



# CONTENTS

## About This Guide xvii

Obtaining Documentation and Submitting a Service Request 2-xxii

---

## CHAPTER 1

### Introduction 1-1

What Is Cisco NAC Appliance (Cisco Clean Access)? 1-1

Cisco NAC Appliance Components 1-2

Clean Access Manager (CAM) 1-4

Clean Access Server (CAS) 1-5

Clean Access Agent 1-6

Managing Users 1-6

Installation Requirements 1-7

Product Licensing and Service Contract Support 1-8

Upgrading the Software 1-8

Cisco NAC Appliance Hardware Platforms 1-8

Supported Server Hardware Platforms 1-9

Minimum System Requirements 1-9

Important Release Information 1-9

Overview of Web Admin Console Elements 1-9

Clean Access Server (CAS) Management Pages 1-10

Admin Console Summary 1-13

---

## CHAPTER 2

### Installing the Clean Access Manager 2-1

Overview 2-1

Summary of Steps For New Installation 2-2

Connect the Clean Access Manager 2-3

Serial Connection to the CAM 2-4

Install the Clean Access Manager Software from CD-ROM 2-5

CD Installation Steps 2-5

Perform the Initial Configuration 2-7

Configuration Utility Script 2-7

Access the CAM Web Console 2-11

Important Notes for SSL Certificates 2-13

CAM CLI Commands 2-15

Troubleshooting Network Card Driver Support Issues 2-16  
 Cisco NAC Appliance Connectivity Across a Firewall 2-16

**CHAPTER 3**

**Device Management: Adding Clean Access Servers, Adding Filters 3-1**

Working with Clean Access Servers 3-2  
     Add Clean Access Servers to the Managed Domain 3-2  
     Troubleshooting when Adding the Clean Access Server 3-4  
     Manage the Clean Access Server 3-4  
     Configure Clean Access Manager-to-Clean Access Server Authorization 3-5  
         Summary of Steps to Configure Clean Access Manager-to-Clean Access Server Authorization 3-5  
         Enable Authorization and Specify Authorized Clean Access Servers 3-6  
     Check Clean Access Server Status 3-7  
     Disconnect a Clean Access Server 3-7  
     Reboot the Clean Access Server 3-8  
     Remove the Clean Access Server from the Managed Domain 3-8  
 Global and Local Administration Settings 3-8  
     Global and Local Settings 3-9  
 Global Device and Subnet Filtering 3-9  
     Overview 3-10  
     Device Filters and User Count License Limits 3-11  
     Adding Multiple Entries 3-11  
     Corporate Asset Authentication and Posture Assessment by MAC Address 3-12  
     Device Filters for In-Band Deployment 3-13  
     Device Filters for Out-of-Band Deployment 3-14  
         Device Filters for Out-of-Band Deployment Using IP Phones 3-14  
     Device Filters and Gaming Ports 3-15  
     Global vs. Local (CAS-Specific) Filters 3-15  
     Global Device Filter Lists from Cisco NAC Profiler 3-15  
     Configure Device Filters 3-17  
         Add Global Device Filter 3-17  
         Display/Search/Import/Export Device Filter Policies 3-20  
         Order Device Filter Wildcard/Range Policies 3-21  
         Test Device Filter Policies 3-22  
         View Active L2 Device Filter Policies 3-23  
         Edit Device Filter Policies 3-24  
         Delete Device Filter Policies 3-24  
     Configure Subnet Filters 3-24

**Switch Management: Configuring Out-of-Band (OOB) Deployment 4-1**

Overview	4-1
In-Band Versus Out-of-Band	4-2
Out-of-Band Requirements	4-2
SNMP Control	4-4
Deployment Modes	4-4
Basic Connection	4-4
Out-of-Band Virtual Gateway Deployment	4-6
Flow for OOB VGW Mode	4-7
Out-of-Band Real-IP/NAT Gateway Deployment	4-9
Flow for OOB Real-IP/NAT Mode	4-11
L3 Out-of-Band Deployment	4-12
Configuring Your Network for Out-of-Band	4-13
Configure Your Switches	4-14
Configuration Notes	4-14
Example Switch Configuration Steps	4-15
OOB Network Setup/Configuration Worksheet	4-19
Configure OOB Switch Management in the CAM	4-20
Add Out-of-Band Clean Access Servers and Configure Environment	4-20
Configure Global Device Filters to Ignore IP Phone MAC Addresses	4-23
Configure Group Profiles	4-23
Add Group Profile	4-24
Edit Group Profile	4-24
Configure Switch Profiles	4-25
Add Switch Profile	4-26
Configure Port Profiles	4-27
Add Port Profile	4-28
Configure VLAN Profiles	4-33
Add VLAN Profile	4-35
Edit VLAN Profile	4-36
Configure SNMP Receiver	4-37
SNMP Trap	4-37
Advanced Settings	4-38
Add and Manage Switches	4-41
Add New Switch	4-41
Search New Switches	4-42
Discovered Clients	4-44
Manage Switch Ports	4-45
Ports Management Page	4-46

