Cisco BioMed Network Admission Control Services for a Scalable and Secure Provisioning of Network Biomedical Devices

Executive Summary

More and more biomedical devices, from patient monitors to infusion pumps, are designed for network connection. While this enables hospitals to efficiently collect and share patient and device information, it also poses security risks. When caregivers, patients, or guests access the hospital network with a variety of communication devices, it introduces an even higher level of risk. The Cisco® BioMed Network Admission Control (NAC) and Network Management System solution is an effective way for hospitals to automate the process of getting biomedical or IT devices onto the network. It isolates biomedical devices from other hosts on an IP network and protects the devices from a variety of security threats.

Challenge: Efficient, Effective Cisco BioMed NAC Deployment and Operation

Cisco NAC Services Benefits

Cisco NAC Services for Biomedical Devices help you to:

- Improve the return on your investment in converging Biomedical and IT network infrastructure.
- Protect your IT infrastructure and business from the latest threats and vulnerabilities by providing timely, targeted security intelligence
- Improve your ability to plan and budget for your network security architecture
- Address evolving business requirements and threats
- Speed deployment and reduce costly deployment mistakes
- Improve solution reliability, maintainability, and performance

As more and more medical devices are IP-enabled, medical facilities face a dilemma. Adding biomedical devices to a converged network can pose significant risks such as viruses, worms, or other malware, which can severely impact the overall network security and availability. It is essential to have a way to connect biomedical, guest, and IT devices to the IP network safely while leveraging their existing network infrastructure. This will provide secure wired or wireless network access for all devices.

The Cisco BioMed NAC solution for healthcare is an effective way for hospitals to automate the process of connecting biomedical, IT, and guest devices on the network.

To effectively deploy a converged network, a medical facility must start with developing a design that reflects your business objectives, existing network infrastructure, security policies, and unique requirements. It is then periodically reevaluated and updated to keep pace with your evolving business environment, network infrastructure, and security threats.

Solution: Services Designed to Increase Your Return on Investment

Cisco Network Admission Control Services help you increase return on your investment in your Cisco BioMed NAC solution by delivering the capabilities that Cisco security experts have identified as essential for its successful deployment, operation, and optimization.

These capabilities are delivered through three services:

- Cisco Security Planning, Design, and Implementation Service
- Cisco Security IntelliShield Alert Manager Service
- Cisco Security Optimization Service

Cisco Security Planning, Design, and Implementation Service

Reducing your BioMed NAC solution deployment cost, speeding deployment time, and getting the best possible protection are dependent on effective planning, design, and implementation. To be fully effective, the solution must be strategically planned and designed, and carefully deployed, configured, tuned, and integrated into your network infrastructure.

The Cisco Security Planning, Design, and Implementation Service helps you effectively integrate Cisco BioMed NAC and improve the quality of your solution through an iterative deployment approach that includes four service capabilities:

- **Security technology readiness assessment:** Identify gaps and recommend changes to your network infrastructure to improve the effectiveness of your Cisco BioMed NAC solution, reduce deployment costs and duration, and allow for smooth solution integration.
- **Security design development:** Better protect business assets and services, more cost-effectively deploy your new Cisco BioMed NAC solution, and avoid costly delays and disruptions during implementation with effective security design.
- **Security implementation engineering:** Improve Cisco BioMed NAC deployment efficiency, accuracy, and success with support from Cisco security engineers using an in-depth, detailed implementation process based on leading practices.
- **Security knowledge transfer and mentoring:** Prepare your staff to effectively operate, optimize, maintain, and manage your Cisco BioMed NAC solution with formal and informal training and ongoing consultation throughout the deployment project and during the stabilization period immediately following the deployment.

Benefits of Cisco Security Planning, Design, and Implementation Service

The Cisco Security Planning, Design, and Implementation Service helps you to:

- Improve the return on your investment in a Cisco BioMed NAC solution by identifying the features that will best meet your business requirements
- Deliver a multilayer defense against security threats and improve network security reliability, maintainability, and performance through world-class network security design
- More effectively mitigate network security threats by using a sound implementation methodology to successfully deploy a new Cisco BioMed NAC solution
- Keep your Cisco BioMed NAC solution operating efficiently by educating your staff on best practices

For more information about the Cisco Security Planning, Design, and Implementation Service, visit www.cisco.com/go/services/security.

Cisco Security IntelliShield Alert Manager Service

In mission-critical environments, IT security staff must take proactive steps to mitigate threats before they can affect the business. To take such steps, organizations need timely, accurate, and credible security intelligence.

The Cisco Security IntelliShield Alert Manager Service filters through the multitude of alerts from reporting organizations to provide strategic, targeted security intelligence you can use to proactively respond to potential IT threats, mitigate risk, and increase business continuity.

Features include:

- Threat information customized to your organization's networks, systems, and applications
- A rigorous verification, editing, and publishing process applied to each new threat and vulnerability report
- One of the most extensive collections of past threat and vulnerability data in the industry
- A built-in workflow tracking system that allows IT managers to monitor vulnerability remediation efforts

Benefits of Cisco IntelliShield Alert Manager Service

The Cisco Security IntelliShield Alert Manager Service helps your IT staff to:

- Protect your IT infrastructure and business from the latest threats and vulnerabilities by providing timely, targeted security intelligence
- Quickly and effectively prioritize remediation activities by delivering accurate, relevant information
- Speed vulnerability remediation by recommending safeguards, workarounds, and links to patches
- Improve vulnerability remediation management with a workflow tracking system

For more information about the Cisco Security IntelliShield Alert Manager Service, visit http://cisco.com/en/US/products/ps6834/serv_group_home.html.

