Network Admission Control Documentation Reference Guide

Revision 2: April 19, 2006

Network Admission Control, Release 2.0 (NAC 2.0) is a network security solution composed of several different Cisco components. It uses the network infrastructure to enforce security policy compliance on devices that try to access network computing resources, thereby limiting damage from security threats.

Customers implementing NAC can allow network access to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can restrict the access of noncompliant devices.

A basic NAC environment consists of three components: a Network Access Device (NAD), an authentication, authorization, and accounting (AAA) server, and a posture agent running on a NAC-compliant host. NADs are often Cisco routers or Cisco switches, the AAA server is the Cisco Secure Access Control Server (ACS), and the posture agent is the Cisco Trust Agent (CTA). An expanded NAC environment has additional NAC-enabled applications running on the host.

This document provides the titles and locations of NAC documentation available at Cisco Systems's web site.

Contents

NAC Framework Documentation

These documents discuss the Network Admission Control solution as a whole:

- Release Notes for Network Admission Control 2.0
- Network Admission Control Software Configuration Guide
- Network Admission Control Deployment Guide
- Network Admission Control Framework Configuration Guide
- Network Admission Control Frequently Asked Questions

NAC Framework Web Resources

These web sites provide information about the Network Admission Control solution as a whole:

- Network Admission Control Web site
- Network Admission Control Program Participants
- Network Admission Control Overview Demonstration
- Network Admission Control: Technical Overview

Network Access Device Documentation

A Network Access Device (NAD) controls which hosts have access to network destinations reachable through that device. Control is defined by a network access policy provided to the NAD by the ACS for a specific host.

Cisco Switch Documentation

Hosts provide posture and identity information to switches by using either IEEE 802.1X protocol or the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP). Switches pass that information to the ACS. Based on posture and identity information, the ACS issues a security policy for the host and returns that policy to the switch. The security policy for the host is enforced by the switch at Layer 2 of the Open System Interconnection (OSI) model.

When NAC is enforced at Layer 2 by using the IEEE 802.1X protocol, NAC is said to use the NAC L2 802.1X method. When NAC is enforced at Layer 2 by using the EAPoUDP protocol, NAC is said to use the NAC L2 IP method.

Table 1 lists the NAC-compliant switches and the NAC methods that they support.

Table 1 Switch Documentation

Supported Platforms and Models	Supported Methods	Operating System Image	Supporting Documents
Cisco Catalyst 2940	NAC L2 802.1X	Cisco IOS Release 12.1(22)EA6 or later	Cisco Catalyst 2940 Series Switch Documentation Release Notes for the Catalyst 2955, Catalyst 2950, and Catalyst 2940 Switches, Cisco IOS Release 12.1(22)EA6 Network Admission Control Software Configuration Guide Cisco IOS Software documentation
Catalyst 2950 Catalyst 2955	NAC L2 802.1X	Cisco IOS Release 12.1(22)EA6 or later	Cisco Catalyst 2950 Series Switch Documentation Cisco Catalyst 2955 Series Switch Documentation Release Notes for the Catalyst 2955, Catalyst 2950, and Catalyst 2940 Switches, Cisco IOS Release 12.1(22)EA6 Network Admission Control Software Configuration Guide Cisco IOS Software documentation

Table 1 Switch Documentation (continued)

Supported Platforms and Models	Supported Methods	Operating System Image	Supporting Documents
Cisco Catalyst 2960	NAC L2 802.1X	Cisco IOS Release 12.2(25)SED or later	Cisco Catalyst 2960 Series Switch Documentation Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches, Cisco IOS Release 12.2(25)SED Network Admission Control Software Configuration Guide Cisco IOS Software documentation
Cisco Catalyst 2970	NAC L2 802.1X	Cisco IOS Release 12.2(25)SED or later	Cisco Catalyst 2970 Series Switch Documentation Catalyst 2970 Switch Command Reference, 12.2(25)SED Catalyst 2970 Switch Software Configuration Guide, 12.2(25)SED Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches, Cisco IOS Release 12.2(25)SED Network Admission Control Software Configuration Guide Cisco IOS Software documentation
Cisco Catalyst 3550	NAC L2 IP NAC L2 802.1X	Cisco IOS Release 12.2(25)SED or later	Release Notes for the Catalyst 3550 Multilayer Switch, Cisco IOS Release 12.2(25)SED Cisco IOS Software documentation

