment meeting to gather information and initiate the review • Perform onsite information gathering • Schedule onsite vulnerability testing • Provide an onsite presentation of preliminary Cisco Unified Communications security gap analysis and findings • Present final Cisco Unified Communications security gap analysis and findings **Deliverable** The Cisco Unified Communications Security Policy and Procedure Report. This deliverable typically includes: • An executive summary of critical findings • Detailed recommendations for strengthening Cisco Unified Communications security technology, policy, and procedures

CISCO UNIFIED COMMUNICATIONS SYSTEM SECURITY DESIGN REVIEW

Helping Ensure That Cisco Unified Communications Services Are Based on a Sound System Security Design

Through the Cisco Unified Communications System Security Design Review, Cisco voice security engineers review and analyze critical Cisco Unified Communication systems, such as Cisco CallManager, Cisco IP phones, and Cisco Unity® software. The Cisco team identifies vulnerabilities and provides you with recommendations to enhance protection against unauthorized access, identity spoofing, toll fraud, and application layer threats. (See Table 2.)

Table 2. Cisco Unified Communications System Security Design Review Activities, Methodology, and Deliverable

Activities	Methodology and Deliverable
• Provide host and operating system discovery of Cisco Unified Communications systems and identify and verify deployed network services • Verify that security is in place for all deployed voice features • Review Cisco Unified Communications application server security to help ensure that server and configuration best practices are implemented • Verify that recommended antivirus software is installed and perform an antivirus configuration review • Verify that host intrusion detection is correctly tuned and configured on IP telephony, Cisco CallManager, and Cisco Unity system servers • Provide recommendations for operating system hardening, phone hardening, user authentication, intrusion detection, and secure remote access, as necessary	**Methodology** • Hold a pre-assessment meeting to gather information and initiate the review • Perform onsite information gathering • Schedule onsite vulnerability testing • Provide an onsite presentation of preliminary Cisco Unified Communications security gap analysis and findings • Present final Cisco Unified Communications security gap analysis and findings **Deliverable** The Cisco Unified Communications System Security Design Specification, which provides detailed recommendations for enhancing system security for Cisco Unified Communications applications

CISCO UNIFIED COMMUNICATIONS NETWORK SECURITY DESIGN REVIEW

Helping Ensure That the Network Security Infrastructure Protects Cisco Unified Communications Systems and Applications

Through the course of this service, Cisco network engineers perform a network security design review to identify vulnerabilities and deviations from your corporate policy and industry best practices that might compromise the security of Cisco Unified Communications. (See Table 3.)

Table 3. Cisco Unified Communications Network Security Design Review Activities, Methodology, and Deliverable

Activities	Methodology and Deliverable
• Perform a security design review of your network infrastructure that supports Cisco Unified Communications systems and applications • Analyze Cisco Unified Communications network security architecture to identify design vulnerabilities • Review voice access layer configuration to check that all security features and best practices are implemented • Perform a detailed security analysis of Cisco Unified Communications infrastructure devices and network components, including: – Voice gateways – Remote-access devices – Intrusion detection systems – Endpoint security – Firewalls – Routers and switches – Security management systems • Provide design recommendations for network topology, device placement, and connectivity improvements, including documentation of protocol, policy, and feature recommendations • Develop sample configurations for firewalls, intrusion detection systems, network admission control points, endpoint protection, routers, switches, voice gateways, VPNs, and access-control servers	**Methodology** • Hold a pre-assessment meeting to gather information and initiate the review • Perform onsite information gathering • Perform network security infrastructure analysis including device configurations • Provide an onsite presentation of preliminary Cisco Unified Communications security gap analysis and findings • Present final Cisco Unified Communications security gap analysis and findings **Deliverable** The Cisco Unified Communications Network Security Design Specification, which details recommended improvements to overall security design, feature configuration, and device integration for Cisco Unified Communications systems and applications

CISCO UNIFIED COMMUNICATIONS VULNERABILITY TEST

Identifying Security Weaknesses in the Cisco Unified Communications Infrastructure

Using advanced, specialized assessment tools, Cisco security engineers test for and exploit vulnerabilities within your Cisco Unified Communications infrastructure to identify security exposures. (See Table 4.) This vulnerability test allows your organization to assess its ability to detect and respond to threats to Cisco Unified Communications systems and to validate voice security policy and procedures.

Table 4. Cisco Unified Communications Vulnerability Test Activities, Methodology, and Deliverable

Activities	Methodology and Deliverable
• Perform an automated scan of Cisco Unified Communications systems to discover and test services • Simulate a controlled network attack to determine potential system, application, and network device vulnerabilities • Perform manual techniques to exploit and confirm identified vulnerabilities • Perform secondary exploitations, including exploitation of trust relationships between hosts and password vulnerabilities • Perform Cisco Unified Communications device configuration reviews to identify security risks • Review device administration practices, including password verification of Cisco Unified Communications infrastructure devices • Analyze and present test results and provide recommendations for architecture, policy, and configuration improvement to help prevent future exploitation	**Methodology** • Hold a pre-assessment meeting to gather information and initiate the review • Perform onsite information gathering • Perform onsite vulnerability testing • Provide an onsite presentation of preliminary Cisco Unified Communications security gap analysis and findings • Present final Cisco Unified Communications security gap analysis and findings **Deliverable** The Cisco Unified Communications Vulnerability Report, which identifies vulnerabilities and provides a recommended remediation plan

WHY CISCO

Cisco Unified Communications can unlock a world of mobility, productivity, and cost benefits for your organization – but only if your Cisco Unified Communications systems and applications are private and secure. Cisco Security Unified Communications services provide the detailed planning, assessment, and design recommendations that your business needs to maintain the integrity, privacy, and availability of Cisco Unified Communications.

AVAILABILITY AND ORDERING

Cisco Security Unified Communications services are available through Cisco and Cisco partners globally. Details may vary by region.

FOR MORE INFORMATION

For more information about Cisco Security Unified Communications services or the Cisco Lifecycle Services approach, contact your Cisco representative.

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

Printed in the USA C78-33499-00 02/06