- Manage Individual Ports (MAC Notification) 4-46
- Manage Individual Ports (Linkup/Linkdown) 4-52
- Assign a Port Profile to Multiple Ports Simultaneously 4-53
- Config Tab 4-54
- Configure Access to Authentication VLAN Change Detection 4-59
  - Windows Client Machines 4-60
  - Macintosh OS X Client Machines 4-61
- Out-of-Band Users 4-64
  - OOB User Sessions 4-64
  - OOB User List Summary 4-64
- OOB Troubleshooting 4-66
  - OOB Switch Trunk Ports After Upgrade 4-66
  - Unable to Control <Switch IP> 4-66
  - OOB Error: connected device <client\_MAC> not found 4-67

**CHAPTER 5**

**Configuring User Login Page and Guest Access 5-1**

- User Login Page 5-1
  - Unauthenticated Role Traffic Policies 5-2
  - Proxy Settings 5-2
- Add Default Login Page 5-3
- Change Page Type (to Frame-Based or Small-Screen) 5-4
- Enable Web Client for Login Page 5-5
  - DHCP Release/Renew with Agent/ActiveX/Java Applet 5-6
- Customize Login Page Content 5-8
- Create Content for the Right Frame 5-11
- Upload a Resource File 5-13
- Customize Login Page Styles 5-14
- Configure Other Login Properties 5-15
  - Redirect the Login Success Page 5-15
  - Specify Logout Page Information 5-16
- Guest User Access 5-17
  - Configure Guest User Registration 5-17
    - Configuring the Guest User Access Page 5-18
  - Enable the Preset "Guest" User Account 5-22

**CHAPTER 6**

**User Management: Configuring User Roles and Local Users 6-1**

- Overview 6-1
- Create User Roles 6-1

User Role Types	6-2
Unauthenticated Role	6-3
Normal Login Role	6-3
Clean Access Roles	6-4
Session Timeouts	6-5
Default Login Page	6-6
Traffic Policies for Roles	6-6
Add New Role	6-6
Role Properties	6-8
Modify Role	6-10
Edit a Role	6-11
Delete Role	6-12
Create Local User Accounts	6-12
Create or Edit a Local User	6-13

**CHAPTER 7****User Management: Configuring Auth Servers 7-1**

Overview	7-1
Adding an Authentication Provider	7-3
Kerberos	7-4
RADIUS	7-5
RADIUS Challenge-Response Impact On the Clean Access Agent	7-7
Windows NT	7-7
LDAP	7-8
Configure LDAP Server with Simple Authentication	7-9
Configure LDAP Server with GSSAPI Authentication	7-11
Active Directory Single Sign-On (SSO)	7-13
Windows NetBIOS SSO	7-13
Implementing Windows NetBIOS SSO	7-13
Cisco VPN SSO	7-14
Allow All	7-16
Guest	7-17
Configuring Authentication Cache Timeout (Optional)	7-18
Authenticating Against a Backend Active Directory	7-18
AD/LDAP Configuration Example	7-19
Map Users to Roles Using Attributes or VLAN IDs	7-21
Configure Mapping Rule	7-22
Editing Mapping Rules	7-27
Auth Test	7-29
RADIUS Accounting	7-31

- Enable RADIUS Accounting 7-31
  - Restore Factory Default Settings 7-32
- Add Data to Login, Logout or Shared Events 7-32
  - Add New Entry (Login Event, Logout Event, Shared Event) 7-33

