

Symbols

`/var/log/ha-debug log`, 517
`/var/log/ha-log log`, 517

Numerics

3500XL Edge Layer 2 switch, configuring AD SSO, 354–355

A

access to resources, troubleshooting issues, 520
access VLANs, 54

ACLs. *See also* policies

Layer 3 OOB traffic control, 59–60

Active Administrator Sessions page, 492

Active Directory SSO, 93

operation, 94–95
prerequisites, 94

AD server, configuring for AD SSO, 360–363

AD SSO (Active Directory Single Sign-On), 345

3500XL Edge Layer 2 switch, configuring, 354–355

AD SSO authentication server, adding, 357

Agent-based Windows SSO, enabling, 364
configuring, 347

DHCP, enabling in NAS, 379–381

domain structure, 346

GPO updates, enabling, 364

Layer 3 3550 core switch, configuring, 352–354

mapping users to multiple roles, 366–368
user attributes, 370–371, 374, 378–379

NAC Agent, downloading, 382, 384

NAM, configuring, 348–349

NAS

configuring, 349–351

user account, creating, 361

ports, configuring, 358

supported devices, 345

traffic policies, configuring, 358

troubleshooting, 509–511

Windows 2003 support tools, installing, 362

Add Exempt Device page (Certified Devices tab), configuring, 246

Add Floating Device page (Certified Devices tab), configuring, 246

adding

CA-signed certificate to NAM, 413–414

checks, rules, and requirements to HSP, 150–151

external authentication servers

LDAP/AD, 224–225

RADIUS, 223

NAS appliances

to network, 201

to NAM, 496–498

to NAM in L3OOB deployment, 322

to NAM in OOB deployment, 289

switch to NAM in L3OOB mode, 328

adjacency mode, effect on OOB operation, 56–58

admin group, creating, 220

admin user account, creating, 222

agent distribution, configuring, 255–257

agent issues, troubleshooting, 500–503

Agent Login page (General Setup tab), configuring, 243–245

agent policy enforcement, configuring, 239–241

agent login, configuring, 243–245

certified devices, configuring, 245–246, 249

web login, configuring, 242–243

Agent-based Windows SSO, enabling for AD SSO configuration, 364

agentless authentication, 14

antivirus update requirements, configuring, 259

API for guest access, 236

applying

NAS logs to troubleshooting process, 516–517

requirements to HSP user roles, 153

assigning roles to local users, 207–208

by external authentication source attribute, 219

by MAC/IP address, 213, 217

by subnet, 217–218

by VLAN ID, 209–211

attributes, mapping users to user roles, 90–91

AUPs (acceptable use policies), 138

components of, 139

enforcing, 139, 142

samples, 139

authentication

- agentless, 14
- Clean Access Certified List, 484–485
 - certification, requiring, 488–489
 - clearing, 486
 - device timer options, 487–488
 - summary of characteristics, 490
- common troubleshooting issues, 518–519
- external authentication servers, 87–88
 - MAC address authentication filters, 92–93
 - mapping users to user roles, 89–91
 - providers lists, 89
 - supported authentication servers, 88
- guest access, enabling, 236
- NAS web login page, customizing, 232–235
- SSO
 - AD SSO, 345–363, 382–384
 - Cisco VPN SSO, 386–396
- authentication URL, Layer 3 OOB traffic control, 61–62
- authentication VLANs, 54, 291
- automatic updating, 240

B

- bandwidth policies, creating, 230–231
- built-in user roles, 133
 - normal role, 134
 - Quarantine role, 135–136
 - Temporary role, 134–135
 - Unauthenticated role, 134
- business drivers for deployment, identifying, 448–449

C

- Campus LAN domain, 131
- case studies, Cisco NAC solution, ROI, 17–18
- CA-signed certificate, adding to NAM, 413–414
- central deployment, 39
- central deployment mode, 276
- central switch, configuring L3OOB, 311–313
- certification process for In-Band mode, 44–47
- certified device timer, 104
- Certified Devices tab
 - Add Exempt Device option, configuring, 246