Table 1 Switch Documentation (continued)

Supported Platforms and Models	Supported Methods	Operating System Image	Supporting Documents
Cisco Catalyst 3550	NAC L2 802.1X	Cisco IOS Release 12.1(22)EA6 or later	Cisco Catalyst 3550 Series Switch Documentation Network Admission Control Software Configuration Guide Cisco IOS Software documentation
Cisco Catalyst 3560	NAC L2 IP NAC L2 802.1X	Cisco IOS Release 12.2(25)SED or later	Cisco Catalyst 3560 Series Switch Documentation Catalyst 3560 Switch Command Reference, Rel. 12.2(25)SED Catalyst 3560 Switch Software Configuration Guide, Rel. 12.2(25)SED Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches, Cisco IOS Release 12.2(25)SED Network Admission Control Software Configuration Guide Cisco IOS Software documentation

Table 1 Switch Documentation (continued)

Supported Platforms and Models	Supported Methods	Operating System Image	Supporting Documents
Cisco Catalyst 3750	NAC L2 IP NAC L2 802.1X	Cisco IOS Release 12.2(25)SED or later	Cisco Catalyst 3750 Series Switch Documentation Catalyst 3750 Switch Command Reference, 12.2(25)SED Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SED Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches, Cisco IOS Release 12.2(25)SED Network Admission Control Software Configuration Guide Cisco IOS Software documentation
Cisco Catalyst 4500 Cisco Catalyst 4900	NAC L2 IP NAC L2 802.1X	Cisco IOS 12.2(25)SG or later	Catalyst 4500 Switch documentation list Catalyst 4900 Switch documentation list Catalyst 4500 Switch Documentation Road Map Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(25)SG Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)SG Network Admission Control Software Configuration Guide Cisco IOS Software documentation

Table 1 Switch Documentation (continued)

Supported Platforms and Models	Supported Methods	Operating System Image	Supporting Documents
Cisco 6500 Series Models: 6503, 6503-E, 6506, 6506-E, 6509, 6509-E, 6509-NEB, 6509-NEB-A, 6513	NAC L2 IP	Cisco IOS 12.2(18)SXF2	Catalyst 6500 Series Cisco IOS Software Documentation, 12.2SX Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2 Cisco IOS Software documentation
Cisco 6500 Series Models: 6503, 6503-E, 6506, 6506-E, 6509, 6509-E, 6509-NEB, 6509-NEB-A, 6513	NAC L2 IP NAC L2 802.1X	CatOS 8.5. or later	Catalyst 6500 Switch Documentation List Catalyst 6500 Documentation Road Map, 8.5 Catalyst 6500 Series Command Reference, 8.5 Catalyst 6500 Series Software Configuration Guide, 8.5 Network Admission Control Software Configuration Guide

Cisco Router Documentation

Hosts provide posture information to routers by using Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), and routers pass that information to the ACS. Based on the posture information, ACS issues a security policy for the host and returns that policy to the router. The security policy for the host is enforced by the router at Layer 3 of the Open System Interconnection (OSI) model. When NAC is enforced at Layer 3 by using the EAPoUDP method, this is referred to as the NAC L3 IP method.

Table 2 lists the NAC-compliant routers and the NAC methods they support.

