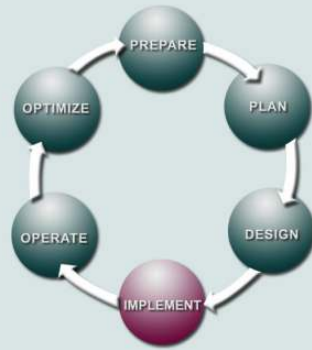


Cisco Security Network Admission Control Implementation Service

Advanced planning, design, and deployment support to help improve network resiliency through policy enforcement

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

Network security products often focus on the boundaries between “internal” and “external” users and devices. With the growing use of contractors, telecommuting, and wireless networks, the boundary between internal and external has blurred, resulting in a greater vulnerability to viruses and worms, lost productivity, and continual, reactive patching of desktops.

The Cisco® Network Admission Control (NAC) solution uses your network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. Organizations using NAC can allow network access only to compliant and trusted endpoint devices (PCs and servers, for example) and can restrict the access of noncompliant or unmanaged devices. By integrating policy enforcement and access-control capabilities throughout the network, NAC can limit exposure to devices that can compromise the security and operation of the network.

To implement NAC successfully, your organization must carefully plan, deploy, and configure NAC to work with your existing infrastructure. As part of the implement phase of the Cisco Lifecycle Services approach, the Cisco Security Network Admission Control Implementation Service, designed for large enterprises, provides expert advice from skilled Cisco security engineers to help ensure a successful Cisco NAC implementation. The service provides rigorous requirements planning, design, and implementation consulting—essential to deploying an effective NAC solution that reduces the risk of noncompliant hosts obtaining access to your network.

Decreasing the Risk of a Successful Attack

Through the Cisco Security Network Admission Control Implementation Service, Cisco security consultants help your organization deploy a NAC solution that integrates with existing network infrastructure, admission policy, endpoint security, and antivirus technologies (Table 1). Employing a consistent and proven methodology for implementing NAC, Cisco experts provide the following services to help ensure the deployment is a success:

- **NAC readiness assessment:** Cisco network engineers analyze NAC deployment requirements and assess the readiness of your organization's network devices, operations, and architecture to support the NAC solution. In addition to identifying components that do not support NAC capabilities, security engineers determine if your network topology supports a scaled deployment and deliver an impact analysis detailing requirements for redundancy, scalability, and hardware and software upgrades. Detailed requirements are provided for:
 - Appliance-based and architecture-based framework approaches to NAC
 - Endpoint security software, including Cisco Security Agent, Cisco Trust Agent, and antivirus software
 - The Cisco NAC Appliance
 - Network router and switch devices with NAC capabilities
 - Cisco Secure Access Control Server (ACS)
 - Cisco VPN 3000 Series Concentrators
- **NAC limited deployment:** Cisco network security engineers install and configure a limited deployment solution, allowing your IT staff to test and gain experience with the NAC solution. This limited deployment can be deployed in a lab, production environment such as a branch office, or for VPN users. The service includes configuration, maintenance, and support documentation for NAC components.
- **NAC design development:** Cisco consultants assist in developing a detailed design for integrating NAC into your network infrastructure. Working with your IT staff, design engineers develop the overall strategy and plan for the NAC solution, providing an in-depth analysis of the technical, procedural, and resource requirements for a corporatewide deployment. Cisco consultants also provide a design specification that defines the network topology and configuration recommendations for network access devices, Cisco Secure ACS, management software, endpoint software such as the Cisco Security Agent, and antivirus technology.
- **NAC implementation engineering:** The Cisco NAC solution must be carefully deployed, configured, and integrated into your network infrastructure, so Cisco security engineers support your team through a full-scale implementation. Cisco consultants work with your IT staff to develop detailed deployment plans, including installation, configuration, integration, and management. After the plans are completed, Cisco security engineers deliver onsite support for installation, configuration, testing, and tuning to help ensure the deployment integrates smoothly into the production environment.

Table 1. Cisco Security Network Admission Control Implementation Activities, Methodology, and Deliverables

Activities	Methodology and Deliverables
------------	------------------------------

<p>Conduct a design workshop to gather business, technical, and operational requirements</p> <ul style="list-style-type: none"> Analyze NAC deployment goals, objectives, and requirements Analyze the impact of integrating NAC with existing IT infrastructure, software operations, and security management procedures Assess your network's readiness to deploy the solution, including the current IT infrastructure, security devices, software operations, and security management procedures Jointly define the architectural, topological, and functional requirements for the solution Develop a detailed design of the system, including network diagrams and sample software configurations for protocols, policies, and features Specify hardware and software requirements, including Cisco security management tools Develop an implementation strategy and plan that details the requirements for solution deployment, integration, and management Develop the solution testing, installation, integration, management, and maintenance plans Provide support for custom installation, configuration, testing, tuning, and integration of the solution for a limited or corporatewide deployment <p>Provide staff with practical education on the operation and management of the solution</p>	<p>Methodology</p> <ul style="list-style-type: none"> Conduct a kick-off meeting to identify the business objectives for the project, introduce the implementation team, and review major implementation tasks and milestones Conduct a design workshop to gather business, technical, and operational requirements Assess network readiness to support NAC and document findings and recommendations Develop a NAC deployment plan Develop a NAC design specification Perform custom implementation, configuration, and integration of the Cisco NAC solution Document NAC operational policies, tuning, and operational procedures Deliver maintenance and support documentation Present an executive summary of the Cisco NAC implementation methodology and production deployment <p>Deliverables</p> <p>A detailed Cisco NAC Network Readiness Assessment Report with analysis, findings, and recommendations</p> <ul style="list-style-type: none"> A Cisco NAC Design Specification with detailed network diagrams and sample configurations for NAC components An optimized Cisco NAC implementation in a production environment
---	---

Benefits

With the Cisco Security Network Admission Control Implementation Service, your organization can:

- **Limit damage due to virus, worm, and spyware outbreaks:** Design and deploy a NAC implementation that helps ensure that all hosts comply with the latest corporate antivirus, endpoint security, and operating system patch policies
- **Increase the value of your network and antivirus investment:** Help ensure that the NAC solution increases the value of your investment in network infrastructure, access control, endpoint security, and antivirus technology
- **Increase your network administration and IT staff productivity:** Help enable the deployment of a systematic, integrated NAC solution that allows your IT staff to enforce host compliance policies and procedures
- **Reduce your implementation and migration times:** Avoid costly mistakes and decrease the need for expensive rework of your network infrastructure to support the new solution
- **Reduce your total cost of network ownership:** Help enable NAC capabilities and prepare for future NAC integration and deployment initiatives

Why Cisco

As the threat of network attacks continues to grow, the need for robust, consistent enforcement of network security and admission policies is critical. The Cisco Network Admission Control Implementation Service provides the expert assistance you need to rapidly and effectively deploy a Cisco NAC solution to better control network access and protect your valuable business assets. Strengthening your team's ability to meet aggressive deployment schedules while decreasing costly disruptions to your network, you can draw on Cisco expertise to design, implement, and optimize a NAC solution and better manage evolving security threats.

Availability and Ordering

The Cisco Security Network Admission Control Implementation Service is available through Cisco and Cisco partners globally. Details may vary by region.

For More Information

For more information about the Cisco Security Network Admission Control Implementation Service or the Cisco Lifecycle Services approach, contact your Cisco representative.



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, Inc.
 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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0701R)