- Add Floating Device option, configuring, 246
- Certified List option, configuring, 245–246
- Timer option, configuring, 249
- Certified List (Clean Access Agent), 484–485**
 - certification, requiring, 488–489
 - clearing, 486
 - device timer options, 487–488
 - summary of characteristics, 490
- Certified List page (Certified Devices tab), configuring, 245–246**
- checklist for creating HSPs, 124**
- checks**
 - for Cisco Clean Access Agent remediation, configuring, 264
 - for HSP, 149–150
 - adding, 150–151
 - validity of, determining, 152
- Cisco ACS, configuring for Cisco VPN SSO, 388**
- Cisco ASA 5510, configuring for Cisco VPN SSO, 388, 392**
- Cisco Clean Access Agent, 28–29, 250**
 - agent installation, 250, 255–257
 - installing
 - alternative methods, 257
 - sample agent installation, 251, 255
 - minimum requirements, 32–33
 - network scanning, configuring, 267–269
 - remediation
 - checks, 264
 - custom rules, creating, 266
 - requirements, 258–265
- Cisco IOS Software, integrated NAC implementation, 16**
- Cisco NAC Appliance, 17**
 - components, 14
 - IP telephony integration, 101
 - In-Band mode, best practices, 101
 - Out-of-Band mode, best practices, 102–104
 - minimum requirements, 30–33
 - scalability, 33
- Cisco NAC Appliance Manager, 24**
 - minimum requirements, 31–32
 - stateful failover, 107–108
 - web console, 24
 - Web GUI, monitoring-related pages, 492–493
- Cisco NAC Appliance Network Scanner, 29–30**
- Cisco NAC Appliance Server, 25, 28**

- fallback feature, 109–110
 - load balancing, 116–118
 - minimum requirements, 31–32
 - stateful failover, 108–109
- Cisco VPN SSO**
 - ACS, configuring, 388
 - Cisco ASA Appliance, configuring, 388, 392
 - configuring, 386–388
 - NAS support, configuring, 393–396
- Cisco Wireless SSO, 99**
 - configuring, 398–399
 - NAM, configuring, 402–403
 - NAS, configuring, 402–403
 - operation, 99–100
 - prerequisites, 99
 - WLC, configuring, 399–401
- Clean Access, Certified list, 484–485**
 - certification, requiring, 488–489
 - certified device timer options, 487–488
 - clearing, 486
 - summary of characteristics, 490
- Clean Access Agent, 26, 81–85**
 - HSP, posture assessment configuration, 143–147
 - remediation, configuring, 143–147
 - Reports page, 480–483
- clearing Certified List, 486**
- CLI monitoring commands**
 - ifconfig, 491
 - netstat, 491
 - top, 491
- Client/Server Adjacency mode, 38–39**
 - Layer 2, selecting, 40
 - Layer 2 Strict Mode for Clean Access Agent, selecting, 41–42
 - Layer 3, selecting, 40–41
- commands**
 - ifconfig, 491
 - ipconfig, 517
 - ktpass, 509
 - mii-tool, 517
 - netstat, 491
 - netstat -an, 517
 - top, 491, 517
- common helpdesk troubleshooting issues, 518–521**
- communication plan for Cisco NAC Appliance deployment, creating, 451**
- components**
 - of Cisco NAC Appliance solution, 14
 - Cisco Clean Access Agent*, 28–29
 - Cisco NAC Appliance Manager*, 24
 - Cisco NAC Appliance Network Scanner*, 29–30
 - Cisco NAC Appliance Server*, 25, 28
 - of embedded NAC solution, 16
- compound mapping rules, mapping users to user roles, 90**
- configuring**
 - AD SSO
 - 3500XL Edge Layer 2 switch*, 354–355
 - AD server*, 360–363
 - AD SSO authentication server*, 357
 - Agent-based Windows SSO, enabling*, 364
 - DHCP, enabling in NAS*, 379–381
 - GPO updates, enabling*, 364
 - Layer 3 core switch*, 352–354
 - mapping users to multiple roles*, 366–374, 378–379
 - NAM*, 348–349
 - NAS*, 349–351
 - NAS settings*, 359
 - ports*, 358
 - traffic policies*, 358
 - agent policy enforcement, 239
 - agent login*, 243–245
 - certified devices*, 245–246, 249
 - updates, performing*, 240–241
 - web login*, 242–243
 - automatic update retrieval, 240
 - Cisco Clean Access Agent, agent distribution, 255–257
 - Cisco VPN SSO, 386–388
 - ACS, 388
 - Cisco ASA Appliance*, 388, 392
 - NAS support*, 393–396
 - Cisco Wireless SSO, 398–399
 - NAM*, 402–403
 - NAS*, 402–403
 - WLC*, 399–401
 - global filters for NAM role assignment, 213, 217
 - guest access, API, 236
 - HA, 405
 - on NAC Appliance Servers*, 418–438