Table 2 Router Documentation

Supported Platforms and Models	Supported NAC Method	Operating System Image	Supporting Documents
Cisco 830 and 870 Series Models: 831, 836, 837	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 800 Series Router documentation Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 1700 Series Models: 1701, 1711, 1712, 1721, 1751, 1751-V, 1760	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 1700 Series Modular Access Router documentation Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 1841 Series	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 1800 Series Integrated Services Router documentation Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 2600 Series Models: 2600XM, 2691	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 2600 Series Multiservice Platform documentation Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 2800 Series Models: 2801, 2811, 2821, 2851	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 2800 Series Integrated Services Router documentation Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 3600 Series Models: 3640/3640A, 3660-ENT Series	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 3600 Series Multiservice Platform documentation Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation

Table 2 Router Documentation (continued)

Supported Platforms and Models	Supported NAC Method	Operating System Image	Supporting Documents
Cisco 3700 Series Models: 3725, 3745	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 3700 Series Multiservice Access Routers Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 3800 Series 3845, 3825	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 3800 Series Integrated Services Routers Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 7200 Series	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 7200 Series Routers Documentation Roadmap Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 7500 Series	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 7500 Series Routers Documentation Roadmap Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation
Cisco 7600 Series	NAC L3 IP	Cisco IOS 12.3(8)T or later	Cisco 7600 Series Routers Documentation Roadmap Cisco IOS Software Releases 12.3 T Cisco IOS Software documentation

Cisco IOS and CatOS Reference Tools

Cisco Feature Navigator

Cisco Feature Navigator is a web-based application that allows you to find the right Cisco IOS and Catalyst OS (CatOS) software release for the features you want to implement on your Network Access Device (NAD). Online help is available for this tool along with an FAQ to answer questions about its operation.

You must be a registered user of Cisco.com to use Cisco Feature Navigator.

Command Lookup Tool

The Command Lookup Tool contains a detailed description of the Cisco IOS and Catalyst OS command syntax, default values, history, usage guidelines, and examples. Use this tool to learn about the commands used to manage the operating system of your Cisco router or switch.

You must be a registered user of Cisco.com to use Cisco command Lookup Tool.

Cisco Aironet Wireless Access Point Documentation

If you need to support wireless endpoints in your NAC environment, you can use this Cisco Wireless Access Point. You also need to use a third-party IEEE 802.1X supplicant that supports wireless endpoints.

The *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points 12.3(7)JA* describes the Aironet Wireless Access Point in the NAC environment.

Table 3 Aironet Wireless Access Point Documentation

Supported Platforms and Models	Supported NAC Method	Operating System Image	Supporting Documents
350 series	NAC L2 802.1X	IOS releases 12.3(7)JA1 and later.	Cisco Aironet 350 Series documentation
1100 series	NAC L2 802.1X	IOS releases 12.3(7)JA1 and later.	Cisco Aironet 1100 Series documentation

Supported Platforms and Models	Supported NAC Method	Operating System Image	Supporting Documents
1130 AG series	NAC L2 802.1X	IOS releases 12.3(7)JA1 and later.	Cisco Aironet 1130 AG Series documentation
1200 series	NAC L2 802.1X	IOS releases 12.3(7)JA1 and later.	Cisco Aironet 1200 Series documentation
1230 AG series	NAC L2 802.1X	IOS releases 12.3(7)JA1 and later.	Cisco Aironet 1230 Series documentation
1240 AG series	NAC L2 802.1X	IOS releases 12.3(7)JA1 and later.	Cisco Aironet 1240 AG Series documentation

Cisco Wireless LAN Controllers

Cisco Wireless LAN Controllers are responsible for system wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco 1000 Series Lightweight Access Points and the Cisco Wireless Control System (WCS) to support wireless applications.

Cisco Wireless LAN Controllers communicate with Cisco 1000 Series Lightweight Access Points over any Layer 2 (Ethernet) or Layer 3 (IP) infrastructure using the Lightweight Access Point Protocol (LWAPP). These devices support automation of numerous WLAN configuration and management functions across all enterprise locations.