**CHAPTER 8**

**User Management: Traffic Control, Bandwidth, Schedule 8-1**

- Overview 8-1
  - Global vs. Local Scope 8-3
  - View Global Traffic Control Policies 8-3
- Add Global IP-Based Traffic Policies 8-4
  - Add IP-Based Policy 8-4
  - Edit IP-Based Policy 8-7
- Add Global Host-Based Traffic Policies 8-8
  - Add Trusted DNS Server for a Role 8-8
  - Enable Default Allowed Hosts 8-9
  - Add Allowed Host 8-10
    - View IP Addresses Used by DNS Hosts 8-11
  - Proxy Servers and Host Policies 8-12
- Add Global Layer 2 Ethernet Traffic Policies 8-12
- Control Bandwidth Usage 8-13
- Configure User Session and Heartbeat Timeouts 8-15
  - Session Timer 8-15
  - Heartbeat Timer 8-15
  - In-Band (L2) Sessions 8-15
  - OOB (L2) and Multihop (L3) Sessions 8-16
  - Session Timer / Heartbeat Timer Interaction 8-16
  - Configure Session Timer (per User Role) 8-17
  - Configure Heartbeat Timer (User Inactivity Timeout) 8-17
- Configure Policies for Agent Temporary and Quarantine Roles 8-18
  - Configure Agent Temporary Role 8-18
    - Configure Session Timeout for the Temporary Role 8-19
    - Configure Traffic Control Policies for the Temporary Role 8-20
  - Configure Network Scanning Quarantine Role 8-20
    - Create Additional Quarantine Role 8-21
    - Configure Session Timeout for Quarantine Role 8-21
    - Configure Traffic Control Policies for the Quarantine Role 8-22
- Example Traffic Policies 8-23
  - Allowing Authentication Server Traffic for Windows Domain Authentication 8-23
  - Allowing Traffic for Enterprise AV Updates with Local Servers 8-23

Allowing Gaming Ports	8-24
Microsoft Xbox	8-24
Other Game Ports	8-24
Adding Traffic Policies for Default Roles	8-26
Troubleshooting Host-Based Policies	8-28

**CHAPTER 9****Clean Access Implementation Overview 9-1**

Clean Access Overview	9-1
Clean Access Agent	9-6
Cisco NAC Web Agent	9-7
Clean Access Updates	9-8
Network Scanner	9-8
Certified Devices List	9-9
Role-Based Configuration	9-10
Clean Access Setup Steps	9-11
Retrieving Updates	9-12
Downloading Cisco Clean Access Updates	9-16
View Current Updates	9-16
Configure and Download Updates	9-17
Configure Proxy Settings for CAM Updates (Optional)	9-19
General Setup Overview	9-20
Agent Login	9-20
Web Login	9-24
User Page Summary	9-26
Manage Certified Devices	9-30
Add Exempt Device	9-32
Clear Certified or Exempt Devices Manually	9-33
View Reports for Certified Devices	9-33
View Switch Information for Out-of-Band Certified Devices	9-33
Configure Certified Device Timer	9-34
Add Floating Devices	9-36

**CHAPTER 10****Distributing the Agent 10-1**

Overview	10-1
Agent Configuration Steps	10-3
Add Default Login Page	10-3
Require Use of the Agent	10-3
Configure Restricted Network Access for Agent Users	10-6

- Configure Network Policy Page (Acceptable Use Policy) for Agent Users 10-6
- Configure the Agent Temporary Role 10-7
- Enable Network Access (L3 or L2) 10-7
  - Enable L3 Deployment Support 10-9
    - Agent Sends IP/MAC for All Available Adapters 10-9
    - VPN/L3 Access for Agents 10-9
    - Enable L3 Support 10-10
    - Disabling L3 Capability 10-12
  - Enabling L2/L3 Strict Mode 10-12
- Configuring Agent Distribution/Installation 10-13
  - Distribution Page 10-13
  - Installation Page 10-15
  - Clean Access Agent Stub Installer 10-17
  - Clean Access Agent MSI Installers 10-19
    - Installing the Clean Access Agent Directly Using MSI 10-19
    - Installing the Clean Access Agent Stub Using MSI 10-21
    - Verify Clean Access Agent MSI Installation 10-21
- Configure Clean Access Agent Auto-Upgrade 10-23
  - Enable Clean Access Agent Auto-Upgrade on the CAM 10-23
  - Disable Clean Access Agent Upgrades to Users 10-23
  - Disable Mandatory Clean Access Agent Auto-Upgrade on the CAM 10-23
  - User Experience for Clean Access Agent Auto-Upgrade 10-24
  - Uninstalling the Clean Access Agent 10-24
    - Uninstall Windows Clean Access Agent 10-24
    - Uninstall Mac OS X Clean Access Agent 10-25
  - Clean Access Agent Setup and Patch (Upgrade) Files 10-25
    - Loading Clean Access Agent Installation Files to the CAM 10-25
  - Clean Access Agent Auto-Upgrade Compatibility 10-26
  - Upgrading from 3.5.0 and Below Clean Access Agents 10-27
    - Clean Access Agent Upgrade Through File Distribution Requirement 10-27
- Manually Uploading the Clean Access Agent to the CAM 10-29
- Downgrading the Clean Access Agent 10-30