Cisco Security Optimization Service

The network continuously changes as part of a business's ongoing operations and growth. After your Cisco BioMed NAC solution is fully operational, ongoing consulting with Cisco security engineers can help you to continually assess, tune, and evolve your solution and the rest of your network security infrastructure to keep pace with changes in your business and new security threats.

The Cisco Security Optimization Service delivers a flexible set of capabilities that can be customized in a subscription to meet your needs in a particular year at a predictable cost, including:

- **Security technology planning support:** Cisco can provide you with a dedicated advisor to assist you in strategic security technology planning, delivering quarterly assistance to help you effectively plan and budget for your network security architecture evolution.
- **Security architecture review:** Help keep your overall network security architecture optimized to address evolving business requirements and threats by periodically identifying measures that might be needed to keep security controls aligned with your company policy and security industry best practices.
- **Security technology readiness assessment:** As your business and secure network grow and evolve and you are preparing to deploy new security technology, Cisco security engineers can help you solidify your requirements and identify measures needed to prepare your network and systems to deploy the technology and take full advantage of its features.
- **Security design support:** Cisco can review and recommend changes to your proposed security technology design, whether for an extension of your Cisco BioMed NAC deployment or for other elements of your security infrastructure.
- **Security posture assessment:** Identify vulnerabilities that allow external untrusted systems to gain access to your internal trusted networks and recommend solutions to correct those vulnerabilities.
- **Security performance enhancement support:** Analyze security devices against configuration best practices, your corporate security policies, and your baseline configuration templates if applicable. Optimize Cisco BioMed NAC device performance and improve your staff's ability to manage the devices by leading interactive tuning sessions.
- **Security change support:** Reduce risk when making critical, scheduled changes to your network's advanced security technologies with a review of modifications to the design, implementation plan, test plan, and rollback plan for the change. Provide implementation support during change windows. Assist with recovery from network outages resulting from unplanned changes.
- **Security knowledge transfer and mentoring:** After your Cisco BioMed NAC deployment, help improve your staff's effectiveness in operating, optimizing, maintaining, and managing your solution through periodic knowledge transfer sessions.

Benefits of Cisco Security Optimization Service

The Cisco Security Optimization Service helps you to:

- Improve your ability to plan and budget for your network security architecture
- Address evolving business requirements and threats
- Speed deployment and reduce costly deployment mistakes
- Improve solution reliability, maintainability, and performance
- Reduce the risk of intentional or accidental access to IT assets and information
- Reduce risk when making changes to the network

For more information about the Cisco Security Optimization Service, visit www.cisco.com/en/US/services/ps2961/ps2952/services_data_sheet0900aecd806ea35f.pdf.

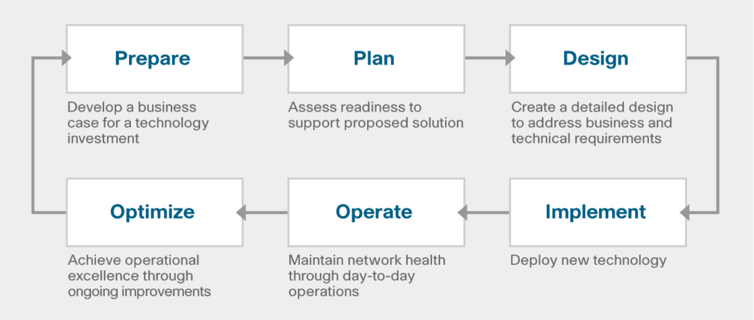
Why Cisco Services

Cisco Services make networks, applications, and the people who use them work better together.

Today, the network is a strategic platform in a world that demands better integration between people, information, and ideas. The network works better when services, together with products, create solutions aligned with business needs and opportunities.

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.

The Cisco Lifecycle Services Approach


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
Optimize
Achieve operational excellence through ongoing improvements
Operate
Maintain network health through day-to-day operations
Implement
Deploy new technology

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.

Cisco and Partner Expertise

Cisco security engineers and Cisco Security Specialized Partners are among the industry's elite in providing integrated, collaborative, adaptive solutions.

Cisco security engineers typically hold one or more Cisco and security certifications and have deployed, secured, operated, and helped optimize the performance of many of the largest and most successful networks in the world. Through their access to the deep engineering expertise of the business units that create Cisco products and solutions, Cisco security engineers are able to support you in deploying a solution that is consistent with Cisco product roadmaps.

Cisco Security Specialized Partners are recognized for their expertise in designing, installing, and supporting comprehensive, integrated network security solutions.

Service activities for the implementation phase of the network or solution lifecycle are delivered primarily through Cisco Security Specialized Partners. However, for technologies and applications that are relatively new, Cisco can perform service activities in conjunction with these partners. Cisco transfers knowledge to broaden and deepen the expertise of our channel partners and your staff.

Availability and Ordering

Cisco BioMed Network Admission Control Services are available globally. Service delivery details might vary by region.

For More Information

For more information about the Cisco Self-Defending Network, visit cisco.com/go/security. For more information about Cisco Security Services, visit cisco.com/go/services/security or contact your local account representative. Service delivery details might vary by region.

Other resources:

- Cisco Security Planning, Design, and Implementation Service data sheet: www.cisco.com/go/services/security
- Cisco Security IntelliShield Alert Manager Service: http://cisco.com/en/US/products/ps6834/serv_group_home.html
- Cisco Security Optimization Service: http://www.cisco.com/en/US/services/ps2961/ps2952/services_data_sheet0900aecd806ea35f.pdf

Cisco Services.
Making Networks Work.
Better Together.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.**