Preface

Document Purpose

This document provides guidance for implementing Network Admission Control (NAC), an industry-wide collaboration sponsored by Cisco Systems. It describes deployment considerations and configuration procedures for Cisco IOS software devices acting as Network Access Devices (NADs). It provides installation guidelines for the Cisco Trust Agent (CTA) on Microsoft Windows client machines. It also provides configuration instructions for Cisco Secure ACS, including configuration with anti-virus software products.

Intended Audience

The audience for this document consists of system engineers and network administrators responsible for the implementation of NAC. This document assumes you are familiar with Microsoft Windows operating systems and client machines and with the configuration and operation of Cisco Secure Cisco Secure ACS. It also assumes you know how to configure Cisco IOS devices, and are familiar with certificate authorities and the trust models provided by digital certificates.

Document Organization

Chapter	Description
Chapter 1, “Introducing Network Admission Control.”	Provides background information about the Network Admission Control (NAC) and describes how it works.
Chapter 2, “Implementing Network Admission Control.”	Describes how to design and Implement NAC.
Chapter 3, “Managing and Troubleshooting NAC.”	Describes how to manage and troubleshoot NAC.
Appendix A “Debug Output and CTA Logs.”	Provides sample output form debugging and CTA logs.
Appendix B “Reference Information.”	Provides a list of acronyms and sources of further information about NAC.