- host-based traffic-control policies, 229–230
- IP-based traffic-control policies, 227
- L2OOB deployment
 - Catalyst 3750 switch*, 279–283
 - example configuration*, 278, 284
 - managed subnets*, 292–293
 - NAC Appliance Server*, 286–288
 - NAM*, 284–286
 - NAM, logging in*, 288
 - NAS, adding to NAM*, 289
 - NAS, editing network settings*, 290
 - port profiles*, 295–296
 - SNMP receiver*, 296–297
 - switch groups*, 293
 - switch port control*, 298
 - switch profiles*, 294
 - user authentication*, 303
 - user role-based VLAN assignment, verifying*, 304–306, 309
 - user roles*, 299, 302
 - VLAN mappings*, 291
- L3OOB deployment
 - central switch*, 311–313
 - discovery host, changing*, 335
 - edge switch*, 313–317
 - example configuration*, 310
 - NAM*, 318–319
 - NAM, logging in*, 322
 - NAS*, 319–322
 - NAS, adding to NAM*, 322
 - NAS, editing network settings*, 323
 - port profiles*, 326–327
 - SNMP receiver*, 328
 - static routes*, 324
 - switch groups*, 325
 - switch port control*, 330
 - switch profiles*, 326
 - user authentication*, 334
 - user role-based VLAN assignment, verifying*, 337, 341–342
 - user roles*, 331
 - web login page, configuring*, 336
- NAC Appliance Servers
 - DHCP failover*, 438–439
 - High Availability mode, 408–411
 - NAM, 167–171
 - GUI*, 173–175
 - HA*, 416–418
 - licensing options*, 172–173
- NAS, 176–179
 - global settings*, 187–188, 192
 - GUI*, 179–181
 - In-Band mode*, 182–184
 - local settings*, 193–198, 201
 - OOB mode*, 186
- OOB mode, 275
 - central deployment mode*, 276
 - edge deployment mode*, 276
 - gateway mode*, 276–277
 - switch support*, 275
 - user access method*, 275
- posture assessment, 143–147
- scanning, 267–269
- SNMP
 - polling*, 478
 - traps*, 478–479
- user custom roles, 203–206
- vulnerability handling on network scanning
 - plug-ins, 269–270
- connecting**
 - NAM to network, 166
 - NAS to network, 176
- creating**
 - admin group, 220
 - admin user account, 222
 - AUPs, 138–139
 - bandwidth policies, 230–231
 - host-based traffic control policies, 229–230
 - HSPs, 123
 - checklist*, 124
 - goals, identifying*, 126–129
 - security domains, defining*, 129–132
 - sponsorship, obtaining*, 124–126
 - IP-based traffic control policies, 227
 - local user accounts, 207–208
 - NAS user account for AD SSO, 361
- CSM (Cisco Content Switching Module), load balancing, 113, 116**
- CSS (Content Switching Services), load balancing, 113, 116**

custom roles
 configuring, 203
 editing, 206
 options, configuring, 205–206
 removing, 207

custom rules, creating for Cisco Clean Access Agent remediation, 266

customizing NAS web login authentication page, 232–235

D

day zero attacks, 9

defining
 NAC user roles, 132–133
 built-in, 133–136
 normal login roles, 136–137
 network access privileges for HSP, 154
 security domains for HSP creation, 129–132

deleting custom roles, 207

deploying HSP requirements, 153–154

deploying Cisco NAC Appliance
 pilot phase, 455–456
 pre-deployment phase, 446
 business drivers, identifying, 448–449
 communication plan, creating, 451
 deployment schedule, 449
 executive summary, 447
 required resources, identifying, 449–451
 scope of deployment, defining, 447
 support plan, creating, 451
 training program, developing, 451
 vision statement, 448
 production deployment phase 1, 456–457
 production deployment phase 2, 457–458
 production deployment phase 3, 458
 proof of concept phase, 454
 sample deployment plan outline, 452–454

deployment modes
 Client/Server Adjacency mode, 38–42
 Network mode, 38
 Post-Client Certification mode, 38

device timer options (Certified List), 487–488

DHCP, enabling in NAS for AD SSO configuration, 379–381

DHCP failover, configuring on NAC Appliance Servers, 438–439

DHCP server, configuring on Catalyst 3750 for OOB deployment, 281–282

Discovered Clients page, monitoring NAC Appliance solution, 466–467

discovery host, configuring in L3OOB deployment, 335

discovery host IP, viewing, 501

downloading NAC Agent for AD SSO, 382–384

E

edge deployment, 39

edge deployment mode, 276

edge switch, configuring L3OOB, 313–317

editing
 custom roles, 206
 NAS network settings in L3OOB deployment, 323
 NAS network settings in OOB deployment, 290

email samples
 for postings, 524–526
 letters to students, 526–527
 NAC Appliance requirement change notification, 523

embedded NAC solution, 15
 components of, 16

enforcing
 AUPs, 139
 HSP requirements, 153–154

errors, troubleshooting out-of-band issues, 506–507

eth0 interface failure, NAM HA failover, 406

eth2 interfaces, configuring HA on NAC Appliance Servers, 419–420

event log
 logging levels, changing, 474, 477
 monitoring NAC Appliance solution, 470–474

example configurations
 L2OOB configuration, 278
 Catalyst 3750 switch, configuring, 279–284
 managed subnets, 292–293
 NAC Appliance Server, configuring, 286–288