Table 4 Wireless LAN Controller Documentation

Supported Platforms and Models	Supported Methods	Cisco Unified Wireless Network Software	Supporting Documentation
Cisco 2000	NAC L2 802.1X	Release 3.1 or later	Cisco 2000 Series Wireless LAN Controller documentation

Table 4 Wireless LAN Controller Documentation

Supported Platforms and Models	Supported Methods	Cisco Unified Wireless Network Software	Supporting Documentation
Cisco 4100	NAC L2 802.1X	Release 3.1 or later	Cisco 4100 Series Wireless LAN Controllers documentation
Cisco 4400	NAC L2 802.1X	Release 3.1 or later	Cisco 4400 Series Wireless LAN Controllers
Wireless Services Module (WiSM)	NAC L2 802.1X	Release 3.1 or later	Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
Wireless LAN Services Module (WLSM)	NAC L2 802.1X	Release 3.1 or later	Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM)
Wireless LAN Controller Module for Integrated Services Routers	NAC L2 802.1X	Release 3.1 or later	Cisco Wireless LAN Controller Module

Cisco VPN Concentrator Documentation

The Virtual Private Network (VPN) Concentrator functions as both a NAC authenticator and an ACS client. The VPN Concentrator is considered a Layer 3 device and uses the NAC L3 IP method for posture validation.

As a NAC authenticator, the VPN Concentrator performs these tasks:

- Initiates the initial exchange of credentials based on IPSec session establishment and periodically thereafter.
- Relays credential requests and responses between the peer and the authentication (ACS) server with the use of Protected Extensible Authentication Protocol (PEAP).
- Enforces network access policy for an IPSec session based on results from the ACS server.
- Implements the configured EAP Status Query method.
- Supports a local exception list based on the peer operating system.

- Requests access policies from the ACS server for a clientless host.

As an ACS client, the VPN Concentrator supports:

- EAP/RADIUS
- RADIUS attributes required for NAC

NAC on the VPN 3000 Concentrator differs from that on Cisco IOS Layer 3 devices such as routers. Whereas routers trigger posture validation (PV) based on routed traffic, the VPN 3000 Concentrator configured with NAC uses the establishment of an IPSec VPN session as the trigger for PV. Cisco IOS routers configured with NAC use an Intercept access control list (ACL) in order to trigger PV based on traffic destined for certain networks. Because external devices cannot access the network behind the VPN 3000 Concentrator without starting a VPN session, the VPN 3000 Concentrator does not need an intercept ACL as a PV trigger. During posture validation, all IPSec traffic from the device is subject to the Default ACL configured for the device's group.

Table 5 VPN Concentrator Documentation

Supported Platforms and Models	Operating System Version	Supporting Documents
Cisco VPN 3000 Series Models: 3005 to 3080	V4.7 or later	VPN 3000 Network Access Device 4.7.0 NAC Administration and Configuration VPN 3000 Network Access Device 4.7.1 NAC Administration and Configuration Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.7; Cisco SSL VPN Client, Release 1.0 Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.7.1 Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.7.2

Cisco Secure Access Control Server Documentation

Cisco Secure Access Control Server (ACS) is NAC's central authentication, authorization, and accounting (AAA) server.

When a host attempts to access the network, ACS requests the host's posture credentials. CTA solicits posture credentials from posture plugins and returns them to the ACS. Based on the credentials received, ACS determines the postures of the individual application and the overall posture token for the host.

Based on the overall posture token of the host, the ACS defines a network access policy for the host and forwards that policy to the NAD where the policy is enforced.