**CHAPTER 11**

**Configuring Agent Requirements 11-1**

- Overview 11-1
- Configuring AV/AS Definition Update Requirements 11-3
  - AV Rules and AS Rules 11-4
  - Verify AV/AS Support Info 11-6
  - Create an AV Rule 11-8

Create an AV Definition Update Requirement	11-9
Create an AS Rule	11-12
Create an AS Definition Update Requirement	11-13
Configuring a Windows Server Update Services Requirement	11-15
Create Windows Server Update Service Requirement	11-17
Map Windows Server Update Service Requirement to Windows Rules	11-21
Configuring a Windows Update Requirement	11-22
Create a Windows Update Requirement	11-24
Map Windows Update Requirement to Windows Rules	11-27
Configuring Custom Checks, Rules, and Requirements	11-28
Custom Requirements	11-28
Custom Rules	11-29
Cisco Pre-Configured Rules ("pr_")	11-29
Custom Checks	11-30
Cisco Pre-Configured Checks ("pc_")	11-30
Using Pre-Configured Rules to Check for CSA	11-30
Copying Checks and Rules	11-30
Configuration Summary	11-31
Create Custom Check	11-31
<b>Registry Checks</b>	11-33
<b>File Checks</b>	11-34
<b>Service Check</b>	11-35
<b>Application Check</b>	11-36
Create a Custom Rule	11-36
Validate Rules	11-38
Create a Custom Requirement	11-39
Create File Distribution/Link Distribution/Local Check Requirement	11-39
Configuring a Launch Programs Requirement	11-42
Launch Programs With Admin Privileges	11-42
Launch Programs Without Admin Privileges	11-42
How the Agent Verifies Digital Signature and Trust on an Executable Program	11-42
Create a Launch Programs Requirement	11-43
Launch Programs via Clean Access Agent Example	11-45
Map Requirements to Rules	11-55
Apply Requirements to User Roles	11-57
Validate Requirements	11-58
Configuring an Optional/Audit Requirement	11-59
Configuring Auto Remediation for Requirements	11-61
Viewing Agent Reports	11-65

Exporting Agent Reports 11-68  
 Limiting the Number of Reports 11-68

**CHAPTER 12**

**Cisco NAC Appliance Agents 12-1**

Windows Clean Access Agent 12-1  
 Windows Clean Access Agent Overview 12-1  
 Configuration Steps for the Windows Clean Access Agent 12-2  
 Windows Clean Access Agent User Dialogs 12-2  
     RADIUS Challenge-Response Windows Clean Access Agent Dialogs 12-15  
     Clean Access Agent Localized Language Templates 12-18  
 Mac OS X Clean Access Agent (Authentication Only) 12-21  
     Mac OS X Clean Access Agent Dialogs 12-21  
     RADIUS Challenge-Response Mac OS X Clean Access Agent Dialogs 12-28  
 Cisco NAC Web Agent 12-32  
     Overview 12-32  
     System Requirements 12-33  
     Configuration Steps for the Cisco NAC Web Agent 12-35  
     Cisco NAC Web Agent User Dialogs 12-35  
 Agent Troubleshooting 12-51  
     Client Cannot Connect/Login 12-51  
     No Clean Access Agent Pop-Up/Login Disabled 12-52  
     Client Cannot Connect (Traffic Policy Related) 12-52  
     AV/AS Rule Troubleshooting 12-53  
     Cisco NAC Web Agent Status Codes 12-53  
     Known Issue for Windows Script 5.6 12-54  
     Known Issue for MS Update Scanning Tool (KB873333) 12-54

**CHAPTER 13**

**Configuring Network Scanning 13-1**

Overview 13-1  
     Network Scanning Implementation Steps 13-2  
 Configure the Quarantine Role 13-2  
 Load Nessus Plugins into the Clean Access Manager Repository 13-3  
     Uploading Plugins 13-4  
     Deleting Plugins 13-5  
 Configure General Setup 13-6  
 Apply Plugins 13-7  
 Configure Plugin Options 13-9  
 Configure Vulnerability Handling 13-10

Test Scanning	13-13
Show Log	13-14
View Scan Reports	13-14
Customize the User Agreement Page	13-16

**CHAPTER 14****Monitoring Online Users and Event Logs 14-1**

Overview	14-1
Online Users List	14-3
Interpreting Active Users	14-4
View Online Users	14-5
In-Band Users	14-5
Out-of-Band Users	14-6
Display Settings	14-10
Interpreting Event Logs	14-12
View Logs	14-12
Event Log Example	14-16
Limiting the Number of Logged Events	14-17
Configuring Syslog Logging	14-17
Log Files	14-19
Log File Sizes	14-19
SNMP	14-20
Enable SNMP Polling/Alerts	14-21
Add New Trapsink	14-22