- NAM, configuring, 284–286
- NAM, logging in, 288
- NAS, adding to NAM, 289
- NAS, editing network settings, 290
- port profiles, 295–296
- SNMP receiver, 296–297
- switch groups, 293
- switch port control, 298
- switch profiles, 294
- user authentication, 303
- user role-based VLAN assignment, verifying, 304, 306, 309
- user roles, 299, 302
- VLAN mappings, 291
- L3OOB configuration, 310
 - central switch, configuring, 311–313
 - discovery host, changing, 335
 - edge switch, configuring, 313–317
 - NAM, configuring, 318–319
 - NAM, logging in, 322
 - NAS, adding to NAM, 322
 - NAS, configuring, 319–322
 - NAS, editing network settings, 323
 - port profiles, configuring, 326–327
 - SNMP receiver, configuring, 328
 - static routes, configuring, 324
 - switch groups, configuring, 325
 - switch port control, 330
 - switch profiles, configuring, 326
 - user authentication, 334
 - user role-based VLAN assignment, verifying, 337, 341–342
 - user roles, 331
 - web login page, configuring, 336
- NAC Appliance Manager, 412
- executive summary, 447**
- external authentication servers, 87**
 - authentication process, 88
 - LDAP/AD, adding, 224–225
 - MAC address authentication filters, 92–93
 - mapping users to user roles, 89
 - using attributes, 90–91
 - provider lists, 89
 - RADIUS, adding, 223
 - supported authentication servers, 88

F

- failure scenarios, risk analysis, 105–106
- fallback feature of NAC Appliance Server, 109–110
- floating devices, configuring, 246

G

- gateway mode, OOB mode configuration, 276–277
- General Setup tab**
 - Agent Login page, configuring, 243, 245
 - Web Login page, configuring, 242–243
- generating self-signed temporary certificates**
 - on primary NAM, 415
 - on secondary NAM, 415–416
- global filters for NAM role assignment, configuring, 213, 217**
- global settings (NAS), configuring, 187–188, 192**
- goals for HSP creation, identifying, 126–129**
- GPO updates, enabling for AD SSO configuration, 364**
- guest access, enabling, 236**
- Guest domain, 131**

H

- HA (high availability), configuring, 405**
 - NAC Appliance Servers, configuring, 418
 - eth2 interfaces, 419–420
 - primary servers, 420–429
 - secondary servers, 429–438
 - NAM, configuring, 416–418
 - troubleshooting, 440, 513–516
- heartbeat packet exchange**
 - during NAM failover, 405
 - on NAC Appliance Servers, 409–411
- helpdesk, common troubleshooting issues, 518–521**
- High Availability mode on NAC Appliance Server. configuring, 408–411**
- host posture assessment features**
 - Clean Access Agent Reports, 480–483

host security policy decision matrix, 128
host-based traffic control policies, creating, 229–230

HSPs (host security policies)

- checks, 149
 - adding, 150–151*
 - validity of, determining, 152*
- creating, 123
 - checklist, 124*
 - goals, identifying, 126–129*
 - security domains, defining, 129–132*
 - sponsorship, obtaining, 124–126*
- NAC appliance enforcement methods, 155–156
- network access policy, 156–160
- network access privileges, defining, 154
- posture assessment, configuring, 143, 146
- requirements, 149–150
 - adding, 150–151*
 - deploying, 153–154*
 - enforcing, 153–154*
 - user role selection process, 153*
 - validity of, determining, 152*
- rules, 149–150
 - adding, 150–151*
 - validity of, determining, 152*
- sample format, 148–149

I

IB (In-Band) mode, 36
identifying goals for HSP creation, 126–129
ifconfig command, 491

In-Band mode, 43

- advantages of, 50
- best practices, 101
- certification process, 44–47
- configuring, 182–184
- disadvantages of, 51

information security, 6

installing

- Cisco Clean Access Agent, 250
 - agent distribution, 255–257*
 - alternative methods, 257*
 - sample installation, 251, 255*