ACS for Windows (V.4.0)

The ACS for Windows is a software implementation of ACS. These are the documents you will need to install and configure ACS for Windows in a NAC environment:

- Cisco Secure Access Control Server for Windows documentation list
- Release Notes for Cisco Secure ACS for Windows V.4.0
- Installation and User Guide for Cisco Secure ACS User-Changeable Passwords
- Installation Guide for Cisco Secure ACS for Windows 4.0
- User Guide for the Cisco Secure ACS for Windows 4.0
- Supported and Interoperable Devices for Cisco Secure ACS for Windows 4.0

ACS Solution Engine (V.4.0)

The ACS Server Solution Engine (ACS SE) is a hardware implementation of ACS. This is the list of documentation for the Cisco Secure ACS Solution Engine:

- Documentation Guide for Cisco Secure ACS Solution Engine
- Release Notes for Cisco Secure ACS Solution Engine
- Installation and Setup Guide for Cisco Secure ACS Solution Engine

- User Guide for the Cisco Secure ACS Solution Engine
- Supported Devices Table for the Cisco Secure ACS Solution Engine
- Installation Guide for User-Changeable Passwords
- Installation and Configuration Guide for Cisco Secure ACS Remote Agents

Registered users of Cisco.com may also access this document:

- Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.0

Cisco Trust Agent Documentation

Cisco Trust Agent (CTA) is NAC's posture agent. CTA software is installed on each host on the network. When a host attempts to access the network, ACS requests the host's posture credentials. CTA solicits posture credentials from posture plugins and returns them to the ACS. Each posture plugin gathers posture information from one application.

On Windows-based network clients, CTA can be installed with a "supplicant" called the Cisco Trust Agent 802.1X Wired Client (802.1X Wired Client). The 802.1X Wired Client is an authentication supplicant for creating secure user connections to an Ethernet switch. The 802.1X Wired Client provides a GUI for monitoring authentication status and managing authorized network access.

Install CTA with the 802.1X Wired Client if your network meets all of these conditions:

- You are authenticating your hosts through a switch.
- You are sending the traffic to the switch on NAC L2 802.1X (EAP-Flexible Authentication using Secure Tunneling, EAP-FAST Protocol).
- The host is running Windows-based operating system.

Install CTA without the 802.1X Wired Client if your network meets either of these conditions:

- You are authenticating your hosts through a switch and you are sending the traffic to the switch on NAC L2 IP (EAP over UDP).
- The host is running a Linux-based operating system, do not install the 802.1X Wired Client.

These are the Cisco Trust Agent (CTA) documents relative to NAC Release 2.0:

- Cisco Trust Agent documentation list
- Cisco Trust Agent Release Notes V.2.0
- Cisco Trust Agent Administrator's Guide V.2.0

Additional NAC-Compliant Components

It is possible that there might be applications installed at the endpoint that interact with NAC components. These applications might require additional NAC infrastructure, or they might need special configuration in order to allow NAC to function properly.

Cisco Security Agent Documentation

Cisco Security Agent (CSA) provides intrinsic, distributed security by deploying agents that defend against attacks across networks and systems. The Cisco Security Agents enforce a set of policies selectively applied to system nodes by the network administrator.

A Cisco Security Agent has its own posture plugin and can send posture credentials to CTA when they are requested.

CSA versions 4.5.1.639 and 5.0.0.176 or later support NAC 2.0.

- Cisco Security Agent documentation list
- Release Notes for Management Center for Cisco Security Agents V.4.5.1
- Installing Management Center for Cisco Security Agents V.4.5.1
- Using Management Center for Cisco Security Agents V.4.5.1
- Policy Descriptions for CSA 4.5.1 (To obtain policy descriptions, you must be a Cisco.com registered user.)
- Release Notes for Management Center for Cisco Security Agents 5.0
- Installing Management Center for Cisco Security Agents 5.0
- Using Management Center for Cisco Security Agents 5.0

Cisco Secure Monitoring Analysis and Response Systems

Cisco Secure Monitoring Analysis and Response Systems (CS-MARS) are high performance, scalable appliances for threat management, monitoring and mitigation, enabling customers to make more effective use of network and security devices by combining network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities.

These documents describe how to configure a NAC device or application to communicate with the CS-MARS.

- Cisco Security Monitoring, Analysis and Response System documentation list
- Cisco Security Monitoring, Analysis and Response System 4.1

Network Admission Control Documentation Reference Guide