**CHAPTER 15****Administering the CAM 15-1**

Overview	15-1
Network	15-2
Failover	15-3
Set System Time	15-4
Manage CAM SSL Certificates	15-6
Generate Temporary Certificate	15-10
Export CSR/Private Key/Certificate	15-11
Verify Currently Installed Private Key and Certificates	15-13
Import Signed Certificate	15-16
View Certificate Files Uploaded for Import	15-18
View and Remove Trusted Certificate Authorities	15-18
Import/Export Trusted Certificate Authorities	15-20
Troubleshooting Certificate Issues	15-21

- No Web Login Redirect/CAS Cannot Establish Secure Connection to CAM 15-21
- Private Key in Clean Access Server Does Not Match the CA-Signed Certificate 15-22
- Regenerating Certificates for DNS Name Instead of IP 15-23
- Certificate-Related Files 15-23
- System Upgrade 15-23
- Licensing 15-26
- Support Logs 15-28
- Admin Users 15-30
  - Admin Groups 15-30
    - Add a Custom Admin Group 15-30
  - Admin Users 15-32
    - Login/Logout an Admin User 15-33
    - Add an Admin User 15-33
    - Edit an Admin User 15-34
    - Active Admin User Sessions 15-35
- Manage System Passwords 15-36
  - Change the CAM Web Console Admin Password 15-36
  - Change the CAS Web Console Admin User Password 15-37
  - Recovering Root Password for CAM/CAS (Release 4.1.x/4.0.x/3.6.x) 15-38
    - Recovering Root Password for CAM/CAS (Release 3.5.x or Below) 15-38
- Backing Up the CAM Database 15-39
  - Automated Daily Database Backups 15-40
  - Manual Backups from Web Console 15-40
    - Creating Manual Backup 15-40
  - Backing Up Snapshots to Another Server via FTP 15-41
  - Backing Up and Restoring CAM/CAS Authorization Settings 15-41
  - Restoring Configuration From CAM Snapshot—Standalone CAM 15-43
  - Restoring Configuration From CAM Snapshot—HA-CAM or HA-CAS 15-44
  - Database Recovery Tool 15-45
  - Manual Database Backup from SSH 15-46
- API Support 15-46

**CHAPTER 16**

**Configuring High Availability (HA) 16-1**

- Overview 16-1
- Before Starting 16-4
- Connect the Clean Access Manager Machines 16-4
  - Serial Connection 16-5
- Configure the HA-Primary CAM 16-6

Configure the HA-Secondary CAM	16-9
Complete the Configuration	16-12
Upgrading an Existing Failover Pair	16-12
Failing Over an HA-CAM Pair	16-12
Useful CLI Commands for HA	16-13
Adding High Availability Cisco NAC Appliance To Your Network	16-14

**APPENDIX A****Error and Event Log Messages** A-1

Client Error Messages	A-1
Login Failed	A-1
Network Error	A-2
Users Cannot Log In During CAS Fallback Recovery	A-3
Clean Access Agent Unable to Upgrade Using MSI	A-4
Clean Access Agent Icon Does Not Install to Taskbar	A-4
CAM Event Log Messages	A-5

**APPENDIX B****API Support** B-1

Overview	B-1
Authentication Requirements	B-2
Administrator Operations	B-2
adminlogin	B-2
<any subsequent operation>	B-2
adminlogout	B-3
Device Filter Operations	B-3
addmac	B-3
removemac	B-4
Certified Devices List Operations	B-4
addcleanmac	B-4
removecleanmac	B-5
clearcertified	B-5
User Operations	B-6
kickuser	B-6
kickuserbymac	B-6
kickoobuser	B-7
queryuserstime	B-7
renewuserstime	B-7
changeuserrole	B-8
changeloggedinuserrole	B-8

Guest Access Operations **B-9**

getlocaluserlist **B-9**

addlocaluser **B-9**

deletelocaluser **B-10**

Report Operations **B-10**

getversion **B-10**

getuserinfo **B-11**

getoobuserinfo **B-11**

getcleanuserinfo **B-12**

getreports **B-12**

---

**APPENDIX C**

**Windows Client Registry Settings C-1**

---

**APPENDIX D**

**Open Source License Acknowledgements D-1**

Notices **D-1**

OpenSSL/Open SSL Project **D-1**

License Issues **D-1**

---

**INDEX**