NAM

- requirements, 166*
- updates, 240–241*

NAS, requirements, 175–176

Windows 2003 support tools for AD SSO, 362

integrated NAC implementation, 16

integrating Cisco NAC Appliance into IP telephony environment, 101

- In-Band mode, best practices, 101
- Out-of-Band mode, best practices, 102–104

internal security

- as weakest link, 6–7
- network admission controls, 8–9
- risks to, 7

Internet domain, 131

IP telephony integration, 101

- In-Band mode, best practices, 101
- Out-of-Band mode, best practices, 102–104

IP-based traffic control policies, creating, 227

ipconfig command, 517

J-K

ktpass command, 509

ktpass.exe file, running on domain controllers for AD SSO configuration, 363

L

L2OOB deployment

- Catalyst 3750 switch, example configuration, 279–284
 - example configuration, 278
- managed subnets, configuring, 292–293
- NAC Appliance Server, configuring, 286–288
- NAM,
 - configuring, 284–286*
 - logging in, 288*
- NAS
 - adding to NAM, 289*
 - editing network settings, 290*
- port profiles, configuring, 295–296
- SNMP receiver, configuring, 296–297
- switch groups, configuring, 293
- switch port control, configuring, 298

- switch profiles, configuring, 294
- user authentication, configuring, 303
- user role-based VLAN assignment, verifying, 304–306, 309
- user roles, configuring, 299, 302
- VLAN mappings, configuring, 291

L2OOB mode, 276**L3OOB deployment**

- central switch, configuring, 311–313
- discovery host, changing, 335
- edge switch, configuring, 313–317
- example configuration, 310
- MAC address discovery process, 58
- NAM, configuring, 318–319
- NAM, logging in, 322
- NAS
 - adding to NAM, 322*
 - configuring, 319–322*
 - editing network settings, 323*
- port profiles, configuring, 326–327
- SNMP receiver, configuring, 328
- static routes, configuring, 324
- switch, adding to NAM, 328
- switch groups, configuring, 325
- switch port control, configuring, 330
- switch profiles, configuring, 326
- traffic control, 58
 - using ACLs, 59–60*
 - using authentication URL, 61–62*
 - using PBR, 60–61*
- user authentication, configuring, 334
- user role-based VLAN assignment, verifying, 337, 341–342
- user roles, configuring, 331
- web login page, configuring, 336

L3OOB mode, 276**Layer 2 Adjacency, 37****Layer 2 mode (Client/Server Adjacency), 40****Layer 2 Strict mode for Clean Access Agent, 41–42****Layer 3 Adjacency, 37****Layer 3 core switch, configuring AD SSO, 352–354****Layer 3 mode (Client/Server Adjacency), 40–41****LDAP/AD, adding new external authentication servers, 224–225****letters to students, email sample, 526–527****licensing**

- NAM options, 172–173
- troubleshooting, 495–496

limiting bandwidth, 230–231**link detection, 424****Linkup traps, 53–54****Linux OS, ktpass.exe file, running on domain controllers for AD SSO configuration, 363****load balancing, 112**

- Cisco NAC Appliance Server, 116–118
- CSM, 113, 116

local settings (NAS), configuring, 193–198, 201**local user accounts, creating, 207–208****locating serial port, 417****logging in**

- normal login user roles, defining, 136–137
- OOB in L2 Virtual Gateway mode, 68–72
- OOB in L3 Real IP Gateway mode, 73–77
- SSO, 36
- troubleshooting, 518
- web login authentication, 47–48
 - network scanning, 48–49*
 - post-web login steps, 50*

logging levels, changing, 474, 477

M

MAC address

- authentication filters, 92–93
- Layer 3 OOB mode discovery process, 58

MAC Notification traps, 52**maintaining high availability**

- NAC Appliance Manager, stateful failover, 107–108
- NAC Appliance Server
 - fallback feature, 109–110*
 - stateful failover, 108–109*
- Spanning Tree N+1, 110–112

managed subnet interface, 293**managed subnets, configuring in Virtual Gateway OOB deployment, 292–293****mandatory components of Cisco NAC Appliance solution**

- Cisco NAC Appliance Manager, 24
- Cisco NAC Appliance Server, 25, 28

mapping

- roles to local users
 - by external authentication source attributes, 219*
 - by MAC/IP address, 213, 217*
 - by subnet, 217–218*
 - by VLAN ID, 209–211*
- rules to Cisco Clean Access Agent remediation requirements, 263
- users to multiple roles for AD SSO
 - configuration, 366–368
 - user attributes, 370–371, 374, 378–379*
- users to user roles, 89–91

mii-tool command, 517**minimum requirements for Cisco NAC Appliance operation, 30–33****monitoring**

- Clean Access Agents, Reports page, 480–483
- Cisco NAC Appliance Manager
 - Active Administrator Sessions page, 492*
 - Web GUI, 492–493*
- NAC Appliance solution
 - Discovered Clients page, 466–467*
 - event logs, 470–474*
 - logging levels, changing, 474, 477*
 - Online Users page, 467–470*
 - OOB monitoring stages and pages, 465–466*
 - Summary page, 463–464*

N**NAC Appliance Agent**

- downloading for AD SSO, 382–384
- troubleshooting, 500–503

NAC Appliance Server

- DHCP failover, configuring, 438–439
- High Availability mode, configuring, 408–411, 418–438
- IB mode, 36, 43
 - advantages of, 50*
 - certification process, 44–47*
 - disadvantages of, 51*
- OOB, 36, 52
 - SNMP, 52–54*

NAC Framework, 15**NAM**

- AD SSO, configuring, 348–349
- configuring, 167–171
 - for Cisco Wireless SSO, 402–403*
 - GUI, 173–175*
- connecting to network, 166
- HA
 - configuring, 416–418*
 - heartbeat packet exchange, 405*
- installing, requirements, 166
- L2OOB, configuring, 284–286
- L3OOB, configuring, 318–319
- licensing options, 172–173
- updates, performing, 240–241

NAM logs, applying to troubleshooting process, 516**NAS**

- AD SSO, configuring, 349–351, 359
- AD SSO support, configuring, 393–396
- adding to NAM, 496–498
- appliances, adding, 201
- configuring, 176–179
 - GUI, 179–181*
- configuring for Cisco Wireless SSO, 402–403
- connecting to network, 176
- global settings, configuring, 187–188, 192
- In-Band mode, configuring, 182–184
- installing, requirements, 175–176
- L2OOB, configuring, 286–288
- L3OOB, configuring, 319–322
- local settings, configuring, 193–201
- OOB mode, configuring, 186
- web login authentication page, customizing, 232–235

NAS logs, applying to troubleshooting process, 516–517**Nessus**

- plug-ins, uploading, 266–267
- scans, obtaining, 266

netstat -an command, 517**netstat command, 491****network access policies, 156–160****network access privileges, defining for HSP, 154****Network mode, 38**

- effect on OOB operation, 65–66
- Real IP Gateway mode, 43
- Virtual Gateway mode, 42

network scanning

- configuring, 267–269
- plug-ins, vulnerability handling, 269–270
- testing configuration, 271
- user agreement page, creating, 271

normal built-in user role, 134**normal login roles, 205****normal login user roles, 136–137****O****obtaining sponsorship for HSP creation, 124–126****Online Users page, monitoring NAC Appliance solution, 467–470****OOB deployment**

- adjacency mode, effect on, 56–58
- L2 Virtual Gateway mode, login process, 68–72
- L3 Real IP Gateway mode, login process, 73–77
- Layer 2
 - managed subnets, configuring, 292–293*
 - NAM, logging in, 288*
 - NAS, adding to NAM, 289*
 - NAS, editing network settings, 290*
 - port profiles, configuring, 295–296*
 - sample configuration, 278–288*
 - SNMP receiver, configuring, 296–297*
 - switch groups, configuring, 293*
 - switch port control, configuring, 298*
 - switch profiles, configuring, 294*
 - user authentication configuring, 303*
 - user role-based VLAN assignment, verifying, 304–306, 309*
 - user roles, configuring, 299, 302*
 - VLAN mappings, configuring, 291*

Layer 3

- discovery host, changing, 335*
- MAC address discovery process, 58*
- NAM, logging in, 322*
- NAS, adding to NAM, 322*
- NAS, editing network settings, 323*
- sample configuration, 310–328*
- switch port control, configuring, 330*
- traffic control, 58–62*
- user authentication, configuring, 334*

user role-based VLAN assignment, verifying, 337, 341–342

user roles, configuring, 331

web login page, configuring, 336

monitoring stages and pages, 465–466

network mode, effect on, 65–66

OOB (Out-of-Band) mode, 36, 52**OOB Management domain, 131****OOB mode**

- advantages of, 77
- best practices, 102–104
- central deployment mode, 276
- configuring, 186, 275
- disadvantages of, 78
- edge deployment mode, 276
- gateway mode, configuring, 276–277
- SNMP
 - MAC Notification traps, 52*
 - SNMP Linkup traps, 53–54*
- supported switches, 78–80
- switch support, 275
- user access method, configuring, 275

optional components of Cisco NAC Appliance solution

- Cisco Clean Access Agent, 28–29
- Cisco NAC Appliance Network Scanner, 29–30

out-of-band issues, troubleshooting, 504–507**P****PBR, 64**

- Cisco NAC Appliance Server, load balancing, 116–118
- Layer 3 OOB traffic control, 60–61

Perfigo, 13**pilot phase for Cisco NAC Appliance deployment, 455–456****plug-ins (Nessus), uploading, 266–267****policy enforcement**

- agent login, configuring, 243–245
- certified devices, configuring, 245–246, 249
- configuring, 239–241
- troubleshooting, 498–499
- web login, configuring, 242–243

polling, 107

port profiles, 54–55
 configuring in Virtual Gateway OOB
 deployment, 295–296
 L3OOB, configuring, 326–327

ports, configuring for AD SSO, 358

Post-Client Certification mode, 38

posture assessment, 82
 configuring, 143–147

pre-deployment phase, 446
 business drivers, identifying, 448–449
 communication plan, creating, 451
 deployment schedule, creating, 449
 executive summary, 447
 required resource, identifying, 449–451
 scope, 447
 support plan, creating, 451
 training program, developing, 451
 vision statement, 448

prerequisites
 for Active Directory SSO, 94
 for VPN SSO, 96
 for wireless SSO, 99

primary servers, configuring HA, 420–429

production deployment phase 1 (Cisco NAC Appliance), 457

production deployment phase 2 (Cisco NAC Appliance), 457–458

production deployment phase 3 (Cisco NAC Appliance), 458

proof of concept phase for Cisco NAC Appliance deployment, 454

provider lists, 89

Q

Quarantine built-in user role, 135–136

Quarantine roles, 205
 troubleshooting users stuck in, 519–520

R

RADIUS, adding new external authentication servers, 223

Real IP Gateway mode, 37, 43

Real IP mode (Layer 3), login process, 73–77

Real IP NAT Gateway, 38

Real-IP Gateway mode, 276–277

remediation, 84
 checks, 264
 custom rules, creating, 266
 requirements, 258–261, 265
rules, mapping, 263

Remote Access domain, 131

removing custom roles, 207

requirements
 for Cisco Clean Access Agent remediation, 258–261, 265
rules, mapping, 263
 for HSP, 149–150
adding, 150–151
deploying, 153–154
enforcing, 153–154
user role selection process, 153
validity of, determining, 152
 for NAS installation, 175–176

requiring Clean Access certification for every login, 488–489

researching HSP enforcement areas, 151

resources for Cisco NAC Appliance deployment, identifying, 449–451

restricting bandwidth, 230–231

risk analysis of failure scenarios, 105–106

risks to internal security, 7–9

ROI (return on investment), case studies, 17–18

roles. *See also* user roles
 assigning to local users, 207–208
by external authentication source attribute, 219
by MAC/IP address, 213, 217
by subnet, 217–218
by VLAN ID, 209–211
 of NAC users, defining, 132–136
normal login roles, 136–137

rules for HSP, 149–150
 adding, 150–151
 validity of, determining, 152

S

- sample Cisco Clean Access Agent installation, 251, 255**
- sample deployment plan outline, 452–454**
- sample emails**
 - for postings, 524–526
 - letters to students, 526–527
 - NAC Appliance requirement change notification, 523
- sample HSP format, 148–149**
- scalability of Cisco NAC Appliance, 33**
- scanning**
 - configuring, 267–269
 - plug-ins, vulnerability handling, 269–270
 - testing configuration, 271
 - user agreement pages, creating, 271
- schedule for Cisco NAC Appliance deployment, creating, 449**
- scope of Cisco NAC Appliance deployment project, defining, 447**
- secondary NAM, HA configuration, 418**
- secondary servers, HA configuration, 429–438**
- security**
 - internal security
 - as weakest link, 6–7*
 - network admission controls, 8–9*
 - regulations, challenges in maintaining compliance, 10
- security domains for HSP creation, defining, 129–132**
- security policy committee, 125**
- selecting**
 - Client/Server Adjacency mode, 39
 - Layer 2, 40*
 - Layer 2 Strict mode for Clean Access Agent, 41–42*
 - Layer 3, 40–41*
 - network mode, 42–43
 - user roles for applying HSP requirements, 153
- self-signed temporary certificates**
 - generating on primary NAM, 415
 - generating on secondary NAM, 415–416
- serial port, locating, 417**
- SNMP, 477**
 - configuring on Catalyst 3750 for OOB deployment, 283–284
 - role in OOB, 52–54
 - traps, configuring, 478–479
- SNMP polling, configuring, 478**
- SNMP receiver**
 - configuring in Virtual Gateway OOB deployment, 296–297
 - L3OOB, configuring, 328
- Softerra LDAP browser, 366–368**
- Spanning Tree N+1, 110–112**
- sponsorship for HSP creation, obtaining, 124–126**
- SSO (Single Sign-On), 36**
 - AD SSO, 345
 - AD server, configuring, 360–363*
 - AD SSO authentication server, adding, 357*
 - Agent-based Windows SSO, enabling, 364*
 - configuring, 347–355*
 - DHCP, enabling in NAS, 379–381*
 - domain structure, 346*
 - GPO updates, enabling, 364*
 - mapping users to multiple roles, 366–371, 374, 378–379*
 - NAC Agent, downloading, 382–384*
 - NAS settings, configuring, 359*
 - operation, 94–95*
 - ports, configuring, 358*
 - prerequisites, 94*
 - supported devices, 345*
 - traffic policies, configuring, 358*
 - troubleshooting, 509–511*
 - Cisco VPN SSO, configuring, 386–388, 392–396
 - Cisco Wireless SSO, configuring, 398–403
 - VPN SSO
 - operation, 96–97*
 - prerequisites, 96*
 - troubleshooting, 512*
 - wireless SSO, 99
 - operation, 99–100*
 - prerequisites, 99*
 - troubleshooting, 512*
- standalone CSS, load balancing, 113, 116**

stateful failover
 of NAC Appliance Manager, 107–108
 of NAC Appliance Server, 108–109

static routes, configuring L3OOB, 324

subnet filters, applying to local user roles, 217–218

Summary page, monitoring NAC Appliance solution, 463–464

support logs, HA-related, 440

support plan for Cisco NAC Appliance deployment, creating, 451

SVIs, configuring on Catalyst 3750 for OOB deployment, 280–281

switch groups
 configuring in Virtual Gateway OOB deployment, 293
 L3OOB, configuring, 325

switch port control, configuring
 in L3OOB deployment, 330
 in Virtual Gateway OOB deployment, 298

switch ports
 configuring on Catalyst 3750 for OOB deployment, 282–283
 port profiles, 54–55

switch profiles, configuring
 in Virtual Gateway OOB deployment, 294
 L3OOB, 326

T

Temporary built-in user role, 134–135

Temporary role, troubleshooting users stuck in, 519–520

testing
 network scanning configuration, 271
 primary server HA configuration, 429

threats to internal security, 7–9

Timer page (Certified Devices tab), configuring, 249

top command, 491, 517

traffic control, Layer 3 OOB, 58
 using ACLs, 59–60
 using authentication URL, 61–62
 using PBR, 60–61

traffic control policies
 configuring for AD SSO, 358
 host-based, creating, 229–230
 IP-based, creating, 227
 troubleshooting, 498–499

training program for Cisco NAC Appliance deployment, developing, 451

traps (SNMP)
 configuring, 478–479
 Linkup, 53–54
 MAC Notification, 52

troubleshooting
 access-related issues, 520
 agent issues, 500–503
 NAM logs, applying to troubleshooting process, 516
 NAS logs, applying to troubleshooting process, 516–517
 common issues encountered, 518–521
 HA, 440, 513–516
 licensing issues, 495–496
 out-of-band issues, 504–507
 policy issues, 498–499
 SSO issues
 AD SSO, 509–511
 VPN SSO, 512
 wireless SSO, 512

tty ports, 417

U

Unauthenticated built-in user role, 134

updates, performing on NAM, 240–241

uploading Nessus plug-ins, 266–267

user agreement pages, creating for network scanning, 271

user authentication, 87–88
 configuring in L3OOB deployment, 334
 configuring in Virtual Gateway OOB deployment, 303
 MAC address authentication filters, 92–93
 mapping users to user roles, 89
 using attributes, 90–91
 provider lists, 89
 supported authentication servers, 88

user login roles, defining, 136–137

user role-based VLAN assignment, verifying, 304–309, 337, 341–342

user roles

- built-in, defining, 133–136
- configuring
 - in L3OOB deployment, 331*
 - in Virtual Gateway OOB deployment, 299, 302*
- custom
 - configuring, 203–206*
 - editing, 206*
 - removing, 207*
- defining, 132–133

V

validity of checks, rules, and requirements in HSP, 152

verifying

- HA status/configuration, 513–516
- primary server HA configuration, 429
- user role-based VLAN assignment, 304–309
 - L3OOB, 337, 341–342*

viewing discovery host IP, 501

Virtual Gateway mode, 37, 42, 276–277

- Layer 2 login process, 68–72

vision statement for Cisco NAC Appliance deployment, 448

VLANs

- authentication VLANs, 291
- configuring in Virtual Gateway OOB deployment, 291
- ID-to-role mappings, creating, 209–211
- port profiles, 54–55

VPN SSO, 96

- operation, 96–97
- prerequisites, 96
- troubleshooting, 512

vulnerability handling, configuring on network scanning plug-ins, 269–270

W-X-Y-Z

Web GUI, monitoring Cisco NAC Appliance Manager, 492–493

web login

- authentication, 47–48
- network scanning, 48–49
- post-web login steps, 50
- with Network Scanner, 81–85

web login authentication page (NAS)

- configuring in L3OOB deployment, 336
- customizing, 232–235

Web Login page (General Setup tab), configuring, 242–243

Windows 2003 support tools, installing for AD SSO, 362

Wireless domain, 131

wireless SSO, 99

- operation, 99–100
- prerequisites, 99
- troubleshooting, 512

WLC, configuring for Cisco Wireless SSO, 399–401